University of South-Eastern Norway

Threats to Container Ports and Preventative Security Measures

Candidate name: Chaiyakrit Aamlid

University of South-Eastern Norway
Faculty of Technology, Natural Sciences and Maritime Sciences

MASTER THESIS

May 2019

Abstract

The purpose of this thesis is to investigate the threats to container ports in order to determine which threats are most prominent currently and which threats are likely to be prominent in the future, as well as investigating the modern preventative security measures effectiveness in countering the identified threats. A multiple case study was conducted. Nine informants from three different regions who have experience working with security in container ports were interviewed. The threats and the security measures found from these interviews were discussed in relation to the relevant theories in the literature review. The results of this study show that smuggling is an often occurrence in the maritime industry, terrorism can cause disruptions to global trade and unauthorized access to container ports could lead to the occurrence of other threats. The trend of digitalization and automation of container ports lead to the result that cyber attacks are the most prominent future threat. The results also indicate that threats cannot be avoided completely with the existing countermeasures, they can only be mitigated. Additional literature of threats to container ports and preventative security measures are provided in this study as well as the need for awareness in these issues.

Keywords: Current and future threats, security, preventative measures, container port, countermeasures

Acknowledgements

I would like to acknowledge the people who contributed in directing me through the process of writing this master thesis. This thesis has provided me with encouragement as it has taught me of my own capabilities. Accomplishing this master thesis is an experience I will cherish as it has provided me with newly learned skills.

I would like to thank the University of South Eastern Norway for providing me the opportunity to gain a graduate degree to further pursue my career goals.

To my supervisor, Kenn Steger-Jensen, thank you for taking time off your busy schedule and providing me with professional guidance and experience, your dedication has kept me on track and focused. I would also like to thank you Anne Haugen Gausdal for taking time off your busy schedule to motivate me through the difficulties of writing this thesis and advising me to maintain my composure. I would like to thank you Clemet Thaerie Bjorbaek for guiding me through the process of meeting the informants that contributed greatly to this study. I would also like to thank the informants for participating in this research, your expertise, experience and knowledge has contributed greatly to this study.

Last but not least, I would like to thank my family, my partner and my friends for your continuous support and encouragement throughout my journey of obtaining a Master of Science degree in Maritime Management.

Table of Content

List of Tables

List of Figures

List of Abbreviations

AAPA	American Association of Port Authorities
AEO	Authorized Economic Operator
AGV	Automated Guided Vehicle
AFP	Agence France-Presse
APM	Arnold Peter Moller
ASEAN	Association of Southeast Asian Nations
ASIS	American Society for Industrial Security
ATS	Automated Targeting Systems
BBC	British Broadcasting Corporation
CBP	Customs and Border Protection
CCTV	Closes Circuit Television
CSI	Container Security Initiative
DoT	Department of Transportation
EC	European Commission
ECMAR	European Council for Maritime Applied Research and Development
EMSA	European Safety Commission
EU	European Union
FOC	Flag Of Convenience
GAO	Government Accountability Office
GDP	Gross Domestic Product
GGA	Generali Global Assistance
HSSE	Health, Safety, Security and Environment
I.D.	Identification
IMO	International Maritime Organization
ISO	International Organization for Standardization
IT	Information Technology
IEC	International Electrotechnical Commission
ISPS	International Port and Ship Security
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NPS	New Psychoactive Substances
MAREX	Maritime Executive

MI	Megaports Initiative
OAS	Organization of American States
OCIMF	Oil Companies International Marine Forum
OECD	Organization for Economic Co-operations and Development
PIN	Postal Index Number
PwC	PricewaterhouseCoopers
PFS	Port Facility Security
PFSA	Port Facility Security Assessment
PFSO	Port Facility Security Officer
PFSP	Port Facility Security Plan
PSO	Port Facility Officer
RAND	Research ANd Development
RSP	Recognized Security Organization
SOLAS	Safety Of Life At Sea
TEU	Twenty-foot Equivalent Unit
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNODC	United Nations Office on Drugs and Crime
U.S.	United States
USD	United States Dollars
WMD	Weapons of Mass Destruction
WTO	World Trade Organization

1. Introduction

Maritime transportation is vital for the global economy as it is the dominant mode of transportation in international trade (Hoffman & Kumar, 2010). Seaborne trade accounts for 80 percent of global trade by volume. The global economy had a major increase in strength in 2017 which contributed to the growth of global sea trade to up to 4 percent, this accounts up to 10.7 billion tons in volume (UNCTAD, 2018).

Seaports are a key component to international trade whereby it connects the global supply chains between the sea and mainland. In terms of volume, seaports are behind over 80 percent of the handlings of the worlds merchandise trade. The performance by seaports are largely determined by the developments in the world trade and economy (UNCTAD, 2018). One can speculate that because of this fact, cargo throughput in the major seaports has increased since the ratio of trade growth to the GDP growth was at an average of 1.5 in 2017, this is the strongest growth in six years (WTO, 2018). However, the performance of seaports cannot be determined by developments in the world trade and world economy alone.

Port security regulations exist for the benefit of protecting seaports from potential threats that could be caused by terrorists or other criminals. The security measures however, came into question following the terrorists attacks on September 11, 2001. The event prompted the United States government and the IMO (International Maritime Organization) to find more effective security measures to stop criminals and terrorists from exploiting the vulnerabilities of the seaports (McNicholas, 2016). The crucial need for revisions and need for more effective security measures for ports facilities and ships led to the adoption of the International Ship and Port Security (ISPS) Code by contracting governments. The code took effect on the 1st of July 2014 and has been the main security code for ship and port facilities ever since. Other acts and codes to protect ports from threats were created by different governments internationally prior to the attacks on Septembers 11th 2001. The protection of the international supply chain involves all levels of government, foreign governments, corporation, organizations and businesses that are involved (Keefer, 2007).

As long as seaports have existed, so have threats to the maritime ports. Crime and criminal activities have always had a presence at ports. From the past few decades the maritime industry has faced growing concerns from terrorist groups, insurgents and militants due to their increase in activity (Edgerton, 2013). As the years have passed there have been knew ways to exploit ports for their vulnerabilities. For example, before the regular uses of containers, stealing cargo stored in boxes was a common act that occurred in seaports by petty criminals,

but then as the container was being used regularly in the 1950s and upwards, criminals and criminal organizations have found ways of accessing ports, stealing containers and transporting them by trucks (Littlejohn, 2017). Stowaways have also existed for years and have been a problem to the maritime industry, but as ships got bigger and the level of trade increased, stowaways were not only people hiding and traveling on their own, but have also become a profitable business for criminal organizations (Chen, Chen, & Wu, n.d.). There are various modern day threats that port security will have to look out for such as corruption, terrorism, cargo theft, extortion, trafficking of all sorts and more. This master thesis will explain further about modern threats to container ports, future threats, the security measures taken to prevent these threats from occurring and the effectiveness of the preventative measures.

According to McNicholas (2016), container ships pose the biggest threat to security. The reason for this is because the majority of them maintain an 'advertised, published, and tight schedule' (McNicholas, 2016, p. 41). Customers and clients depend on containers to run their businesses, hence, why many of them use the just-in-time inventory approach, this helps manufacturers keep costs low. Approximately 752.2 million TEUs (Twenty-foot equivalent unit) was handled by ports worldwide in 2017 (UNCTAD, 2018), because of the amount of containers handled and because of the schedules needed to be maintained for delivery, some ports are reluctant to fully screen or inspect many containers properly. High security inspections of all containers may cause a delay to ship schedules and may also cause congestion at ports.

There are various preventive security measures taken to minimize the likelihoods of particular threats from occurring. The ISPS Code is an amendment made to the to the Safety of Life at Sea (SOLAS) convention to ensure that these preventative security measures are taken, this Code features minimum requirements and regulations that each port internationally needs to abide by (Bhattacharjee, 2017). The ISPS Code also features a non-mandatory section that provide suggestions on how to follow the requirements in the mandatory section. The Code itself also provides details on the roles that must be taken by contracting governments, government agencies, local administrations and shipping and port industries (IMO, 2002). Other preventive measures taken are screenings (trucks, containers, visitors, employees), access controls, security structures (walls, fences, facilities), use of surveillance equipment, background checks (visitors, employees), security awareness trainings, container security (sealing, screening, inspection), inspections (cargo) and more.

It is not only important to concentrate on current threats but it is equally or if not more important to focus on future threats to container ports. The world itself is becoming more

digitalized and technology driven. In response to that, many container ports are following this trend by using automated technology for cranes, vehicles and security. Information Technology is also being gradually used more within the operations of ports. With all this technological and digital advances comes criminals that want to exploit it. The volume of cyber attacks have grown in an alarming rate in recent times with nearly 17 million attacks reported weekly (Forbes, 2018), Reports suggest that ships and ports involved with the maritime transport industry are extremely exposed to cyber attacks, this has led to the IMO introducing guidelines and recommendations on maritime cyber risk and to ensure that awareness is raised on cyber risk, threats and vulnerabilities (IMO, 2017). Furthermore, the ISPS code till now has not yet covered regulations related to digital risks, many believe now is the time to address that particular problem in order to prevent perpetrators from causing damage (Borchert, 2014).

1.2 Research Objective

The objective of this research is to investigate the current and future type of threats that concerns container ports in order to determine which of those are the most prominent, and to investigate the effectiveness of modern preventive security measures with regard to countering the identified threats.

1.3 Research Question

In order to fulfil the objectives of this master thesis, the following research question is proposed:

What are the most prominent current and future threats to container ports and how effective are modern preventative security measures in countering the identified threats?

1.4 Thesis Structure

This thesis is structured with seven chapters. The first chapter is the introduction chapter and it provides background to the topic of this thesis. The second chapter is the methodology and it explains the research method and research design for this study. The third chapter is the literature review and it provides a review of the subjects associated to this topic and features theories and ideas from various authors and organizations, furthermore this chapter includes theoretical framework describing the theory. The fourth chapter is the Case Study and Further Methodology chapter, it explains the components of a case study and provides a description of the cases that were investigated in this study. Furthermore, this chapter provides the methods for collecting data and building the interview guide. Moreover, this chapter provides information with regards the profile of the informants, reliability and validity issues and issues

with regards to ethics. The fifth chapter contains the findings of this study and the empirical data gathered from the methodology used. The sixth chapter presents the analysis and discussion of the findings and how it relates to the theoretical framework. Finally, the seventh chapter is the conclusions where the answers to the study are identified, limitations to this study are also discussed and suggestions for further research is provided.

2. Methodology

This chapter reveals the research methodology that was used to answer the research question. The research strategy and research method of this study are discussed and explanation is given with regards to the choices of methodology made by the author.

2.1 Research Strategy

The chosen research strategy for this master thesis is the qualitative approach since the author decided that this would be the ideal approach to answering the stated research question. In order to understand the choice the author has made, qualitative and quantitative study are briefly defined and explained.

Greener (2008) explains that 'a quantitative approach to research is likely to be associated with a deductive approach to testing theory, often using number or fact and therefore a positivist or natural science model, and an objective view of the objects studied' (p. 18). The strategy focuses on quantifications as oppose to words. When it comes to the relationship between research and theory, the deductive approach is used. Testing theories in quantitative research is not uncommon (Bryman & Bell, 2007). Creswell (2003) states that quantitative research is based on postpositivist claims on the development of knowledge by way of hypotheses, measurements and observations and the reduction of specific variables. The norms and practices of positivism and natural scientific models are accepted and incorporated in this type of research (Bryman & Bell, 2007).

Bryman & Bell (2007) stated that the relationship between research and theory in qualitative research commonly includes inductive approaches to developing theories. Data collected is based on an individual's interpretation to their social world with words (Bryman & Bell, 2007). In this case, data can be collected by interviews, surveys, questionnaires and case studies. According to Creswell (2003), researchers have the intent of developing a theory or pattern and usually base their knowledge claims on multiple meanings of individual experiences, social meanings and historical construct. Individuals, institutions and groups have their own experiences and practices, hence, qualitative research methods attempt to document, interpret and develop understanding on those practices, processes and experiences (Frankfort-Nachmias, Nachmias, & DeWaard, 2015). Unlike quantitative research, qualitative research rejects the norms of positivism and the norms of natural scientific model (Bryman & Bell, 2007).

A research method is not limited to using one strategy. Some researchers incorporate qualitative and quantitative measures to answer their research question(s), this depends on how they conduct their study and its objectives (Stake, 2003). However, the chosen strategy for this research is the qualitative approach. The author deemed it necessary to attempt to understand the experiences and practices of individuals in order to answer the research question. The qualitative approach enables the author to conduct research based on the individuals view of the topic within their social world.

2.2 Research Design

According to Yin (2003) a research design is defined as 'a logical plan for getting from here to there, where here may be defined as the initial set of questions to be answered, and there is some set of conclusions (answers) about these questions' (p. 19). The research design provides a framework for the analysis and collection of data (Bryman & Bell, 2011). According to Bryman and Bell (2011), there are five important research designs that are commonly featured in studies which are experimental designs, cross-sectional designs, longitudinal design, case study design and comparative design.

In order to answer the research question that was stated in the first chapter, the author decided to conduct multiple case studies that were exploratory by design. A case study is defined by Yin (2003) as 'an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident' (p. 13). Yin also further added that within a case study, multiple sources of information, evidence, findings and data are used. The definition of a case study is similarly defined by Scholz and Tietje (2002) as 'an empirical inquiry that investigates a contemporary problem within its real-life context' (p. 9). A case study can be done by analysing a single individual, multiple individuals, an organization, a country's economy, an industry, an implementation processes or other matters of concern (Yin, 2003). A case study is not limited to a single individual, entity or event but may also include multiple sources of analysis that is not as well defined (Stake, 1995). According to Yin (2003) there are three conditions that determine whether or not a case study should be conducted. The conditions are: (1) when "what", "how" or "why" is associated with the question the researcher is interested in; (2) depending on the extent of control over behaviour events; (3) when contemporary events cannot be manipulated or controlled.

When a holistic or an in-depth investigation is required on a complex issue, a case study could be a useful method for research as it allows exploration and understanding of the meaningful characteristics within real-life issues (Zainal, 2007). According to Oates (2006), case studies are characterized in four ways. First of all, case studies are focused on depth rather than breadth. This means that researchers would try to gain as much detail as they can on an instance of the phenomenon that is being investigated. Secondly, The case itself is examined within its natural setting, the researcher should not tamper, manipulate or disturb the existing case in its setting. Thirdly, a case study is a holistic study, researchers try not to focus on isolating individual factors, but instead focus on the inter-connection and inter-relation of complexed processes and relationships. Lastly, case studies use multiple sources and methods. Data can be obtained from a wide range of sources instead of just a single source. Both quantitative and qualitive data is appropriate in a case study, the methods of collecting data can include interviews, questionnaires, observations and other methods. An example of collecting data from multiple sources is if a researcher were to conduct a study about life of employees within a single company, the researcher could conduct interviews on as much employees as possible instead of just one or two.

A case study research is defined by Gall et al (1995) as 'the in-depth study of instances of a phenomenon in its natural context and from the perspective of the participants involved in the phenomenon'(p.545). Case studies can be undertaken in three forms which are exploratory, explanatory and descriptive. An explanatory case study is used if a researcher wanted to explain a causal link in real life interventions. For example, it tries to explain why a phenomena between two variables have occurred. Trying to identify the correlation between two variables can be complex and therefore surveys may not be suitable for this type of case study. An exploratory case study is used when the topic of research has an undefined, single set of outcomes. The researcher explores a certain research problem in order to gain a higher understanding. This kind of case study can be used if there is a lack of literature on a certain topic, the researcher could then investigate the topic in its real-life instance. A descriptive cast study describes a phenomenon or an intervention and its real-life context. The outcome of the study is done by conducting rich, detailed analysis and consists of discussions of what has occurred and how various people perceive it (Yin, 2003).

Multiple-case studies allows researchers to find out and analyse the context of a topic within different settings. Several cases are examined in order to understand the similarities and differences between them. This is oppose to a single case study which only allows the researcher

to analyse and gain understanding on one setting or a single unique case (Baxter & Jack, 2008). According to Yin (2003), multiple case studies can be used to augur contrasting results for reasons that are predictable or to predict similar results in the study. The advantages of conducting multiple-case studies are first of all, it generates reliable and robust evidence (Baxter & Jack, 2008). Secondly, analysing several cases allows the researchers to discover whether or not the findings are individual to one case or if similar results can be found in other cases. This is due to the comparative nature of this type of study (Eisenhardt, 1991). Thirdly, multiple cases permit a wider scope of exploration of the chosen research question as oppose to a single case study (Eisenhardt & Graebner, 2007). Lastly, according to Eisenhardt and Graebner (2007), multiple cases 'create more robust theory because the propositions are more deeply grounded in varied empirical evidence'(p. 27). Eisenhardt and Graebner (2007) further added that relationships and constructs are described or portrayed with further precision. This is because multiple cases can provide more exact definitions and determine appropriate levels of construct abstraction.

A multiple case study on three cases was conducted in this research. Three different cases were selected by the author in order to understand the point of views of the informants in three different regions. After further research on threats and the effectiveness of preventative security measures, the author wanted to understand whether or not the different locations would have an effect on the answers provided by the informants. This was necessary because the ISPS Code governs security for port facilities that partake in international trading worldwide, hence, it is vital to discover if the regional locations have an effect. The nature of the study is exploratory, since the author explored the threats to container ports in order to understand which threats are prominent currently and which threats will be prominent in the future. Data was collected through semi-structured interviews where informants provided information with regards to what they thought, based on their experiences were the most prominent current threats, what they deemed to be the most prominent future threats, the preventive measures used in their ports and their views with regard to the ISPS Code and its effectiveness on threat mitigation. Conducting these interviews from multiple individuals from three different settings enabled the author to discover if the findings in one case can be found in other cases, therefore, this design enables a wider scope of exploration and understanding.

2.2.1 Research design for this study

The literature review is based on the threats to container ports and the modern preventative security measures. The threats have already been discussed and presented by other authors and organizations. Similarly, the preventative counter measures to these threats have either been adopted by the international organizations that govern security in container ports or recommended by other authors and organizations. Data was collected by interviewing container port employees and personnel from three different regions, this was to find out what they thought were the current and future threats to container ports and what kind of processes they have undertaken to enhance their security. Furthermore, the informants were asked about their opinions regarding the ISPS Code, which contributes to this study because a part of the Code is made mandatory for container ports to follow. Discovering the threats and preventative security measures from both the theory and the informants provides room for discussion and comparisons. The effectiveness of the preventative security measures are based on the discovered theories in the literature review and the findings provided by the informants.

3. Literature review

Threats are handled by a variety of methods today and have a natural demand for traceability and control of flow from suppliers to customers. The approach of the literature review for this study identifies and explains the threats to container ports as well as the preventative security measures. The references to these theories are limited and are based on the regulations enforced by international organizations such as the IMO. Other theories are based on the findings of other authors and other international organizations such as the United Nations (UN) and other affiliated organizations. Firstly, the literature review explains what is meant by port security and why there is a need for it. Secondly, the modern threats to container ports are identified and explained with regards to what they are, what impacts do they have on container ports and why it is important for container ports to avoid them from occurring. Relevant theories from other authors and organizations are used in order to accomplish this. Thirdly, the preventative security measures are identified and explained based on the requirements of the ISPS Code, theories developed by other authors and initiatives that have been adopted by certain container ports to counter certain threats. This section attempts to provide information about the measures being used and recommended measures that could be used according to various sources. On top of this, the thesis attempts to explain criticisms that these security measures have received in order to understand why they have not been adopted by some ports and why they may not be effective in countering threats, these explanations are provided by various authors and organizations. Lastly, the study attempts to explain the direction port security measures may be headed in the future based on new technological advancements and trends in the industry, these theories are based on the findings of various authors and may provide evidence as to why new security measures are needed.

Statistics with regard to how often a certain threat occurs on a container port are highly limited. The author attempted to use statistics from published scientific studies as much as possible. Links to certain news articles are indicated in some areas of the literature to provide an understanding of what happened in the event of a threat becoming a reality. Arguments against certain security measures were provided by studies from various authors and studies conducted by international port-related organizations. Some theories are more valid than others, this was due to the limited sources available with regards to this topic. Lastly, specific information of ports security plans was difficult to find, this is due to the secretive nature of these plans, ports are reluctant to provide details regarding their security practices because if the information got into the wrong hands, criminals may know their routines.

3.1 Port security

The term port and security is defined by the IMO in the following way; port is defined as 'the geographical area defined by the Member State or the designated authority, including port facilities as defined in the International Ship and Port Facility Security (ISPS) Code, in which maritime and other activities occur' (IMO, 2003). The IMO defined the term security as 'a condition whereby the level of risk is deemed acceptable' (IMO, 2003). Port security measures involve activities such as counter-terrorism and the enforcement of law and treaties. Other port security measures include the inspection and protection of cargo that has accessed through the ports and protection of the seaport facilities (Ismail, n.d.). Measures are in place to secure the ports by limiting its vulnerabilities from potential threats and risks. Port security includes fighting crimes such as the trafficking of narcotics, the trafficking of human beings and smuggling. Furthermore, port security includes the protection of passengers and crews (Gujar, Ng, & Yang, 2018).

In all intermodal logistical supply chains, ports are a nodal point and securing ports from threats should be regarded as a high priority (Robinson, 2002). The IMO issues rules that regulate port security internationally. This is done through the ISPS Code. Additionally, there are other measures in place used to securing ports on top of the mandatory ISPS Code such as the Container Security Initiative (CSI) which was launched in the United States of America, Megaports Initiatives (MI) (Ismail, n.d.) and regulations that were set out by national legislations. These initiatives are explained later in the thesis.

3.2 Modern threats

The definition of a threat is widely confused and misinterpreted by many individuals. The term "threat" is often mistakenly confused with the term "risk". A threat is defined as an act or actor that may bring harm or damage to a country, organization, person, or facility. Therefore, the key component of a threat is action or the potential for action (Edgerton, 2013). Threats that may concern ports globally are listed below, these threats are provided by various authors and organizations:

3.2.1 Terrorism

The terrorist attacks on September 11th, 2001 have strengthened security in various ports around the world, due to this event, an amendment of the SOLAS convention was made, hence introducing the ISPS Code (Glaser & Vitello, 2015). According to the Organization for Economic Co-operation and Development (OECD) (2002), terrorist attacks can cause huge

destruction on physical assets and other infrastructures, hence providing large amounts of costs to rebuild them and later, costs will be increased in efforts to strengthen its vulnerabilities. Edgerton stated in 2013 that there is no internationally accepted definition for terrorism, however, Edgerton (2013) indicates that most definitions identify some common attributes, these attributes include: (1) Use of violence or threatened use of violence; (2) Intended to advance a political, religious or ideological cause; (3) Influencing or intimidating a government or population. According to Poushter and Huang (2019), in a 26 nation survey about the greatest international threats, eight countries named terrorism (especially by ISIS) as the greatest threat. Some of the countries that provided this answer include Russia, France, Italy, Indonesia, Israel and the Philippines. Despite terrorism being one of the greatest threats to national security in many countries, according to the 2008 Research ANd Development (RAND) Terrorism Database, only two percent of international terrorist strikes from the last 30 years have been on assets within the maritime sector (Chalk, 2008).

According to OECD (2002), terrorist attacks can cause several economic consequences to the actors within the supply chain. Firstly, after a terrorist attack, security within the nation will become more controlled and tight, this drops efficiency for trade. Secondly, the private and public sectors will start spending more on security. The private sector would likely spend on national security and further military operations, and the public sector will spend to increase their security for their infrastructures, employees and information. Organizations face the challenge of having to find a balance between security and efficiency. Thirdly, a nation may start to develop security measures such as initiatives to enhance its national security, the consequence of this is that international trade costs will rise, an example of this is after the September 11th terrorist attacks, the United States government developed initiatives such as the Container Security Initiative and the Megaports Initiative (Glaser & Vitello, 2015). Lastly, the added security measures could increase the waiting time for several actors in the supply chain (OEDC, 2002).

An example of a terrorist attack on a port is the 2004 Ashdod Port Attack in Israel. Two suicide bombers found their way into the port by hiding in a container which was inspected twice and cleared for inspection. One bomber blew himself up next to a group of workers located at the machine repair workshop, the second bomber blew himself up in a storage and refrigeration area. The attack took 12 lives, including the bombers and up to 16 people were injured (Lorenz, 2007). In the aftermath of the attack, many individuals called for stricter

inspections of containers despite the fact that Israeli ports had far more rigorous security checks than any other country at the time (Maritime Union of Australia , 2005)

3.2.2 Hazardous materials

Hazardous materials are a threat to the environment and in many cases, can also be used for the means of committing acts of terrorism. According to Christopher's book that is titled 'Port Security Management", hazardous materials are solids, liquids, or gases that can injure or harm living organisms and cause damage to property and/or the environment' (Christopher, 2015, p. 333). According to this definition, hazardous materials can cause harm to civilians, facilities, the environment, properties, wildlife and living organisms. Although hazardous materials can be used by terrorists to secure their motives by way of building WMDs, untrained employees in ports or on ships that have little experience in handling hazardous materials are also regarded as a high threat due to the damage that may be caused. The mishandling of hazardous materials can cause harm and may lead to destruction.

