

University of Mississippi

eGrove

Electronic Theses and Dissertations

Graduate School

2012

The Perceived Effectiveness of Container Security at Seaports Along the Gulf Coast

William Augustus Neely

Follow this and additional works at: <https://egrove.olemiss.edu/etd>



Part of the [Transportation Commons](#)

Recommended Citation

Neely, William Augustus, "The Perceived Effectiveness of Container Security at Seaports Along the Gulf Coast" (2012). *Electronic Theses and Dissertations*. 208.

<https://egrove.olemiss.edu/etd/208>

This Thesis is brought to you for free and open access by the Graduate School at eGrove. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.

THE PERCEIVED EFFECTIVENES OF CONTAINER SECURITY AT SEAPORTS ALONG
THE GULF COAST

A Thesis
presented in partial fulfillment of requirements
for the degree of Master of Criminal Justice
in the Department of Legal Studies
The University of Mississippi

by

WILLIAM A. NEELY, III

May 2012

Copyright William A. Neely, III 2012
ALL RIGHTS RESERVED

ABSTRACT

With approximately 90% of the world's goods shipped via cargo containers, it is vital for the security of these containers to be complete and effective. However, given the volume of containers transiting U.S. seaports, the task of providing subsequent security is complicated and, arguably, improbable. Nevertheless, the data analyzed throughout this study disputes that the current cargo container paradigm can be enhanced to accommodate the significant workload.

The research conducted throughout this study provided perceptions that were indicative of a security environment that could be and must be improved. More specifically, the data revealed that the biggest threat facing containers was their susceptibility to be exploited for smuggling purposes. In addition, all of the participants acknowledged the use of a layered security framework at their respective ports. However, this "layered" approach was insufficient to scan even a fraction of the containers imported to the U.S. As a result of the limitations associated with container security, the majority of containers receive no form of inspection until their arrival to U.S. seaports. This makes it impossible to inspect and, even, scan 100% of containers. With that in mind, the participants in this study believe that container security could progress, but without knowledgeable, proper and efficient use of technology, no such improvement is achievable. Furthermore, unilateral cooperation from the rest of the global seaport community is essential for container security to advance. Finally, the insurmountable task of providing a dynamic and resilient security framework hinges on CBP's ability to facilitate and collaborate with the entire seaport community.

Keywords: container, WMD, terrorism, security, deputy port directors, inspection, scan

DEDICATION

This work is dedicated to my friends and family. Their support, patience and encouragement, undoubtedly, gave me the fortitude to complete this research. I would also like to dedicate this work to the men and women serving in all branches of the United States military.

LIST OF ABBREVIATIONS AND SYMBOLS

WMD weapon of mass destruction

CTPAT Customs Trade Partnership Against Terrorism

ATS Automated Targeting System

SFI Secure Freight Initiative

ISF Importer Security Filing

TWIC Transportation Worker Information Credentials

CSI Container Security Initiative

OSC Operation Safe Commerce

TEU Twenty equivalent unit

USCG United States Coast Guard

CBP Customs and Border Protection

DOE Department of Energy

GAO Government Accountability Office

NII Nonintrusive imaging

TSA Transportation Security Agency

IMB International Maritime Bureau

ISO International Organization of Standardization

IAEA International Atomic Energy Association

VACIS Vehicle and Cargo Inspection System

ACKNOWLEDGEMENTS

I would like to acknowledge the faculty members who served on my committee: Dr. Michael P. Wigginton, Jr., Dr. Linda Keena, and Dr. Carl J. Jensen. Without their patience and dedicated effort to assist me through this process, I wouldn't have been able to complete this thesis. Most importantly, I would like to thank Dr. Michael P. Wigginton, Jr. for introducing me to the complicated, yet noteworthy world of transportation security and, more specifically, the importance of container security. Furthermore, his persistent tolerance of my stubbornness made this thesis possible and for that I will always be always be thankful. I would like to thank Dr. Linda Keena for her detailed knowledge of the APA manual and her generous willingness to extend that knowledge to me at a moments notice. Also, I would like to thank Dr. Carl J. Jensen for his guidance and assistance through this entire process. The unwavering cooperation and guidance that my committee exhibited made this thesis achievable and their sacrifices will not be forgotten.

Also, I would like to thank Assistant Professor Robert Mongue, J.D., Interim department chair Dr. Stephen L. Mallory, Ms. Carol Reid and the faculty of the Department of Legal Studies for their continued support and dedication towards myself and my fellow graduate students. Additionally, I would like to thank SFC Cameron C. Campbell for introducing me to the online world of the Government Accountability Office, where from a significant majority of my research was based and referenced.

Finally, I would like to thank all of the participants at the seaports mentioned within this study. Without their enthusiasm to cooperate and share their particular knowledge, this study

wouldn't have been feasible. Their generous effort and constant professionalism made this research a more agreeable experience. Although my words of gratitude will never be able to equal the amount of appreciation that I'm attempting to illustrate, their assistance through this process will not soon be forgotten.

TABLE OF CONTENTS

	Page
ABSTRACT.....	ii
DEDICATION.....	iii
LIST OF ABBREVIATIONS AND SYMBOLS.....	iv
ACKNOWLEDGMENTS.....	v
LIST OF FIGURES	ix
CHAPTER 1: INTRODUCTION.....	1
Threats to Containers	3
Primary Agencies Involved in Container Security	6
Previous Initiatives and Actions Taken	7
Ports of Interest.....	11
Statement of the Problem.....	12
Purpose of the Study	14
Assumptions and Limitations	15
Significance of the Study	16
Definition of Key Terms.....	16
CHAPTER 2: LITERATURE REVIEW	21
Twenty Equivalent Units	24
Piracy	26
Types of Vessels Targeted by Piracy.....	32
Organized Crime and Terrorism	36
Container Theft.....	38
Stowaways	39
Agencies Responsible for Security	42
Seaports of the Study	43
Operation Safe Commerce.....	47
Container Security Initiative	49
24 Hour Rule.....	52
Automated Targeting System	54
Secure Freight Initiative.....	57
Strategic Trade Corridor Strategy.....	61
Importer Security Filing.....	63

MegaPorts Initiative.....	68
Customs Trade Protection Against Terrorism	72
Transportation Workers Information Credentials.....	76
The Consumer and Security.....	79
CHAPTER 3: RESEARCH DESIGN AND METHODOLOGY	84
Method	85
Population Sample	85
Data Collection and Instrumentation	88
Data Analysis	89
CHAPTER 4: ANALYSIS OF RESULTS	91
Restatement of the Research Questions.....	91
Interpretation of Results and Statements of Significance.....	91
Emergent Themes	104
CHAPTER 5: CONCLUSIONS, DISCUSSIONS, AND RECOMMENDATIONS	109
Summary and Conclusions	109
Discussion of Implications & Recommendations for Future Research.....	112
REFERENCES	119
APPENDICES	136
VITA.....	158

LIST OF FIGURES

1. Tonnage in 2009.....	137
2. Number of TEUs imported in 2009.....	138
3. What is a TEU.....	139
4. Types of Vessels Targeted by Pirates.....	140

CHAPTER ONE: INTRODUCTION

Introduction

Almost 90 percent of the world's manufactured goods move by container, much of it stacked many stories high on huge container ships ("Container Security Initiative," 2008). Furthermore, of over the 100 million containers moved through the maritime transport system in 2005, about 11 million arrived and were offloaded at domestic seaports in the United States ("Container Security Initiative," 2008). Due to the large volume of cargo, containers have become the most significant threat to maritime transportation.

Prior to the advent of containers, cargo such as fruit, textiles and coffee was boxed or stacked loose or on pallets in hatches below decks and loaded and unloaded via conveyor belts, physical manpower, ship cranes, or nets (McNicholas, 2008). Now, specialty containers have been constructed to handle nearly all cargoes from toxic chemicals, to airplane parts, to automobiles, to hanging garments, bagged sugar and grains, case lots, as well as a huge variety of refrigerated and frozen products (McNicholas, 2008).

McNicholas (2008) explained:

The development of the modern container—the most efficient, safe, and flexible method to transport cargo across the ocean and land—was a watershed event in maritime transportation and served as a catalyst for the evolution of seaports from only handling break bulk and bulk cargoes and vessels to also—or exclusively—receiving and loading cargo containers. (p.34)

Primarily, commercial vessels are responsible for transporting cargo containers. And today, approximately 90% of cargo transported around the world is by way of commercial vessel and 93% of its packaged in containers (Kaluza, Kolzsch, Gastner & Blasius, 2010). McNicholas (2008) defined a container as a closed or open top van or other similar body on or into which cargo is loaded and transported without chassis aboard ocean vessels. Furthermore, containers come in various sizes and types to accommodate a variety of goods such as dry, refrigerated, and liquid and do not have their own wheels (“World Shipping Council,” 2011).

The effects of container shipping have proven paramount to the progressive and efficient flow of global trade. The evolution of commercial shipping reached a profound echelon with the introduction of the cargo container. The modern container first appeared in the 1950s (“World Shipping Council,” 2011). On April 26, 1956, a crane lifted fifty-eight aluminum truck bodies aboard an aging tanker ship moored in Newark, New Jersey (Levinson, 2006). Five days later the *Ideal-X* sailed into Houston, where fifty-eight trucks waited to take on the metal boxes and haul them to their destinations. Such was the beginning of a revolution (Levinson, 2006). However, Publicover (1999) argued that the U.S. military was the first to experiment with the use of containers for shipping in the mid 1960’s. Nevertheless, this advancement created an entirely new paradigm for the transportation of cargo. Yet, with all the benefits this advancement generated for maritime cargo transportation, it invented new vulnerabilities that were susceptible to exploitation.

In the early years of containerization, very little emphasis was put on standardization (McNicholas, 2008). Containers came in various sizes. As a result, McLean’s, Sea-Land Service typically used a 35 foot container, while Matson Lines, which sailed between the West Coast of the United States and Hawaii, decided on 24-foot long containers (McNicholas, 2008). However, it wasn’t until 1970, at the urging of McLean, that some standards were proposed and

adopted by the International Standards Organization (ISO), with the 20 and 40 footers becoming the basic units (Schuler, 2008).

While there are several versions/dimensions associated with the modern shipping container, most commonly they either are 20 or 40 feet long, eight feet wide, and eight feet six inches in height (Department of Transportation, 2010). The 20 foot containers, or twenty foot equivalents (TEUs), are more widely used. Moreover, the aforementioned standardization has made it possible to ship enormous amounts of containers on a single load/deck. Some SuperMax vessels can transport over 14,000 TEUs at one time. For example, the M/V EMMA MAERSK regularly carries up to 11,000 TEU containers to a designated seaport, discharge a portion of their containers, and reload as planned (McNicholas, 2008). Furthermore, MAERSK plans to have a larger container ship built by 2013, which will be capable of transporting approximately 18,000 TEUs (Martin, 2011). For further information see Table 3A: What is a TEU?

Threats to Containers

However, this commercial advantage has increased the likelihood of weapons of mass destruction (WMD) successfully penetrating maritime security and, subsequently, entering the United States undetected. More specifically, it has been argued that a cargo container would be the most likely way to secrete such a weapon. Nevertheless, with the millions of containers shipped globally, the ability of criminals and terrorists to exploit this means of transportation has become an overwhelming concern. Additional threats include: stowaways, piracy, drug and contraband smuggling, sabotage, hijacking, unauthorized use, cargo tampering, hostage-taking, vandalism, use of the vessel to carry perpetrators and their equipment, and the use of the vessel as a weapon (McNicholas, 2008).

These threats are determined by an individual's ability to successfully manipulate the containers themselves. Such issues concerning the integrity and, inevitably, exploitation of container security begin with the physical characteristics of cargo containers. It is inconceivable to monitor all cargo once it has been loaded aboard a shipping vessel. Sweet (2006) explained physical and procedural security needs to be constantly monitored to provide a sufficient level of security commensurate with the current threat environment. Therefore, certain precautions have been established in order to mitigate this impediment.