3.2.3 Unauthorized access into port facilities

One of the challenges that are presented to ports is granting access to people without highly disrupting operations, commerce, trade and other port-related business. In the worst case scenario, criminals or terrorists may gain access and damage important infrastructures and assets, these damages include loss of life, economy, environment and port facility structures (Christopher, 2015). Furthermore, the U.S. Department of Transportation (DoT) (1997) added that criminals who gain successful access to port facilities may try and steal cargo as well as try and perform other forms of criminal activities, such as smuggle weapons, narcotics, money, contrabands or even stowaways. Moreover, the DoT (1997) added that terrorists could try and place bombs or other explosive devices in the port facility.

3.2.4 Cargo theft

Cargo theft is a large concern for supply chain industries worldwide. For many centuries, cargo theft has existed and in the U.S. it has amounted up to $15-$30 billion dollars a year in losses. The figure given is an approximant number due to some incidents being unreported and many reported incidents differ in numbers (Turner, 2018). The individuals working within the transport system may also be involved such as the stevedores, company employees, ship crews or government officials (Edgerton, 2013), however, these individuals may also be part of or colluding with organized crime groups. According to the U.S. DoT Volpe Center (1999), these are some of the methods used to steal cargo: (1) Opening containers

stacked at terminal yards or transfer facilities, removing goods, and transporting them from ports or intermodal facilities by personal automobile or delivery trucks; (2) Falsely claiming that a truck was hijacked leaving a port or warehouse, when the driver is actually complicit in the crime, and receiving a cut of the profits; (3) Dismantling containers, removing key merchandise, re-sealing containers and continuing shipment; (4) Relying on an organized network for spotting, stealing, and fencing merchandise; (5) Driving off in a loaded tractor-trailer via fraudulent paperwork; (6) Speeding through fences and security checkpoints; (7) Stealing loaded trucks off the street or from storage yards.

3.2.5 Extortion

Extortion can be defined as threatening or forcing someone to hand over their goods, materials, services or cash. Many ports around the world are affected by extortion practices, whether it is done by organized crime organizations or officials and employees that work in the ports. Extortion was the cause of congestion and the cause for consumers paying higher charges for their containers in Manila's ports in the Philippines (Chua, 2014). Nigeria is another country that faces big extortion problems, the New Telegraph Newspaper claims that up to 12.6 billion Naira's (approximately 35 million USD) are being lost annually due to extortion in the ports of Nigeria (Akomolafe, 2017). Extortionists that are employed by the port would get their way by blacklisting or threaten to blacklist truck drivers that report them (Ships & Ports, 2019). This allows them to turn away any trucks that do not pay the extortion fee. Extortion causes congestion in the ports, port officials may be reluctant to solve the issue due to the large amounts of money that are made (Chua, 2014).

3.2.6 Trafficking, Smuggling and Customs violations

Trafficking is extremely common in the maritime industry. The trafficking of narcotics, stolen goods, weapons, money and illegal wildlife products are some of the items are trafficked in ships. Human trafficking is one of the most serious problems globally and can lead to victims being forced into slavery or sexual exploitation (Gutauskas, 2009). Trafficking is a business that is done by organized crime groups, a person may want the opportunity to be taken to a more economically successful country in order to escape poverty, war or other difficult situations they may face in their home country (McNicholas, 2016). Organized crime groups make money from trafficking persons in a number of ways, a person may pay the organized crime groups, if the person does not have money there are other methods of payment that can be done, for example, an organized crime group can convince the potential victim to carry drugs

with them on their journey to their destination or force them into debt. If a person is forced into debt the organized crime group may force them to work for long hours for a small amount of money until their debt is paid off (Edgerton, 2013). Women and children that are victims of human trafficking may be and have been forced into sexual exploitation in order to pay off their debts (Gutauskas, 2009).

Drug trafficking is considered as a transnational threat, the process of drug trafficking can lead to terrorism, arms trafficking, trafficking of people, illegal migration and money laundering (United Nations, 2018). As stated by Edgerton (2011), a Lebanese man named Ayman Joumaa was charged for trafficking cocaine and laundering money on December 2011, he was raising money for the terrorist group named "Hezbollah" and he was also laundering money for the Mexican cartel group named "Los Zetas". As mentioned above, human trafficking is also a method of the trafficking of narcotics as victims of human trafficking can be used to carry drugs in their journey. The UNODC (2018) has reported that a total of 8607 tons of cannabis, cocaine, opium, methamphetamine, pharmaceutical opioids, amphetamine, synthetic New Psychoactive Substances (NPS), ecstasy, heroin and morphine combined has been seized in 2016. Regarding those seizures, according to UNODC (2015), in 2014, 60 percent of all cocaine seizures were during maritime transportation and three seizures at sea accounted for 74 percent of all heroin entering into Australia. However, Perez (2014) estimated that around 70 to 80 percent of all cocaine that is consumed worldwide was transported through sea. UNODC's 2018 World Drug Report claims that the production of cocaine, heroin and methamphetamines have increased and the plant-based drug productions are at a record number. Containerized shipping is being utilised as a form of smuggling, however, very few detections have been made (UNODC, 2011). Maritime transportation has accounted for the largest amount of quantities of drugs seized, this surpasses other modes of transportation such as rail and air (UNODC, 2015).

The trafficking of illegal wildlife products was once seen as a low-level crime but has now increased drastically in its value. This particular sort of trafficking is only bested by the trafficking of narcotics, arms and human beings but nevertheless has a value that generates up to $20 billion US dollars annually (Trelawny, 2015).

Not to be confused with trafficking, smuggling is the transportation of narcotics or other illegal material. Once financial gain is involved in the process, then it is known as trafficking (Wiseman Law Firm, 2012). The system within the container industry is based on time, the amount of cargo being transported is large in volume, because of this, companies try and deliver

freight and goods as quickly as possible to keep up with the volume. In order to keep up with the flow, inspections and checks on imported containers occur rarely, as little as 5 percent in the U.S. and this leaves the industry highly vulnerable to smuggling (Richardson, Gordon, & Moore, 2009). According to McNicholas (2016), maritime smuggling routes are altered depending on the changes in the shipping trade lanes or the changes in seaport operations. Evidence of this is shown on the UNODC trafficking flows, this is indicated on the maps of their annual "World Drug Reports" (UNODC, 2015, 2016, 2017, 2018). An example of this is shown in Figure 1. This is the main cocaine trafficking flow from 2012 to 2016 according to UNODC's World Drug Report of 2018. The map shows that a numerous amount of drugs reach its destination by crossing sea:

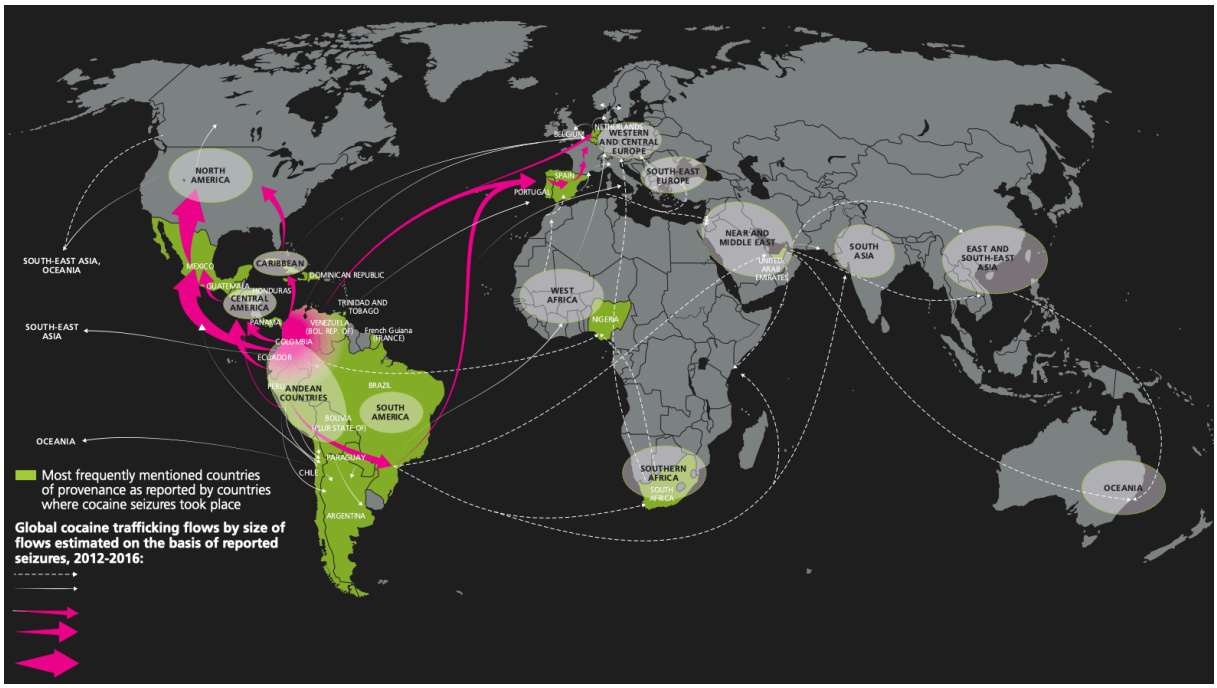

Figure 1: Main cocaine trafficking flows 2012-2016 (UNODC, World Drug Report 2018, 2018)

Customs violation, on the other hand, involves stating false information of the transported cargo in order to minimize what needs to be paid in terms of tax or duties. For example, somebody may claim to have furniture in their cargo but in reality, there are hazardous goods stored within the container (Edgerton, 2013).

3.2.7 Hijacking

Details with regard to hijackings at ports were difficult to obtain for the purpose of this study, nevertheless, hijackings in ports are still a threat to be aware of. Examples of what could

be hijacked are vessels that a berthed, port vehicles or vehicles that have authorizations to be in the port. Potentially, a terrorist might hijack a vehicle from outside the port area in order to get access to the port area (Christopher, 2015).

3.2.8 Corruption

There is no single agreeable definition for corruption, but for the purpose of this research, the definition of used will be described as "the abuse or misuse of power or trust for self-interested purposes rather than the purposes for which power or trust was given" (Nichols, 2017). Different countries around the world vary in the levels of corruption, this means that certain ports would have more confidence and trust in carrying out operational and security requirements more than others. The corruption perceptions index is generally used to determine the level of corruption in certain countries. For example, Canada is listed 9 out of 180 in the ranking and Venezuela is ranked 160 out of 180, ships traveling from a port in Venezuela to Canada may have to be inspected further due to the questionable security methods or requirements Venezuela may have (Edgerton, 2013). According to Klitgaard (1988), corruption can include, but not limited to acts such as extortion, bribery, influence peddling, embezzlement and fraud. Due to the transnational nature of the maritime industry, it is understandable that corruption plays a significant role in the level of trust and confidence one country may have for another. A country with a low ranking on the corruption perception index may find it hard to gain trust or confidence from a country that is ranked higher, which may limit the amount of trade that could potentially be established between them (Edgerton, 2013). Many have speculated that corruption and culture are correlated, however, a study by Seleim and Bontis (2009) lacked any empirical evidence to conclude. According to Larmour (2012) in the book "Corruption: Expanding the Focus", it cannot be confirmed that corruption is linked to culture, but "Ideas about culture still seem useful in understanding how people recognise and respond to what is judged to be corrupt behaviour" (p.173)

3.2.9 Poorly trained security personnel

The threat of having poorly trained security personnel cannot be ignored. A port will risk infiltration if the security personnel did not have adequate training. Security personnel that are poorly trained may not have a full comprehension of what to be aware of whilst on the job. 80 percent of all maritime accidents are caused because of human error and accidents, therefore security personnel should have the acquired training to avoid this from occurring (Berg, 2013).

It is vital for security personals at ports to have the knowledge, ability and skills in their line of work if threats at a certain seaport are to be reduced (Christopher, 2015).

3.2.10 Cyber-attacks

In recent times, the threat of cyber-attacks is becoming more and more of a challenge for seaports. The European Council for Maritime Applied Research and Development (ECMAR) (n.d.) suggests that cybersecurity will become an important issue as the maritime industry becomes more automated and digitalized. Cyber-attacks have been a major cost for industries, McNicholas (2016) ranges the costs on the industry from $300 billion USD a year on the low side and over $1 trillion USD on the more realistic side. McNicholas further claims that the costs are expected to reach$ 2 trillion US dollars by 2019. According to this, industries will have to be prepared for cyber-attacks in the future and find security measures to tackle a cyber-attack situation if they were to occur. Ports are a vital part of global trade, therefore, disruptions to the ports could cost ports significantly in terms of cash and time. Furthermore, as mentioned by Generali Global Assistance (GGA), a port and other industries may have to incur long term loses such as losing trust from their customers and having their reputation tarnished due to having their security breached (GGA, 2018). A survey conducted by PricewaterhouseCoopers (PwC) showed that 87 percent of their customers were willing to take their business elsewhere if a cyber-attack were to happen or if their data had been breached (Neveux, 2018).

Maersk fell victim to a cyber-attack on June 2017 which was caused by ransomware, this attack disrupted operations in 76 of its container terminals (AFP, 2017). This attack affected terminals around the world including places such as the Port of Rotterdam, Mumbai Port and Port of Gothenburg. Agence France-Presse (AFP) (2017) reported that the attacks forced Maersk to shut down its computer systems, this forced some terminals to discontinue operations, however, some of the terminals were able to use manual systems to operate. The attack disrupted operations on several APM terminals, which is a part of the AP Moller Maersk conglomerate. One of the APM terminals that could not continue operations was the terminal in Elizabeth, New Jersey. Trucks were lined up a mile long outside the gates because they were not able to collect their containers (Greenberg, 2018). The APM terminal at the Port of Gothenburg was affected by not being able to get containers out (The Local, 2017) and, the APM terminal at the Port of Rotterdam was affected by having to perform more labour extensive container handling. Furthermore, The APM terminal at the Port of Rotterdam was also affected due to the IT system shutdown, this forced the company to perform other methods

of communication (AFP, 2017). It was reported that the cyber-attack costed Maersk up to $300 million USD (Milne, 2017), this resulted in Maersk placing cyber security as one of the company's main priorities and to do that, they developed a cyber security plan which they have stated will guide them to improve their cyber security. (Maersk, 2018). Other notable cyber-attacks on container terminals include the attack on the Port of Barcelona (Ilascu, 2018) and the attack on the Port of San Diego (BBC, 2018), both occurred on September 2018 just 1 week apart. In order to put into perspective about the threat that cyber-attacks poses, according to Poushter and Huang (2019), a 26 nation survey about international threats showed that four countries were mostly concerned with cyber-attacks, these countries are the U.S., Japan, South Africa and the Netherlands.

Hackers can hack into the ports IT systems and find out details with regard to the arrivals of the cargo from ships, they may also gather information with regards to the details of security. This would allow the criminals and hackers to steal containers that have arrived at the ports, this was the method used by hackers and drug traffickers to obtain narcotics in the Port of Antwerp which was discovered on October 2013 (Bateman, 2013). Hackers may also get into the system and circulate fraudulent invoices for non-existent fees (Ott, 2014). On July the 5th 2017 the IMO released guidelines on maritime cyber risk management, this also listed some systems in the maritime domain that could be vulnerable to cyber-attacks as shown in Table 1:

Table 1: Systems vulnerable to cyber-attacks (IMO, Guidelines on maritime cyber risk management, 2017)

Systems vulnerable to cyber-attacks include, but not limited to:
• Bridge systems; • Cargo handling and management systems; • Propulsion and machinery management and power control systems; • Access control systems; • Passenger servicing and management systems; • Passenger facing public networks; • Administrative and crew welfare systems; and • Communication systems.

3.2.11 Stowaways

Stowaways have evolved from single personals travelling alone unaided to being an organized crime business (McNicholas, 2016). Stowaways are disruptive for port operators and are also extremely costly. From the 20th of February 2011 to the 20th of February 2012 the IMO reported that the P&I Clubs have had cases totalling up to 774 incidents which involved 1,640 stowaways, the P&I Clubs further estimated that the situation and the problems of stowaways cost approximately $15.3 million US Dollars annually (IMO, 2013). Stowaways are motivated to migrate mainly for economic reasons. Many of them are desperate to escape poverty, war, violence or they would like to travel to a more economically stable country to be able to support themselves better or their families. As stated before, some stowaways may not have the funds to travel so they may have to pay off crime organizations by means such as working for almost nothing to pay their debts off, smuggling drugs and women and children may become victims to sexual abuse. Some may ask the question "how do stowaways reach their destination?". Stowaways may sneak themselves into containers from the initial port of transportation whilst port laborers are loading a particular vessel. Criminal organizations may also pay off port officials or crew members on ships to get people to sneak on. Lastly, Stowaways may just sneak themselves onto vessels from ports and try their best not to get detected (Edgerton, 2013). Stowaways that sneak or get sneaked into containers risk their lives in a very dangerous journey, an example of this is when Chinese stowaways were found in containers located in the ports of western United States, some were found alive in the worst state and some were found dead (Cambell & Gittings, 2000).

3.3 Measures taken to mitigate the threats

This section of this chapter covers the security measures that can be taken to counter the threats shown above. The theories are provided by international organizations, various authors, international initiatives and national legislations. Theories regarding why these countermeasures are not favoured are also presented.

3.3.1 International Ship & Port Facility Security Code (ISPS Code)

The ISPS code is an amendment made to the International Convention for the Safety of Life at Sea (SOLAS) and has come into existence due to the terrorist attacks on September 11th, 2001. The code itself did not however, come into force until the 1st of July 2004 (IMO, n.d.). After the terrorist attacks, there was a concern that ships had far too easy access to seaports, the concern gradually grew upon the realization that terrorists could potentially transport their

weapons to seaports and hence formulate another terrorist attack (Edgerton, 2013). Furthermore, without strengthening security, terrorists may also be able to hijack vessels from seaports and blow them up in busy areas such as ports or areas close by seashores (Bergqvist, 2014). The IMO describes the ISPS code as a "comprehensive set of measures to enhance the security of ships and port facilities" (IMO, n.d.). The IMO has further has written that the purpose of the ISPS code is to "provide a standardised, consistent framework for evaluating risk", furthermore, government agencies and officials are then enabled to take action against threats with regard to the changes in the vulnerabilities to the ship and port facilities. Governments, port officials and other port authority figures can then correspond and determine what security measures should be taken depending on the level of security needed.

The ISPS code is made up of two sections, Part A and Part B. Part A is the mandatory section of requirements in which companies and governments have to follow, Part B, on the other hand, is not mandatory but serves as a guidance to the mandatory requirements. The requirements written in Part A include a variety of details that include the contracting governments, government agencies, local administrations and the shipping and port industries. This includes the establishment of a framework involving co-operation between the parties previously mentioned to detect threats to security and preventive measures against incidents that could affect the ship or port facilities. In this section, the roles and responsibilities of these parties are also made clear in an effort to tighten up security for international and national maritime trade. This section also provides details with regard to the collection and exchange of information concerning security. Part A also provides methodologies for security assessments to ensure that there are plans in place in the situation where levels of security are changed. Another objective for this section of the code is to ensure that adequate maritime security measures are in place.

The requirements of contracting governments are to set security levels and to further provide guidance for protection if a security incident were to occur. There are three security levels mentioned that the contracting governments are required to understand; security level 1 means that the minimum security measures shall be maintained and conducted at all times, security level 2 means that extra protective security measures need to be taken and that the risk from a security incident is heightened, and security level 3 refers to the moment where a security incident is can happen and is probable therefore further protective security measures shall be maintained, whether or not the target is specific. Contracting governments are also responsible for conducting port facility security assessments based on establishing critical assets and

infrastructures, the threats to those infrastructures and the vulnerable areas in the ports facility. Furthermore, contracting governments are required to communicate to the port or ship facilities regarding the threat. An example of a security level 3 situation and a situation where government contractors had to communicate is when the United Kingdom government raised the ISPS code to level 3 for British flagged ships sailing in Yemeni waters on August 2013, the level was elevated due to high amounts of activity caused by Al Qaeda affiliated terrorist groups in Yemen. (Bergqvist, 2014).

According to Wu and Zou (2009), "the ISPS Code has significantly increased security awareness for threats at ports and has effectively deterred the threats to port facilities from its source" (p. 95). Furthermore, according to Mazaheri and Ekwall (2009), the ISPS Code has its advantages since it has provided better safety, security and lower risk, better control of flow of goods and personnel entering in and out of the port, better documentation procedure since there now is a unit standard and has created a nicer working environment. Moreover, according to UNCTAD (2007), governments have provided assistance in enforcing the Code and has provided assistance in assessing and accepting the PFSP. They either do these duties themselves or delegate this task to a Recognized Security Organization (RSP). Lastly, according to Anyiam (2014), despite the fact that the Code has provided additional paperwork, the documentation involved keeps those involved in the maritime sector vigilant to threats. This alertness and awareness could minimize or prevent crimes and terrorist attacks on port facilities. Anyiam (2014) also noted that the Code cannot stop these attacks completely, this includes other conventions, but the Code at least increases awareness with regard to the threats.

The ISPS Code requires ports to build a Port Facility Security Plan (PFSP). According to the ISPS Code (2003), a PFSP is 'a plan developed to ensure the application of measures designed to protect port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of security incident' (p. 5). The person that is in responsible for the PFSP is the Port Facility Security Officer, according to the ISPS Code (2003) is 'The person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for the liaison with the ship security officers and company security officers' (p. 5).

3.3.1.1 Port facility security

Part A paragraph 14 of the ISPS Code outlines the requirements for port facilities with regards to the change in security levels set by the contracting governments. The security

procedures should cause minimal interference and delay to passengers, personnel associated to ships, visitors, goods and services. This part of the code also specifies the security measures that must take place in a security level 1 in order to protect the port facilities from incidences. These measures can take into account the guidance that is provided in Part B of the Code. The measures are to:

> 'Ensure the performance of all port facility security duties and that security communication is readily available, controlling access to the port facility, monitoring of the port facility berthing areas, anchoring areas and restricted areas to ensure only authorized persons have access' (p. 16).

It is also stated that supervision should take place on the handling of cargo and the handling of the ship's stores. For security level 2 situations, the ports should provide additional protective measures and at security level 3 situations the ports should provide further specific protective measures. Both measures should be detailed and specified in the PFSP. It is also added that during a security level 3, the contracting governments should give security instruction of which the port facilities are required to respond to.

3.3.1.2 Port facility security assessment

Details with regard to the port facility security assessment (PFSA) is located in Part A paragraph 15 of the ISPS Code. The PFSA is an important part of developing and updating the PFSP. This section requires the contracting governments to carry out the PFSA. The contracting government has the option of allocating this assignment to a recognized security organization. If this were to be the case, the contracting government would then have to review and decide if they want to approve it. When threats change and the port facility is introduced to some changes, the PFSA shall be reviewed and updated in order to accommodate these changes. The PFSA should also be updated and reviewed periodically, the time between updates and reviews are not specified in the mandatory section of the ISPS Code. The PFSA should identify and evaluate the important assets and infrastructures of the port facility in order to protect. It should also identify the possible threats that are likely to occur against the assets and infrastructures, this is so that security measures can be prioritized towards them. Also, countermeasures and procedures should be identified, selected and prioritized in order to reduce the vulnerabilities of the port facilities. The PFSA should also identify weaknesses which are not limited to the human factors in the policies, procedures and infrastructures.

3.3.1.3 Port facility security plan

The PFSP is developed based on the PFSA and should have provisions for the three security levels that were previously mentioned. A recognized security organization may also prepare the PFSP which is subject for approval by the contracting government in charge at the location of the port. The plan should be built to address the measures to prevent unauthorized weapons or dangerous devices that could be used against persons, ships or ports from entering into the port facility. There should also be measures in place that prevent unauthorized access into the port facility and measures that ensure the security of the cargo and the cargo handling equipment. Lastly, there should be measures that ensure the information in the PFSP is secured. The ISPS Code lists nine procedures that should be addressed in the PFSP such as reporting security incidents, procedures for periodically reviewing the plan as well as updating it, procedures for evacuation in case of threats, procedures auditing the PFSP and more. The responsibilities and roles of the port security personnel and their contact details should also be identified. The PFSP may be changed if approval is granted by the contracting government.

3.3.1.4 Training, drills and exercises

According to paragraph 1.3 of part A, one of the functional requirements of the ISPS Code is the ensure familiarity with the security plans and procedures through training, drills and exercises. The training, drills and exercises are mentioned in Part A paragraph 18 of the ISPS Code. Every paragraph of this part suggests considering the guidance in Part B. This part specifies that the PFSO is required to have knowledge for training others and that they have received training themselves. Secondly, it states that the security personnel should understand their duties and their responsibilities as stated in the PFSP. Furthermore, they should also be competent in performing the duties that were assigned to them. Thirdly, it states that drills should be conducted throughout appropriate intervals. The drills take into account the changes to the port facilities, the working operations in the port facilities, changes of employees, the type of port or terminal, the type of vessels the port accommodates and other information related to the port. Lastly, it states the PFSO should take part in the drill and exercises, this is to ensure that the PFSP is being followed correctly and effectively.

Part B paragraph 18 provides guidance and recommended procedures with regard to training, drills and exercises. It provides further information with regards to the requirements needed for the PSFO and the security personnel such as the type of training they need and the knowledge they should acquire for their roles in all security levels. This section also suggests

that drills should be conducted every three months for the purpose of acquiring effective implementations of the provisions stated in the PFSP. The drills that are carried out should be based on the threats that are recognized in the PFSP and it should test these elements on an individual basis. It also mentions that joint exercises with personnel such as the company security officers, ship security officers and those involved with the contracting governments should take place at least once a year with no more than 18 months between exercises. The exercises that are mentioned may be full scale or live, seminars or tabletop simulations or exercises that are combined with other exercises. The examples for other exercises mention are the ones that are run by port state authority and exercises that include responding to emergencies. What the information shows is that there is no internationally enforced method of designing these training systems. The trainings that ports partake in is left in the hands of contracting governments who accept these training regimes based on their own assessments to risk.

3.3.1.5 Cargo inspection and scanning according to the ISPS Code

Part B paragraph 1.21 notes that the port state control has the right to inspections on the ships and may request provisions of information regarding a variety of items which includes the cargo. Paragraph 18.1 of part B insists that the PFSO should have knowledge and receive training in some security aspects that were noted in the paragraph, this includes the methods of conducting inspections, audits control and monitoring, the fact that these mentioned areas of knowledge are not included in the mandatory section of the Code may be a concern for others. In addition to that section, it also includes methods of physical searches non-intrusive inspections. When it comes to the handling of cargo, the PFSP should establish security measures that should be applied during these processes. Paragraph 16.32 of part B states that in a security level 1 there should be routine checks on cargoes, cargo transport units and cargo storage areas. Furthermore, there should be checks to ensure that the correct cargo is entering the port facility in accordance to the equivalent cargo documentations or delivery notes. This paragraph also suggests checking seals to ensure that they have not been tampered with.

Paragraph 16.33 of part B provides guidelines for checking cargo at a security level 1. This includes a visual and physical examination and, using scanning equipment, dogs or other mechanical devices. Paragraph 16.35 of part B suggests the same measures taken in 16.32, however, it entails measures for security level 2, therefore the checks should be more detailed and intensified. Paragraph 16.36 of part B is similar to paragraph 16.33, however, this is also

with regard to a security level 2, and it notes that scanning and checks of cargo should increase in frequency.

In a security level 3, paragraph 16.37 of part B suggests that there should be restriction or suspension of the movement of cargo or operations in the port facility. Furthermore, with regards to hazardous and dangerous goods, this paragraph suggests that these cargos should be verified with regard to their location in the port facility.

3.3.1.6 Limitations of the ISPS code

This section briefly discusses the flaws of the ISPS code. For the purpose of this research, this part of the thesis will only focus on the weaknesses and limitations of the ISPS code on ports. The ISPS code enforces minimum security requirements for ports, ships and contracted governments. This section will discuss topics such as the enforcement of the ISPS code, the difference in standards to risk management between nations, the level of varying expertise and resources in some nations, the issue of container security within the wider supply chain and the remedies of the ISPS code after an attack.

First of all, the IMO lacks the ability to enforce the ISPS code. Instead, the IMO monitor compliances to the regulations (Raymond, 2004). The role of enforcing the ISPS code belongs to the contracting governments. Nations around the world have different risk profiles and thus rely on contracting governments to enforce the appropriate measures of security. The standards of security amongst different nations vary, some developing countries such as those in the Flag of Convenience (FOC) registries may lack the required resources or expertise to enforce the required standards (McNaught, 2005). In some areas, contracting governments are left to audit the ports in their nations in order to inspect if they are following the requirements of the national legislation. It seems like the IMO trust these contracting governments to enforce these rules. Contracting governments could perhaps outsource this task to specialized auditing firms in order to guarantee effectiveness.

Secondly, it must be noted that containers are vulnerable to threats during its movement within the supply chain. The ISPS Code can be seen as too lenient when it comes to container security. Along the supply chain, containers could be tampered with by criminal organizations or terrorist groups due to the ISPS Codes narrow focus on ships and ports. The issue of implementing a higher standard of container security is said to be unachievable, because of the high costs that could potentially come with it (McNaught, 2005).

Thirdly, the ISPS Code is known for its preventative measures to avoid potential attacks, however, if an attack were to occur the ISPS code does not address details of responding to them. Remediation issues are often left for domestic contracting governments to deal with and as previously stated, they might lack the expertise or the resources to deal with the situation (McNaught, 2005).

Corkhill (2014) highlights that the ISPS Code does not tackle container security well enough. The example given was the misdeclaration of good in containers, some products inside could be materials to create bombs and a lot of them are made of materials that are barely detectable.

Mazaheri and Ekwall (2009) argue that the Code induces higher operative expenses and it has a high implementation cost. Furthermore, with regard to its implementation, they also state that there is no predefined model for the distribution of costs. Instead, ports are left to decide how much they will spend on different areas of their security. They also stated that even though the code is good for ports that have had a lack of security measures before, the Code could have over complicated the defined security processes for more established ports.

According to Edgerton (2013), the Code does not do enough in regards to providing detailed requirements for background checks for either port visitors or port employees. This results in varying standards as to how ports conduct their access procedures. The self-regulating nature of the Code has forced governments to develop their own standards of access control and background checks which do not guarantee security.

The ISPS Code fails to separate and recognize the different types of ports and terminals as well as their operations. The Oil Companies International Marine Forum (OCIMF) ((2003) indicated that there is a shortage of information and guidance that focuses on how port facilities and terminals operate, as well as how they should implement the security measures of the Code.

According to Cox (2013), the ISPS Code is limited in its effectiveness because the Code is only partially mandatory and it lacks the application of meaningful port security measures. The Code is largely suggestive and is limited in scope. Part B of the Code provides more extensive details on the security mechanics, however, since it is optional and not mandatory, its implementation cannot be enforced.

The Code highlights limited details with regard to waterside security. The only mentioned waterside security activities are associated with water patrols, security awareness for ships on both shore side and waterside, agreements between private security companies

about waterside security services and restricting access to port facilities by way of the waterside. However, waterside security measures are only mentioned in Side B meaning that they are not compulsory, and furthermore, the Code does not provide guidance as to how to strengthen security on the waterside and does not provide guidance of assessing waterside risks. According to McNicholas (2016), terrorists or criminals could potentially use divers to attach explosive devices or drugs to vessels. Christopher (2015) suggests that small boats and vessels could target ports from the waterside with criminal intentions such as smuggling or conducting a terrorist attack. According to Edgerton (2013), there are waterside security measures that exist elsewhere, however, there has been no in-depth look to determine its effectiveness. Christopher (2015) suggests that assessing risk from the waterside is difficult, the suggested measures include hiring patrols on the waterside, placing hired security on the port facilities to look monitor the waterside, developing waterway barriers to enhance security and placing cameras to inspect the waterside. However, these measures will increase costs for equipment and power. Security measures for the waterways can also be seen as restrictive, inefficient and disruptive to operations (Christopher, 2015).

Lastly, Mazaheri and Ekwall (2009) confirmed four disadvantages in their study about 'Impacts of the ISPS Code on port activities'. These four disadvantages are that the work presented by the ISPS Code slows down progress, the ISPS Code brings more paperwork, higher costs in terms of operations and implementation and it also creates more administrative work. However, their study showed that 80% of participants agreed that the ISPS Code has increased the level of security, which Mazaheri and Ekwall (2009) confirm was the goal of the Code in the first place.

Despite the problems of the ISPS Code and the amount of security related issues absent, the Code provides a basis for global maritime security and has enhanced further research on the topic (Helmick, 2007). An example of this is when the U.S. implemented the ISPS Code. After the codes implementation grants were provided for research and development of maritime security with technology as the main emphasis. Fifteen million US dollars were provided per fiscal year from 2003 until 2008. According to Helmick (2007), the research conducted in the U.S. included:

> (1) Methods to enhance targeting and inspection; (2) Equipment to detect explosives, chem/bio agents, and nuclear materials; (3) Improved container tags, seals, and tracking sensors; (4) Tools to mitigate the consequences of a terrorist act at ports and; (5) Application of existing technologies from other sectors to port security (p.17).

3.3.1.7 Cost challenges of the ISPS Code

Ports face a variety of challenges when it comes to implementing effective security measures. A study by Chang and Thai (2016) on port security quality and customer satisfaction suggest that enhancing security quality at ports might not only heighten costs, but may also lower customer convenience. Edgerton (2013) states that to implement effective security measures, the port will have to spend. One of the main objectives for the existence of ports is to be profitable, the costs of implementing effective security measures could decrease the ports profitability potential. Contracting governments attempt to persuade ports to increase their security by enforcing regulations in order to protect commerce and national security, however, the ports often chafe at these mandated regulations because of costs and inefficacy (Edgerton, 2013). Governments have been known to support ports by acquiring new technology to enhance security and comply with the enforced regulations, for example, the U.S. government provides port security grant funds. However, the grants provide little to no funds for training and maintenance, meaning that these costs have to be covered by the port (Edgerton, 2013). According to UNCTAD (2007), the initial costs of implementation of the ISPS range between $13,500 USD and $50 million per respondent government. Moreover, the compliance costs per year range between $1,500 USD and $27 million USD. As for the ports themselves, UNCTAD (2007) ranges the initial cost to be between $3,000 and $35.5 million USD. The annual costs for ports are reported to be between $1,000 USD and $19 million USD. The ranges of costs depend on the location of the port, the size of the port, the operations procedures, equipment, manpower and infrastructure UNCTAD (2007). A study that was conducted by UNCTAD (2007) showed that equipment was the highest initial cost when implementing the ISPS Code. The lowest initial costs were operations/procedures and security level changes to 2 and 3. The results are shown in figure 2:

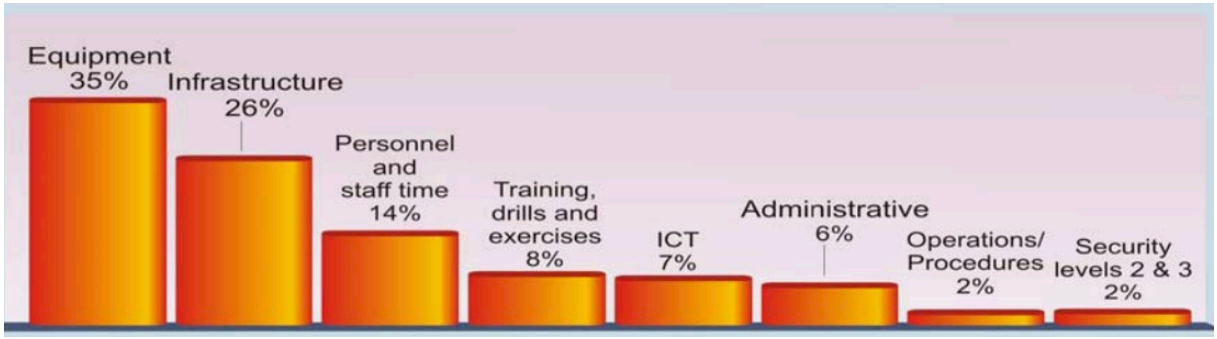

Figure 2: ISPS Code related initial costs for ports (UNCTAD, 2007)

The study also focused on the annual costs for ports that implement the ISPS Code. The highest cost was Personnel and staff time. This relates to the employed manpower. The lowest costs were the change to security level 2 and 3. The results of the study are shown in figure 3:

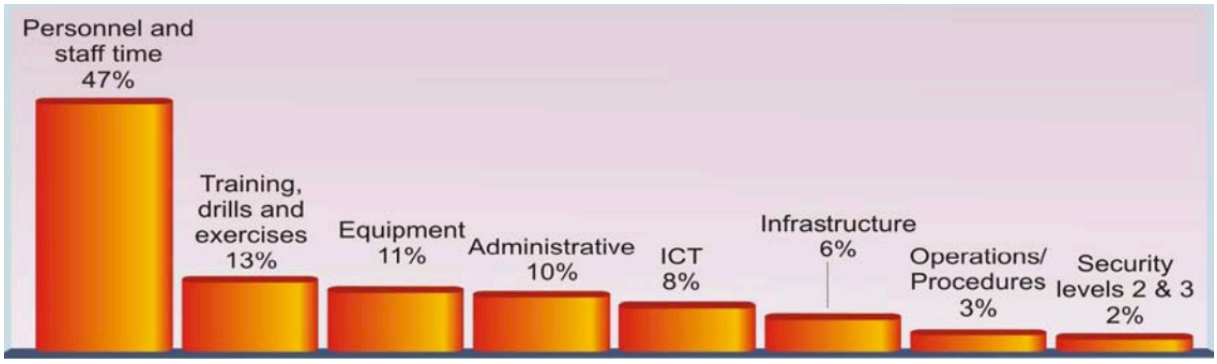

Figure 3: ISPS Code related annual costs for Ports (UNCTAD, 2007)

3.3.2 Container security

The term "container security" does not have a generally accepted definition (Gujar, Gosh, & Yan, 2014). The definition developed by Zhao, Yan & Zhang (2016) is as followed: 'The retention of safety and security (and the prevention of contamination, damage, or destruction) of the container, the containerized cargo and/or containerized supply-chain assets'. Inspections, security initiatives and sealing are some of the common practices of securing containers. First of all, the practices of inspections of containers vary in different ports (Longo, 2010). Longo (2010) has written an example of how one port carries out its container inspections. The ports name is purposely suppressed from the article due to the confidential nature of such information. The port in Longo's description complies to the Container Security Initiative (CSI), this is a system of bilateral information of transfer where members of the CSI ensure that certain steps to the security of containers are completed before the container is shipped to its own ports (Singla, 2016). The unnamed port in Longo's (2010) example receives a manifest of the ship's cargo 24 hours before it departs. From the manifest, there is a list of containers that should be inspected as they may pose a risk depending on a variety of factors. When the cargo arrives, the containers that may pose a threat are places in a segregation area before they can be moved to the inspection area for inspections. The movement from the segregation area to the inspection area depends on the amount of manpower and equipment available for inspections to take place. The containers are moved to the inspection area by trucks. Once at the inspection area the containers are scanned. There are two methods of scanning at this port, either the container is moved under the scanning equipment or the scanning equipment is moved over the container. This creates a digital image for officers to

analyse. Next, the officers perform a physical and visual inspection of the container. Furthermore, the containers are also screened for radioactive, chemical and biological substances. In this example, the containers were opened and inspected inside. If the officers decide that the container poses a threat, it is moved to another terminal area for more decisive inspections.

Zhao, Yan & Zhang (2016) described the process of how containers that arrive at domestic ports are inspected. Firstly, the containers are sent to the primary screening located at the gateway of the container terminal. According to McNicholas (2016), some of the screening devices that are used in the primary stage include X-ray imaging devices, isotope identification devices and radiation portal monitors. If the primary screening shows signs of alert, the container is sent for further inspections known as the secondary screening. If the secondary screening also poses alarms, the transportation of other containers are also put to a halt. More physical inspections such as opening containers and inspecting the interior may have to take place if the primary and secondary screening causes alerts.

Container security initiatives are another form of increasing security for containers. In this thesis, the CSI is used as an example in order to understand what impacts container security initiatives can have on ports and the actors involved in its operations. On January 2002 the US Customs and Border Protection (CBP) agency launched the CSI. The CSI came into existence after the attacks on September 11, 2001, with the purpose of tightening container security against threats such as terrorism within the supply chain before they reach US shores (CBP, 2018). The CSI requires ports abroad to pre-inspect containers and cargos before they are transported to the U.S. This is to prevent the smuggling of WMDs and other banned substances (Yang, 2010). When the CSI came into effect at the start of 2002, the US signed a Memorandum of Understanding with 20 major ports that frequently export cargos and containers to the US. On June 2007, this accounted for 68 percent of imports into the US at the time (Romero, 2003). 23 ports located in 23 different countries had signed a Memorandum of Understanding with the U.S. Nowadays, 60 of the world's largest ports have signed a Memorandum of Understanding with the US (Yang, 2010). The CBP listed three core main elements of what the CSI consists of:

1. Identifying high-risk containers: The CBP finds items that may pose a potential threat to national security by using Automated Targeting Systems (ATS). The item in the container could be WMDs, dirty bombs or other illegal tools that could be used for terrorist acts.

2. Pre-screening and the evaluation of containers before they are shipped to the US. The idea of this core element is to have containers pre-screened as early in the supply chain where possible, this could be at the port of departure.
3. Using technology to pre-screen containers that are seen as high-risk. The purpose of using high quality technology is to ensure that the timing for screening is decreased. The technology used may include devices such as X-ray machines, radiation detection devices and gamma ray machines. (CBP, 2018).

Implementation of the CSI does provide issues for ports. Stricter security measures have increased the logistics costs and have had a negative impact with regards to the effectiveness and the efficiency of operations in the supply chain (Yang, 2010). Firstly, Barnes and Oloruntoba (2005) claimed that security measures such as the CSI and ISPS can prevent the threat of terrorism, however, these measures can affect the operations of businesses, diminish the competitiveness of firms and lessen performances. Secondly; lead time, transportation costs and warehousing costs have increased for those ports that comply to the CSI. The mentioned lead time and costs have increased because shippers are put in a situation where they must delivery cargo or containers to ports 48 hours ahead of time (Yang, 2010). Lastly, an inspection of all containers in accordance to the standards of the CSI increases costs significantly and can also have an impact with regard to delays on cargo handling (Yang, 2010). The costs of inspection per container vary and depend on factors such as the location, the extent, the size of the container, the inspection equipment and the container inspection services or company.

There are numerous issues with modern container security. Firstly, in order to implement security measures, container ports must realise that costs can be added, delays can happen and this can cause uncertainties in the transportation process (Zhao, Yan, & Zhang, 2016). Disruptions within the supply chain can be caused by security related situations at any point, including ports that can be unfavourable to the operations (Yang, Wang, & Li, 2013). Secondly, ports may have their own standards to security, however, there is no single organization that sets standards and governs for the entire movement of containers within the global supply chain (Bakir, 2007). In addition, there is also no single organization that governs the security of containers within the global supply chain (Tang, Xu, Yang, & Chen, 2013). Thirdly, there are numerous threats within the containerized supply such as the ones that were mentioned earlier in this chapter. A breach of security caused by a threat in a single part of the supply chain may affect security in the entire supply chain (Bichou & Talas, 2014). Lastly, Zhao, Yan and Zhang (2016) mention that the different members within the containerized supply chain have contrasting objectives. For example, the objectives of the port is to decrease

clearance charges, increase the clearance efficiency and decrease the amount of clearance time. The state's main concern is about illegal activity or threats such as contraband hidden within the containers. Businesses such as those that are in the private sector are most concerned about costs, disruptions to the supply chain and the time of operations.

3.3.3 Protection against dangerous cargo and nuclear materials

An example of an initiative that protects ports from dangerous cargo, nuclear materials and radioactive materials is the Megaports Initiative (MI) which was introduced in 2003. The MI is led by the US National Nuclear Security Administration (NNSA) and they work with foreign customs, port authorities, terminal operators and other relevant entities with three objectives in mind, according to the NNSA (n.d.) the objectives are: (1) Preventing terrorists shipping illicit materials by using seaports; (2) Detecting radioactive and nuclear materials that are shipped in sea cargo and; (3) Interdicting hazardous and harmful materials before they are used against the U.S. or the allies of the U.S.

This mission of the MI is to enhance detection capabilities for nuclear and radioactive materials within container cargos that are being shipped internationally. The MI supports foreign ports to do this by providing radiation detection equipment as well as alarm communication systems. According to the NNSA, the MI provides various support such as the comprehensive training of foreign personnel, technical support of the installed rational detection systems and maintenance coverage in the short-term (2010). In return for providing the support, the NNSA requires that data with regards to seizures and detections of both radioactive and nuclear materials are shared to them, the data sharing only comply if these materials were detected with the use of the provided equipment (NNSA, n.d.)

In 2015, a goal was set to have 50% of the world's maritime containerized cargo scanned, by then, 100 seaports were identified to have installed the radiation detection system and at the time, 27 ports have successfully completed installation. At the time, 16 ports were at various stages of development. These efforts by the MI are in place to mitigate the smuggling of nuclear materials and mitigate terrorists using maritime transportation as a tool (Christopher, 2015).

3.3.4 100 percent container scanning

One of the most well-known acts that enforce 100 percent container scanning for imported containers is the 9/11 Commission Act of 2007 in the U.S. Through this act, ports that export containers to the U.S. must perform 100% scanning and radiation detection procedures.

The Act aims to protect the U.S. from terrorist risk from the global supply chain. It has been criticised for being a disguised protectionist measure that transfers risks to its partners (Alix, Carluer, & Slack, 2010). The Act has been praised and criticized. According to Wolf (2013), the Act can help reduce the number of weapons for terrorist activity entering into the U.S. Wolf (2013) also claimed that according to the RAND Corporation and the Congressional Research Service, a terrorist attack on a U.S. port could cause tens of thousands of deaths and disrupt global trade immensely. The RAND Corporation and the Congressional Research Service estimates the cost of a terrorist attack on a U.S. port to range between $45 billion USD to $1 billion USD (Wolf, 2013).

However, despite the positives of the Act, there have been numerous criticisms. The European Commission (2010) argued that the act has been disruptive for EU ports, terminal operators and terminal operators. At the time of writing, larger ports were scanning around 0.1 percent and smaller ports were scanning between three to five percent. 100 percent scanning would introduce high costs and seriously disrupt the flow of international trade (European Commission, 2010). Furthermore, this Act transfers the control of good to the export point which leads; to reconfigurations of ports and terminals; the need for space to facilitate additional containers; the need for a redesign of port procedures and scanning and radiation detection would increase operational costs (European Commission, 2010). The European Commission (2010) estimated the costs of 100 percent scanning for all EU ports to range between 280 million euros and 430 million euros. Furthermore, the EU commission added that this would cause less handling capacity on terminals and a longer dwell and turnaround time for inland modes of transportation and feeder vessels. Moreover, they added that according to the Act, scanning equipment is not specified, this would lead to ports purchasing cheaper ones and therefore, security will not improve as some scanners are not able to detect certain illegal materials. Lastly, containers would still be highly vulnerable to being tampered with along the supply chain, even after the scans have taken place. Alix, Carluer and Slack (2010) argue that 100 percent inspections will increase congestion at some ports, increase the amount of personnel needed for scanning and operations which increases costs. Lastly, they also say that ports would have to spend large amounts of money on new technology and new equipment (Alix, Carluer, & Slack, 2010).

3.3.5 Surveillance equipment

One of the most vital tools for any security system is the use of CCTV. In order for the tool to be effective as a perimeter system, these characteristics should be considered: (1) has a

clear line of site; (2) has detection for thermal imaging; (3) visible light detection; (4) can capture high definition images; (5) the cameras should be able to not only monitor but record as well (6) should be able to have a clear view in the dark (Russel & Arlow, 2015). With regard to container ports, there are a few aspects to take into consideration before purchasing surveillance cameras. First of all, the location of container terminals. The location of container ports and its environment are highly corrosive as they are situated close to salt water. Also, container port activities take place outdoors, meaning that harsh weather such as heavy rain, sunlight, fog, humidity or snowfall should be taken into consideration. Second of all, the landscape of container ports changes due to the activities that take place such as the movement of containers and stacking. The placement of containers and the heights of which they are stacked can be a challenge when determining the placement of the surveillance cameras. Lastly, ports should not only consider the restricted areas inside, but they must also consider the areas close to the port that is open to the public. Monitoring gates, fences and other areas open to the public near the port could prevent unwanted incidents before they occur (ONCAM, 2019). Paragraph 15.15 of Part B in the ISPS Code suggests using surveillance equipment to mitigate the identified port facility vulnerabilities.