For example, once containers have been loaded and stacked, a container seal is attached. These seals are virtually the only physical line of defense for the container. However, container seals are not locks. McNicholas (2008) elaborates, while a seal may have several characteristics of a lock—material used in the manufacture of the device, sturdiness, etc.—its primary purpose is as a tamper-evident device and not to prevent unauthorized access. In addition, container doors can be removed and replaced without breaking the seal and radio frequency identification (RFID) seals can be reset after unauthorized openings (Pinto & Rabadi, 2008). Furthermore, high security cable seals can be defeated in under 10 minutes by using a common drill and a coat hanger—and, with the use of a bit of green plastic fill, leaves no sign of alteration and is reusable (McNicholas, 2008)

The inspection process for containers begins well before cargo is ever loaded. Empty containers are inspected in container yards, port terminals and at the cargo loading location. For the most part, this inspection is conducted by personnel and/or K-9 teams (McNicholas, 2008). According to the Customs Trade Partnership Against Terrorism (2006) (C-TPAT) container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. Procedures must be in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors (C-TPAT,

2006). There is a seven-point inspection process that is recommended for all containers: Front wall, left side, right side, ceiling/roof, inside/outside doors, outside/undercarriage (C-TPAT, 2006). However, the integrity of a container during its transport from point A to point B in the logistics chain cannot be guaranteed. Given sufficient time, opportunity and a remote location, people will be able to open a container and tamper with its contents (van de Voort, O'Brien, Rahman and Valeri, 2003).

However, although the majority of containers are transported by sea, containerized cargo is conveyed utilizing multiple modes of transportation including air and ground resources (i.e. rail road and truck). For instance, once a container has been off-loaded at the port of entry, the container will, ultimately, proceed to the distributor and consumer by way of rail road and truck. Nevertheless, while all modes of transportation have specific vulnerabilities to warfare, criminal and terrorist attacks, perhaps no sector is more dangerously exposed than ports and intermodal freight transportation systems to which they are connected (McNicholas, 2008).

Also, there is an inherent tension between commerce and security. This tension can make scanning significant numbers of containers upon destination in port a cumbersome process. The uninterrupted flow of commerce is directly related to container security. More specifically, the efficient facilitation of container security dictates the fluctuation of product pricing. Bakshi, Flynn and Gans (2009) noted the extra delays would lead to increases in transportation lead times, resulting in higher inventory levels in supply chains, and ultimately in higher cost for consumers. Establishing a medium that mitigates maritime threats while decreasing the inherent tension between commerce and container security is the most effective way to move forward. However, initiating a solution that satisfies all of these requirements becomes extremely complicated and expensive.

For the aforementioned reasons, seaports and, more specifically, containerized cargo are extremely susceptible to exploitation. In fiscal year 2006, more than 11.6 million maritime containers arrived at United States seaports, an average of 32,000 a day (“Container Security Initiative,” 2008). More importantly, only a small fraction of these containers will be checked and inspected by Customs and Border Protection (CBP) for WMDs or other contraband. Hall (2006) noted that the U.S. Department of Homeland Security is responsible for security at more than 140 U.S. seaports. Additionally, Hall’s (2006) research noted that DHS has only 69 mobile gamma ray trucks and enough drive-through radiation detectors to check 37% of the millions of cargo containers that arrive at the ports each year. Only 6% of those containers are ever physically inspected. More specifically, at the Port of Newark, NJ, about 7% to 8% of the 5,000 containers that arrive each day are deemed “high risk” and examined by gamma ray truck (mobile VACIS unit that utilizes a low level gamma ray radiation source to penetrate vehicles and cargo). Of those, approximately 20 a day are given a complete inspection (Hall, 2006, p. 2). Nonetheless, given the fundamental design that is associated with international seaports, a single proven method could be utilized at multiple seaports.

Primary Agencies Involved in Container Security

The maritime sector, by its very nature is a complex, international, open transportation network, poses several additional challenges from a security standpoint (McNicholas, 2008). Therefore, effective container inspection is necessary to provide a sufficient blanket of security capable of meeting these demands. Even though container security has just recently received more attention than decades past, container safety and security has long been considered a critical aspect in the overall security of seaports. For example, The International Convention for

Safe Containers (1972) explained, “The container itself emerged as the most important aspect to be considered within maritime transportation” (p.1).

To accomplish the abovementioned objectives, many conventions and committees have assembled for this purpose. Among those primary organizations presiding over these procedures is the United States Coast Guard (USCG) and CBP, as well as other contributing agencies (i.e. Harbor Police, local municipality, state and other federal agencies). Aside from the physical security of the container itself, the USCG is the lead agency for port security. The U.S. Department of Transportation (2005) explained the Navigation and Vessel Inspection Circulars (NVIC) 9-02 tasked the USCG with five (5) main goals: a) build Maritime Domain Awareness (MDA), b) ensure positive/controlled movement of High Interest Vessels, c) enhance presence and response capabilities, d) protect critical infrastructure and enhance Coast Guard force protection, and e) increase domestic and international outreach. However, the USCG has questioned their ability to handle this responsibility single-handedly.

The Commandant of the Coast Guard, Admiral Thomas H. Collins, has admitted that the agency currently does not have the resources or personnel to scrutinize the security plans of more than 10,000 foreign vessels that enter U.S. ports annually (U.S. Department of Transportation, 2005). It will take cooperation between local and global organizations to alleviate this strain. Coordination between the U.S. Department of Transportation, the Maritime Administration, the CBP, local and state authorities, and international partners will be essential (Sweet, 2006).

Previous Initiatives and Actions Taken

Subsequent to 9/11 and passage of the Maritime Transportation Security Act, numerous security measures have been initiated to enhance container and port security. In November of 2001 the Customs Trade Partnership Against Terrorism (C-TPAT) was created in direct response

to 9/11. C-TPAT (2006) stated CBP challenged the trade community to partner with them to design a new approach to supply chain security focused on protecting the United States against acts of terrorism by improving security while simultaneously speeding the flow of commerce. Not long after C-TPAT was passed, the Maritime Transportation Security Act (MTSA) was created. MTSA is the U.S. equivalent of the International Ship and Port Facility Security Code (ISPS), and it was signed in 2002, but not fully implemented until July 1, 2004 (McNicholas, 2008). MTSA integrates the myriad of federal, state, and local law enforcement agencies tasked with securing the international borders of the United States and its seaports (Sweet, 2006). Further, McNicholas (2008) noted MTSA requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include security patrols, personnel identification procedures, access control measures, and/or installation of surveillance equipment, etc.

In addition to C-TPAT and MTSA and in order to specifically improve maritime container security, the Security and Accountability for Every Port Act (SAFE Port Act) was enacted in October 2006 and requires, among other things, that the CBP conduct a pilot program to determine the feasibility of scanning 100 percent of U.S.-bound containers (GAO, 2008a, p. 11). However, the ability to scan 100% of all in-bound cargo has been seen as an unattainable goal. Such a justification further reveals the importance of conducive relationships and, ultimately, “total” port security.

One way to initiate a form of total port security is through the articulation of technology. Technology has been described as a force multiplier. Undoubtedly, taking advantage of technology is the quickest and most efficient means possible to facilitate container security. As previously mentioned, subsequent to the terrorist attacks of September 11, 2001 all aspects of port security were under review. The possibility that a WMD would be smuggled into the United

States via cargo containers became more conceivable. The SAFE Port Act signed by President George W. Bush, authorized the development of technology inspection equipment that would enable United States CBP agents to inspect cargo containers for hazardous materials without opening them (Ituh, 2010).

Innovative inspection devices include: CD-2 Human Occupancy Detectors, hand-held Radioactive Isotope Identification Devices (RIID), Radiation Portal Monitors (RPM), truck mounted Mobile VACIS (gamma ray imaging) Inspection Systems, Relocatable VACIS Inspection Systems, and X-ray Imaging Systems (McNicholas, 2008). With such technology at the disposal of facilitators, acquiring an increased level of scans is approachable. Nevertheless, technology is only as effective as the personnel who operate it. More specifically, all of the abovementioned security devices require personnel to review images, drive portable inspection systems, manually scan containers, etc. Therefore, in order to take complete advantage of these security innovations, adequate personnel must be competent and efficient.

In the past, to sufficiently inspect high risk containers, a trained professional would have to physically open the container and spend countless hours conducting a search. For example, it takes five CBP inspectors 3 hours to inspect one TEU (Sweet, 2006). More specifically, if CBP officers inspected every container, shipments would back up and “we would cripple the economy” (Hall, 2006). Therefore, in order to mitigate such inhibitors, ports must exploit technological assets. Moreover, utilizing technology in order to share intelligence would expedite the security process. In an attempt to satisfy this request, the 9/11 Commission (2007) stated a container loaded on a vessel in a foreign port shall not enter the United States unless the container was scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel.

However, in order for such an option to be achieved, a time-efficient inspection process is required. Presently, the ability to inspect 100% containers in a punctual manner has been scrutinized and perceived as an unfeasible goal. Nevertheless, proper use of nonintrusive imaging (NII) techniques allow for a 40-foot container to be completely scanned in approximately 6 seconds (McNicholas, 2008). Identifying equilibrium within the security process that supports technological assets and effectively facilitates global maritime cooperation is the most viable option to acquiring an increased level of container scans/inspections. Bakshi et al. (2009) noted the current inspection plan being advanced by the DHS can handle only a small percentage of the total load, and significant congestion delay will result. Instead, Bakshi et al. (2009) proposed an alternate inspection protocol that emphasizes screening—a rapid primary scan of all containers, followed by a more careful secondary scan of only a few containers that fail the primary test—holds promise as a feasible solution.

In the last decade the container inspection process has received more attention. Yet, the procedure still has major concerns which could hinder the supply chain. In addition, Bakshi et al. (2009) identified three areas of concern: firstly, if there is limited scanning and radiation detection capacity, the delays resulting from waiting in inspection lines could require containers to sit idle at ports for durations that are longer than required in the absence of inspections. Secondly, there could be an adequate level of scanning and radiation capacity but if the nonintrusive imaging (NII) equipment generates more alarms than there is human inspection capacity to resolve, then the result would again be delays as containers wait in inspection lines (Bakshi et al., 2009). Finally, Bakshi et al. (2009) noted, the need to divert containers from their usual movements within port terminals, redirecting them through a centrally-managed government inspection facility, has the potential to engender significant terminal congestion.

Several security techniques have been implemented in order to prevent tampering.

However, these techniques don't have control over containers once they have been loaded onto commercial vessels destined for U.S. ports. Two of the more prominent and successful initiatives, the Secure Freight Initiative (SFI) and the Container Security Initiative (CSI), have been employed at multiple international seaports worldwide. Through CSI, CBP officers work with host customs administrators to establish security criteria for identifying high-risk containers. Those agencies use NII and radiation detection technology to screen high-risk containers before they are shipped to U.S. ports ("Operational Csi Ports," 2006). Furthermore, these security measures have been adopted by several foreign seaports. Some of the ports include: Montreal, Vancouver and Halifax, Canada; Santos, Brazil; Rotterdam, The Netherlands; Bremerhaven and Hamburg, Germany; Colombo, Sri Lanka; Port Salalah, Oman; and Port Qasim, Pakistan ("Operational Csi Ports," 2006). The previous statement is further proof that the recognition of container security has become a pivotal point in maritime transportation.

In addition, the SFI has combined with CSI in the security of containers. It is important for these initiatives to complement one another when employed. Executive Director Allen Gina of CBP explained SFI is a comprehensive model for global supply chain security that enhances security while keeping legitimate trade flowing (Blumenthal, 2007). Furthermore, it leverages information, host country government and trade partnerships, plus the latest technology to validate the security of goods in maritime shipping containers and reduce the risk of terrorism (Blumenthal, 2007).

Ports of Interest

Most ports along the Gulf coast have the tendency to become overshadowed by the larger international ports located on the eastern and western coasts. However, Gulf Coast seaports are

nonetheless vulnerable to the aforementioned threats according to the annual imported TEUs and tonnage figures (Please see Table 1A and 2A located in the Appendices). Most importantly, the expansion of the Panama Canal is to be completed in 2014. Upon this completion, the majority of containers transported to the East and West coasts will no longer be necessary. The widening of the Panama Canal is going to allow for larger ships to transit and deliver more cargo, specifically containers in a capacity that has never been seen at seaports along the Gulf Coast. Without proper security protocol emplaced at seaports located along the Gulf Coast, this increase in commerce could turn out to be a logistical and defensive nightmare. The ports identified include: Port of Galveston, Port of Miami, Port of Houston, Port of New Orleans, Port of Gulfport, Port of Mobile, and the Port of Tampa.