3.3.6 Employee background check

Background checks are important for security and should be conducted to would-be employees and current employees. The reasons why ports should perform background checks on their current and future employees is so that safety in the workplace can be guaranteed and furthermore, reduce the likelihood of a threat from occurring (Kunz, 2017). Background checks are also important to secure trust from the employer to the employee and hence, gives the employer assurance that the employee would not be liable for any increased levels of threats. There are a variety of details that can be gathered if a full background check is established such as employment history, criminal records, training history and reference details (Christopher, 2015). If an employee with a criminal record is hired and causes violence in the workplace, the port could potentially face charges for neglect (Kunz, 2017). Moreover, if somebody who does not have the proper training or experience is hired, that person can potentially cause harm in the port area, for example, if someone was hired to operate cranes in the port with no proper training or experience, they may cause an accident with large consequences such as fatal injuries. Hiring the wrong person without a proper background check according to laws and regulations could cause the port to suffer financially, suffer from a loss of reputation and may affect the level of trust they have with current customers.

3.3.7 Access controls

In order to prevent unauthorized personnel entry into ports, vessels and port facilities, there must be an established access control. Unauthorized personnel entering ports may have the intent on committing acts of terrorism, smuggling drugs, committing acts of violence or they may be trying to sneak into vessels. They also might try to sneak unauthorized items into the port area or perhaps they may intend on stealing cargo. According to Andritsos (2014), an access control system has three essential functions which are entitlement, identification and documentation. Entitlement refers to specifications on entry to the port such as who can enter, from where can they enter, the duration of their entry and how frequently can they enter. Identification is needed to confirm that the correct person is entering the port area and that the person has provided correct identification. Lastly, documentation means that all accesses should be documented, security personnel should document and take note of all personnel and vehicles entering and leaving the port area (Andritsos, 2014).

Access control procedures are not limited to building parameters around the port facilities then locking, securing and guarding them at all times (Russel & Arlow, 2015). The access control procedures would be different for employees and visitors. Employees should be given access only to the areas where they are to perform their duties and not go to areas where they are not permitted to enter. Employees should have a photo that identifies their credentials or perhaps a card/badge from the port showing their photo and the information of their employment (Christopher, 2015). If an employee were to leave their job, it is the duty of the management of the company or the security personnel to ensure that access keys are returned and the accessibility functions of their key cards become invalid for entry (Christopher, 2015). Visitors to the port, on the other hand, should have authorization from their organizations that states the duty they are to perform at the area (Christopher, 2015). Upon arrival at the port facilities the visitors should present photo identification for the purpose of documentation, security officials must then assure that visitor logs are maintained with details such as the name of the visitor, purpose of the visit, the organization of the visitor or perhaps the duration of the visit to the port (Christopher, 2015). Entry or access to the port with the use of cards, PINs or fingerprints is a form of identity management. Identity management is important for access control since the methods are based on the following categories such as something you own (key cards, badges) something you know (PIN codes, passwords) and physical characteristics (fingerprints, eye scanners) (Andritsos, 2014). It must be noted that access procedures to the ports are noted and made clear in the organizations security regulations and by national or

international regulations such as the ISPS code (Andritsos, 2014). The ISPS Code (2003) provides guidance in Part B by suggesting that the PFSP should identify appropriate locations for access for each security level. Moreover, that part of the Code also suggests limiting the number of access points into the port facilities, however, this is only in the event of a security level 2 or 3 escalation. In regards to barriers, paragraph 16.17 of part B suggests that restricted areas should be bound by fencing or other barriers that the contracting governments deem appropriate. However, it must be noted that ports operate as a business, and they must find the right balance between controlling access and efficiency of throughput in order to satisfy their customers (Christopher, 2015).

3.3.8 Countermeasures for corruption

According to Edgerton (2013), in order to counter corruption, an organization or a company should assess its internal threats by having transparency of its activities and operations. The methods include interacting with governments and others in the same industry to confirm that all operations are carried out in an appropriate manner. Christopher (2015) suggests using the methods of the Organization of American States (OAS), which advocates more monitoring, inspections, higher cooperation between companies and state and greater commitments to resources. The OAS, according to Christopher (2015), also advocated that there should be more enforcement of stricter penalties for those that are involved in corruption and transnational crime. Lastly, there should be more regulations and prosecutions for those that are involved in illegal activities such as corruption.

3.3.9 Information Technology Security

This section discusses briefly of a measure that can be taken to deal with cyber threats. A cybersecurity plan can enable ports to protect their digital information and their assets. McNicholas (2016) developed a cybersecurity plan which encompasses effective components for dealing with cyber threats. According to McNicholas (2016), a level cybersecurity plan includes identification of the organization’s priorities, defining the applicable cybersecurity standards, assessment of the risks, remediation planning for the organizations vulnerabilities, penetration testing and monitoring. These components belong to the basic cybersecurity process and are presented in figure 4:

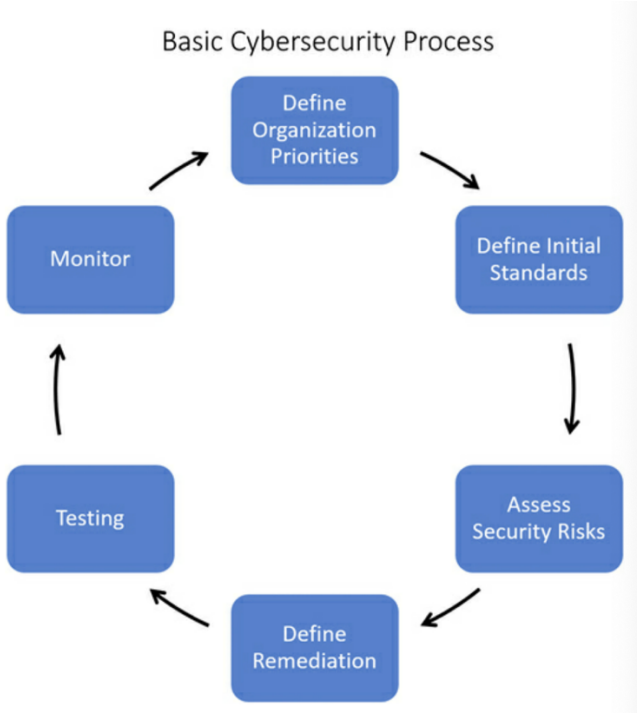

Figure 4: Basic cybersecurity process (McNicholas, 2016, p. 294)

Firstly, the organizations should identify their priorities. This means defining what is important to the organization and what the organization wants to protect in order to proceed with operations. For a container terminal, this could be their customers, facilities, cargos, reputation etc. Afterwards, the organization should prioritize and determine which one of these things are most important. This occurs so that the organization can determine how much of its budget should be allocated towards each one.

Secondly, a cybersecurity standard must be defined. Some examples of existing standards include ISO/IEC 27001, NIST framework, NIS directive and others. Each standard will not fully address the needs of a port fully, however, the frameworks provided allow customization in order to fulfil the needs of a port.

Thirdly, in the risk assessment of cyber-attacks stage, organizations should define what needs to be protected, what kind of cyber-attacks or cyberthreats are possible, the amount of damage a particular threat can cause and the chances of a certain threat from occurring. Organizations can also define the countermeasures that are available against the threats before moving on to the next stage.

The next stage involves remediation planning. The plans can include technical tasks, human procedures and processes. For example, if a cyber incident were to occur the plan could involve procedures on how to communicate the plan. Also, the plan can include procedures for

training, education and technical processes such as adding firewalls. If a successful cyberattack occurs, the plan may also include procedures to respond it. The remediation plan usually coincides with the findings in the risk assessment, this involves identifying countermeasures that are plausible for various solutions. The costs of employing the identified counter measures should also be taken into consideration. Changes to the organization and the threats are a possibility, therefore, it is important to continuously perform security analyses between certain intervals. This may also have an effect on the costs.

The next stage requires penetration testing, this is done to expose vulnerabilities to the system and to ensure that the countermeasures are effective. The testing is effective when done under actual working conditions, this will enable the organization to understand how their employees respond to cyber breaches or attacks.

The monitoring stage involves monitoring the systems, monitoring all areas of security and monitoring the employees compliances to the regulations that addresses cyber issues. Lastly, when the cybersecurity plan has been finalized, the next phase is to implement the cybersecurity plan. Much like the ISPS Code's PFSP, the cybersecurity planning is a continuous process and should be analysed regularly. This is done in order to respond to the changes made to the port facilities, port systems and the changes in threats.

3.3.10 Security awareness training

According to the Part A paragraph 17.2 of the ISPS Code, one of the duties and responsibilities of the PFSO is the enhance security awareness and vigilance of personnel at the port facility. This is not limited to security personnel but also includes laborers, visitors, stakeholders, customers and other personnel associated to the port in any way. When applied correctly, security awareness trainings can provide port facility personnel with understanding for security at the port, this will strengthen the port's security posture greatly (Christopher, 2015). According to Christopher (2015), a security awareness program should include the following aspects:

> (1) provide port users with a basic introduction to port security; (2) illustrate why it is important for port users to understand the need for a culture of security in the port facility; (3) outline a basic framework for understanding the relationship between risk and vulnerabilities at seas ports; (4) show specific ways in which port users can help to reduce the risks associated with those vulnerabilities as part of the port's overall security infrastructure (p. 144).

Training the port facility employees and users in basic awareness can enable assistance to port security personnel. These assistance include, but not limited to detecting unlawful activity, identifying personnel that is acting suspiciously, identifying vehicles that are not meant to be in the port facility, identifying suspicious activity and identifying concerns that are or may be related to safety and security (Christopher, 2015).

Supply chain Security

According to McNaught (2005), the scope of the ISPS Code is extremely limited in addressing security against threats and should not be viewed as a stand-alone solution. Instead the ISPS Code should be seen as one component for securing ports from threats. Many scholars have argued that the ISPS Code is too limited because it only covers the port and ship interface, the Code does not cover the overall supply chain (Edgerton, 2013). The supply chain is vulnerable to disruptions and past terrorists attacks have proven that to be true (Rice & Caniato, 2003). After the September 11th terrorist attack, companies within the supply chain industry have adopted a variety of initiatives and concepts in order to reduce exposing the supply chain vulnerabilities (Martens, Crum, & Poist, 2011). Some standards, legislations, concepts and initiatives that have been adopted by container ports for safeguarding the supply chain includes: the Authorized Economic Operator (AEO) (Laszuk & Ryciuk, 2016), Megaports Initiative (MI) (GAO, 2012) and the Container Security Initiative (CSI) (Banomyong, 2005).

3.4 Future of Port Security

The container port industry have started adopting automation at an accelerating pace. Automation is seen to be safer due to the lack of human-related incidents and performances are said to be more predictable during operations (Chu et al., 2018). Moreover, ports will be able to handle container more efficiently since automation has been proven to reduce cycle times and shorten unnecessary box moves. Dingeldey (2017) reported that ports are increasingly investing in automation due to competition and pressure, this indicates that the amount of automated terminals will rise despite the high upfront costs, however, once automation is implemented, ports benefit from lower operating costs.

Automation is not a new topic in the container terminal domain, ever since 1993, the Port of Rotterdam became the world's first automated container terminal after introducing the first Diesel-hydraulic Automated Guided Vehicle (AGV) (Stehouwer, 2012). According to Chu et al (2018), An automated port is defined by five components that create value when each component is implemented individually. However, in order for a port to greatly benefit from

automation, these components need to be coordinated and integrated. These five components are automated equipment, equipment control systems, terminal control tower, human-machine interactions and interactions with the port community.

It is clear that container terminals can benefit largely from automation, however, fully automated ports increase their exposure to vulnerabilities such as cyber-attacks (Dingeldey, 2017). According to The Maritime Executive (MAREX, 2019), the American Association of Port Authorities (AAPA) has stated that the ports in the U.S. need close to $4billion USD to improve on port and supply chain security to cover the next 10 years. An estimated amount of $1.2billion USD was claimed to be needed for threats such as tackling cybersecurity, drone mitigation and other security threats. It was also reported by MAREX (2019) that they needed $2.62 billion USD to improve port facility security systems, infrastructures and equipment. 85 percent of member ports of the AAPA anticipated that cyber threats to their ports will increase over the span of the next ten years. 78 percent of the members also anticipated that future security grant funding should be used to improve their cyber security. The intent to increase their cyber security was instigated by the Maersk cyber-attacks in June 2017. The attack costed Maersk around $300 million USD despite the fact that the attack was not directed to them (Dingeldey, 2017).

Ports should not only consider the threats that may arise because of technological advancements inside the port, but they should also consider the threats they may arise because of technological advancements outside the ports. Frith (2018) stated that terrorists have the potential of deploying explosives with the use of drones. Drones have developed to the point where they can fly long ranges, endure harsh conditions and carry heavier objects. The ISPS Code mentions that there should be procedures for preventing weapons, dangerous substances and devices entering the port, however, the Code does not have measures against aerial threats such as drones. By 2020, the amount of drones is expected to reach 12 million, this may lead to PFSP's including counter measures for them in the future (Frith, 2018). The existing combating tool against drones is the "D-Fence maritime drone detection and defeat system" which was developed by Martek Marine. This system could detect drones in the range of roughly 5kms and identify the position of the pilot. This could perhaps be used as a tool against drones for ports in the future.

3.5 Summary of theory

The threats to container ports were identified based on the theories of other authors and the security measures adopted by international organizations in order to protect ports from them. Moreover, further security measures were identified based on the international communities efforts to protect their ports and containers from threats, these further measures were adopted due to the fact that the ISPS Code had not addressed certain methods for certain threats. Various authors have presented other measures that they regarded as effective in countering threats, such as the one explained for IT security. The future of port security is not certain, however various authors have provided theories on the trends of the industry, therefore, allowing discovery as to what may be the potential threats in the future and how ports may attempt to counter them. Arguments against certain security measures were provided based on the theories various authors have developed.

4. Case Study and Further Methodology

In this chapter, the case for the study is explained along with the methods used to collect and analyse data. Furthermore, the profiles of each informant is provided as well as the reliability and validity of this study and the ethical considerations.

4.1 Case Study: Threats to container ports and preventative security measures

Multiple case studies were conducted in this study. The author selected informants who have experience in working at container ports in three different regional locations. This is based on the assumption that threats would be different based on the setting of the container ports and therefore have an effect on the type of security measures each region have adopted. Three cases were selected and nine informants from nine different ports were interviewed. Case 1 is based in the Scandinavian region and made up of five informants, case 2 is based in the South East Asian region and is made up of three informants and case 3 is based in a country that borders the pacific ocean and is made up of a single informant. The description of the cases are provided below.

4.1.1 Description of the cases

The first case is made up of five ports from the Scandinavian region. For the purpose of this thesis, the case will be known as region 1. The ports that are located in this area border or have channels that lead to the North Sea. All the ports comply to the European Maritime Safety Agency (EMSA) regulations. One of these regulations, known as (EC) No 725/2004 obliges the agency to inspect each port facility to ensure that the local governments are complying to the security requirements of the European Union (EU). Average wages in this region are higher than the regions in the two other cases. All the ports in this case are state owned.

The second case is made up of three ports from the South East Asian region. For the purpose of this thesis, the case will be known as region 2. The ports are in countries that are part of the Association of Southeast Asian Nations (ASEAN) intergovernmental organization. One of the ports have a container handling rate higher than all the other ports that were analysed in this thesis. The average wages in this region are comparatively lower than the two other cases mentioned. The level of participation in tertiary education is relievedly low compared to the other regions mentioned. All the ports in this case are run and operated by the states they are in.

The third case is made up of one port which borders the Pacific Ocean. This case will be known as region 3. The container volume in this port is lower than the largest the port in

region 1, however, it trafficked larger volumes than the other four ports in region 1. The average wages are lower than region 1 but are higher than region 2. The level of participation of tertiary education is on the same level as region 1, which are both significantly higher than region 2 and the world average. The port mentioned in this case is private, unlike the ports in the other cases.

4.2 Collection of Data

As mentioned previously, the chosen method of collecting data for this master thesis was through conducting interviews. Interviews are conversations between two or more individuals that include a set of assumptions that are usually not applied in regular conversations (Oates, 2006). The direction of the interview depends on the agenda of the researcher, meaning that interviews are not like random occurring conversations but instead are controlled by the interviewer in order to obtain useful information for their study (Oates, 2006). In order to decide how an interview should be conducted, the researcher would need to be aware of these three types of interviews, which are structured interviews, semi-structured interviews and unstructured interviews. For the purpose of understanding the differences between the types of interviews and understanding the authors choice, the three types of interviews are briefly explained.

The features of structured interviews are that the interviews use pre-determined, standardized and identical questions for every sample that is interviewed (Oates, 2006). The questions are read out the same for every interview and the interviewer should take note of the answers to each question without further comment. Further comments by the interviewer may lead to the interviewer imposing their views to the interviewee and hence, may affect the outcome to further questions (Oates, 2006).

In a semi structured interview, the researcher will still have an agenda to be covered but they do not have to be covered in a particular order. For example, the researcher might ask a question and the interviewee might cover another topic whilst answering that question, the interviewer may then avoid asking that question since it had already been covered. The interviewer may want to ask new questions depending on the answer the interviewee might have provided, this could be in order to get more information of a particular subject or topic. Additional questions may also be asked by the interviewer with the intent of continuing a good flow to a particular conversation or to get more into an issue the interviewer was not prepared for.

An unstructured interview is more free flowing than the two other interview types that were previously mentioned. The interviewer would not have as much control. The free flowing conversation would mean that the interviewer could ask questions that come to mind during the interview, it is important that the interviewer does not interrupt the interviewee as this could disrupt the flow of the conversation and the interviewee may find it rude, hence, the dynamics of the interview could change for the worse. Furthermore, disrupting the flow of the interview might potentially hinder an opportunity for the researcher to gain relevant information. The researcher in this particular interview would introduce the topic in the beginning and then allow the person being interviewed to develop their ideas and speak freely (Oates, 2006).

Interviews can be conducted in a variety of methods. It can be face-to-face, on the phone, on skype and through a variety of available online features. An interview may also be written online, the interviewer types the questions to the interviewee and expects them to type back with answers. However, conducting interviews by typing is perhaps considered limited due to the fact that the interviewee may provide less expansive and shorter answers (Oates, 2006). Furthermore, the interviewer would need to know whether the person typing is who they claim to be. Typed-online interviews can have a single advantage, the interviewer would not need recorders to transcribe the data collected since the answers are already written. Spoken interviews can enable the interviewed individual to explain the answers to each question in more detail and hence, providing the researcher with richer data. Telephone calls have their limitations as well. In a telephone call, the interviewer misses out on inspecting facial expressions which may change the context on how the answers can be perceived. Skype calls allow the interviewer to view the body movement and facial expressions of the participant. This helps gain richness as the interviewer can detect gestures such as hand movements and facial expressions (Oates, 2006).

The chosen method of data collection for this mater thesis is by conducting semi-structured in-depth interviews. Semi-structured interviews will allow the researcher to a certain extent have control of the interview and will also allow the researcher to conduct the interview with a relatively well structured flow. The researcher in this particular type of interview may also ask additional questions which may not be present in the interview guide, but would contribute to the study and the agenda of the researcher, this would depend on the flow of the interview, the information the interviewee provides and whether or not the issue raised was an issue the researcher was prepared for.

4.3 Interview guide

An interview guide was used when the author conducted the semi-structured interviews and it can be viewed in APPENDIX A. Interview guides are valuable when the researcher conducts extensive interviews in which the questions are open ended. It helps the interviewer keep track and allows the researcher to follow the steps that were planned.

According to Bryman (2012), interview guides for semi-structured interviews consist of list of topics that need to be covered specifically. During the interviews, the order and phrasing of the questions are flexible. The author adopted this approach in order to encompass the flow of the interview. The interview guide questions was ordered in a logical sequence and was built with the focus of the research question in mind. The questions were written so that they were comprehensible to the informants and with the hope that the topics were relevant.

The formulation of questions for the interview guide was created following Bryman's (2012) approach as shown in figure 5:

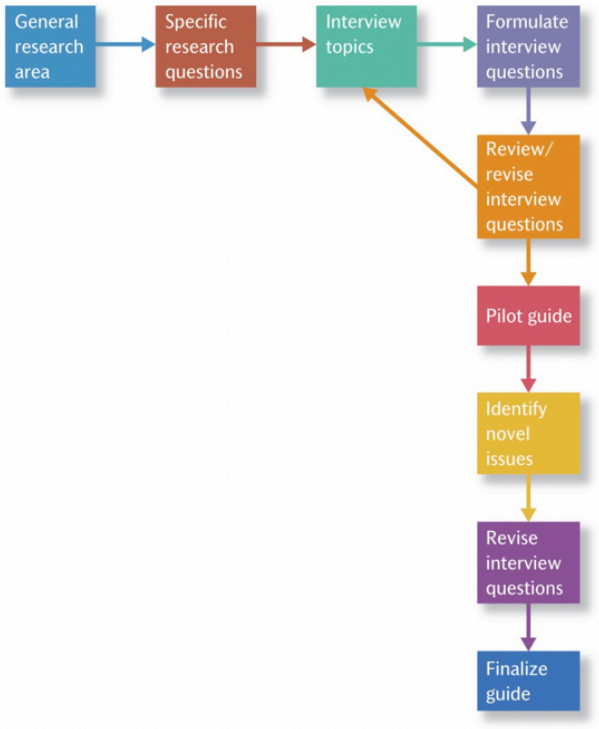

Figure 5: Formulation of questions for an interview guide (Bryman, Social research methods (4th e.d.), 2012, p. 476)

After the interview questions were formulated following the establishment of the topics for the interviews, the author reviewed and revised the interview questions with the supervisor. After that process, the author commenced to pilot the interview guide with an officer at a port

located in Thailand. This helped identify various weaknesses and issues, such as questions that sounded similar or questions that may have provided unrelated answers. After the interview guide was reviewed and corrected once again, the guide was eventually finalized.

The interview guide consisted of 31 questions and was structured in six sections. The first section was based on the informants profile and comprised of 3 questions. These question were asked so that the author could learn about the informants background, experience working in the industry and their positions in their current organization. The informants background provided the author with understanding of their knowledge of port security. The second section was built up of questions in relation to current threats where the author wanted to find out the most prominent threats to container port security today. The questions were asked so that the author could discover what the informants suggested were the most prominent threats globally and what were the most prominent threats at their respective ports are. The third section is almost related to the previous section, but instead, the author wanted to find out what the informants suggested were the prominent threats in the future. The next section comprised of questions in relation to how threats could be mitigated so that they do not occur. The author was able to discover how the ports at the informants location conducted these processes and their opinions on the contracting governments role. In the fifth section, the author asked the informants about the ISPS Code with topics relating to its strengths, weaknesses, challenges of implementation, vulnerabilities it exposed, what they have added to their security system besides for the ISPS Code and whether they thought the Code needed to be amended. The last section was the closing. Here the author asked if the informants had any more additional comments. This was so that the informants could provide more information that could be valuable for this study. Lastly, the author asked the informants if it was acceptable for them to be contacted after the interview. This question was asked in case the author needed additional information or needed clarity on the answers.

4.4 Sample

The chosen sampling for this research was purposive and theoretical sampling. The latter is a sampling technique that is guided by the theoretical framework (Marshall & Rossman, 2016). Nonprobability sampling enables the researcher to collect data from individuals who relate to the topic of the study. This type of sampling has biased elements as the researcher is able to select individuals who they think would best contribute to the study. Probability sampling allows the researcher to select samples out of randomness. The author decided not to perform this kind of sampling because the data obtained is likely to be highly unreliable. This

kind of sampling would be more suited for a quantitative research where the study aims to answer a hypothesis.

There are three main types of nonprobable sampling. Firstly, there is convenience sampling; this type of sampling gives the researcher the freedom to select whoever they find as oppose to finding those that are most qualified to provide data about the topic. Neighbours, co-workers or even friends of the researcher are not excluded from being selected. Researchers conducting this kind of sampling with those they have close relations with might find that the data collected are one-sided. The data collected can be limited in terms of richness. However, convenience sampling can also be useful, for example, a student can interview other students to discover if the facilities on a school campus are adequate for learning (Cooper & Schindler, 2014).

Secondly, purposive sampling occurs when the researcher selects participants based on how much valuable data they can contribute to the study. In this type of sampling, the researcher handpicks those that they believe can provide valuable data that is most relevant to the research question (Oates, 2006). The researcher is obliged to collect data from certain individuals that have a wide range of expertise on a particular phenomenon (Crossman, 2018). For example, a researcher that conducts a study regarding a particular navigation system on vessels may collect data from ship captains. Cooper & Schindler (2014) suggests that purposive sampling is most appropriate for an exploratory research design.

The third type is referred to as snowball sampling. The researcher collects data from one individual, then afterwards they ask the participant to provide contacts that can be useful for the study. If the process is successful, the amount of samples increases as if it was a snowball rolling down a hill. However, the researcher should ensure that the provided contact is a worthy participant for the data collection, the researcher must rely on their own judgement as well.

The Author decided to select purposive sampling for this master thesis. The chosen sampling allows the author to select individuals that have knowledge on different aspects of a phenomenon. This research is exploratory by design, hence, why purposive sampling is appropriate for a qualitive research design that uses in depth semi-structured interviews as a method for collecting data.

The participants for the interviews are chosen based on their experience working with or in container ports. Selected participants have work experience in organizations. The study selected nine participants that can provide data covering different aspects of the topic, therefore

are not limited to a single type of position within the container port industry. Furthermore, the informants are employed in nine different ports. The purpose of interviewing informants with different backgrounds and in different ports is to gain a larger insight of the topic and to understand a variety of point of views based on their experiences and knowledge. The backgrounds of the informants are: a harbour captain with seven and a half years' experience, has a background as an electrician and has education with respect to security and the ISPS Code. This informants duties include security, traffic control and electrical areas; a Head of Health, Safety, Security and Environment (HSSE) with six and a half years' experience in the tug boat industry, five years at sea and eight months in the current industry. The informant has experience with the ISPS Code on sea and on land and in terms of security, this informant works with parameter protection and on permits; a port director with 20 years' experience and has a background as a naval officer and as an economist. This informant is most responsible for security at the port; a port operation and marketing advisor who is second in command behind the harbourmaster and also holds a role as the assistant PSO (Port Security Officer), holding a bachelor degree in nautical science and has been working at sea for seven years as an officer. This informant has worked in the current port for three years and works with the ISPS Code, Security and with the response team; a port captain with nine years of experience and has a background working as a ship officer and after that was a manager for a total fleet for ten years; a head of security and a principle PFSO with 25 years of experience in the current industry, this informant has completed courses such as the close protection course and the certified protection professional through the American Society for Industrial Security (ASIS); a general manager for commercial and head of sales with 18 years of experience in freight forwarding and in the RoRo industry, holding an Master in Business Administration; a chief officer for port operations with over 10 years of experience, holding two masters in degree in supply chain management and port management; a Head of Operations at a port with 18 years of experience, holding a Master degree in Business Administration and has completed courses in port development and a course on Port Facility Security Offer (PFSO). The selected informants have backgrounds in working directly or in ports. Five of the informants are located in the Scandinavian region (Region A), three of the informants are located in the South East Asian (Region B) and one of the informants is located in a port that borders the Pacific Ocean (Region C). The location of the informants were purposefully selected in order to have a perspective of what kind of threats affect different ports, and to explore the security measures used by them with considerations regarding the resources available to them. Lastly, having informants from different ports also provided information with regard to their opinions on the effectiveness of

the modern security measures and whether or not they have adopted additional security measures.

The informants were contacted by e-mail and phone call. The interviews were conducted from the beginning of March 2019 till the beginning of April 2019. Five of the interviews were conducted face-to-face at the ports where the informants were employed at and the remaining four interviews were conducted through skype. All the interviews were conducted in English. Before each interview, the author asked each informant for permission to record and permission was granted by all informants. All the recorded interviews were transcribed fully by the author. The profiles of each informant is shown in table 2. Note that 1, 2 and 3 indicates the region of which the informants ports are located.

Table 2: Informants profile

Informant	Profession	Type of meeting
1a	Harbour Captain	Face-to-face
1b	Head of HSSE	Skype
1c	Port Director	Face-to-face
1d	Port Operation and Marketing Advisor, Assistant PSO	Face-to-face
1e	Port Captain	Face-to-face
2a	General Manager	Skype
2b	Chief Officer for Port Operations	Face-to-Face
2c	Head of Operations	Skype
3a	Head of Security and Principle PFSO	Skype

4.5 Data Analysis

Analysing qualitative data is not bound to a single technique or process. There have been many techniques and processes developed by a number of researchers, however, there is no single structured way of analysing qualitative data (Bryman & Burgess, 1994). Due to the nature of qualitative analysis, it is vital to focus on the relationship of the research design, the data collection method and the method of which data is analysed. Moreover, in order to find a suitable technique, researchers should take into account on the links between the research design, research strategy and research techniques. A dynamic process for analysing qualitative data is one that links theories, problems and methods together (Bryman & Burgess, 1994).

The chosen qualitative data analysis technique for this master thesis was developed by Miles, Huberman and Saldana (2014). They believe that analysis contains three concurrent flows of activity which are: data condensation, data display and conclusion drawing or verification. This analytic technique mostly resembles the ethnographic method and features some qualities from grounded theory (Miles et al, 2014). An interactive model regarding the components of data analysis is show in figure 6:

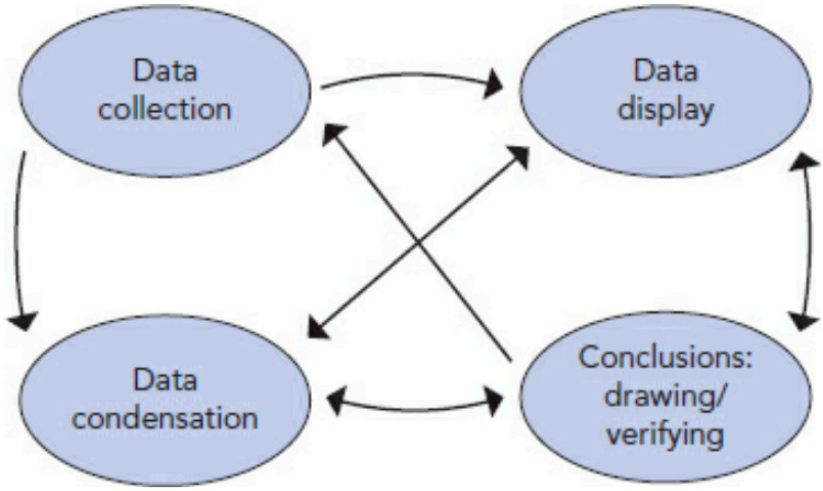

Figure 6: Components of data analysis (Miles, Huberman, & Saldana, 2014, p. 14)

Data condensation is focused on transforming the collected data into words. The data was collected from semi-structured interviews which were recorded and then transcribed fully into written texts. At this stage of the process, the transcribed interviews were coded. This means that the most relevant and meaningful data were selected and focused on with the goal of making the data stronger. Other activities in this stage of data analysis are writing summaries and theme development.

Data display is referred to as ‘an organized, compressed assembly of information that allows conclusion drawing and action’ (Miles et al, 2014, p. 12). Upon the collection of data in qualitative research, in this case from interviews, the data can be extremely bulky and structured poorly. Proper data displaying procedures can enable researchers draw justifiable summaries, conclusions or enable the researchers to procced to the next stage of analysis (Miles et al, 2014). Data can be displayed in tables, graphs, charts, matrices, scatter diagrams etc. This helps the researcher form data in an organized way so that it is immediately and easily accessible. Having extended-large amounts of information could be difficult to process, therefore, it is important to display data in an organized way.

Drawing and verifying conclusions is the third stream of analysing. Researchers interpret the meaning of things within their study by noting patterns, explanations, causal links and propositions from the start of their data collection processes (Miles et al, 2014). From the methods of data condensation and data display, if done properly, researchers should be able to draw a final set of conclusions. It should be noted that the steams of analysis can take place contemporaneously meaning that a variety of conclusions can be made at different times, however, a final conclusion can be noted once the entire data collection process has been completed.

4.6 Research Quality: Reliability and Validity

The quality of the research can be partly established under these important criteria’s which are reliability and validity (Bryman, 2016). According to LeCompte and Goetz (1982), reliability and validity can be defined internally and externally. External reliability refers to the replicability extent of the research. Whether or not the researcher can use the same method and gather the same results from previous studies. Internal reliability refers to a situation where there is more than a single individual observer in a research group, and they are in agreement to what they see and hear (LeCompte & Goetz, 1982). Internal validity refers to ‘whether there is a good match between researchers’ observations and the theoretical ideas they develop’ (Bryman, Social Research Methods, 2016, p. 273). External validity refers to the degree of the findings in the research and whether or not generalizations can be made throughout various social settings.

In this study, to ensure reliability and validity, the methods were clearly explained in the attempt of ensuring that the study can be replicated with similar results. The process of selecting the informants was defined and the process of data collection were described. The

interview guide attempts to explain the questions clearly in order for informants to have a definitive understanding of what is being asked. Moreover, regarding the interview questions, the author ensured that the answers provided by the informants were accurate by asking similar questions in different ways. The author assured that the contact details of the informants were received in the event where clearer understanding of an answer was needed. However, According to Bryman and Bell (2011), to ensure full reliability in a qualitative study such as this one, one must be able to freeze the setting which is impossible. Also, conducting the study in different settings may provide results that vary to this study, this study attempts to ensure that this would have minimal impact by conduction three case studies in three different settings. Nevertheless, as the methods are clearly stated, replication of this study should be possible.

4.7 Ethical consideration

Anyone who performs a research should be aware of the ethical issues, especially when participants are involved with regards to the collection of primary data (Palaskar, 2018). The important principles to ethical considerations that relate to this study are written by Bryman and Bell (2007): the research should not harm the research participant whatsoever; the dignity of the participants should be respected and prioritized; before the study, full consent should be given by the participants in order to further the research; to ensure that the privacy of each research participant is protected; to ensure that there is an adequate level with regard to confidentiality of the data obtained; to ensure that the research participants and their organizations remain anonymous; that there are no exaggerations or deceptions with regards to the aims and objectives of the research; that information with regards to communication is provided honestly; the data collected from primary sources must not be biased or misleading in any way when represented in the findings.

Information of security procedures that are carried out by ports are sensitive information therefore, within this study the names of the ports are not stated and the names of the informants are kept confidential. The informants were listed as informant 1a, 1b, 1c, 1e, 1d, 1e, 2a, 2b, 2c and 3a. This was in accordance to their regions. Before each interview, the author presented the aims and objectives of this research without misleading the informants. The informants were also told that they are able to read the findings before the paper was finalized, this was to ensure that the informants identity remained confidential and that the information regarding the security practices were not directly linked to the port. Furthermore, the transcriptions from all the interview were deleted at the end of the research along with the recordings. The content of the transcriptions and recordings were strictly kept between the author and the supervisor.

5. Findings

The findings are presented in this chapter. The findings are structured and organized in accordance to the interview guide which are currents threats, future threats, countering threats and ISPS Code. These findings are based on the experience, measures and the point of views of nine informants who are based in three different regions. Towards the end of the chapter there is a sub-chapter referred to as similarities between the cases, this sub-chapter was built in order to establish the similarities that were found amongst the three different cases.

5.1 Current Threats

The current threats top ports were investigated globally and to the informant's ports. Regarding what type of threats should port employees worldwide be are of in the container port system, and which threats are the most important to focus on why, six informants from all three regions agreed that smuggling of contraband such as narcotics and hazardous materials was the major threat that port employees have to be aware of. One informant stated:

> In the container system, you cannot see what is inside. Even if something is declared like agriculture products, there may be something else inside. Some have been known to mis declare goods inside to avoid being charged and taxed. They get privilege by not paying a lot of money. Inside the container it may be some kind of dangerous good which if not stored correctly, may start a fire or even explode (2a).

Two informants saw terrorism as an important threat to container ports worldwide. One of them also mentioned that ensuring the correct people entering ports was an issue, since those that chose to break into ports by finding their way through or around fences could be potential terrorists. The other talked about the effects of terrorism and its impact on the supply chain:

> There is always a threat to the supply chain. Container ports are an important part in the supply chain in the movement of goods, and of course if a terrorist organization or individuals want to disturb the supply chain for a specific country, then of course going for a large container port would make huge damage (1b).

Two informants mentioned that cyber-attacks were the most important threat to be aware of. One of them believed that cyber-attacks can do a lot of damage by shutting down operations in the entire terminal. Another believed that it was time to start educating people to catch up and understanding the new technology that is entering the port system. Yet another explained to the author about the impacts of cyber-attacks today:

> To really shutdown shut down a port or container terminal, you have to do it cyber wise I think. Even the municipality here, they get hacked every once in a while and we get our emails almost shut down. I don't know how much valuable information they have but container terminals, you shut down this container terminal and you do some damage even though we are not the biggest one (1d).

Another informant linked cyber-attacks to port employees and mentioned some concerning elements within the industry:

> Cyber-attacks is most important since all industries are depending on technology and cyber innovation. People need to be educated for the rise of new technology. It is a concern for different generations as some may feel uncomfortable with this new revolution of technology and it takes time to learn. Criminals can easily use new technologies to set up an attack (2c).

Regarding the threats to the ports of informants, five informants mentioned controlling unauthorized access, three informants stated that the low level of education of their own workers was a threat, two informants identified terrorism, two informants mentioned cyber-attacks, one informant stated smuggling and one informant mentioned stowaways. The two informants that stated cyber-attacks as a threat to be aware of globally, are also the same informants that said cyber-attacks was a current threat that concerned their port the most.

Five informants stated unauthorized people entering their ports was a concern, because that could disrupt daily operations. The worst case scenario is that the people entering may be potential terrorists who are trying to disrupt the supply chain. One informant stated that ports including ferry terminals should be more aware since he believed that ferries are the biggest terrorist target, a view that was shared by another informant. For one port that imports hazardous goods regularly, that informant was concerned that unauthorized people may enter and attempt to steal them for unlawful ambitions. He explained that 'These people may not have bad intentions, they could have entered the port by mistake or are just curious. This is something that disturbs the day to day business' (1d).

The three informants that mentioned the lack of education of their workers as a threat are all located and employed the same region (2). One of them noted that the level of the workers' education influenced the amount of accidents in the port area. One of the informants suggested that threats are more likely to occur because of the negligence of the less educated workers. Two informants stated:

> Workers here have only received medium and low education. Sometimes they do not follow work instructions. Accidents happen quite often when they do not wear safety equipment such as shoes or helmets (2a).

> Majority of staff employed here are undergraduates or high school graduates. This is because port work are labour intensive. Low education may increase the chances of a threat occurring. People with lower education tend to be more negligent (2b).

In the topic of terrorism, two ports from two different areas highlighted terrorism as the threat that their port employees needed to be aware of. However, the reasons because of this was different. One of them did not think the port he was employed at was ready for a terrorist attack because it was uncommon to ports within the country: 'We never encountered a terrorist attack and we never prepared for it. That kind of thing is unexpected' (2b). The other Informant claimed that his port was more prepared for terrorist attacks due to a recent terrorist within the country. The attack was not on the port, but nevertheless, the informant claimed that it still had an impact on them and due to that particular terrorist attack, the level of awareness was raised throughout the entire country.

Two informants were mostly concerned with the threat that could come from the seaside, they believed that from landside the port was protected, however, the seaside still remained exposed. One of them stated:

> You are never able to secure the waterfront. So you have the fences and the gate, you have all the systems on the shore side. But securing the waterfront is impossible unless you have a guard going all the time, which you do not because it is too expensive (1e).

Table 3 presents the findings with regards to what the informants insist are the prominent threats to be aware of globally and the prominent threats to be aware of in their ports:

Table 3: Prominent threats globally and prominent threats at informant's port.

Level of awareness / Type of threats	Threats to be aware of globally Informants	Threats to be aware of in informant's own port Informants
Smuggling	1a, 1b, 1e, 2a, 2b, 3a	1b
Unauthorized access	1c	1a, 1b, 1d, 2a, 2b
Seaside security		1c, 1e
Cyber attacks	1d, 2c	
Stowaways		1e
Security awareness		1d
Terrorism	1b, 1c	2b, 3c
Uneducated workers		2a, 2b, 2c

5.2 Future Threats

Autonomous technology and the use of digitalization is a big topic for discussion in the container port industry, with that in mind, the informants were asked what they think are the future threats that may concern container ports the most. All of them agreed that cyber-attacks was the future threat that concerned container ports the most. They mentioned a variety of ways that cyber-attacks could be used against container terminals. Two informants said that it is a concern how individuals could manipulate the numbers or the location of containers. One of the same and another informant mentioned that the more digitalized a port is, the more vulnerable they are to cyber-attacks, especially when there is heavy reliance on the IT infrastructure, for example, if hackers took control of the system, they may be able to move a container to an area where it is not meant to be which could allow criminals to unload illegal substances. Another informant mentioned that an attack on a port could have a negative effect on a ports reputation and damage relationships to their customers.

One informant mentioned that cyber-attacks or hacks could be a new form of piracy, especially when automated vessels are taken into account. This informant gave an example by stating 'One yacht owner, he was in a helicopter and hacked the computer on a yacht so that

people thought that they were going one way, but in reality it was on a totally different course and hijacked'. He also mentioned that this kind of hijacking could take place whilst the ship was berthed in a port. In addition to the cyber security issues mentioned in the current threat section, one informant added that hackers could manipulate drivers permits, entrance permits and licence information in order to deceive their way into ports. Although this has not occurred, he believed that technology can cause a high amount of uncertainties in relation to threats, he stated 'everything is being digitalized, everything is being automated even if you want to say it or not. It's the only direction the port industry is going'. The informant continued and gave an example of a port that has installed a new system:

> Where you can go online and apply for a temporary drivers permit inside the facility. You upload a picture of yourself and you enter the license plate, and of course, you show you have a ISPS diploma. Eventually you get a drivers permit and these permits of course, it's also viable for hacking.

Regarding what kind of impact cyber-attacks can have on container ports worldwide, huge, extreme, massive and mayhem were some of the words used to describe the type of impact cyber-attacks could have. Five out of nine informants used the Maersk cyberattack on June 2017 to describe the scale. One informant stated:

> Maersk lost billions in just a month. It will have a major impact. I believe that cyber terrorism will escalate and terrorists will start digitalizing themselves as well. Like when Osama bin Laden took down a commercial ground in New York, a lot of companies lost a lot of money. I think that terrorism will develop into a more digital world as well where they will try to affect the world economy instead of just harming a few amount of people (1d).

Regarding preparedness for future threats (cyber-attacks), one port answered that they were prepared, while seven ports answered that they were not prepared and one port was not sure. Some of the informant that evaluated their ports as not prepared stated that they were preparing or discussing cyber-attacks. One informant stated:

> We have a cyber security department who constantly keep up with the threat out there and the department is growing in numbers to keep up with and counteract the threat that is out there. Maybe not so prepared. We certainty are in a better position than we were some years ago (3a).

Another informant is on the verge of preparation by planning to conduct a penetration:

> Hopefully after the penetration test we will be more prepared, we have to look at the systems carefully before we implement new systems instead of having to do a lot of work afterwards. We have just installed a lot of systems and we are not quite sure how these systems are working

One informant on the other hand claimed that his port was prepared for cyber-attacks and this was due to experience, 'At the moment we are very well prepared as we have had a large scale cyberattack. So, huge amount of resources has gone into preventing that from happening again' (1b).

5.3 Countering threats

In answering the question if local port authorities and contracting governments doing enough to secure container ports from potential threats, and if not, what more can they do, Three informants agreed fully that contracting governments and local port authorities are doing enough to counter threats. They mentioned that there was various forms of communications between multiple parties within the government and if there was new information regarding threats, their ports would be notified. One informant explained that:

> We work very closely with the port authority on the security side. We have strong support from other government organizations in this country. We work together with a lot of experts who share the latest information and we have a good network. So if something happens, we know where we can get additional recourses to handle threat (1b).

Three informants agreed that in some aspects, enough was being done and in other aspects there was more to be done. They agreed that in terms of following the standard security measures of the national legislation and the ISPS code, both entities are doing enough. They also agreed they are doing enough since the amount of incidents in their respective ports have been low. However, in negative terms, one informant found that when it came to changing legislations for reasons such as the IMO issuing concerns on potential threats, contracting governments are usually not interesting unless they saw that the changes were highly beneficial. Another informant stated that when it came to raising focus, raising the level of security awareness and changing the attitudes of the employees, the contracting governments are not doing enough. Another informant claimed that he was concerned with the lack of specific checks on container traffic that have transited internationally. One informant, on the other hand stated that contracting governments are doing too much on physical security and too little on

cybersecurity. Since the level of threat in region 1 is low, this informant indicated that too much money and time are being spent on the physical security aspect. This informant added that his port is doing a lot of work preparing for the call of an autonomous vessel, therefore more resources and time needs to be spent on cybersecurity.

To the question "What preventative security measures can be taken to mitigate the chances of a threat from occurring in terms of training, drill and exercises?", all informants stated that their ports conduct at least four trainings, drills or exercises per year, which corresponds to their security plans. The amount and type of training depended on each ports domestic legislation within their nations. The identified types of training were refresher training, training in the event of a change in security level, whether if it was level 2 or 3, and exercises and drills of various scenarios. Two informants conduct large joint trainings annually, One of them also claimed that his port had joint training with the military last year for a security level 3 scenario. Two informants claimed that their ports also conduct further scenario trainings, which occur depending on the written PFSP. One of the informants claimed that his port also has drills to raise employees awareness, in this scenario, a box which has "ISPS object" written on it is placed somewhere in the port in the hope that employees would find and return it. Two informants explained their training activities in the following way:

> There are security and safety drills as a master plan of the Port Authority and individual port which follows the PFSP during the year. Normally the PFSP would be formed in relation to the port activities. We also have information exchanges on a national level where we link up with all parties and authorities (2c).

> Under the requirements of our domestic legislation for the ISPS Code. We have regular refresher training which takes place quarterly. We exercise annually for the level 2 escalation. We also undertake exercises or drills every quarter at a lower level. So we focus on one particular aspect of scenario. We also undertake a mystery shopper monthly check on the security staff at the main gate. So we have an operative who is unknown to the security staff on duty who will attempt to gain access by pulling their way in or telling lies. This is recorded and the outcome is forwarded to me shortly thereafter (3a).

Smuggling, trafficking and stowaways are a major problem for many ports, the informants were asked how should the industry reduce the chances of these acts from occurring. All informants mentioned that if they suspected any tampering with the container seals, they

have the right to open the containers and inspect inside, they usually do not open the containers if the seals are attached due to their trust for their customers. Two ports mentioned that using initiatives such as the CSI, MI and profile scanning has been highly beneficial. One informant suggests that more container checks, scans and inspections should be conducted at the port of origin. One informant mentioned 100 percent inspections, however believed that this was unrealistic, and two informants mentioned the use of more technologically advanced scanning systems. The informant suggested that less advanced scanning systems are not as effective to detecting contraband. Five informants mentioned that inspections was the role of the customs, one of those informants stated that they have meetings with the customs to align their processes. Four informants claimed that their ports inspected only five percent of imported cargos annually. One informant did not think stowaways was a problem for container terminals, however he claimed that containers are ideal for illegal goods, he stated:

> Containers are not a great choice for stowaways. It is not an option for a stowaways to go into container terminals. But, containers are great for transferring illegal goods such as narcotics or other type of unwanted or illegal goods. That is basically the most biggest threat to the day to day businesses, that container ports are used for transporting illegal goods (1b).

In some areas, port employees and port security personnel have been known for taking bribes, operating with criminal organizations and stealing. Regarding what can be done to ensure that this does not happen, three informants mentioned background checks as a solution, this ensures that employees or potential employees do not have a criminal history. One informant briefly stated that to have good employees, his port has good relationships with various government organizations. Two informants suggested that tough repercussions was the answer. One of them claimed ‘setting high costs as a penalty would let employees know that bribing and conducting criminal activity is not worth it, this is our logic’ (2c). Another informant suggested putting people together to conduct operations could stop employees from conducting illegal activity and also mentioned about following employees movement with their analytic cameras. However, he also claimed that this would be costly and time consuming. One informants port gets employees to sign an agreement stating that they would not conduct this kind of illegal activity. He also stated that taking the ISPS and HSE courses helped. One informant stated that in many countries, included his, there is no remedy to stop bribes taking place due to cultural reasons. He continued to explain about a situation of a port located in region 2:

> Bribing occurs every day, whether it is the crane operator or the port officer. You cannot change it. If I am the top management of the port, and I decided to try and stop bribing from occurring by initiating an autonomous port, there will be a big strike, and I might get shot and die somewhere. They see bribing as a part of their salaries since it pays for their extra expenses. They have depts to pay for, families to look after and children to send to school, a lot of that is covered by the bribes. If you tried to stop bribing now, these people are as good as dead. They cannot support themselves with just their salaries. The labour unions are on their side and they support the bribes (2b)

After that, the author asked the informant if increasing the wages of the employees would stop the bribing, to which the informant answered 'no it will not, we have tried that before and it did not work. This is how our culture is like' (2b).