Statement of the Problem

The September 11, 2001 terrorist attacks changed the outlook of the perceived threat on United States soil. As a result, seaports have developed into an important aspect of homeland security. The maritime industry has been an integral factor in the global economy. Without the use of commercial vessels and containerized cargo, the global economy would come to a sudden and unexpected halt. It is conceivable that terrorists would target U.S. seaports in order to cripple our economy. Furthermore, the consensus among security experts is that the most probable way Americans would be targeted by a nuclear weapon would be for al Qaeda or a future adversary to smuggle it into the United States (Flynn, 2008). A Government Accountability Office (2003) study found in May 2002, the estimated costs associated with U.S. port closures resulting from a detonated WMD could amount to \$1 trillion, assuming a prolonged economic slump due to an enduring change in our ability to trade. Given the status of our present economy, such an attack would be devastating.

Additionally, the constant threat of radical Muslim groups who show interest in acquiring WMDs has placed major emphasis on alternative modes of transportation. Many terrorist groups have developed an inexplicable fascination with the aviation industry. This perceived fascination has almost negated the possibility of terroristic sabotage at seaports in the United States. Although there have been no publicized events of terrorist attack within the U.S. seaport community, this does not mean that terrorist activity is absent. However, Al Q'aeda has publicly taken credit for their involvement in the October 2000 bombing of the U.S.S. Cole (Sweet, 2006). Although the bombing of the U.S.S. Cole took place in Yemeni waters at the Port of Aden, this act of terror was a clear indication of their intentions.

Nevertheless, the absence of surmountable attacks at seaports could lead to the belief that terrorist's value and depend on the maritime industry. Therefore it can be argued that any major attack on maritime transportation could eliminate their most successful form of conveyance. More specifically, the commercial shipping of containerized cargo poses as an efficient way for terrorists to infiltrate and smuggle contraband, equipment, and WMD into the United States with virtually no risk of detection. Furthermore, while there have been no known incidents of containers being used to transport WMDs, criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances (GAO, 2008c). It is critical for the seaport community to identify the factors that encourage the tampering of cargo containers.

The security measures implemented at United States seaports are a decisive factor in combating potential terrorist attacks. The regulation and security of seaports is a multi-faceted operation. No single factor will completely neutralize a terrorist threat. Furthermore, with the mass amounts of containers passing through seaports unchecked, there is a seemingly high and

realistic probability that the components capable to improvise a weapon of mass destruction have already slipped through and into the United States without detection.

Many of the containers transported into the United States via the maritime shipping industry, ultimately, pass through seaports without an examination by CBP. CBP officials must be able to balance security and commerce. The balance of the inherent tension between security and commerce is tantamount to success. For example, strict security measures would impede commerce, while less strict security places emphasis on commerce. The latter would, inevitably, make our seaports extremely more vulnerable. One study found, “It would cost a U.S. seaport approximately \$58 billion for a complete shutdown/closure lasting 12 days (“Container Security Initiative,” 2006). Instances such as these can be avoided with an effective approach to container security. However, since an estimated 95 percent of U.S. imports move by sea, the security environment must place a premium on detecting, identifying and tracking terrorist networks with interests in disrupting maritime commerce (GAO, 2009). In order to successfully neutralize the threat of terrorist attacks it is imperative to formulate a layered approach to containerized cargo security transported into United States seaports.

Purpose of the Study

The purpose of this exploratory qualitative study was to analyze and assess maritime security and the perceptions of port deputy director security administrators and USCG officials of United States seaports. The researcher conducted personal interviews of those securing officials. The research questions guiding this study were:

1. What are the main threats to seaports along the Gulf Coast?
2. What is the main threat to containers?

3. How do port security administrators and the USCG perceive containerized cargo threats?

Assumptions and Limitations

The researcher assumed the participants were truthful in their answers. The sample was composed of port deputy directors and USCG. However, in qualitative research, assumptions may also constitute limitations. Even with the absolute certainty in an honest answer, it can not always guarantee the accuracy. There were regulations that attempted to negate this detriment. In addition, this research was limited to telephonic interviews given the geographic restrictions. Furthermore, given the current level of scrutiny the maritime community has received in recent years, there was a possibility that the sample's responses may be biased. The findings should not be subjected to a limited generalization because the participants were all selected from separate ports. The findings should not be deemed representative of the entire population of deputy directors, assistant deputy directors, and port security directors. In addition, given the recent increase in findings pertaining to empirical research, it should not be difficult to accredit previous research.

The method of this study utilized the qualitative research technique. More specifically, the data collection of this study employed in-depth interviews. Boyce and Neale (2006) indicated that "in-depth interviewing is a qualitative research technique that involves conducting intensive individual interviews with a small number of participants to explore their perspectives on a particular idea, program, or situation" (p.3). The population sample of multiple deputy directors was used because their separate and particular perceptions of implemented security measures would provide a more comprehensive answer group. Additionally, the researcher relied on the professional opinions of other researchers who met the criterion for this study.

The researcher attempted to compensate for the potential problems of this study by asking the deputy directors to sign an Informed Consent Form that guaranteed confidentiality and voluntary participation. Moreover, the researcher tape recorded all interviews and transcribed them verbatim. Finally the researcher asked detailed questions, particular to the profession of the participant in order to “explore new issues in depth” and to “provide much more detailed information than what is available through other data collection methods, such as surveys” (Boyce & Neale, 2006, p. 3).

Significance of the Study

The data collected provided the perceptions of port deputy directors regarding implemented security measures at the Port of Galveston, Port of Miami, Port of New Orleans, Port of Gulfport, Port of Mobile, and Port of Tampa. The perceptions of the participants were utilized to develop more effective container security measures at designated seaports. The perceptions of these participants indicated the perceived effectiveness of the implemented container security measures. Lastly, this study contributed to the lack of research pertaining to the perceived effectiveness as it concerns deputy directors. Depending on the findings generated by this study, other significant seaports should be able to apply these findings to current implemented container security techniques.

Definition of Key Terms

The following terms are defined for the purpose of clarification in understanding the study.

Automated Targeting System (ATS). “Program used to assist border inspectors with interdicting illegal drugs and other contraband” (U.S. Congressional Research Service, 2009b, p. 12).

Container. “A metal box, typically 8 ft wide by 8½ ft high by 20 ft or 40 ft long, that can be used on and moved between a tractor-trailer, a rail car, or a ship” (Medalia, 2005, p. 1).

Container Security Device. “Communicate evidence of tampering and the will register every legitimate, as well as unauthorized, opening of the container” (“Container Security Initiative,” 2006, p. 1).

Container Security Initiative (CSI). “The screening of containers that pose a risk for terrorism is accomplished by teams of CBP officials deployed to work in concert with their host nation counterparts” (GAO, 2003, p. 1).

Customs and Border Protection (CBP). “Officials who screen data for all containers” (Medalia, 2005, p. 2).

Customs-Trade Partnership Against Terrorism (C-TPAT). “A joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security” (“Container Security Initiative,” 2006, p. 1).

Deputy Director. “Participates in the development and implementation of the goals and objectives of the unit; formulates policies and goals for, and directs the effective and efficient operation of a major section/division within the unit” (Deputy Director, p. 1).

Freight consolidator. “Consolidates shipments into a complete container, and transports them across the border” (U.S. Congressional Research Service, 2005b, p. 13).

Freight Forwarder. “Transports container to the receiving organization” (Scheiber, 2003, p. 30).

Importer Security Filing (ISF). “Program seeks data on U.S. imported containerized cargo (prior to the loading of this cargo on ships at foreign ports) for 10 additional variables and information on ship stowage plans and container status messages from shipping lines” (Government Accountability Office, 2010).

International Port and Ship Facility Security (ISPS) Code. “The code contains detailed, security-related requirements for governments port authorities and shipping companies in a mandatory section together with a series of guidelines about how to meet these requirements in secondary, non-mandatory section” (Sweet, 2006).

Maritime Security Transportation Act. “Integrates the myriad of federal, state, and local law enforcement agencies tasked with securing the international borders of the United States and its seaports” (Sweet, 2006).

Measure of effectiveness. “The extent and accuracy of the data that supported the operation” (Scheiber, 2003, p. 17).

Megaport Initiative. “A key component of a multi-agency, multilayered, defensive network that strengthens the overall capability of partner countries to deter, detect, and interdict illicit trafficking in special nuclear and other radioactive materials at key international seaports” (U.S. Department of Energy, 2010).

Operation Safe Commerce (OSC). “Was created to provide a test-bed for new security techniques that have the potential to increase the security of container shipments” (CBP, 2002).

Port operations personnel. “Lead official responsible for the security and safety of the vessels and waterways in his or her geographic zone” (U.S. Congressional Research Service, 2005b, p. 14).

Port Security. “Guards containers until another freight forwarder transports it to the receiving organization” (Scheiber, 2003, p. 30).

Qualitative research. “Methods used to understand some social phenomena from the perspectives of those involved, to contextualize issues in their particular socio-cultural-political milieu, and sometimes to transform or change social conditions” (Glesne, 2005, p. 4).

Seaport. “Means all piers, wharves, docks, and similar structures, adjacent to any waters subject to the jurisdiction of the United States, to which a vessel may be secured, including areas of land, water, or land and water under and in immediate proximity to such structures, buildings on or contiguous to such structures, and the equipment and materials on such structures or in such buildings” (U.S. Congressional Research Service, 2005d, p. 29).

Secure Freight Initiative (SFI). “Pilot program to test the feasibility of scanning 100 percent of U.S.-bound container cargo” (Government Accountability Office, 2009, p. 7).

Security and Accountability for Every (SAFE) Port Act. “Authorized the development of high technology inspection equipment that would enable United States CBP agents to inspect cargo containers for dangerous materials without opening them” (Ituh, 2010).

Strategic Trade Corridor Strategy. “One of the two initiatives added to the layered maritime security approach in order to specifically augment SFI” (Government Accountability Office, 2009).

Transportation Worker Information Credential (TWIC). “Program aims to protect the nation’s maritime transportation facilities and vessels by requiring maritime workers to complete background checks and obtain a biometric identification card in order to gain unescorted access to the secure areas of regulated facilities and vessels” (GAO, 2009, p. 7).

Twenty Equivalent Unit (TEU). “The 20-foot container or TEU became the industry standard reference, now cargo volume and vessel capacity are commonly measured in TEU” (World Shipping Council, 2011).

Twenty Four Hour Rule. “Rule that requires manifest and bill of lading information to be submitted to CBP 24 hours in advance of the cargo being loaded on a ship at a foreign port” (Customs and Border Protection, 2006).

Summary

This thesis presents the findings of the researcher as well as relevant and available literature. This study examines the perceptions of deputy directors of operations or security at selected seaports regarding the effectiveness of implemented container security measures. The perceptions of the selected officials were explored to establish similarities and differences in their perceptions.

Chapter 2 provides a review of pertinent literature. The literature review indicated the importance of continuing research regarding the perceived effectiveness of implemented container security measures at designated seaports. Understanding the reasoning behind a successful technique is essential to improving container security.

Chapter 3 contains the methodological design implemented and descriptions of the subjects, instruments, and procedures. The researcher's rationale for selecting a qualitative method was to gather pertinent information by personally interviewing port officials in regards to container security. Further, the study's purpose and research questions are clearly provided for the reader. Chapter 4 presents an analysis of the data gathered from the research and Chapter 5 was devoted to providing conclusions, policy recommendations and suggestions for container security based on the research and findings.

CHAPTER 2: REVIEW OF RELATED LITERATURE

Introduction

According to the Government Accountability Office (2008) study, “while Customs and Border Protection has noted that the likelihood of terrorists smuggling WMDs into the United States in cargo containers is low, the nation’s vulnerability to this activity and the consequences of such an attack are potentially high” (p. 9). Comparatively, “terrorists could use shipping containers or vessels to smuggle personnel and weapons...and if attacks were successful it would not only harm the United States but also disrupt the global economy” (Thibault, Brooks, & Button, 2006, p. 3). There is an interest in protecting seaports in the United States from terrorist attack.

More specifically, terrorist capabilities to exploit containerized cargo to transport weapons of mass destruction (WMDs) are frequently disregarded as a possibility. According to GAO (2008) study, theft and smuggling of weapons-usable nuclear material is not a hypothetical concern, but an ongoing reality: the International Atomic Energy Agency (IAEA) has documented 18 cases of seizures of stolen plutonium or highly enriched uranium (HEU) over the past decade. In addition Ituh (2010) stated, “Container security is not primarily about port security; it is about everywhere security indispensable and ubiquitous, a container is an excellent vector, or carrier, for weapons of mass destructions (WMDs) such as nukes or dirty bombs” (p.48).

The vulnerability of the maritime container transport system could be easily exploited by those who wish to do so. To better illustrate this point CSI (2006) found that on October 18,

2001, port authorities in the southern Italian port of Gioia Tauro discovered a stowaway within a well-appointed shipping container complete with bed, heater, toilet facilities and water.

Furthermore, the man's belongings included a cell phone, a satellite phone, a laptop computer and ominously, given previous events, airport security passes and an airline mechanic's certificate valid for several international airports (CSI, 2006)

The security of seaports is a multi-faceted operation. Additionally, there are several factors that make containerized cargo vulnerable to manipulation. Ergo, there are several security measures that need to be utilized to neutralize each individual threat. The U.S. Congressional Research Service (2005d) stated, "Right now, none of these initiatives has changed the intermodal transportation environment sufficiently to fundamentally reduce the vulnerability of the cargo container as a means of terrorism" (p. 6). The previous statement alludes to the need for a security environment that requires the use of multiple techniques/procedures. Cohen (2005) noted, "There is no way to completely inspect all the millions of containers entering the United States. Given the difficulties of complete inspections, defense needs to be layered, with checks at multiple stages on a container's journey" (p.48).

In regards to the previous statement the Director of DHS, Stephen L. Caldwell, agreed by stating, "CBP has developed a layered security strategy that provides multiple opportunities to mitigate threats and allows CBP to focus its limited resources on cargo containers that are the most likely to pose a risk to the U.S." (GAO, 2008a, p. 7). However, there have been significant and extensive reviews of previous initiatives in order to optimize efficiency. For example, Bakshi, Flynn, and Gans (2009) concluded that a modified-Secure Freight Initiative (SFI)/ "Industry-centric regime" should be able to provide better inspection coverage than CSI at a lower unit cost.

Nonetheless, an international seaport's extreme vulnerability to exploitation leaves major concerns. The sheer magnitude of containers being imported and exported severely complicates the security process. Without the complete cooperation of existing agencies and security affiliates, efficient container security is difficult to maintain. Both governments and shipping lines have long been concerned with the security of the global container supply chain (Thibault et al., 2006). However, due to the lack of manpower and resources, port officials have turned to technology to assist in the inspection of containers.

Security administrators and facilitators alike utilize technologies that have been proven successful on a limited scale. Moreover, most seaports observe the success or failure of competitors and/or partners before making a decision that could affect the input and output of the seaport itself. Many prior studies on the adoption of technology have embraced this perspective (e.g. Loh and Venkatraman, 1992). Comparatively, rational adopters make decisions and choices based on the information that is received via communication and social networks (Rogers, 1995). More specifically, the success or failure of a security technique depends on the perceived effectiveness. In other words, for a security technique to be considered a success, it must first be perceived as a success by those facilitating the technique and, more importantly, by those considering adopting the technique. Lun, Wong, Lai, and Cheng (2008) found that organizations in the container transport chain tend to adopt similar container transport chain management practices as they integrate processes, develop standards, and adopt technology in order to achieve effective communication, quality improvements, and cost reductions to enhance container transport security.

In order to achieve container security on such a large scale, cooperation is a critical factor for all seaports to consider. Lee and Whang (2005) stated, "The risk of a security breach at any one link in the global supply chain could compromise the security of the entire container

transport chain” (p. 21). Banomyong (2005) added, “global economic integration relies upon efficient global supply chains but integration can only succeed if security is a guarantee as there is a relative degree of mistrust among trading nations”(p. 6).

The maritime transport system is faced with numerous threats which have become more sophisticated and dynamic in recent years. Therefore, it should be noted that security threats aren't limited to “terrorism”, but also include stowaways, piracy, drug/ contraband smuggling, cargo tampering, use of the vessel to carry perpetrators and their equipment, and the use of the vessel as a weapon (McNicholas, 2008). Most importantly, all members of the transport system would benefit from a more cooperative and collaborative relationship.

Twenty Equivalent Units (TEUs)

Containerization is one of the single most factors responsible for the high-level of efficiency attributed to modern day commerce. Containers became standardized carriage of freight, starting from the 1950's and really taking hold in the 1960's (“Standard Shipping Container,” 2009). Furthermore, standardization now applies across the global industry, thanks to the work of the International Organization for Standardization (ISO) that in 1961, set standard sizes for all containers (“World Shipping Council,” 2011). Bohlman (2001) illustrated the previous point by stating, “World trade continues to grow and freight containers are, and are expected to remain, the most economical balance between cargo security, transportation costs and speed of delivery for the majority of packaged cargo” (p.13). More specifically, cargo containers accomplished this by initiating standards. Shipping containers by their very nature are ‘Standard’ (“Standard Shipping Container,” 2009).

ISO regulations are very specific and for several reasons. Simply put, containers are designed to carry cargo. However, their design also allows for maximum storage, both for the

cargo inside and for the subsequent placement onboard commercial supply vessels. The design is regulated by the ISO. Container sizes are usually defined by the length e.g. 20ft or 40ft. The second variant is the height, most commonly eight feet six inches but with nine feet six inches becoming more common. The width is generally 8ft but can also be 2.5m (“Standard Shipping Container,” 2009). The length in a twenty equivalent unit (TEU) could vary to 24 or 35 feet and still be expressed as 1 TEU. Further, only the width at 8 feet remains consistent between the various sizes (Shipping Housing Container Guide, 2010). TEUs are the most common and widely used container. The World Shipping Council (WSC) (2011) explained the 20-foot container or TEU became the industry standard reference, now cargo volume and vessel capacity is commonly measured in TEU (Please see Table 3A located in Appendix A). However, recent research has indicated that in the 21st century the 48 and 53 foot containers are more popular for international ocean-going ships (Shipping Housing Container Guide, 2010).

The most significant factor for TEU usage is its ability to circumvent limitations associated with the conveyance procedure. Ocean-going and short sea container vessels have been optimized for their carriage at the standard dimensions in order to facilitate safe and efficient transport. Furthermore, the WSC (2011) noted container sizes must be standardized so that the containers can be efficiently stacked - literally, one on top of the other - and so ships, trains, trucks and cranes at the ports can be specially fitted or built to a single size specification. The standardization of cargo containers made it possible for commercial vessels to transport thousands of TEUs at a time (“World Shipping Council,” 2011). This process is single handedly responsible for the speed of commerce today. Bohlman (2001) illustrated this point by stating “Containerization has reduced the time and cost of moving goods across the oceans to market by 84 % and 35 % respectively” (p. 13).

However, with all the added benefits that come from containerization, vulnerabilities have surfaced. For example, the physical characteristics of a standard TEU do not typically come fitted with sophisticated security deterrents. In most cases, these containers are fashioned with a dual bolts and locking arms that operate as a locking mechanism. Furthermore, it is standard procedure to apply additional locks that can reinforce the existing mechanism. However, most containers are sealed with mechanical bolts that can be cut and replaced or have doors that can be removed by dismantling hinges (Bridis, 2006). These locking mechanisms can be easily defeated with access to simple hardware (e.g. power drill, hack saw, screw driver, etc.). The right door hardware has long been considered the Achilles' heel of oceangoing container security. Several years ago when this method first appeared, the perpetrators would use a steel chisel and hammer to remove the rivet from the door handle ("Cargo Container Vulnerabilities," 2005).

In addition, Bridis (2006) noted that containers could be opened aboard some ships during week long voyages to America. More specifically, due to the time involved in transit (and) the fact that most vessel crew members are foreigners with limited credentialing and vetting, containers are vulnerable to intrusion during the ocean voyage (Bridis, 2006). Exacerbating this concern is the fact that that the sheer volume and the nature of the shipping continuum make marine shipping containers a target for exploitation by terrorists (Customs and Border Protection, 2007).

Threats to Seaport Security

Piracy

Piracy and the repercussions it produces is a major threat to the maritime environment and, particularly, containerized shipping. Identifying this threat is an important step in revising

the current container security framework. Furthermore, understanding the legislation defining piracy will permit administrators to improve and expand current security limitations.

The United Nations Convention on the Law of the Sea (UNCLOS) (1982) stated:

According to article 101 piracy is defined as: “a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State.

b) Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

c) Any act inciting or of intentionally facilitating an act described in subparagraph (a) or (b).” (p. 1)

Similarly, the U.S. Code (2002) defined piracy as, “pursuant to 18 USCS § 1651, whoever, on the high seas, commits the crime of piracy as defined by the law of nations, and is afterwards brought into or found in the United States, shall be imprisoned for life.”

The threat of piracy has received more attention in recent years. However, this problem has frequented the maritime community for centuries. Evans (2004) explained that throughout maritime history, maintaining security onboard vessels at sea and in port along waterfronts has been an ongoing challenge. Additionally, from Blackbeard’s days as the world’s most infamous pirate... to the Straits of Malacca pirates, the maritime environment has always been rife with opportunity for criminals to perform acts of violence and other crimes on the sea (Evans, 2004).

In regards to Somali piracy, Spittle (2011) found, “The predatory pattern evolved from defensive piracy that began early in the last decade as a response by local fishermen to unlicensed foreign trawlers and the dumping of toxic waste” (p.2). Furthermore, many of the

pirates claim to have begun as fishermen and said they were stopping illegal foreign fishing boats from stealing Somali fish (Doyle, 2009). Whatever the reason, piracy has become a ubiquitous threat to containerized cargo and commercial vessels.

According to the International Maritime Bureau (IMB), over 3,300 cases of piracy have occurred since 1993 (Walters, 2007). The aforementioned statement reveals how serious an issue piracy has become. Furthermore, the Gulf of Aden has become an area of increasing concern. However, piracy is a global dilemma. Carafano, Weitz and Andersen's (2009) research concluded that over 10 percent of the global waterborne transportation of oil passes through the Gulf [of Aden]. About 7 percent of the world's maritime commerce transits the Suez Canal. Additionally, about 80 percent of the vessels transiting the Gulf of Aden carry cargo to and from Europe, East Africa, South Asia, and the Far East, although a significant portion of the cargo carried is eventually bound for the United States (Carafano et al., 2009). The waters off the coast of Somalia and the Gulf of Aden are not the only areas conflicted with piracy.

This problem has grown to encompass and threaten many maritime trade corridors around the globe. Walters (2007) stated nine locations represented over two-thirds of the piracy world-wide. Of those, the Gulf of Aden represented only 2%. Whereas, the Malacca Straits represented 11.6% and Indonesia accounted for 28%. Combined, the Malacca Straits and Indonesia generated over 40% of the piracy attacks world-wide (Walters, 2007). Moreover, McNicholas (2008) found that between the years 2002-2007, a total of 63% of the attempted and actual pirate attacks occurred along the coast of Southeast Asia and Africa. Additionally, the coast of Indonesia had the highest number of attacks in 2006 and Nigeria has the third highest number of attacks and the most kidnap victims (McNicholas, 2008).