On how they secure their ports from unauthorized access, all ports followed the procedures of the ISPS Code. All the ports had fences securing the parameter. Only two ports did not have surveillance cameras but were in the process of installing them. With regards to entering through the gates, five ports had 100 percent I.D. card checks, whether if the card is checked by scanners or checked by security guards. In one of the informant's port, the identification cards must be visible at all times. The gates at these ports are opened remotely. Ports of three informants have a free flowing system through the gates, meaning that the gates are usually open. The free flow of vehicles was adopted in order to avoid queues and traffic. These ports make up for this security wise by having security personnel stationed around the port facilities, this also include the gates. Lastly, the gates at informant one informant's port differ, some gates have security personnel stationed and in other parts of the port the gates are opened manually. This port has cameras that detects abnormal movements and behaviours such as those that are loitering. He further claimed that the people who use the port have learned to react when there are other people in the facility that they do not know. One informant explains the access control method at his port:

> We have 100 percent I.D. check. Everybody that goes into the port have to identify themselves to security. If you get a pass card, you do the identification once. Visitors who come once in a while need to visit the security every time. We have spot checks or random check depending on the security level. We also ensure that the personnel gaining entry are using their own pass card (1b).

Regarding the major challenges that prevent ports from implementing effective security measures, the most mentioned challenge was costs. One informant stated that costs are especially an issue when the level of security increases, when this happens, the ports are forced to hire more on duty security personnel to patrol all the time. Another informant added to this and stated that in the situation where the level of security rises, ports tend to contact the more well established security firms, where in this case was Securitas. Since the security level increase effects all ISPS ports in the country, there may not be enough security personnel to satisfy the needs of all ports. One informant mentioned that keeping daily operations running smoothly was a challenge, in order to do this, ports would need manpower and sufficient systems in place. He also claimed that the systems are in place, however, it depends on how much money a port would be willing to pay for it. Two informants stated that culture could be a challenge for some ports. One of them claimed that culture could be the cause of port employees unwilling to change for new security measures. The other informant also stated that it could also depend on the security measures and requirements the local governments put in place since other countries could interpret the ISPS Code in different ways. The challenge for one informant was that it is near impossible to be prepared all the time. Two informants claimed that protecting the seaside of the port was a challenge and mentioned the same reasons as earlier. Two informants answered that criminals and terrorists organizations were always one step ahead, which made it difficult to protect the ports. One of them claimed that these organizations seemed to be one step ahead of the ports when it came to the cyber issues, however, the other informant claimed that if terrorists wanted to attack a port they could do so unexpectedly, he used the twin tower attacks as an example.

In answering if they have encountered a security challenge in the port, and if so, what happened and how they dealt with the situation, two informants had trespassers coming into the port attempting to steal some tools or cargo, and both ports responded by contacting the police. The trespassers in one of the ports were not found and were not able to steal anything. In the other port, the trespassers were apprehended by the police and they were caught because they were identified on the surveillance cameras. One informant still faces challenges with regard to stowaways, and the port has dealt with the situation by implementing 100 percent inspections on all cargo that is to be exported. Three informants abstained from answering this question, one of them stated ‘we classify this because the if the information got into the wrong hands then they know how we deal with such things’. One informant answered that implementing

more controlled checks for vehicles entering and leaving the port became a challenge. Informant he continued to explained:

> We have around 10,000 people coming in and out every day. When we tried to tighten our security by checking every single person coming in or out of the port, it became very challenging. Most people start work around eight in the morning and it became impossible to check everyone's I.D. This caused queues, caused many people to be late for work and interfered with operations, they complained a lot about this so we had to be more lenient again. Controlling access is still a major problem in our port today (2b).

Only two informants stated that their ports never had a security challenge.

5.4 ISPS Code

Regarding the strengths of the ISPS code when it comes to limiting the chances of a threat from occurring, most informants from all three regions agreed that the ISPS Code has helped by providing a good fundamental approach to security. Most informants from have also stated that their ports are more secure because of this Code. Two informants were pleased with the improvement with regard to controlling the access of people coming in and out of the port. They also stated that before the Code came into effect, anybody could drive into the port for any reason. One informant argued, however, that despite the security measures being minimal, it has provided more security and obstacles such as fences and gates. Six informants commented about the Code being successful in getting government organizations to be more involved with security at the ports. Strict regulations have enforced governments to conduct inspections and ensure that the ports are operating at the required security level. Furthermore, two informants stated that the government is also monitored to ensure that they are inspecting ports. Three informants commented on the risk assessment approach, they stated that the PFSP has enabled ports to assess the possible security incidents and test security measures with the use of drills, therefore, the PFSP is regularly being updated which enables the ports to be updated with counter measures against existing threats. Other mentioned strengths are that the Code is good for communication and exchanging information with government organizations which on top of the PFSP assessment, helps ports decide the best security approach.

Regarding the weaknesses of the ISPS Code and anything vital missing in it, Three informants suggested that the Code needs to include cyber aspects. One of those informants mentioned that the Code is meant to take preventative measures against identified threats, cyberthreats are on the rise and yet the Code has failed to mention it. Two informants stated

that the Code needs to differentiate between the type of terminals, for example, container terminals and oil terminals should have separate Codes for security preventative measures. One informant stated that:

> It looks at all terminals the same. If you are a container terminal then you do not have the same problems as a cruise ship. A cruise ship is more interesting for a terrorists. If you had it separated, you could have some kind of standard countermeasures in the different ports and then you could do some kind of analysis on the whole area around it. We do it for all ISPS terminals in this country. After, we put up the same countermeasures in every terminal. For me, I think it costs too much (1e).

Two informants agreed that the Code needed to be reviewed in its entirety and refreshed since it had been a long time since the Code came into effect. One of them stated 'It is an ancient law, it is an ancient regulation and it needs to be updated. Since 2004, no major changes has been done and a lot of things have happened since 2004' (1d). Two informants noted that the Code provides security measures for access from the landside, however, the code does not provide measures for security on the seaside. One of them stated "We have quite a few regulations regarding fences, gates and everything but the waterfront is still open. You're open to the water. I have no solution on that problem' (1c). The other weaknesses that were mentioned are that the code concerns only exported goods and not the goods coming in, the Code should consider the sizes of the ports and have different regulations for them, and, the Code needs to be less detailed and focus more on the security principles. Only one informant considered the Code to be good as it is since there has been a low number of threats that has concerned his port. The findings of strengths and the weaknesses of the ISPS Code are summarized in the table 4:

Table 4: Strengths and weaknesses of the ISPS Code

Strengths	Weaknesses
• Ports are more secured since there are now measures in place • Raised security awareness • Government involvement in security • Communication and information exchange increased • Requires ports to adapt to changes in threats with the use of PFSP and risk assessment • Reliability increased	• The Code needs to differentiate the type of terminals • Lacks regulations for seaside threats • Needs to include cyber aspects • Needs to be fully reviewed and refreshed • Guidelines needed when it comes to updating the PFSP • More consideration needed for scans or inspections of imported containers.

Implementing the ISPS Code also has some challenges, and most of the informants agreed that implementing the requirements of the Code was expensive. One informant stated that because the same code applied for all ports in the country, it was a struggle for smaller ports that only received one ship a month. Another informant stated that his port struggled to comply with the requirements in the beginning of the Codes commencement, this led to the port having to hire a security company which was costly. Especially when the security level was raised to level 2. Four informants claimed that finding the balance between security and cost of operations was difficult. Increasing the level of security meant increasing the running costs of the port. One informant added that his port tried to implement the ISPS Code too good which lead to a lot of spending, the port then learned from this and has taken other measures such as putting up fences and cameras, which allowed the port to operate more sufficiently. Furthermore, he stated that full implementation of the ISPS Code was not only costly for the port but also costly for its customers. Another informant mentioned that the difficulties of implementing the ISPS Code in the initial phase was to find the best security practices that applied for different type of ports. Different people involved had various views about the best practices which turned out to be a struggle. One informant mentioned that his port found it costly to purchase new technology and to ensure that they were still relevant for measures against threats in the future. Two informants mentioned that changing other employees attitudes towards complying and operating with the Code was difficult as they were hesitant to changing their ways. One informant stated that changing the national legislation to comply with the ISPS Code was a challenge, but since parts of the Code is already mandatory internationally, this was

not the case anymore. Lastly, one informant stated that from his experience, getting employees to comply with the requirements of the code is still difficult. He explained:

> Management just ignore it and they just try to do everything on a minimal. In the past, I have seen some companies do just one training in ten years but they can have reports to send to the contracting government every year. They do just one training and only once and they take a lot of photos.

Regarding the kind of vulnerabilities the ports would expose if they had only followed the mandatory ISPS Code requirements for their security, most of the informants stated that the lack of container inspections would be an issue. One informant told the author that opening sealed containers for inspections would not be a possibility, only scanning procedures with the use of machines would be an option. This would then lead to port employees having to rely on manifests from the shipping lines. He explained that 'Now there are support tools such as the container security initiatives (CSI), Megaports Initiatives, profile scanning and the NSW method to fulfil the gaps' (2c). One informant explained that 100 percent screening at the port of origin may be unrealistic, however, he believes that there is more effort being put into it nowadays. Another informant explained that he is in favour of more inspections, however, the costs for additional technology and manpower would be highly expensive. One informant believes that the ISPS Code lacks information with regard to safety for employees and another informant believes that the ports would be highly exposed to threats from the seaside.

Regarding what they have added to their security system that is not part of the ISPS Code, most informants mentioned that they have installed camera surveillance, and two were in the process of installing it. The cameras used at one informants port is highly technological and detects movement as well as signal alarms. Two informants stated that their ports have added electric boundary fences. One of them explained how the fences at his port worked by stating:

> It gives the finger a nasty shock if they attempt to climb over it. It is also monitored. If you hang on it whilst it is pulsing, after the third pulse it signals an alarm to our security control room. The operator brings the cameras to bear on that zone that is activated and send the control (3a).

Only one port conducted 100 percent inspections on cargoes that was going to be exported. This was due to the stowaway issue that concerns the port. Furthermore, two informants explained about the extra security legislations and initiatives at their ports. One of

them mentioned the EU directive, NIS directive for IT security and a national legislation for parameter protection. He further explained that these legislations and initiatives are linked together with the ISPS Code and can all be used depending on what the threats are. The other informant mentioned the CSI, MI, custom processes, cargo scanning profile, AEO and ISO.

Regarding if the current ISPS Code needed to be amended, and if so, why, two informants said that the ISPS Code is fine as it is, one of them said that this was due to the low level of threats within his region. As for the other informant, he said that the ISPS Code is sufficient and covers the needs of the port because of the other legislations the port follows, he added that all the legislations covers the security needs of the port. One informant said that the Code is fine as it is, as long as the PFSO updates the PFSP often with effective procedures with regard to the threats of concern. Three informants stated that the Code will need to be reviewed in its entirety because it has been fifteen years since the Code had come into effect and a lot has changed in the world. One of them added that the Code should encompass cyber issues and another informant stated that it needs to be reviewed to decide whether or not the it is needed. He further stated that it needs to be reviewed to find out if it has benefited ships and ports in anyway, for example, in the instance of a change in security level, ports could rely on the police or military, and also, the change in security level would affect the entire nation and not just the single threatened area. One informant said that the Code needs to consider cybersecurity since many port operations are becoming more digitalized and autonomous. Another informant believed that the Code was is bureaucratic, he stated:

> This port, in a global perspective, is very small. You have me as the director, then you have the PSO and then you have the PSFO. So that is three layers. We have to have it. We cannot skip the PSO. It needs to be less bureaucratic (1c)

He further talked about how some terminals should be except from the ISPS Code and explained ‘For instance, we have a terminal where we only load stones, nothing but stones. And the ISPS Code is completely irrelevant for that terminal’ (1c).

Table 5 presents the findings of the ISPS section with regards to the challenges, vulnerabilities, added security measures and the need for amendment:

Table 5: ISPS Code challenges, vulnerabilities, added security measures and the need for amendment.

Topic	Findings	Informant
Challenges of ISPS Codes implementation	Costly	1a, 1c, 1d, 1e, 2b, 2c, 3a
	Getting employees to follow	2b
	Correct understanding of the Code	2c
	Getting the Code in place before commencement date	3a
	Finding the best practices for different terminals	1b
Vulnerabilities of only following the mandatory ISPS Code requirements	Container security	1c, 1e, 2b, 2c, 3a
	Seaside security	1c
	Safety of employees	1a
Added security measures apart from the ISPS Code	Surveillance cameras	1a, 1b, 1c, 1d, 1e, 3a
	Advanced gate system	1a, 1d, 3a
	Electric fences	1b, 3a
	100% cargo inspection	1e
	EU legislation, NIS Directive	1b
	Megaports Initiative, CSI, Customs process, Cargo Scanning profile and ISO	2b, 2c
Amendment of the Code	Does not need to be Amended	1a, 2b
	Needs a full review	1d, 1e, 3a
	Encompasses cyber issues	2b, 3a
	Less bureaucratic	1c
	Consider different types of terminals	1c
	Fine as long as the PFSP is updated accordingly	2c

5.5 Similarities between the cases.

Regarding the shared similarities that was mentioned between all cases involved in this study, all cases had at least one informant mention that smuggling was a current threat to be aware of globally. The smuggling of people was not mentioned, however, what was mentioned was the smuggling of narcotics, weapons, hazardous goods and other illegal contraband. This was the only current threat that was mentioned by participants from all three cases. Every

informant stated that cyber-attacks is going to be the concerning threat in the future. In regards to cyber-attacks, informants from all cases also said that their port was not prepared for it, however, this was not shared amongst all informants since only one stated that they are prepared for it. Regarding the strengths of the ISPS Code, informants from all cases were positive that the Code required them to update their PFSP and perform frequent risk assessments, this helped ports adapt to changes in threats and have counter measures for them. Three informants from three regions stated that the weakness of the ISPS Code was that it does not have regulations for cyber issues. They reckon that the Code should encompass procedures for them. Regarding the challenges of the Code, informants from the three cases mentioned that it was costly with regards to purchasing equipment, procedures for level changes and implementing various infrastructures. Lastly, when asked about the vulnerabilities the ports will expose if they only followed the measures of the ISPS Code, informants from the three cases said that container security would be lacking. Not being able to open the containers for inspections and having the container checked from the port of origin were some of the instances mentioned.

Regions 1 and 2 shared a few a similarities. Firstly, informants from both cases mentioned that unauthorized access and cyber-attacks as a current threat. Also, informants from each case agreed that the ISPS Code has secured their ports than before the ISPS Code came into implementation. Region 2 and 3 only had one single similarity, one informant from both cases mentioned terrorism as a threat that concerned their ports. Region 1 and 3 had more similarities, firstly, informants from both regions agreed that the Code enabled government involvement to port security. Secondly, all informants from both cases mentioned that they have added surveillance cameras. The other similarities some informants from region 1 shared with the informant in region 3 was that they had electric fences and advanced gates. Lastly, regarding if the ISPS Code needed to be amended or not, a few informants from case 1 agreed with the informant in Case 3 that the Code needed a full review and revision.

The main difference between the cases was found in Case 2. This region seemed to have problems with regards to bribing, corruption and employment of uneducated workers. However, the informants named uneducated workers as a threat as they thought this was the main cause for accidents. They did not name bribing and corruption as a threat as they suggested that this was a part of the culture in the region.

6. Discussion

In the previous chapter, the findings were presented, interpreted and described. This chapter discusses the significance of the findings along with the relevant literature. The structure of this chapter is similar to the previous chapter, however, instead of having a sub-chapter named "similarities between the cases", a sub-chapter named "main differences between cases" is added. At the end of this chapter, there is a table that provides the main findings and the theories from the literature review that relate to them.

6.1 Current threats

Informants from all three regions commented that smuggling is the threat that container ports should be aware of the most. Informants mentioned that containers are an ideal method to transport narcotics and it is difficult to determine if there are narcotics hidden inside. The annual World Drug Reports of the UNODC presents the routes and flows of drugs around the world, a lot of those flows follow the same routes as ships. This theory is supported by McNicholas (2016) who claims that smuggling routes are altered depending on the changes in the shipping trade lanes or the changes in seaport operations. UNODC (2011) reported that containerized shipping is being utilised as a form of smuggling, however, it was also reported that very few detections have been made. A notable statistic with regards to seizures is that 60 percent of all cocaine seizures were during maritime transportation (UNODC, 2015). Perez (2014) estimated that around 70 to 80 percent of all consumed cocaine was transported by sea. UNODC (2018) stated that the production of drugs such as cocaine, heroin, and methamphetamines have increased, this could suggest that drugs being transported with maritime conveyances have increased as well. Furthermore, all informants mentioned that their ports scan no more than five percent of imported containers annually. These statistics leave many people wondering how much contrabands are actually flowing through the supply chains, one can argue that most drugs travel through container terminals undetected.

Unauthorized access was equally mentioned by the informants. Informants from two regions believed that unauthorized personnel who manage to find their way into ports could cause disruptions to operations, even if these people do not have ill intentions. On a more severe note, some informants stated that if access control was not performed correctly, terrorists may gain access into the ports and commit terrorist acts. Two informants have also stated that their ports were almost robbed after individuals had found their way in without granted access. Christopher (2015) supports these findings by stating the challenges when it comes to granting access are ensuring that people do not disrupt operations and other port-related business.

Moreover, terrorists who gain entry could incur damage to port facility infrastructure and assets which may cause loss of life and damages to the environment. The DoT (1997) also claimed that criminals who gain access may try to steal cargo and smuggle in narcotics, currency, stowaways, and contrabands. The findings and theory indicate that granting access to the wrong people could lead to other threats such as terrorism, smuggling, theft and other crimes.

Four informants from three regions mentioned terrorism as a current threat to be aware of. One informant claimed that his port is made to be aware of terrorism because of a recent terrorist attack within the country. Another informant suggested that his port has never faced a terrorist attack, therefore they are not prepared for it if it were to occur. Another informant mentioned that a terrorist attack on a large container port could impose huge damage to the global supply chain. According to the OECD (2002), terrorist attacks have induced organizations in the private and public sectors to spend on their security. After the September 11th terrorist attacks, security measures posed on a national level in the U.S. became more tight and controlled, which was no different from the claims of the first informant. The OECD (2002) also mentioned that trade efficiency within a supply chain drops after a terrorist attack and that waiting time will be increased. Furthermore, terrorist attacks can cause destruction to important physical assets and infrastructures of the supply chain. The RAND terrorism database claimed that of all terrorist attacks only two percent of those attacks have been on the maritime sector (Chalk, 2008). However, eight countries in a 26 nation survey listed terrorism as their greatest threat to national security (Poushter & Huang, 2019). Moreover, terrorism has been the cause for increased supply chain transportation costs due to extra security needed to avoid them. Terrorism has also been the cause to loss of lives in ports and has damaged port infrastructure and assets, therefore, terrorism cannot be overlooked as one of the most prominent current threats in the container terminal industry.

In this study, the findings suggest that smuggling, terrorism and unauthorized access are the threats that container port employees need to be aware most. Smuggling and unauthorized access were equally mentioned most by the informants, however, terrorism and smuggling were mentioned by informants from all three regions in this study. The theory shows that smuggling is an important threat to focus on due to the high amount of undetected contraband flowing through various maritime routes. Moreover, the highest amount of narcotics seized is from maritime conveyances. Terrorism provides a large threat to container ports as it may cause loss of life, disruptions to global trade and extremely high costs. Although attacks on container ports are relatively low compared to attacks on other infrastructures and facilities, the impacts it could

cause cannot be ignored. Lastly, the theory has suggested that unauthorized access to container ports could lead to the two previously mentioned threats. Additionally, cargo theft could happen because of this as well. Unauthorized access of personnel creates a variety of unknowns. The theory does not directly suggest that these are the most prominent threats to container ports today, the findings indicate otherwise. This indicates that more awareness and measures could be needed for smuggling, terrorism and access control.

6.2 Future threats

According to ECMAR (n.d.), cybersecurity will become an important issue since the maritime sector is becoming more automated and digitalized. A question regarding what the future threats to be aware of most was asked, all informants mentioned cyber-attacks. Some informants expressed their concerns regarding how hackers have been able to manipulate the system to change the numbers and location of the containers. Another informant mentioned that criminals could hack the system to move containers to another area in the port to unload narcotics. Other notable mentions were that hackers could hack drivers permits to gain access into ports, and another informant stated that criminals may be able to hijack container vessels that are berthed in ports by hacking its systems. The author could not support these findings with theoretical evidence and has deemed these claims to be pure speculation.

One informant mentioned that a cyberattack could ruin the reputation of the port, this will lead to the port losing trust from their customers and losing their customers as well. According to GGA (2018), industries could suffer from a loss of reputation and a loss of trust from their customers in the event of a data breach caused by a cyberattack. Furthermore, a survey by PwC showed that 87 percent of their customers would take their business elsewhere if they were to be hacked (Neveux, 2018).

When the informants were asked about what kind of impact cyber-attacks could have on container ports worldwide, some of them described it as huge, mayhem, extreme and massive. Five informants from two regions used the attacks on Maersk and APM terminals as an example. The attack on Maersk caused the company to shut down its servers which caused disruptions to 76 of their terminals worldwide (AFP, 2017). The servers being shutdown caused some ports to stop their operations completely, this was the case in Elizabeth, New Jersey (Greenberg, 2018). Other ports such as the APM terminal in Rotterdam were forced to operate with manual systems (AFP, 2017). In the end, the attack costed Maersk up to $300 million USD (Milne, 2017). The findings are supported by the theory as it shows the economic and financial

implications cyber-attacks can cause. Furthermore, the literature has also suggested that cyber-attacks on container ports are not a rarity and it has damaged operations for many terminals. However, despite the fact that most of the informants named cyber-attacks as a prominent future threat, it cannot be overlooked as a threat to current container terminal operations as well. The threat of cyber-attacks today is large, however, as the maritime industry becomes more automated and digitalized, it must be regarded as one of the most prominent threats for the future as well.

The informants were asked if their ports were prepared for cyber-attacks. Only one informant from region 1 answered that his terminal was prepared and this was due to experience. The informant said that his terminal was hit by a large scale cyberattack, this prompted them to invest huge amounts of resources to prevent it from occurring again. This claim is similar to what Maersk (2018) has stated, they reported that cybersecurity became a priority for them after the attack, and have launched a cybersecurity plan to improve. The theory does support the findings in the case that a cyberattack has enforced concern for ports to prepare for cyber-attacks, however, this does not provide evidence that all ports would improve their cybersecurity in the event of an attack. It cannot be stated that all ports are prepared for cyber-attacks and it cannot be stated that all ports are not prepared for cyber-attacks. Digitalization and automation have yet to reach its peak (ECMAR, n.d.), and as history has shown, hackers have been able to exploit new vulnerabilities created by digitalization and automation.

One informant claimed that his port was preparing for cyber-attacks by conducting a penetration test. The informant was hoping that the test would prepare the port more for cyber-attacks, the aim of the penetration test is to have a careful look at the systems before implementing new systems. McNicholas (2016) mentioned penetration testing in the fifth stage of the basic cybersecurity process. McNicholas wrote that this was done to expose vulnerabilities to the system and to ensure that the countermeasures are effective. The informant provided no mention about the countermeasures, however, provided an explanation about testing the systems to understand how they work, this could be interpreted as testing their vulnerabilities as well.

Cyber-attacks have been proven to disrupt operations at container ports and incur high costs. The theory has provided evidence as to what kind of impact it can have. The findings suggest that cyber-attacks are a threat that is discussed to a large extent at the informant's ports. The preparedness of container ports is not covered by the theory, however, most ports in this study stated that they were not prepared. Automation and digitization continue to be a trend in

the container port industry, if ports do not enhance their cyber systems, they leave themselves vulnerable to breaches. Hackers have shown their capabilities in the past, this should provide reasoning as to why container ports need to prepare themselves for cyber-attacks. Further studies should be conducted regarding effective security measures to combat cyber threats.

6.3 Countering threats

The informants were asked about what kind of training, drills or exercises they conducted at their ports to mitigate the chances of a threat from occurring. All of the informants answered that they conducted at least four training, drills and exercises per year as stated in their PFSP. One informant referred to these trainings as a refresher training. This is similar to paragraph 18.5 part B of the ISPS Code, which proclaims that drills should be conducted every three months to ensure effective implementation of the provisions of the PFSP.