As a result of this threat, the security of cargo, equipment and personnel has remained a topic of concern. Since the advent of piracy, crew members have been presented with the

obligation of administering security. From a shipboard or seaside viewpoint, the earliest attempts at self-defense against maritime piracy involved arming the crew and defending the ship to the last man (Flynn, 2008). Furthermore, regardless of the port state's ability to maintain coastal and port security, ship owners and vessel operators considered the defense of the ship and the safety of the cargo to be the responsibility of the shipmaster and crew (Flynn, 2008). The International Chamber of Commerce (ICC) (2011) explained that before 1992, shipmasters and ship operators had nowhere to turn to when their ships were attacked, robbed or hijacked either in port or out at sea. More surprisingly, local law enforcement either turned a deaf ear, or chose to ignore that there was a serious problem in their waters. This lapse in vessel security, eventually, generated enough attention to get international authorities involved.

The International Chamber of Commerce (2011) stated the ICC International Maritime Bureau (IMB) is a specialized division of the ICC. IMB's main task is to protect the integrity of international trade by seeking out fraud and malpractice. More specifically, concerned at the alarming growth in the phenomenon, this led to the creation of the IMB Piracy Reporting Centre in 1992 (ICC, 2011). The Centre is based in Kuala Lumpur, Malaysia. It maintains a round-the-clock watch on the world's shipping lanes, reporting pirate attacks to local law enforcement and issuing warnings about piracy hotspots to shipping (ICC, 2011).

Moreover, the IMB has separated piracy attacks into three categories: 1) low-level armed robbery, 2) medium-level armed robbery, and 3) major criminal hijacks (Chalk, 2008). According to Chalk (2008) low level armed robbery attacks are anchorage attacks mounted against ships at harbor. Furthermore, the "low level" attack was characterized as opportunist attacks mounted close to land by small, high-speed craft crewed by maritime "muggers" normally armed with knives (Chalk, 2008). Their purpose is typically to seize cash and portable high-value personal items with an average haul of \$5,000–\$15,000. Whereas, medium-level

armed robberies are represented by violent thefts involving serious injury or murder by well-organized gangs who usually operate from a “mother ship” and are equipped with modern weaponry (Chalk, 2008). Finally, major criminal hijacks are well-resourced and meticulously planned, employing highly trained and heavily armed syndicates working in conjunction with land-based operatives and brokers (Chalk, 2008). Most piracy incidents that reach the media’s attention illustrate the more detrimental or major criminal degree of hijacking. However, it should be understood that the majority of piracy attacks remain unpublicized.

Still, Chalk (2008) explained when a major criminal hijack occurs a vessel will first be seized and its cargo offloaded at sea. The ships are then renamed and reregistered under flags of convenience and issued with false documentation to enable them to take on fresh payloads. In addition, Chalk (2008) noted the new cargo, which is never delivered to its intended destination, is taken to a designated port where it is sold to a buyer who is often a willing participant in the venture. The latter represents the most significant and challenging threat to deter. According to IMB data, Somali pirates hold 33 vessels and 758 hostages (Spittle, 2011). In addition, in January alone the bureau recorded 35 attacks, claiming seven ships along with 148 new hostages (Spittle, 2011).

Surprisingly, even with aforementioned accumulated losses, some ship owners are apprehensive to ask for assistance. Officials with the IMB in Kuala Lumpur assert that most ship owners are reluctant to alert authorities about attacks on their vessels, largely because subsequent investigations and delays result in costs that the ship companies themselves must bear (Chalk, 2008). With annual piracy estimates ranging between \$5 billion and \$7 billion, some ship companies would rather take the risk of an attack than add to the surmountable deficit (Spittle, 2011). Furthermore, exacerbating this reluctance is the fear that reporting incidents will merely raise maritime insurance premiums by forcing owner-operators to acknowledge that they were

not practicing basic security measures (Chalk, 2008). In some instances, these anti-piracy security costs equate to a higher cost than an actual attack. Additionally, Chalk (2008) found that the combined magnitude of losses associated with reporting incidents would, in most cases, greatly outweigh those resulting from a piracy attack; in instances of low-level theft, ransacking, and hostage taking. More specifically, costs tend to represent only two to ten percent of the value of the targeted boat and its cargo (Chalk, 2008).

The Piracy Reporting Centre (PRC) division of the IMB uses a two-pronged approach in order to mitigate these challenges. This objective targets those individuals who are most likely to be affected if attacked (i.e. ship-owners, ship master, insurance companies, etc.).

The International Chamber of Commerce (2011) stated:

The main function of the PRC is two fold: 1) To be the single point of contact for ship Masters anywhere in the world who are under piratical or armed robbery attack. The information received from the Masters is immediately relayed to the local law enforcement agencies requesting assistance. 2) The information received from the ship Masters is immediately broadcast to all vessels in the Ocean region - thus high-lighting the threat to a Master enroute into the area of risk. (p. 2)

Even with the staggering number of piracy cases in the past twenty years, there have been two significant maritime events, in particular, that demonstrated the vulnerability of ships at sea and caught the attention of the world through close media coverage: the hijackings of the *Santa Maria* and the *Achille Lauro* (Flynn, 2008). In regards to the *Santa Maria*, Chalk (2008) explained in 1961, the *Santa Maria*, a 21,000-ton cruise ship was hijacked by a group of 70 men led by Captain Henriques Galvao (a Portuguese political exile) to bring global attention to the Estado Novo in Portugal and fascist regime in Spain (p.48).

Also, in 1985, The *Achille Lauro*, another cruise ship, was hijacked by the Palestinian Liberation Organization (PLO) in an attempt to obtain the release of 50 fellow incarcerated terrorists being held in Israel. The attempt was unsuccessful and one American citizen was, inevitably, killed (Walters, 2007). However, it should be mentioned that prior to the IMB definition of piracy in 2005, the hijackings of the Santa Maria (political protest) and the Achille Lauro (terrorism) were not considered piracy (Chalk, 2008). In support, Walters's (2007) found, "According to the political offenses exemption exception, piracy must be initiated for "private ends" such as personal profit to be considered piracy."

Therefore, the IMB (2005) created its own working definition: "An act of boarding or attempting to board any ship with the apparent intent to commit theft or any other crime and with the apparent intent or capability to use force in the furtherance of that act" (p.1). This definition successfully jettisons any exception or requirement that would allow piracy to evade jurisdiction (Walters, 2007). Nevertheless, these hijackings accurately revealed the vulnerability facing commercial shipping liners in the current maritime environment. Moreover, with maritime commercial vessels transiting trade corridors with nearly 90% of the world's cargo, there are countless targets for criminals and terrorists to target.

Types of Vessels Being Targeted by Terrorists

More recently, terrorists have shifted their focus to commercial vessels and the cargo being transported. Piracy affiliates are cognizant of the value that can be associated with such vessels. McNicholas (2008) noted that, "A freighter is a general term encompassing a wide variety of oceangoing ships. However, currently, few conventional freighters remain in service. Instead, specialized ships are built for particular trades (McNicholas, 2008). Most ships can be classified into three categories: bulk dry carriers, container ships and oil tankers. Furthermore,

these three categories do not only differ in the ships' physical characteristics, but also in their mobility patterns and networks (Kaluza, Kolzsch, Gastner & Blasius, 2010). Therefore, with general knowledge criminals, terrorists, and pirates can pick and choose their targets depending on their intentions.

For example, bulk carriers are designed to carry one type of cargo at a time. Products include fertilizers, iron ore, coal, and grain (McNicholas, 2008). Additionally, tankers carry just one type of cargo—crude oil (McNicholas, 2008). Liquefied natural gas (LNG) tankers transport natural gas, and while this would seem a natural target for terrorists, the ship's outer hull, ballast tanks, void space and pressurized tanks are built from stainless steel, making it very difficult to penetrate (McNicholas 2008). Finally, chemical tankers carry many different grades of petroleum and liquid chemical cargo (McNicholas, 2008). Moreover, the Coast Guard considers cruise ships to be highly attractive targets to terrorists and cruise ships can represent high-prestige symbolic targets for terrorists (GAO, 2010c).

Pirates have started targeting container ships and tankers in recent years (Carafano et al., 2009). Their reasons for targeting such vessels remain undetermined. However, it can be deduced that container ships and tankers represent the more vulnerable of the types of vessels. Moreover, GAO (2007b) noted, our nation's economy and security are heavily dependent on oil, natural gas, and other energy commodities of which nearly half of the nation's oil is transported from overseas by tankers. This type of ship could be a target for terrorist activities due to its slow speed and low freeboard—the distance from the water line to the main deck—which may permit easier boarding from a smaller vessel (McNicholas, 2008). In addition, container ships follow regularly repeating paths whereas bulk dry carriers and oil tankers move less predictably between ports (Kaluza et al., 2010). Furthermore, John Pike of Global Security stated the cargo ship *Maersk Alabama* was attacked by pirates early on the morning of April 8, 2009

and presumed hijacked. More specifically, the vessel was en route to Mombasa, Kenya, when it was assaulted about 300 miles off Somalia's coast (“Maersk A-Class,” 2011). The previous statement demonstrates the growing audacity hijackers.

According to the IMB, 30 percent (490 of 1,650) of vessels reporting pirate attacks worldwide from 2006 through 2010 were identified as tankers (GAO, 2011). The vast areas at risk for piracy off the Horn of Africa, combined with the small number of military ships available for patrolling them, make protecting energy tankers difficult (GAO, 2007b). Additionally, GAO’s (2011) research found that, “Pirate attacks on energy tankers have tripled in the last five years. From January to June in 2011, 100 tankers were attacked, a 37 percent increase from 2010.” Given the U.S.’s dependence on oil and other energy sustaining substances, the increase in attacks on tankers could be interpreted as a direct attempt to harm the U.S. economy. In comparison, Spittle (2011) stated, “In early 2010 *Maran Centaurus*, a Greek-owned tanker was reported to have fetched between \$5.5 million and \$7 million after being held for 50 days” (p.3). Additionally, in November (2010) last year a South Korean oil tanker, the *Samho Dream*, captured in April, set a new record when it was released after a payment of \$9.5 million (Spittle, 2011).

However, McNicholas (2008) explained, “Attacks on bulk carriers (ships specifically designed to transport unpackaged bulk such as grain, oil, etc.) from 1995 to 2006 show that these types of ships are the clear favorite targets, accounting for 60% of all ships attacked” (p.38). Nevertheless, from a security standpoint, this carrier would be considered as one of the last types of vessels that a terrorist would use to carry out a hostile mission (McNicholas, 2008, p.38).

In contrast, over 9 million passengers departed from U.S. ports on cruise ships in 2008, and according to agency officials, cruise ships are attractive terrorist targets (GAO, 2010c). Terrorists could emplace and detonate an improvised explosive device (IED) inside a cruise ship

compartment killing hundreds or thousands of innocent victims. For this reason, a cruise ship could be viewed as a high value target for terrorists. As mentioned previously, the hijacking of the cruise ship Achille Lauro and killing of passenger Leon Klinghoffer by terrorists in 1985 was a watershed event for the cruise industry, leading to major changes in cruise line security procedures (GAO, 2007b).

Nevertheless, in 2006, worldwide reported attacks against ships decreased from 276 to 239 (McNicholas, 2008). This decline in incidents is probably attributed to proactive measures taken by ship crews at designated hotspot areas and the heightened presence of naval forces in these areas (McNicholas, 2008). However, Erik Rabjerg Nielsen, the director and head of operations and deployment for Maersk Line stated, “In 2010 one hijacking attempt was registered every six days, and in 2011 there’s been a large increase in the activity. The problem has never been larger than right now” (Pelton, 2011).

However, Carafano et al. (2009) found, “In 2007, 53 container cargo ships were attacked transiting the Gulf of Aden, compared to 52 chemical tankers. Additionally, McNicholas (2008) stated, “From a security perspective, container ships pose perhaps the greatest threat because the majority of them maintain an advertised, published, tight schedule” (p.39). Furthermore, this presents a large opportunity for criminal or terrorist entities to ship explosives, persons, or equipment, via containers (McNicholas, 2008).