Several informants also noted that they conducted drills and exercises for changes to the security level. Paragraph 18.4 Part B of the ISPS Code explains that "the objective of the drills and exercises is to ensure that port facility personnel are proficient in all assigned duties, at all security levels" (p.87). One informant stated that these trainings are conducted under the requirements of their domestic legislation for the ISPS Code. Section 18.1 of Part B entails that the PFSO should have knowledge and receive training in a number of issues, one of those indicated is that they should have training and knowledge of the relevant government legislations and regulations (p.85).

Three informants from region 1 also explained that they took part in major joint trainings with the military and other ports. It was also explained that some trainings and exercises were for information exchanges with relevant parties and authorities. The joint trainings and exercises did not occur often, one informant explained that they took place once the opportunity presented itself. The trainings with the military were for different levels of security and the joint trainings with other ports were for different scenarios. These training methods are supported by paragraph 18.6 part B of the ISPS Code. It indicates that various types of exercises may include relevant authorities of the contracting government and the participation of the PFSOs. The Code further states that these trainings should be carried out at least once annually but no more than 18 months in between the exercises. The exercises mentioned in this part of the Code includes a full scale or live exercises, tabletop simulations or seminars, and combined exercises with other entities such as emergency response and port state authority exercises.

The other training methods mentioned were the mystery shopper and the ISPS Code object awareness procedure. Firstly, the mystery shopper tests the security staff at the main gate, an unknown operative to the security staff drives to the gate and tries to get access into the port facility by telling lies, the outcome is recorded and sent to the principle PFSO for analysis. Secondly, one informant demonstrated the type of training he conducts at his port to raise awareness, the informant places a box that has "ISPS object" written on it somewhere in the port facility, then he waits and sees how long it takes until one port employee or security personnel discover it. The box is placed in the port facility at random times, the informant suggests that this helps to increase awareness. These types of trainings are not supported by the theory.

The informants were asked about how the container port industry could reduce the chances of smuggling, trafficking and stowaway incidents from occurring. All informants mentioned that security personnel should check if the seals of the containers have been tampered with, if so, they would open the containers to conduct physical inspections. They explained that they did not usually inspect imported containers due to their trust for their customers. The process of seal inspection, as noted already, is mentioned in the ISPS Code paragraph 16.32 and 16.35 of part B. Paragraph 16.32 line 4 mentions that 'at a security level 1, the PFSP should establish the security measures to be applied during cargo handling, which may include: checking of seals and other methods used to prevent tampering upon entering the port facility and upon storage within the port facility' (p.78). Paragraph 16.35 line 4 is similar, however, it regards to a security level 2, which writes "the PFSP should establish the additional security measures to be applied during cargo handling to enhance control which may include: increased frequency and detail in checking of seals and other methods used to prevent tampering" (p.79).

Some informants mentioned that inspections and checks should occur more frequently at the port of origin and another informant stated that 100 percent inspections would be beneficial, however, he deemed this unrealistic. With reference to the 9/11 Commission Act of 2007 which enforces 100 percent scanning for containers headed to the U.S. at the port of origin, Wolf (2013) insists that this could reduce the amount of terrorist activity in the country by reducing the flow of smuggled weapons, this would save global trade and save lives. Wolf (2013) further argued this case by pointing out the figures suggested by the RAND Corporation and the Congressional Research Service, which range the cost of a terrorist attack on a U.S port to be between $45 billion USD to $1 billion USD. However, the European Commission (2010)

argues that despite the increase in scanning and inspections at the port of origin, containers will still be highly vulnerable to tampering along the supply chain and therefore, 100 percent scanning at the port of origin could be deemed ineffective. It can be suggested that in order to increase security measures against smuggling, security should be improved along the supply chain and not just at the port of origin.

Another point noted by the informants is that using more technologically advanced scanning systems can reduce smuggling, trafficking and stowaways activities in containers. The informants suggested that using less technologically advanced scanning systems are less effective when it comes to reducing the flow of contraband. This statement is supported by the European Commission (2010) who explains that if an Act came into effect, and the type of scanning system is not specified, some dangerous materials and contraband can continue being transported undetected.

In some areas, port employees and port security personnel have been known for taking bribes, operating with criminal organizations and stealing. The informants were asked about the countermeasures that could be taken. The most answered solution was to conduct background checks, this was mentioned by informants from region 1 and region 3, the informants state that this was to ensure that they did not have criminal backgrounds. Christopher (2015) mentions that full background checks can provide details regarding employment history, criminal records, training history and references. Background checks may not prevent corruption in ports, however, it may be a good estimate to suggest the likelihood of it occurring from the ports own employees.

Two informants from region 1 and 2 suggested enforcing strict penalties at a high cost would stop bribes and other criminal activities conducted by the port employees. This claim is supported by the OAS, who according to Christopher (2015), advocates that there should be higher enforcement of stricter penalties for port employees that are involved in corruption and transnational crime. Another informant from region 1 suggested more monitoring by use of security personnel and surveillance cameras were the answer, this claim is also supported by the OAS (Christopher, 2015) who advocates using monitoring through methods of higher cooperates with the government. The findings are supported by the theory, however, the effectiveness of these measures cannot be determined.

One informant from region 2 stated that there is no existing measure to counter corruption and bribes at ports. He continued to state that this is part of the culture within the

country and the act of bribing is even supported by the labour unions. The informant also noted that the port tried to solve the problem by increasing wages, however, this was unsuccessful. However, according to Seleim and Bontis (2009) and Larmour (2012), the link between corruption and culture cannot be confirmed. Therefore this informants statement about culture and corruption cannot be supported. Moreover, the enforcement of stricter penalties has several implications. The study has not provided evidence regarding current penalties for corruption, it can be determined that different countries have different laws regarding this.

As stated in paragraph 1.3 in part A of the ISPS Code, one of the functioning requirements of the code is to prevent unauthorized access to port facilities and its restricted areas. Paragraph 14 in part A states that controlling access to the port facility is a measure that should be taken to prevent security incidents. Paragraph 16 in part A suggests that the PFSP should address measures to prevent access to unauthorized personnel to the port facilities. These are the mandatory requirements of the ISPS Code for access control. Regarding how the informant's ports conducted their access control procedures, all ports had fences that secured the ports parameters. Most of them stated that their ports installed surveillance cameras in order to monitor the ports parameters, gates and other premises. Informants in region 1 and 3 stated that their ports did 100 percent identification checks to those that try and gain access through the gates.

Regarding the fences and cameras, paragraph 15.15 of part B of the ISPS Code suggests using permanent barriers or surveillance equipment to mitigate the identified port facility vulnerabilities. Furthermore, with regards to the fences, paragraph 16.17 of part B recommends that restricted areas should be bounded by fencing or other barriers that the contracting governments deem appropriate. Regarding the 100 percent identification checks, according to Andritsos (2014), access control systems should have three essential functions, which are entitlement, identification and documentation. 100 percent identification checks fall under the identification function. Andritsos (2014) describes this as a confirmation that the correct person is entering the port area and that person has provided the correct identification. The findings are supported by the theory regarding access control measures.

One informant in region 2 stated that one of the challenges of his port is access control. The port attempted to control the access of personnel and vehicles entering the port, but this ended in failure and caused long queues into the port and caused many workers to arrive at the port late. Eventually, the port had to revert to implementing more relaxed procedures. According to Christopher (2015), ports operate as a business. This means that they need to find

the right balance between controlling access and efficiency of throughput in order to satisfy their customers. The efficiency of throughput not only relates to customers, but it also relates to port employees as well, therefore, if port employees are arriving late, the efficiency of throughput decreases. Finding this balance is perhaps a challenge for many ports, especially the larger ones that have large container traffic.

The findings suggest that ports find the ISPS Code methods effective in countering some of the threats mentioned in this section, this is indicated because the methods used are located in the nonmandatory section of the Code. It can also be stated that the ports in this study prioritize implementing effective security measures, but at the same time, the cost aspects of enhancing security cannot be ignored. In theory, 100 percent cargo scanning and more enhanced supply chain security could be regarded as effective countermeasures, however, it creates several cost implications that negatively impact the profitability of container ports.

6.4 ISPS Code

Regarding the strengths of the ISPS Code, five informants from three regions agreed that their ports are more secured than before the measures came into effect. Some of them were pleased that there are at least measures in place to secure ports. This claim is supported by Wu and Zou (2009), who stated 'the ISPS Code has significantly increased security awareness for threats at ports and has effectively deterred the threats to port facilities from its source' (p. 95). This quote by Wu and Zou also supports the findings that the Code has raised awareness. It also supports one informant's claims that it has helped increased reliability for ports due to effectively deterring threats.

Another strength mentioned by the informants from region 1 and 3 is that the ISPS Code has contributed to getting the government involved in security and, that there has been an increase in communication and information exchange. UNCTAD (2007) support this claim by saying that governments have provided assistance in implementing the Code. This includes assessing the threats and accepting the PFSP. This claim cannot be supported by all ports. According to McNaught (2005), the standards of security vary in different countries, especially those that are developing. Due to the fact that the IMO lack the ability to enforce the ISPS Code, contracting governments may lack the required resources or expertise to enforce the required security standards.

One informant stated that one of the strengths of the Code was that it required ports to adapt to changes in threats. This enabled risk assessment to take place regularly and allow for

updates to the PFSP when needed. As specified in paragraph 1.2 at part A of the ISPS Code, one of the objectives of the Code was "to provide a methodology for security assessments" (p.4). This was so that plans and procedures could be in place in order to react to changes in the security level. Paragraph 15.4 of part A establishes that the PFSA should be updated and reviewed periodically, this takes into account the changing threats or minor changes to the port facility. According to paragraph 16.1 of part A, a PFSP 'shall be developed and maintained, on the basis of a PFSA' (p.18). The theory supports the findings in this case, however, if there is no entity to enforce regularly assessments, the outcome could potentially be a poor and outdated PFSP.

The informants mentioned the weaknesses of the ISPS Code. Most informants in region 1 stated that in order for the Code to be more effective, it needs to have procedures for different types of terminals. Some of them claim that container terminals and oil terminals would require different procedures for implementing security measures. The OCIMF (2003) indicated that the ISPS does fail to separate and recognize the different types of ports and terminals, the operations were a particular highlight. They stated that there was a shortage of information and guidance with regards to how different port facilities and terminals implement the security measures of the ISPS Code. Thus, the theory supports the findings.

Informants from three regions mentioned that the Code needs to encompass cyber aspects. Cyber-attacks are not mentioned in the ISPS Code and many authors have made the case as to why it is a threat that must be handled. McNicholas (2016) and Milne (2017) have shown that costs related to cyber-attacks are incredibly high. GGA (2018) and Neveux (2018) provided valid points as to how ports could potentially lose their customers from a cyber breach. Bateman (2013) reported that cyber breaches have led to criminal activities in ports such as the smuggling and trafficking of narcotics. Lastly, Poushter and Huang (2019) have shown that four countries out of 26 have indicated cyber-attacks as their largest national threats. The theory suggests that it may be time for ports to have standards, codes or legislations for cyberattack prevention that are mandatory. However, as for now, there are no global mandatory regulations for cyberattack preventions for container terminals.

Two informants from region 1 mentioned that the Code lacks requirements and guidance for waterside threats and that they were unsure about how to approach this. The Code does mention some security aspects on waterside security for port facilities but does not go into much detail. All the Codes with regards to waterside security are located in part B. Firstly, paragraph 15.16 suggests that ports should consider waterside access to the port facilities, this is in relation

to physical measures that may be used to mitigate threats to the identified vulnerabilities. These physical measures include permanent barriers, alarms, surveillance equipment, etc. Secondly, in the same paragraph, it mentions that it should include considerations of existing agreements with private security companies that provide waterside security services. Thirdly, paragraph 16.8 suggests that the PFSP should establish 'the means of alerting and obtaining the services of waterside patrols and specialist search teams' (p.73), this includes procedures such as underwater and bomb searches. Fourthly, paragraph 16.19 recommends additional measures for security level 2, this includes the use of 'patrol vessels to enhance waterside security' (p.75). The next mentioned suggestion is in paragraph 16.25, which mentions that waterside areas that are next to ships may be considered as a restricted area. Lastly, paragraph 16.28 mentions that waterside patrols should increase in number and frequency in a security level 2, these patrols should include the restricted areas and the port facility areas. These measures are not mandatory but rather serve as guidance or recommendation. It can be stated that following these provisions could be costly due to the extra equipment and manpower needed for further patrols, this does not benefit ports with limited finances. Further study is needed to support the claims of the informants since there are measures stated.

Regarding the challenges of fully implementing the code and the challenges of fully implementing security measures, almost all of the informants from three different regions suggested that it was costly. Several informants stated that costs were especially high when the security level changed, their ports have only experienced a security level 2 but never a security level 3. Other informants highlighted that hiring security personnel and purchasing new technology as a major cost factor, the informants in region 2 agreed that purchasing new technology is costly, however, hiring security is not costly for them. According to Mazaheri and Ekwall (2009), the Code induces higher operative expenses and it has a high cost for implementation. UNCTAD (2007) conducted a study that showed the distributions of these costs. With regards to the costs that were mentioned by the informants, UNCTAD (2007) concluded that equipment was the highest initial cost at 35 percent, this was followed by infrastructure at 26 percent, then personnel and staff time at 14 percent. In terms of annual costs, personnel and staff time took 47 percent of the share of costs, equipment was in third with 11 percent of the share. The theory does support the findings with regards to technology and the employment of security personnel. However, in the same study, a rise in security level was only at two percent of the share of initial and annual costs, therefore the theory cannot support this finding.

One informant noted that full implementation of the Code and increasing security at the port have made it costly for their customers. According to Chang and Thai (2016), enhancing security quality at ports might not only heighten costs but may also lower customer convenience. Throughout this study, different theories suggest that when security is enhanced, costs are usually increased. For example, when taking only one cost aspect into account such as increasing scanning, Alix, Carluer and Slack (2010) written that purchases for new equipment and new technology would have to be made. Additional costs of operations will ensue if ports employ more personnel to operate the scanning procedures. Once ports increase costs, this may lead to an increase in costs towards their customers as well. Findings with regard to costs effects on customers due to an increase in security are supported by the literature.

The informants were asked what sort of vulnerabilities their ports would expose if they had only followed the mandatory security requirements of the ISPS Code, most of the informants from three different regions agreed that there would be a lack of container security with regards to inspections and scanning. Corkhill (2014) agrees with this and stated that the ISPS Code does not tackle container security well enough. Corkhill (2014) further added that many containers contain goods that have not been declared and many of these goods could be dangerous and are made of undetectable material. Part B of the ISPS Code paragraph 16.33 and paragraph 16.36 provides guidelines for checking cargo, this includes physical examination, using scanning equipment, dogs or other mechanical devices in security level 1 and 2 situations. However, since these paragraphs are located in part B, this means that they are not mandatory procedures. There is no mention of using scanning equipment in Part A. The only mention of cargo security in part A for port security personnel is in paragraph 14, where it is stated that the supervision of cargo handling should take place. Contracting governments should include physical examination and scanning of cargo to ensure more security of the cargo.

The informants mentioned various security measures when they were asked regarding what they have added on top of the ISPS Code. These measure includes cybersecurity measures (NIS Directive), measures to for protection against dangerous cargo and nuclear materials (MI), measures for container security (CSI), measures for supply chain security (AEO), measures for increased detections (profile scanning), measures for further inspections (100% cargo inspection), measures for security standards (ISO) and other access control procedures (electric fences, advanced gate system and advances surveillance cameras). According to McNaught (2005), the ISPS Code is highly limited in terms of addressing security measures against threats, hence, the Code should not be seen as a stand-alone solution. Instead, The ISPS Code should

be seen as a single component for securing ports from threats. The informants described the ISPS Code as a tool that could be used depending on the situation, however, they have other tools as well to address other threats. The ISPS Code stands out due to the fact that a part of it has been made mandatory. However, the informants have mentioned other measures that provide enhanced security to their ports. The findings fully support the theory.

Regarding whether the Code needed to be amended, the most noted answer was that it should be fully reviewed, this was stated by informants in region 1 and 3. The informants claimed that the Code had come into enforcement for the first time 15 years ago and should be reviewed whether if it is needed, if it is effective today and if there is anything crucial missing. These claims are highly debatable and would require further research.

One informant claimed that the Code was too bureaucratic and that documentation processes needed to be simplified and less time-consuming. According to Mazaheri and Ekwall (2009), some of the disadvantages of the ISPS Code is that it brings more paperwork and creates more administrative work which can slow down progress. The findings are supported by the theory in this regard, however, Anyiam (2004) stated that the documentation and additional paperwork could be beneficial because it keeps personnel in the maritime sector vigilante of threats. This could perhaps mitigate the chances of an attack on a port or stop attacks from happening completely.

Despite the increased costs and documentation that comes with the Codes implementation, the theory suggests that the Code is an effective tool for enhancing security at container ports, even more so if the recommendations in Part B are implemented. The Code does fail to cover a variety of aspects which include but not limited to cyber issues and in-depth container security measures. This proves that the Code cannot be seen as a single solution for container port security. Moreover, ports in this study have adopted other initiatives and directives to enhance their security, this may be because of the Codes limitations. Some informants suggested that the Code needs a full review and a few amendments, but the Code has proven to be an effective tool for enhancing security measures, further study on this matter would be beneficial to determine which aspects of the Code is in need for amendment.

6.5 Main differences between cases

The main difference found between the cases was in region 2. Informants explained that acts of corruption are a common occurrence at their ports. According to Edgerton (2013), the corruption perception index can be used to determine whether one country is more corrupted than the other. It can be determined that corruption is more common in some countries than in others.

The other major difference found in Case 2 compared to the other cases is that the informants suggested that employing uneducated workers is a threat. The explanation used was that uneducated workers are likely to cause more accidents than those that were educated. When asked to define an uneducated worker, one informant explained that it was workers who had not completed secondary or tertiary education. This study covered poorly trained security personnel as a threat and provided explanations from Berg (2013) and Christopher (2015), however, this study did not cover secondary and tertiary education of employees being a factor for fewer accidents, therefore, further research is needed.

Table 6 provides a summary of the findings and their relevant theories. The findings that are indicated in bold are not supported by findings and could be expanded in further research.

Table 6: Summary of findings and the relevant literature

Topic	Main findings	Supporting theories
Current threats	Smuggling	UNODC, 2011. 2015; McNicholas 2016; Perez, 2014
	Unauthorized access	Christopher, 2015; DoT, 1997
	Terrorism	OECD, 2002; Chalk, 2008; Poushter and Huang 2010
Future threats	Cyber attacks	ECMAR, n.d.; GGA, 2018; Neveux, 2018; AFP, 2017; Milne, 2017
	Preparedness of ports for cyber attacks	
	Penetration test	McNicholas, 2016
Counter measures	Quarterly drills and exercises	ISPS Code, 2003
	Training for changes in security level	
	Training under domestic legislations	
	Joint trainings	
	Checking seals for tampering	
	Cameras	
	Fences	
	100 percent inspections	Wolf, 2013; European commission, 2010
	Scanning systems	European commission, 2010
	Background checks	Christopher, 2015
	High penalties	Christopher, 2015
	100 percent identification checks	Andritsos, 2014
	Balance between security and efficiency of throughput	Christopher 2015
	Placement of ISPS Object	
	Mystery shopper	
	Link between culture and corruption	

	Government involvement in security	UNCTAD, 2007; McNaught, 2005
	Raised security awareness	Wu and Zou, 2009
	Requires adapting to changes in threats	ISPS, 2003
	Needs to differentiate the types of terminals	OCIMF, 2003
	Needs cyberattack countermeasures	McNicholas, 2016; Milne, 2017; GGA, 2018; Neveux, 2018; Bateman, 2013; Poushter and Huang, 2019
	Costly	UNCTAD, 2007; Mazaheri and Ekwall, 2009; Chang and Thai, 2016; Alix, Carluer and Slack, 2010
	Lack of container security	Corkhill, 2014
ISPS Code	ISPS Code cannot act as a stand-alone solution	McNaught, 2005
	Additional paperwork and administrative work	Mazaheri and Ekwall, 2009; Anyiam, 2004
	Effective procedures for waterside security	
	Costly when changing of security levels occur	
	Code needs to be fully reviewed and updated	
Main differences between cases	Level of corruption varies between countries	Edgerton, 2013
	Link between culture and corruption	

7. Conclusion

This study deals with current and future threats to container ports and the effectiveness of the preventative security measures used by container ports today. The objective of this study is to gain understanding about the current and future type of threats to container ports in order to determine which of those threats are the most prominent and to investigate the effectiveness of the modern preventative security measures in countering the identified threats.

The research question of this study is: *What are the most prominent current and future threats to container ports and how effective are modern preventative security measures in countering the identified threats?* In order to answer this, the question is divided into three parts which are current threats, future threats and the effectiveness of modern preventative security measures.

The findings identified smuggling, unauthorized access and terrorism as the most prominent current threats to container ports. Smuggling is a threat that those associated with container ports need to be aware of. Contrabands such as narcotics are being transported with the use of maritime conveyances. This includes the utilization of containers. Maritime transportation accounts for most of the seizures of narcotics compared to other modes of transportation. A lot of contrabands are being transported through container ports undetected. Ports are a nodal point for supply chain logistics and further indications show that imported containers are not inspected regularly. Containers are vulnerable to being tampered with along the supply chain because there is no international body that regulates its security. Most informants agreed that more container security measures are needed in order to prevent smuggling from occurring. New technologies and ideas have been developed but smuggling still remains a concern for container ports.

Terrorism is another current threat that those associated with container ports need to be aware of. Terrorism on ports has contributed to the loss of life, damages to port infrastructure and disruptions to operations. A terrorist attack on a large container port could result in high costs for maintenance and disruptions to the global supply chain. Container ports have not been as affected by terrorist attacks compared to other facilities, which indicates that some ports are unprepared with regards to recovering afterward.

Unauthorized access to ports can lead to other threats such as cargo theft, smuggling and terrorist attacks. If access control procedures are not conducted properly, thieves, terrorists and criminals could find their way into ports. Even those that find their way into ports without

the intention of committing a crime could also disrupt operations. Providing access to unauthorized personnel provides a variety of unknowns.

The findings indicate that the most prominent future threat is cyber-attacks. Cyber-attacks on container ports have caused large disruptions to operations and heavy costs. Cyber-attacks have been known to damage the reputations of container ports which encouraged customers to take their businesses elsewhere. Container terminals that have felt the impact of these attacks are located all over the world. They have been known to stop operations completely or enforce operations with manual systems due to a server shutdown. Container ports today are becoming more automated and digitalized which could lead to higher cyber vulnerabilities. These attacks are not a rarity and those that have not prepared or are not preparing leave themselves vulnerable to breaches.

The answer to *How effective are modern preventative security measures in countering the identified threats*, is that there are no existing measures that can completely avoid threats from occurring, attacks are unpredictable and can happen at any time, only effective countermeasures to mitigate the chances of threats from occurring exists. The ISPS Code can be useful for mitigation efforts, a container port benefits in these mitigation efforts by having a PFSO and a contracting government that regularly assesses the situation around the port and provides insightful updates to the PFSP. Changes to the environment occur often and ports in different regions are more probable to experience some threats than others, this means that the PFSP should include drills, trainings, exercises and countermeasures that are specifically designed for them and their threats. The roles of the port personnel should be established and they should have training with regards to security awareness. In order to ensure higher effectiveness of security measures, the ISPS Code cannot be seen as a stand-alone solution, this is because of its limitations in addressing security measures. There are initiatives and directives that exist to support ports to enhance its security, initiatives such as the CSI and MI came into existence to enhance national security in a nation, however, they may also be used to increase the effectiveness of security measures in container ports. Costs are a huge factor when it comes to a ports effectiveness in threat mitigation efforts. Container ports are a business and extra costs for enhancing security such as employing personnel and purchasing advanced technology directly affect a ports profitability. In order for ports to enhance their security in relation to costs, a port may have to identify a trade-off.

7.1 Limitations and recommendation for further research

One of the main limitations of this study is that the topic of security has many confidential aspects, it was difficult to obtain in-depth explanations of the security measures and processes that took place in the ports of the informants. Questions with regards to security processes were vaguely answered by most informants. Second, each case in this study had few informants, case 1 had five informants, case 2 had three informants and case 3 had one informant. The study attempted to gain an understanding of threats and security measures from different settings to increase the aspect of generalization, this was not the case since there were few informants in each region. Third, official statistics regarding the threats occurring in container ports were difficult to obtain, these figures may have supported the findings better. Fourth, conducting a qualitative study to support the findings would have strengthened the possibilities of generalization. On the topic of further research, it should be analysed whether the waterside security measures mentioned in the ISPS Code are effective in countering threats, if not, what waterside security measures can be taken instead. Moreover, there was a claim that corruption and culture were linked, if this was identified to be true, it could provide further arguments as to why it should be considered as a prominent threat. Also, the theory indicated that the ISPS Code provided highly effective countermeasures and has also indicated that it had several limitations, therefore, a study should be conducted to determine what aspects to keep, what aspects to amend and what aspects should be added in to ensure effective security measures. Studies should also be conducted with regards to how container ports could prepare for cyber-attacks, the findings lacked this information.