There are numerous counter piracy measures being utilized throughout the world. Spittle (2011) states Operation Atalanta, the European Union (EU) contingent for counter piracy, which was originally created mainly to protect the United Nation’s World Food Program shipments to Somalia, but has expanded to take on a general anti-piracy role. Another contingent, Operation Ocean Shield, a North Atlantic Treaty Organization (NATO) standing maritime group with a similar remit to the EU force and with overlapping national contributions has a presence in high

risk shipping corridors. In addition, the U.S. contributed additional naval forces as part of the multinational anti-piracy effort, Combined Task Force 151 (CTF 151) (Carafano et al., 2011). Still, other nations participating in anti-piracy operations include Great Britain, Germany, France, Denmark, Greece, Italy, Turkey, Russia, Pakistan, India, Malaysia, China and Saudi Arabia. In 2009, about 20 naval ships patrolled the waters in and around the Gulf of Aden (Carafano et al., 2011). This effort represents global collaboration toward a shared threat. If this same view was accepted by the global community in regards to container security much could be accomplished (See Table 4A located in the Appendices).

Organized Crime/Terrorism

The nexus between piracy and organized crime has become clear over the past 10 years, and the thin line between certain incidents of piracy and terrorism has become increasingly blurred (McNicholas, 2008). Somali terrorist organizations operating off the Horn of Africa such as Al-Shabab have taken notice to the advantages of manipulating the maritime supply chain. Carafano et al. (2009) stated Al-Shabab benefits from the pirate activities in several ways. Pirates are used to smuggle goods and weapons from Yemen to Somalia. In addition, there are documented cases where pirates have transported foreign fighters into the country, and terrorists out, including one of the perpetrators on a bombing in Yemen in March 2009 that killed four South Korean tourists (Carafano et al., 2009). GAO (2008a) supported Carafano et al.'s previous statements by explaining while there have been no known incidents of containers being used to transport WMDs, criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances. Therefore, it is not unlikely that terrorist organizations would exploit the container conveyance system in a similar manner.

More specifically, some reports suggest that pirates have been helping train and equip the militias so that they can expand Islamist control over the Somali coastal waters (Carafano et al., 2009). Furthermore, McNicholas (2008) stated “The Free Aceh Movement, a separatist group which—according to research conducted at the Singapore-based Institute of Defense and Strategic Studies—utilizes piracy to fund its fight against the Indonesian government” (p. 171). On the other hand, Walters (2007) stated that, “organized crime syndicates are also busily engaged in the business of piracy. More importantly, Gottschalk and Flanagan (2000) found that Southeast Asia and South America seem particularly prone to this type of piracy. Organized crime affiliates and terrorists have come to realize that this industry can be exploited more efficiently with a cooperative agreement.

In comparison, Carafano et al. (2009) found, “Ransom and increased security costs in the Gulf of Aden total less than a billion dollars a year. Pirate attacks affect a small fraction of the ships transiting the gulf.” Whereas, the U.S. confronts transnational criminal cartels that smuggle guns, drugs, people, and money as part of a \$25-billion-a-year enterprise that threatens U.S. sovereignty and directly affects many citizens in the U.S. and Mexico (Carafano et al., 2009). Furthermore, Mayhew (2001) stated, “Worldwide, cargo losses have been estimated at \$30 billion a year, and the incidence is probably increasing. Organized crime is responsible for nearly half of these losses.” Publicover (1999) added, “Transnational criminal operations use the entire international shipping cycle, in particular, the maritime and trucking transportation shipping system and the freight forwarding sector, to support stolen merchandise trafficking.” Containerization played a critical role in improving the shipping process and, inevitably, the entire flow of commerce world-wide. However, this revolution has negative side effects that continue to aggravate the maritime community.

Container Theft

Containerization has played a pivotal role in modern day commerce efficiency. However, Publicover's (1999) research found, "The "container revolution" which has increased transportation efficiency and spawned the rapidly growing intermodal freight transportation industry, may have inadvertently encouraged organized criminal presence in freight transportation" (p.8). The previous statement must be considered as a viable explanation for the perpetual existence of container theft. Publicover (1999) adds, before cargo was containerized "break-bulk" (goods that must be loaded individually) was extremely vulnerable to theft at all points within the global supply chain, especially off-loading. Mayhew (2001) supported Publicover's claim by stating, "Cargo is particularly vulnerable while in the process of being loaded or unloaded from trucks, or through documentary fraud.

Still, containers not only revolutionized shipping but also served as a security mechanism for cargo. When first introduced, containers successfully reduced pilferage. Estimates indicated that during the early years of the container revolution, theft of containerized cargo dropped to less than a tenth of a percent (Publicover, 1999). Nevertheless, after the initial honeymoon period during which criminals adjusted to the new container system, other patterns of theft developed (Publicover, 1999). For example, Mayhew (2001) found that organized crime gangs involved in drug smuggling or illicit arms shipments may hide items on vessels or in listed cargo that is later stolen. More specifically, containers stored in terminals could now be stolen as a whole, opened and made subject to pilferage, or serve as a conduit for drug smuggling (Publicover, 1999).

Furthermore, large-scale theft at freight forwarding yards frequently follows collusion between a truck driver and a warehouse employee, with between 80 and 99 percent of cargo thefts, in the United States and Australia, involving employees in one way or another (Atkinson 2001; Ackerman 1997). Similar behavior could be present in freight forwarders and other

personnel associated with the loading and off-loading of containers. Comparatively, Publicover (1999) found that, “Criminals act with apparent information about cargo manifests, suggesting that collusion is occurring with transportation employees. However, Atkinson (2001) stated, “While lone employees have been historically responsible for most cargo theft, crime syndicates pose an increasing threat. Surprisingly, Mayhew (2001) found, “Under-reporting is widespread as freight-forwarders may prefer to protect their supply of customers and fear bad publicity.”

In order to mitigate these challenges Mayhew (2001) explained, “Security and customs authorities should be aware of all vessel movements, have up-to-date detailed cargo information (destination, consignees, special handling) and be alert to unusual documents because discrepancies may indicate illegal activity”(p. 5). However, it is increasingly more difficult to deter. Estimates indicate that well over 80 percent of all theft and pilferage of transportation cargo is accomplished by, with the collusion of, persons whose employment entitles them access to the cargo that is stolen (Publicover, 1999).

Stowaways

According to the International Maritime Organization (IMO) a stowaway is defined as a person who hides aboard a ship, airplane, etc. to get free passage, evade port officials, etc (“International Convention for,” 2011). Stowaways are generally regarded as a low-level threat. McNicholas (2008) explains, “The overwhelming majority of stowaways are looking for economic opportunity and a better life for themselves and probably their families” (p.173). Nevertheless, the threat stowaways pose to security should not be overlooked. In 2002, reports surfaced that a group of twenty-five Islamic extremists had entered the U.S. by stowing away in shipping containers (Booth & Altenbrun, 2002). More specifically, these extremists were

believed to enter through ports in Florida, Georgia, and California (Booth & Altenbrun, 2002). That being said, this threat should be regarded as probable and dangerous.

However, the ensuing legislation makes dealing with such problems complicated. The standards and recommended practices for stowaways reflect the Guidelines on the Allocation of Responsibilities to Seek the Successful Resolution of Stowaway Cases (Resolution A.871 (20)), adopted in 1997, which established basic principles to be applied in dealing with stowaways (“International Convention for,” 2011). However, Booth and Altenbrun (2002) stated, “United States law relating to stowaways is contained primarily in the Immigration and Naturalization Act (INA)” (p.44). And within this law it states that stowaways do not have a right to Immigration and Naturalization Services (INS) hearing and are subject to immediate removal from the U.S. (Booth & Altenbrun, 2002).

In addition, the guidelines in the Allocation of Responsibilities to Seek the Successful Resolution of Stowaway Cases states that the resolution of stowaway cases is difficult because of different national legislation in the various countries involved (“International Convention for,” 2011). Booth and Altenbrun (2002) agreed with the IMO’s claim stating, “Since the U.S. is a signatory of the 1967 Protocol Relating to the Status of Refugees, and they are subject to the enforcement of the 1951 Convention, which prohibits a state from expelling or returning a refugee to a territory” (p. 44). More specifically, the 1951 Convention explains expulsion of a refugee is prohibited to a place “where his/her life of freedom would be threatened on his race, religion, nationality, membership of a particular social group or political opinion” (p.44).

To mitigate complications such as the aforementioned, the IMO guidelines advocate close co-operation between ship-owners and port authorities (“International Convention for,” 2011). One such example is the INA’s establishment a financial burden on any ship owner which transports a stowaway, including a \$3,000 fine for any stowaway who escapes ashore (Booth &

Altenburn, 2002). In comparison, the IMO guidelines say that every effort should be made to avoid situations where a stowaway has to be detained on board a ship indefinitely (“International Convention for,” 2011).

However, the guidelines and legislation do not just affect the ship-owner. These stipulations recommend that a much more elaborate investigation be conducted.

The “International Convention for” (2011) stated

The guidelines then go on to establish in greater detail the responsibilities of the master, of the ship-owner or operator, of the country of the first scheduled port of call after the discovery of the stowaway (the port of disembarkation), of the country where the stowaway first boarded the ship, of the stowaway's apparent or claimed country of nationality, of the flag State of the vessel, and of any countries of transit during repatriation. (p. 2)

The intricacies of this process discourage ship owner and operator cooperation. Nevertheless, strict guidelines are inherent in order to maintain a thorough process that is accommodating to the stowaway and, in addition, to the ship owner and operator. Finally, in 1998, the Facilitation Committee issued a Circular inviting IMO Member Governments and international organizations in consultative status to provide the Organization with information on stowaway incidents (“International Convention for,” 2011). More importantly, this process diverts administrators and other personnel from more significant issues.

The majority of stowaway incidents is actually organized human smuggling operations and managed by local or transnational human trafficking organizations (McNicholas, 2008). The aforementioned statement represents a small portion of organized crimes’ broadening scope. These organizations have an infrastructure within the port and contacts developed within the port entities, such as port police, stevedores, local security guards deployed onboard the ship,

container and seal checkers, etc (McNicholas, 2008). In addition McNicholas's (2008) research found in poor countries—such as Colombia, Ecuador, Haiti, Honduras, and Dominican Republic—a port security guard makes his “real” pay collecting bribes and generally must pay his supervisor for the opportunity to be positioned closer to the dock. McNicholas (2008) further explained, “Being positioned closer to the dock puts personnel in a more opportune position to collect larger and more frequent bribes” (p.174). With a lack of integrity absent in ports such as the aforementioned, deterrence becomes less probable.

The previous threats represent the multiple approaches available to those aspiring to infiltrate and exploit containerized cargo. More so, this myriad of threats makes facilitating an effective security fabric complicated. Therefore, this responsibility is shared between a collection of agencies. Now, while there are some agencies that carry most of the burden, additional agencies frequently cooperate.

Agencies Responsible for Security

United States Coast Guard (USCG)/Customs Border Protection (CBP)

The two main agencies responsible for maritime security are the U.S. Coast Guard and Customs and Border Protection. A key challenge for U.S. security analysts and policy makers is prioritizing the nation's maritime security activities among a virtually unlimited number of potential attack scenarios (U.S. Congressional Research Service, 2007). The USCG is responsible for protecting, among other things, U.S. economic and security interests in any maritime region (GAO, 2010a). Whereas, U.S. CBP is responsible for keeping terrorists and their weapons out of the United States, securing and facilitating trade, and cargo container security (GAO, 2010a). However, Wright (2007) found that as the significance of port security increases,

so does the involvement of local, state and federal law enforcement agencies. U.S. Congressional Research Service (2007) supported Wright’s claim by stating, “The USCG, the U.S. Navy, and other federal agencies conduct ongoing port security training exercises domestically and overseas” (p.8).

However, the USCG and CBP do have limitations. GAO (2011) noted the Coast Guard is limited in the degree to which it can bring about improvements abroad when security is substandard, in part because its activities are limited by conditions set by host nations. In comparison, in October 2007, Coast Guard officials stated that there is reluctance by certain countries to allow the Coast Guard to visit their ports due to concerns over sovereignty. Also, the Coast Guard lacks the resources to assist poorer countries (GAO, 2010a). Therefore, in order to mitigate these challenges GAO (2010c) explained that officials have worked with other federal agencies and international organizations to secure funding for training and assistance to countries that need to strengthen port security efforts.