References

Agence France-Presse. (2017, June 29). *Cyberattack blocks Maersk terminals, new orders*. from The Local: https://www.thelocal.dk/20170629/cyberattack-blocks-maersk-terminals-new-orders

Akomolafe, B. (2017, May 8). *Truckers lose N12.6bn yearly to extortion at ports*. from New Telegraph Newspaper: http://www.newtelegraphng.com/2017/05/truckers-lose-n12-6bn-yearly-extortion-ports/

Alix, Y., Carluer, F., & Slack, B. (2010). The new US 100% container scanning law: Impacts on the international supply chain. *International Journal of Transport Economics, 37(1)*, 53-76.

Andritsos, F. (2014, June 2). *Port Security & Access Control: a Systemic Approach .* from ResearchGate: https://www.researchgate.net/publication/249009738_Port_Security_Access_Control_a_Systemic_Approach

Anyiam, H. (2014, August 12). *ISPS: Operational Benefits, Administrative Burdens*. from The Maritime Executive: https://www.maritime-executive.com/article/ISPS-Operational-Benefits-Administrative-Burdens-2014-08-12

Bakir, N. O. (2007). A Brief Analysis of Threats and Vulnerabilities in the Maritime Domain. I I. Linkov, R. J. Wenning, & G. A. Kiker, *Managing Critical Infrastructure Risks* (pp. 17-49). Springer Netherlands.

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

Barnes, P., & Oloruntoba, R. (2005). Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. *Journal of international management, 11(4)*, 519-540.

Bateman, T. (2013, October 16). *Police warning after drug traffickers' cyber-attack*. from BBC: https://www.bbc.com/news/world-europe-24539417

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report, 13(4)*, 544-559.

British Broadcasting Corporation. (2018, September 28). *San Diego hit by ransomware attack*. from British Broadcasting Corporation: https://www.bbc.com/news/technology-45677511

Berg, H. (2013). Human factors and safety culture in maritime saferty. I A. Weintrit, & Neumann, *Marine Navigation and Safety of Sea Transporation: STCW, Marine Education and Training (MET), Human Resources and Crew Manning, Maritime Policy, Logistcs and Economic Matters* (pp. 107-115). Boca Raton: Taylor & Francis Group.

Bergqvist, L. H. (2014, July 17). *The ISPS Code and Maritime Terrorism*. from The Maritime Executive: https://www.maritime-executive.com/article/The-ISPS-Code-and-Maritime-Terrorism-2014-07-17

Bhattacharjee, S. (2017, October 7). *What Are The Security Levels Under ISPS Code?* from Marine Insight : https://www.marineinsight.com/marine-safety/security-levels-under-isps/

Bichou, K., & Talas, R. (2014). Overview of contemporary supply chain security initiatives. I K. Bichou, J. S. Szyliowicz, & L. Zamparini, *Maritime Transport Security: Issues, Challenges and National Policies* (pp. 24-39). Cheltenham: Edward Elgar Publishing.

Borchert, H. (2014). *Maritime Security at Risk: Trends, Future Threat Vectors, and Capability Requirements.* Lucerne : Borchert Consultiing & Research AG.

Bryman, A. (2012). *Social research methods (4th e.d.).* Oxford: Oxford University Press.

Bryman, A. (2016). *Social Research Methods.* Oxford: Oxford University Press.

Bryman, A., & Bell, E. (2007). *Business research methods (2nd ed.).* Oxford: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods (3rd ed.).* Oxford: Oxford University Press.

Bryman, A., & Burgess, R. G. (1994). *Analyzing Qualitative Data.* London: Routledge.

Cambell, D., & Gittings, J. (2000, January 15). *Death in pursuit of the American dream*. from The Guardian: https://www.theguardian.com/world/2000/jan/15/duncancampbell.johngittings

Customs and Border Protection. (2018, December 17). *CSI: Container Security Initiative*. Hentet fra U.S. Customs and Border Protection: https://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief

Chalk, P. (2008). *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States.* Santa Monica: RAND Corporation.

Chang, C.-H., & Thai, V. V. (2016). Do port security quality and service quality influence customer satisfaction and loyalty? *Maritime Policy & Management, 43(6)*, 720-736.

Chen, Y.-H., Chen, S.-L., & Wu, C.-H. (n.d.). *The Impact of Stowaways and Illegal Migrants.* from CiteSeerX: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.469.8872&rep=rep1&type=pdf

Christopher, K. (2015). Port Security Management. Boca Raton: Taylor & Francis Group, LLC.

Chu, F., Gailus, S., Liu, L., & Ni, L. (2018, December). *The future of automated ports*. from McKinsey and Company: https://www.mckinsey.com/industries/travel-transport-and-logistics/our-insights/the-future-of-automated-ports

Chua, R. (2014, October 16). *What the senate found out on port extortion*. from ABS-CBN News: https://news.abs-cbn.com/focus/10/16/14/what-senate-found-out-port-extortion

Cooper, D. R., & Schindler, P. S. (2014). *Business Research Methods (12th ed.).* New York: The McGraw-Hill Companies, Inc.

Corkhill, M. (2014, June 19). *Container safety outweighs security*. from Maritime Security Review: http://www.marsecreview.com/2014/06/container-safety-outweighs-security/

Cox, S. L. (2013). The advent and future of international port security law. *National Security Law Journal, 1(1)*, 77-123.

Cresswell, J. W. (2003). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Thousand Oaks: Sage Publications.

Crossman, A. (2018, September 28). *Understanding Purposive Sampling*. from ThoughtCo.: https://www.thoughtco.com/purposive-sampling-3026727

Dingeldey, P. M. (2017, December 22). *Port Automation and Cybersecurity Risks*. from Maritime Executive : https://www.maritime-executive.com/editorials/port-automation-and-cybersecurity-risks

Edgerton, M. (2013). *Effective Maritime and Port Security.* Hoboken: John Wiley & Sons, Inc.

Eisenhardt, K. M. (1991). Better Stories and Better Constructs: The Case for Rigor and Comparative Logic. *The Academy of Management Review, 16(3)*, 620-627.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: opportunities and challenges. *Academy of Management Journal, 50(1)*, 25-32.

European Commission. (2010). *Secure Trade and 100% Scannng.* Brussels : European Commission.

European Council for Maritime Applied R&D. (n.d.). *Maritime Technology Challenges 2030.* Brussels: European Council for Maritime Applied R&D.

Forbes, V. L. (2018, August 21). *The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges* . from Future Directions International: http://www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/

Frankfort-Nachmias, C., Nachmias, D., & DeWaard, J. (2015). *Research Methods in the Social Sciences 8th edition.* New York: Worth Publishers.

Frith, J. (2018, August 9). *ISPS Code fails to contemplate aerial threats from drone*. from Docks the Future: https://www.docksthefuture.eu/isps-code-fails-to-contemplate-aerial-threats-from-drones/

Gall, M. D., Borg, W. R., & Gall, J. P. (1995). *Educational Research: An Introduction (6th ed).* White Plains: Allyn & Bacon.

Generali Global Assistance. (2018). *The imapct of cybersecurity incidents on financial institutions .* Washington DC: Generali Global Assistance.

Glaser, B. S., & Vitello, J. A. (2015). *Taiwan's Marginalized Role in International Security: Paying a Price.* Washington DC: Center for Stategic and International Studies.

Government Accountability Office. (2012, October). *Combating Nuclear Smuggling: Megaports Initiative faces funding and sustainability challenges*. from Government Accountability Offices: https://www.gao.gov/assets/650/649759.pdf

Greenberg, A. (2018, August 22). *The untold story of Notpetya, the most devastating cyberattack in history*. from Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greener, S. (2008). Quantitative versus qualitative? I S. Greener, *Business Research Methods* (s. 18). Copenhagen: Dr. Sue Greener & Ventus Publishing Aps.

Gujar, G., Gosh, P., & Yan, H. (2014). *Maritime Security: A New Outlook.* Saarbrücken: LAP Lambert Academic.

Gujar, G., Ng, A. K., & Yang, Z. (2018). *Contemporary Container Security.* Cham: Palgrave Macmillan.

Gutauskas, A. (2009). *Human Trafficking and Its Treatment in Criminal Law.* Vilnius: Mykolas Romeris University Faculty of Law.

Helmick, J. S. (2007). Port and maritime security: A research persepctive. *Journal of Transportation Security, 1(1)*, 15-28.

Hoffman, J., & Kumar, S. (2010). Globalisation - The Maritime Nexus. I C. T. Grammenos, *The Handbook of Maritime Economics and Business, 2nd edition.* London: Lloyd's List.

Ilascu, I. (2018, September 21). *Port of Barcelona Suffers Cyberattack* . from Bleeping Computer: https://www.bleepingcomputer.com/news/security/port-of-barcelona-suffers-cyberattack/

International Maritime Organization. (2002). *ISPS Code.* London: IMO Publishing.

International Maritime Organization. (2003). *Code of practice on security in ports .* Geneva: International Maritime Organization.

International Maritime Organization. (2013, April 12). *Facilitation Committee (FAL), 38th session: 8 to 12 April 2013*. from International Maritime Organization: http://www.imo.org/en/MediaCentre/MeetingSummaries/FAL/Pages/FAL-38th-session-.aspx

International Maritime Organization. (2017, July 5). Guidelines on Maritime Cyber Risk Management. from International Maritime Organization: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

International Maritime Organization. (n.d.). *SOLAS XI-2 and the ISPS Code*. from International Maritime Organization: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

International Maritime Organization. (n.d.). *What is the ISPS Code*. from International Maritime Organization: http://www.imo.org/blast/mainframe.asp?topic_id=897#what

Ismail, M. A. (n.d.). Port operation and management: port safety vs port security. Sintok: University Utara Malaysia.

Keefer, W. J. (2007). *Container Port Security: A Layered Defense Strategy to Protect the Homeland and the International Supply Chain.* Raleigh: Scholarly repository at Cambell University School of Law.

Klitgaard, R. (1988). *Controlling Corruption.* Berkeley: University of California Press.

Kunz, R. (2017, November 15). *7 Reasons to Run a Background Check on Each and Every Employee*. from Trust Employees: https://www.trustedemployees.com/learning-center/articles-news/7-reasons-run-background-check-every-employee/

Larmour, P. (2012). Corruption and the Concept of Culture: Evidence from the Pacific Islands. I M. Barcham, B. Hindess, & P. Larmour, *Corruption: Expanding the Focus* (pp. 155-178). Canberra: Australia National University Press.

Laszuk, M., & Ryciuk, U. (2016). The importance of Authorized Ecornomic Operator institution for the security of supply chain in the international good turnover of Polish enterprises. *Eurasian Journal of Business and Management* , 32-41.

LeCompte, M. D., & Goetz, J. P. (1982). Problems of Reliability and Validity in Ethnographic Research. *Review of Educational Research, 52(1)*, 31-60.

Littlejohn, D. (2017, September 6). *Bandits steal shipping containers from Port of Los Angeles with $1 million worth of merchandise*. from Daily Breeze: https://www.dailybreeze.com/2014/03/28/bandits-steal-shipping-containers-from-port-of-los-angeles-with-1-million-worth-of-merchandise/

Longo, F. (2010). Design and integration of the containers inspection activities in the container terminal operations. *International Journal of Production Economics 125(2)*, 272-283.

Lorenz, A. J. (2007, October 1). *The Threat of Maritime Terrorism to Israel.* from Terrorism Info: https://www.terrorism-info.org.il/Data/pdf/PDF_19294_2.pdf

Maersk. (2018). *2018 Annual Report.* Copenhagen: Maersk. from Global News Wire: https://ml-eu.globenewswire.com/Resource/Download/3b5d6bab-974e-44bb-abaa-97fbabde11c5

Maritime Union of Australia . (2005, November 15). *Port Blast*. from Maritime Union of Australia : https://archive.is/20060823030308/http://www.mua.org.au/journal/julaug_2004/ashdod.html

Marshall, C., & Rossman, G. B. (2016). *Designing Qualitative Research (6th ed.).* Thousand Oaks: SAGE Publications.

Martens, B. J., Crum, M. R., & Poist, R. F. (2011). Journal of Business Logistics, 32(2). *Examining Antecedents to Supply Chain Security Effectiveness: An Exploratory Study*, 156-166.

Mazaheri, A., & Ekwall, D. (2009). Impacts of the ISPS code on port activities: a case study on Swedish ports . *World Review of Intermodal Transportation Research*, 326-342.

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

McNicholas, M. A. (2016). *Maritime Security.* Butterworth-Heinemann.

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook (3rd ed.).* Thousand Oaks: Sage Publications.

Mill, J. S. (1882). *A stystem of logic, ratiocinative and inductive, being a connected view of the principles of evidence, and the methods of scientific investigation.* New York: Harper & Brothers.

Milne, R. (2017, August 16). *Moller-Maersk puts cost of cyber attack at up to $300m*. from Financial Times: https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff

(n.d.).

National Nuclear Security Administation . (2010). *Office of the Second Line of Defense: Megaports Initiative.* Washington DC: National Nuclear Security Administration.

National Nuclear Security Administation. (n.d.). *Megaort Initiative .* from Homeland Security Digital Library : https://www.hsdl.org/?abstract&did=473907

Neveux, E. (2018, June 20). *Reputation Risks: How Cyberattacks Affect Consumer Perception*. from Secure Link: https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception/

Nichols, P. M. (2017). What is Organizational Corruption? I M. S. Aßländer, & S. Hudson, *The Handbook of Business and Corruption: Cross-Sectoral Experiences* (p. 3). Bingley: Emerald Publishing Limited.

Oates, B. J. (2006). *Researching Information Systems and Computing.* London: Sage Publications.

Oil Companies International Marine Forum. (2003, December). *Guidance for oil terminal operators on the International Maritime Organization (IMO) International Ship and Port Facility Security (ISPS) Code.* from Oil Companies International Marine Forum : https://www.ocimf.org/media/8922/48ac1e9a-12e2-45b5-bfb0-84437535de77.pdf

ONCAM. (2019, January 10). *Choosing the right security solutions for seaports*. from ONCAM: https://www.oncamgrandeye.com/featured/choosing-the-right-security-solutions-for-seaports/

Organisation for Economic Co-operation and Development . (2002). *Econimic Consequences of Terrorism .* Paris: Organisation for Economic Co-operation and Development .

Ott, C. (2014). *Fraud in the maritime industry.* from Skuld: https://www.safety4sea.com/wp-content/uploads/2014/09/pdf/Fraud_in_the_maritime_industry.pdf

Palaskar, J. (2018). Research eithic. *Journal of Dental & Allied Sciences, 7(1)*.

Perez, A. L. (2014). *Mares de Cocaina.* Grijalbo.

Poushter, J., & Huang, C. (2019, February 10). *Climate Change Still Seen as the Top Global Threat, but Cyberattacks a Rising Concern*. from Pew Research Center: https://www.pewglobal.org/2019/02/10/climate-change-still-seen-as-the-top-global-threat-but-cyberattacks-a-rising-concern/

Raymond, C. Z. (2004). *The Challenge of Improving Maritime Security: An assessment of the implementation of the ISPS Code and initial responses as to its effectiveness .* Singapore: IDSS Commentaries.

Rice, J. B., & Caniato, F. (2003). Supply Chain Management Review, 7(5). *Building a secur*, 22-30.

Richardson, H. W., Gordon, P., & Moore, J. E. (2009). *Global Business and Terrorist Threats.* Cheltenham: Edward Elgar Publishing Limited.

Robinson, R. (2002). Ports as elements in value-driven chain systems: the new paradigm. *Maritime Policy and Management, 29(3)*, 241-255.

Romero, J. (2003). Prevention of Maritime Terrorism: The Container Security Initiative. *Chicago Journal of International Law, 4(2)*, 597-605.

Russel, D. L., & Arlow, P. C. (2015). *Industrial Security: Managing Security in the 21st Century.* Hoboken: John Wiley & Sons, Inc.

Scholz, R. W., & Tietje, O. (2002). *Embedded Case Study Methods: Integrating Quantitative and Qualitative Knowledge.* Thousand Oaks: Sage Publications .

Sekaran, U., & Bougie, R. (2016). *Research Methods for Business; A Skill-Building Approach (7th ed.).* Chichester: John Wiley & Sons Ltd.

Seleim, A., & Bontis, N. (2009). The relationship between culture and corruption: A cross-national study. *Journal of Intellectual Capital, 10(1)*, 165-184.

Ships & Ports. (2019, February 4). *Is extortion by security operatives still rampant?* from Ships & Ports: http://shipsandports.com.ng/extortion-security-operatives-still-rampant/

Singla, S. (2016, July 21). *What is Container Security Initiative (CSI) and how does it Work?* from Marine Insight: https://www.marineinsight.com/marine-safety/what-is-container-security-initiative-csi-and-how-does-it-work/

Stake, R. E. (1995). *The Art of Case Study Research.* Thousand Oaks: Sage Publications.

Stake, R. E. (2003). Case Studies. I N. K. Denzin, & Y. S. Lincoln, *Strategies of Qualitative Inquiry* (pp. 134-164). Thousand Oaks: Sage Publications.

Stehouwer, A. (2012, December 21). *Celebration of 20 years AGV's* . from Port of Rotterdam: https://www.portofrotterdam.com/en/news-and-press-releases/celebration-of-20-years-agv%E2%80%99s

Tang, D., Xu, D.-L., Yang, J.-B., & Chen, Y.-w. (2013). Security Based Operation in Container Line Supply Chain: a Literature Review. I B. Vitoriano, J. Montero de Juan, & D. Ruan, *In Decision Aid Models for Disaster Management and Emergencies* (ss. 95-115). Paris: Atlantis Press.

The Local. (2017, June 29). *Cyber attack 'worst possible timing' for Gothenburg port*. from The Local: https://www.thelocal.se/20170629/cyber-attack-blocks-maersk-terminal-in-gothenburg

The Maritime Executive. (2019, January 28). *U.S. Ports Want $4 Billion to Enhance Security*. from The Maritime Executive: https://www.maritime-executive.com/article/u-s-ports-want-4-billion-to-enhance-port-security

Trelawny, C. (2015). *Tackling the traddicking of illegal wildlife products.* IMO.

Turner, B. (2018, September 5). *Cargo Theft Statistics: Unreported Incidents May Greatly Understate the Numbers*. from LPM Insider: https://losspreventionmedia.com/insider/supply-chain-security/unreported-cargo-theft-incidents-make-it-difficult-to-grasp-scope/

U.S. Department of Transportation . (1997). *Port Security: A National Planning Guide.* U.S. Department of Transportation.

U.S. Department of Transportation Volpe Center. (1999, May). *Intermodal Cargo Transportation: Industry Best Security Practices.* from U.S. Department of Transportation Volpe Center: http://www..volpe.dot.gov/infosrc/strtplns/nstc/cargo/index.html

UNCTAD. (2007, March 14). *Maritime Security: ISPS Code implementation, costs and relating financing*. from UNCTAD: https://unctad.org/en/Docs/sdtetlb20071_en.pdf

UNCTAD. (2018). *Review of Maritime Transportation 2018.* New York: United Nations Publications.

United Nation conference on Trade and Development. (2007, March 14). *Maritime Security: ISPS Code Implementation, Costs and Related Financing*. from United Nation conference on Trade and Development: https://unctad.org/en/Docs/sdtetlb20071_en.pdf

United Nations. (2018, October 4). *Illicit Drug Flows, Organized Crime Grow as Terrorism Spreads across Borders, Third Committee Delegates Stress amid Calls for Stronger Justice Systems*. from United Nations: https://www.un.org/press/en/2018/gashc4228.doc.htm

United Nations Office of Drugs and Crime. (2011). *The Transatlantic Cocaine Market.* New York: United Nations.

United Nations Office on Drugs and Crime. (2015). *World Drug Report 2015.* New York: United Nations.

United Nations Office on Drugs and Crime. (2018). *World Drug Report 2018.* Vienna: United Nations.

United Nations Office on Drugs and Crime. (2019). *Drug Trafficking*. from United Nations Office on Drugs and Crime: https://www.unodc.org/unodc/en/drug-trafficking/index.html

Wiseman Law Firm. (2012, August 10). *What is the difference between drug tafficking and smuggling?* from The Wiseman Law Firm: https://www.wisemantriallaw.com/blog/2012/august/what-is-the-difference-between-drug-trafficking-/

Wolf, J. (2013, July 9). *Scanning Cargo Containers Is More Important than Scanning Emails*. from Atlantic Council: https://www.atlanticcouncil.org/blogs/new-atlanticist/scanning-cargo-containers-is-more-important-than-scanning-emails

World Trade Organization. (2018). *World Trade Statistical Review 2018.* Geneva: World Trade Organization.

Wu, S., & Zou, K. (2009). *Maritime Security in the South China Sea: Regional Implications and International Cooperation.* Farnham: Ashgate Publishing Limited.

Yang, Y.-C. (2010). Impact of the container security initiative on Taiwan's shipping industry. *Maritime Policy & Management, 37(7)*, 699-722.

Yang, Z., Wang, J., & Li, K. (2013). Maritime safety analysis in restrospect. *Maritime Policy & Management, 40(3)*, 261-277.

Yin, R. K. (2003). *Case Study Research Design and Methods (2nd ed.).* Thousand Oaks: Sage Publications.

Zainal, Z. (2007). *Case study as a research method.* Skudai: Universiti Teknologi Malaysia.

Zhao, X., Yan, H., & Zhang, J. (2016). A critical review of container security operations. I *Maritime Policy & Management, 44(2)* (pp. 170-186). Routledge Taylor & Francis Group.

APPENDIX A: Interview Guide

Informant's profile:

1.1 Can you please explain your education background?

1.2 How many years' experience do you have in your current industry?

1.3 Can you please tell me about your position in the company and describe it?

Current threats:

2.1 What type of threats should port employees worldwide be aware of in the container port system? – and are there any other threats you have in mind? – which threats would you say are the most important to focus on and why?

2.2 What are the current threats that concern your port most and why?

2.3 How do you overcome or deal with these threats to ensure that they do not occur?

2.4 How different are the type of threats depending on the location of the port?

Future threats:

3.1 Autonomous technology and the use of digitalization is a big topic for discussion in the container port industry, with that in mind, what do you think are the future threats that may concern container ports?

3.2 What kind of impact do you think cyber attacks can have on container ports worldwide?

3.3 What are the future threats that concern your ports most?

3.4 How do you intend to handle these future threats? Have you started and do you have action plans to prevent them from occurring?

3.5 What sort of knowledge, skills or competence does your port need in order to handle these future threats?

3.6 How prepared are you for these future threats? – how did you prepare for them?

Countering threats:

4.1 Are local port authorities and contracting governments doing enough to secure container ports from potential threats? – if not what more can they do?

4.2 What preventative security measures can be taken to mitigate the chances of a threat from occurring in terms of training, drills and exercises?

4.3 Smuggling, trafficking and stowaways are a major problem for many ports, how can the industry reduce the chances of these acts from occurring? – how should ports ensure that a container doesn't have contrabands or stowaways hidden inside?

4.4 In some areas, port employees and port security personnel's have been known for taking bribes, operating with criminal organizations and stealing. What can be done to ensure that this does not happen?

4.5 How do you secure the port from unauthorized people from entering?

4.6 How prepared are container ports in tackling cyber attacks? And what measures can be taken to stop it from occurring?

4.7 What are some of the major challenges that prevent ports from implementing effective security measures?

4.8 Have you encountered a security challenge in this port? If so, what happened and how did you deal with the situation?

4.9 Is there a quality control system in this port? If so, can you please explain it?

4.10 Is there a system in this port where employees can anonymously report problems?

The ISPS Code:

5.1 What are the strengths of the ISPS code when it comes to limiting the chances of a threat from occurring?

5.2 What are the weaknesses of the ISPS code and is there anything vital missing in the ISPS Code?

5.3 What are the challenges of fully implementing the ISPS code?

5.4 If container ports were to only follow the mandatory security requirements of the ISPS code, what sort of vulnerabilities will the port expose?

5.5 What have you added to your security system that is not part of the ISPS code and why have you added it in?

- What resources did you need in order to accomplish and prepare for this?

5.6 Does the current ISPS code need to be amended?

- if so, why and in what areas?

Closing:

6.1 Do you have any additional comments about this topic?

6.2 If I have any more additional questions, may I please contact you again?