Additionally, GAO (2010c) stated that CBP has made progress in working with the SFI ports to scan U.S.-bound cargo containers; but because of challenges implementing scanning operations, such as equipment breakdowns, the feasibility of scanning 100 percent of U.S.-bound cargo containers remains largely unproven. This statement hinders the supportive nature that is needed in order to overcome 100% scans and similar obstacles.

Seaports of the Study

Port of Tampa, Florida

An economic impact study, based on 2005 activity, concluded that the Port of Tampa impacted virtually all industries in the Tampa Bay region (“Tampa Port Authority,” 2011). The

port contributes nearly \$8 billion to Tampa Bay's economy and is responsible for almost 100,000 direct and indirect jobs ("Tampa Port Authority," 2011). In 2009, the Port of Tampa handled 36,703,639 short tons of cargo along with 48,788 TEUs ("Tampa Port Authority," 2011). The Port of Tampa is Florida's largest port and largest cargo tonnage port ("Tampa Port Authority," 2011). In addition, the Port of Tampa is one of the world's largest premier fertilizer ports ("Tampa Port Authority," 2011).

Port of Mobile, Alabama

The port of Mobile is the only deep-water port in Alabama, and was the 9th largest by tonnage in the nation in 2008. In 2010, the port of Mobile handled 23.4 million tons of cargo ("Alabama State Port," 2011). In addition, the port of Mobile dealt with 120,603 TEUs. The Port of Mobile imports: Heavy Lift & Oversized Cargo, Containers Coal, Aluminum, Iron, Steel, Copper, Lumber, Wood pulp, Plywood, Fence Posts, Veneers, Roll and Cut Paper, Cement, and Chemicals ("Alabama State Port," 2011). Exports: Heavy Lift & Oversized Cargo, Containers Coal, Lumber, Plywood, Wood pulp, OSB, Laminate, Flooring, Roll and Cut Paper, Iron, Steel, Frozen Poultry, Soybeans, and Chemicals ("Alabama State Port," 2011). The port encompasses approximately 4 million square feet ("Alabama State Port," 2011).

Port of Gulfport, Mississippi

The Port of Gulfport has gained a solid reputation as the second largest importer of green fruit in the United States and the 3rd busiest container port on the US Gulf of Mexico ("Mississippi State Port," 2011). In 2009, the port handled over 2 million tons of cargo, 198,900 TEU's and 235 ships. In addition the Port of Gulfport is a bulk, break-bulk and container seaport

which encompasses 204 acres, has nearly 6,000 feet of berthing space and averages over 2 million tons of cargo a year shipping over 200,000 TEU'S ("Mississippi State Port," 2011).

Port of New Orleans, Louisiana

The Port of New Orleans is at the center of the world's busiest port complex – Louisiana's Lower Mississippi River ("Port of New," 2011). Its proximity to the American Midwest via a 14,500-mile inland waterway system, six Class 1 railroads and the interstate highway system makes New Orleans the port of choice for the movement of cargoes such as steel, rubber, coffee, containers and manufactured goods ("Port of New," 2011). The Port's general cargo volume has averaged 8.6 million tons from 2003 through 2007 ("Port of New," 2011).

Port of Galveston, Texas

In 2009, the Port of Galveston handled only 11,108 TEUs and almost 5,849,777 short tons of cargo ("Port of Galveston," 2011). Furthermore, the Port of Galveston received 788,931 cruise ship passengers ("Port of Galveston," 2011). Also, in 2009, their largest import was grains totaling 3,037,793 short tons ("Port of Galveston," 2011).

Port of Miami, Florida

Cargo destined for more than 100 countries and 250 ports around the world flow through the Port of Miami ("Port of Miami," 2010). In 2007, imports totaled some 4.37 million tons and exports were 3.46 million tons, totaling 7.84 million annual tons ("Port of Miami," 2010). Among the Port's top trading partners, China ranked highest for the second year in a row ("Port of Miami," 2010). Due to its strategic location, last year the port included among its top ten

trading partners countries from the Far East, South and Central America, Europe and the Caribbean (“Port of Miami,” 2010).

Port of Houston, Texas

The Port of Houston is a 25-mile-long complex of diversified public and private facilities located just a few hours' sailing time from the Gulf of Mexico (“Port of Houston,” 2011). The port is ranked first in the United States in foreign waterborne tonnage (14 consecutive years); first in U.S. imports (19 consecutive years); second in U.S. export tonnage and second in the U.S. in total tonnage (19 consecutive years) (“Port of Houston,” 2011). More than 220 million tons of cargo moved through the Port of Houston in 2009 (“Port of Houston,” 2011).

Port of Corpus Christi

Strategically located on the western Gulf of Mexico, Port Corpus Christi is the sixth largest port in the United States in total tonnage (“Port of Corpus,” 2009). With a straight, 45' deep channel, the Port provides quick access to the Gulf, the United States inland waterway system and the world beyond (“Port of Corpus,” 2009). The Port delivers outstanding access to overland transportation with on-site and direct connections to three Class I railroads and uncongested interstate and state highways (“Port of Corpus,” 2009). The Port is protected by a state-of-the-art security department and an award-winning Environmental Management System.

Implemented Security Measures

Operation Safe Commerce (OSC)

Officials responsible for security at U.S. seaports have come to the conclusion that attaining 100% scans of inbound containers is a formidable objective to achieve. Senator Pat Murray, founder of OSC illustrated this by stating, “Container traffic is critical to the health of our economy, but we do not know enough about what is in the more than 6 million containers that enter our nation each year” (Customs Border Protection, 2002, p. 1). This awareness has led to the belief that container security can be accomplished with the use and implementation of contemporary technological assets. In 2002, OSC was created to provide a test-bed for new security techniques that have the potential to increase the security of container shipments (CBP, 2002).

In comparison Mullet, Palma, Seneviratne and Rodriguez (2004) noted, OSC is a federally funded TSA project and collaborative effort between the federal government, business interests, and the maritime industry to develop and share the best practices for the safe and expeditious movement of containerized cargo. Initially, Congress provided \$28 million in funding for OSC to improve the security of container shipments through pilot projects involving the United States' three largest container ports of entry (Los Angeles/Long Beach, New York/New Jersey, and Seattle/Tacoma) (CBP, 2002). Combined, these ports are believed to receive the majority of containers that enter United States seaports.

A modern approach to accomplish the objectives described in OSC is for seaports to move away from primary reliance on a system of control at the borders that lie within U.S. jurisdiction and toward point-of-origin controls (National Research Council, 2003). More specifically, point-of-origin controls are to be supported by controls developed within

international supply chains and accompanied by a concentric series of checks built into the system at points of transshipment and at points of arrival (National Research Council, 2003). In comparison, the OSC program initiated at the Ports of Tacoma and Seattle in 2004 noted that with all the benefits, port officials found that no single project has defined the ultimate solution (Department of Homeland Security, 2005). Instead, container security will require a layered approach in order to be successful (Department of Homeland Security, 2005). The foundation of OSC takes a partnership approach to developing innovative new ways for ports to track and protect cargo entering the United States from all over the world (Department of Homeland Security, 2005). It is critical for the U.S. to demonstrate due diligence, before a global partnership is attainable. The National Research Council (2003) noted the United States' world trade partners will expect reciprocity and controls on U.S. exports to aid the security of their imports.

In 2005, The U.S. *Office for Domestic Preparedness* awarded the ports of Los Angeles and Long Beach an additional \$6.9 million for OSC Phase III ("Operation Safe Commerce," 2005). Phase III goals included: maintaining and communicating accurate data on cargo; verifying that empty containers have not been tampered with before being loaded; verifying that cargo loaded into containers are absent threat items; verifying that the integrity of containers is not breached in transit ("Operation Safe Commerce," 2005). This program was able to make accurate assessments pertaining to container security and provided valuable recommendations that acted as a rubric for subsequent initiatives to follow. The Maritime Commerce Security Plan noted OSC has allowed us to understand better the complexity of supply chain security from origin to destination, the impact of security technologies and business practices on supply chains, and the limits of current technology ("Operation Safe Commerce," 2005). However, due to the

lack of detailed information regarding current status, it seems that OSC has dissolved into subsequent initiatives.

Container Security Initiative (CSI)

The primary purpose of CSI is to protect the global trading system and the trade lanes between CSI ports and the United States (U.S. Customs and Border Protection, 2008). In addition, Banomyong (2005) agreed, “The purpose of the Container Security Initiative (CSI) is to secure what is believed to be the most vulnerable but indispensable link in the global supply chain: the ocean going container.”

U.S. Customs and Border Protection (2008) list the 3 core elements as follows:

- 1) Identify high-risk containers. CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence.
- 2) Prescreen and evaluate containers before they are shipped. Containers are screened as early in the supply chain as possible, generally at the port of departure.
- 3) Use technology to prescreen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade. This technology includes large-scale X-ray and gamma ray machines and radiation detection devices. (p. 1)

Depending on where you look, there is also a fourth core element: the use of smarter, tamper evident containers (“Encyclopedia: Container Security,” 2006, p. 1). However, this element has been suspended indefinitely due to certain economic factors, most notably the lack of federal funding. CSI was manifested with the specific intention of utilizing United States customs officials. Under the Container Security Initiative (CSI), a team of CBP officers is deployed to work with host nation counterparts to target all containers that pose a potential threat (CBP,

2008, p. 1). In comparison, GAO (2009a) stated, this program was attempting to further the borders of the United States. Furthermore, by dispensing officials to cooperating seaports around the globe, the U.S. government could adequately expedite the inspection process and, in turn, alleviate prospective interference with the economy (GAO, 2009a).

More specifically, depending on the distance to be traveled, every cargo container is subjected to and exposed at several links in the supply chain. The risk of a security breach at any one of the nodes or links can compromise the security of the entire container transport chain (Lee & Whang, 2005). In order to mitigate this risk, Sweet (2006) stated, “CSI asks companies to implement automated data screening prior to loading the containers and the manifest rule requires that manifest data be submitted to U.S. Customs at least 24 hours before loading of cargo in transit to the United States” (p. 174).

The utilization of a “no later than” policy ensures that the officials will designate a pre-determined amount of time to conduct pre-screening. However, given the significant amount of cargo containers imported daily, it still seems that more time is needed in order to adequately pre-screen all containers before their arrival. Furthermore, United States Congress (2006) passed the SAFE Port Act on September 29, 2006, which added strength to CSI by mandating incoming cargo to U.S. ports will contain data elements from both the shipper and the carrier. Additionally, Bakshi, Flynn and Gans (2009) stated “The program [Automated Targeting System], announced in January 2002, uses rules-based software to identify containers bound for the US that are at “risk” of being tampered with by terrorists. This software takes intelligence gathered by CBP officials and, sequentially, produces a “score” that determines the probability of a container transporting contraband. Bakshi et al. (2009) found, a key input to this system is the container's shipping manifest, which contains information about the container's sender, recipient, and contents. Additionally, once transmitted, manifests are analyzed at CBP's National Targeting

Center in Arlington, Virginia, and containers that are identified as suspect are flagged to be inspected by the local customs authority at the port or origin, before they are shipped to U.S. ports (Bakshi et al., 2009).

The initial objective was to implement CSI at ports that transport large volumes of cargo containers into the United States, in a way that will facilitate detection of potential security concerns at their earliest possible opportunity (Roach, 2003). Additionally, McNicholas (2008) stated, CSI is now operational at 58 ports in North, Central, and South America; the Caribbean; Europe; Africa; the Middle East; and throughout Asia. CSI attempts to take full advantage of the current technological framework in order to maintain a proactive stance which will continue to reach out to actors in the global supply chain.

The most common container inspection devices within seaports are gamma-ray and X-ray imaging. Additionally, nonintrusive imaging (NII) technologies play a key role in CBP's layered strategy and enable CBP to screen or examine a larger portion of the stream of commercial traffic quickly, while facilitating the flow of legitimate trade, cargo, and passengers (Ahern, 2009). These mechanisms are most typically employed because they provide inspectors with proficient images. Imaging technologies utilize electromagnetic radiation to non-invasively provide a picture of container contents. Images are typically created by subjecting containers to either gamma-rays or x-rays and measuring transmission of the rays through cargo (Cirincione, Cosmas, Low, Peck & Wilds, 2007).

The advantage with gamma-ray inspection devices is speed. Some studies indicate that gamma-ray scanners can inspect up to 30 TEU per hour and that the limiting rate is the speed with which images are interpreted, as opposed to 20 TEU per hour for x-ray scanners (Cirincione et al., 2007). This process is much too slow to accommodate the likelihood of 100% scans. However, another aspect is cost. Most seaports favor gamma-ray scanners because they are

considerably less expensive. Comparatively, one gamma-ray scanner costs \$1 million, whereas x-ray scanners can cost as much as \$4.5 million (Cirincione et al., 2007)

However, there are disadvantages to using gamma-ray and x-ray technology. Gamma-rays' and x-rays' provide a picture of the cargo, which then must be interpreted to determine whether the image appears dangerous or not (Cirincione et al., 2007). Nevertheless, a skilled CBP officer can accurately determine threats with this technology. Yet, making accurate decisions can be time consuming. For an officer to determine the threat accurately, he would have to compare the image with a picture of the manifest in order to verify they match (Cirincione et al., 2007).

However, even if the capacity of scanning equipment were to be scaled up (by a factor of 20-67 per hour) to accommodate 100% scanning, the associated per-container costs would be an order of magnitude higher than those required for the Secure Freight Initiative (Industry-centric) scheme (Bakshi et al. 2009). Furthermore, the current CSI protocol relies on highly sensitive high-energy x-ray radiography to scan containers that are thought to pose a potential threat. This is a time-consuming procedure (Bakshi et al. 2009). Given the aforementioned technological limitations, guidelines have been established to supplement and accommodate this process.

24 Hour Rule

It is tremendously difficult to facilitate effective container security if all imported containers simply came into port unannounced. Advanced warning is a significant factor in the application of efficient container security. In addition to CSI there are several internal assets that aid this procedure. Customs and Border Protection (2006) explained, "The 24-Hour Rule, implemented in January 2003, requires manifest and bill of lading information to be submitted to CBP 24 hours in advance of the cargo being loaded on a ship at a foreign port." In addition, the

24-Hour Rule allows CBP officers to pre-screen and target high-risk shipments and containers before they arrive in a United States port (CBP, 2006). The Automated Targeting System (ATS) supports the 24 hour rule. Moreover, CBP (2006) stated, in support of the 24-Hour Rule, bill of lading information is entered into CBP's sophisticated automated systems. Furthermore, ATS reviews bill of lading information in support of the 24-Hour Rule. Then ATS applies hundreds of targeting rules to pre-screen every arriving shipment and assigns a level of risk for terrorism to each oceangoing container headed to the United States before it leaves the port of lading (CBP, 2006).

However, Bakshi, Flynn and Hans (2009) found that it typically takes several hours, past the 24-hour mark, before a request that a container be pulled reaches terminal management. In order to mitigate this, DHS established the 96-Hour Advance Notification of Arrival Rule which requires submission of detailed crew, cargo, vessel history, and passenger information to DHS's new National Vessel Movement Center. This deadline enables advance boarding of suspect vessels well before they reach our shores (Babul, 2004).

The amount of cargo imported to the United States seriously complicates the inspection process. Given the volume of people and goods seeking entry into the United States every year, it is impractical to physically inspect every person or shipment that arrives at a U.S. port of entry (U.S. Congressional Research Service, 2009, p. 12). Cooperation within the global supply chain could alleviate a significant amount of strain. More specifically, unilateral global cooperation would create an aspect of layered security which would make it much more difficult for criminals and terrorists to penetrate.

Nelson Cabrera (2010) of Lily and Associates found the 24 hour rule will apply to any shipment landing at a European port for inland destination. Transshipment and freight aboard the vessel will also be subject to rule restrictions. This 24 hour notification rule is very similar to the

U.S. Customs 24 hour rule, which has been in effect since 2002 (Cabrera, 2010). However, in the U.S., there is only one regulatory agency overseeing and enforcing the rule. The European Commission 24 hour rule documentation will be reported to and enforced by 27 different EU countries (Cabrera, 2010). Nevertheless, this attempt shows the growing support of the global community. As a result, future endeavors should be more successful.

Automated Targeting System (ATS)

Utilizing an intelligence approach to container security can significantly benefit container security. Furthermore, taking advantage of intelligence gathering and subsequent dissemination seems the most viable option when considering a prolonged security technique. CBP currently adjusts the Automated Targeting System (ATS) based on intelligence information it receives and has initiated a process to track suggestions submitted by CBP targeting officers at the seaports for modifying ATS (GAO, 2006). The calculations within ATS take the guess-work out of locating high risk containers.

In addition, GAO (2007) explained, “ATS is a complex mathematical model that uses weighted rules that assign a risk score to each arriving shipment based on shipping information (e.g., manifests, bills of lading, and entry data).” However, depending on the score received from the automated targeting system, potential cargo that could be marked as “high risk” may be overlooked (GAO, 2007). These security initiatives are interdependent upon one another. In order for the overall container security paradigm to successfully deter threats, all other initiatives must operate proficiently with one another. Without having the most accurate ATS score, in-bound goods transiting the United States pose a potential security threat because higher-risk cargo may not be identified for inspection at the port of arrival (GAO, 2007, p. 24).

Surprisingly, GAO's (2006) research found, "CBP does not yet have a comprehensive, integrated system in place to analyze security inspection results and incorporate them into ATS." More so, ATS (2007) stated, "The current port security regime is a "house of cards," in which containers are often not inspected and the government does not truly know which containers are high risk"(p.2). The previous statement alludes to the fact that a collaborative and cooperative effort is needed in order to facilitate effective container security. Without the cooperation of all port associates, both international and domestic, the container security paradigm will continue to be less effective. Furthermore, more resources are needed. Current staffing shortages at foreign seaports participating in CSI are resulting in thirty-five percent of high risk containers not being inspected before they are shipped to the U.S. (ATS, 2007).

In response to a 2004 recommendation that CBP initiate an external peer review of ATS, CBP contracted with a consulting firm to evaluate CBP's targeting methodology and recommend improvements (GAO, 2006). The contractor's final report, issued in April 2005, found and identified many strengths in the ATS targeting methodology, such as a very capable and highly dedicated team and the application of a layered approach to targeting (GAO, 2006). In addition, Pinto and Rabadi (2008) explained, data gathered on U.S. import containers will be encrypted and transmitted in near real time to the CBP's National Targeting Center, where it will be combined with other data, to improve the risk scoring for targeting high-risk containers. Ergo, one of the most significant advantages associated with ATS is its ability to take the intelligence from cooperating agencies and integrate with the current operating system.

For example, GAO (2006) noted that CBP's Office of Intelligence (OINT) is responsible for acquiring, reviewing, analyzing, and disseminating intelligence. Furthermore, OINT officials mentioned they receive information from the intelligence community, which includes federal agencies such as the Central Intelligence Agency and the Federal Bureau of Investigation (GAO,

2006). Furthermore, according to OINT officials, OINT disseminates information to CBP's offices at the seaports to, among other things, support these offices' targeting efforts related to cargo containers (GAO, 2006). This ability makes ATS extremely flexible and versatile. In addition, CBP officers can also conduct queries or create lookouts in ATS that will search all manifest data in the system to identify those containers whose manifest information may match or be similar to data contained in the intelligence information (GAO, 2006).

Pre-screening cargo is a valuable part in the overall scheme of container security. Huzienga (2005) found the vast majority of system alarms encountered by our nation's ports are due to naturally occurring radioactive material (NORM) alarms, not nuclear material. Prescreening can be used to identify which containers have high levels of naturally occurring radiation, and hence, each cargo container can be classified as NORM or non-NORM as well as high-risk or low-risk. Furthermore, McLay et al. (2008) explained that accurate prescreening intelligence is the most important factor for effective screening, particularly when sensors are highly dependent, and that sensors with high true alarm rates can mitigate some of the risk associated with low prescreening intelligence and sensor dependencies.

Nonetheless, it should be noted that recently ATS has expanded its scope. DHS recently published a "Notice of Privacy Act system of records" for the Automated Targeting System, which it says performs screening of both inbound and outbound cargo, travelers, and conveyances ("DHS Announces New," 2007). This expansion is indicative of the increasing threat associated with transportation security. In order for international seaports, both in the United States and abroad, to accommodate a higher level of scanning, additional initiatives have been created. Such initiatives include the Secure Freight Initiative.

Secure Freight Initiative (SFI)

SFI is an initiative that deploys integrated nuclear detection devices, X-ray or gamma ray imaging machines, and container identifying-optical character recognition devices to foreign seaports in order to support inspection of U.S. bound containerized cargo (McNicholas, 2008). The goal of SFI is to build upon existing port security measures by enhancing the U.S. government's ability to scan containers for nuclear and radiological materials overseas and better assess the risk of U.S.-bound containers (GAO, 2008a). Furthermore, data gathered on containers bound for the United States in foreign ports participating in the SFI is transmitted in near real-time to U.S. CBP officers working in overseas ports and to the Department's National Targeting Center (GAO, 2008a).

DHS developed several overarching initiatives, such as CSI and SFI, to increase the likelihood that nuclear and radiological material would be detected, identified, and interdicted during shipping (U.S. Congressional Research Service, 2009). Comparatively, GAO (2009b) stated, "In April 2009, the Secretary determined that CBP would focus deployment of the SFI program to foreign locations of strategic importance in a way that will maximize security benefits given its limited resources" (p. 7). The importance of obtaining the perspectives of officials directly involved with the inspection process is paramount. GAO (2009b) noted that site visits were conducted at six of the seven foreign ports that have been involved in the SFI program, and spoke with foreign government, CBP, and terminal operator officials during these visits. These ports included: Busan, South Korea; Puerto Cortes, Honduras; Salalah, Oman; Southampton, United Kingdom; Hong Kong; and Singapore (Secure Freight Initiative, 2009).

As of April 2010, SFI has been operational at five of these seven seaports (GAO, 2010b). However, initiating SFI globally still remains a challenge. In October 2009, CBP made progress with the SFI ports ability to scan U.S.-bound cargo containers; but the feasibility of scanning 100

percent of U.S.-bound cargo containers at over 600 foreign seaports remains largely unproven (GAO, 2010c). While CBP works to address the complex challenges the maritime community has encountered, the focus now is on determining how to achieve efficient expansion while maximizing the security benefit and containing the cost (Ahern, 2009). In order to mitigate these challenges CBP and Department of Energy (DOE) have made improvements. CBP and DOE have been successful in integrating images of scanned containers onto a single computer screen that can be reviewed remotely from the United States (GAO, 2010b).

Yet, the obstacle of a cooperative global mission still remains. GAO (2010b) further states the SFI ports' level of participation, in some cases, has been limited in terms of duration (e.g., the Port of Hong Kong participated in the program for approximately 16 months) or scope (e.g., the Port of Busan, Korea, allowed scanning in one of its eight terminals). In addition, the Port of Singapore withdrew its agreement to participate in the SFI program and, as of April 2010, the Port of Oman had not begun scanning operations (GAO, 2010c). Furthermore, since the inception of the SFI program in October 2007, no participating port has been able to achieve 100 percent scanning (GAO, 2010c). However, Ahern (2009) stated the lessons learned from the SFI deployments in Pakistan, Honduras, Southampton and Hong Kong demonstrate that scanning U.S.-bound maritime containers is possible on a limited scale.

While the feasibility to attain 100% scan rates at larger ports remains a challenge, the smaller ports have been increasingly more successful in recent years. Some of these challenges include: safety concerns, logistical problems with containers transferred from rail or other vessels, scanning equipment breakdowns, and poor-quality scan images (GAO, 2010c). Scanning containers with Radiation Portal Monitors (RPM) equipment is generally less time-consuming than scanning with other NII equipment. While the actual NII scanning time per container can take as little as 20 seconds, depending on the system, the entire inspection time can take longer

than 6 minutes (GAO, 2010b). In contrast, it takes 4 to 7 seconds for a tractor trailer to pass through a RPM (GAO, 2010b). GAO (2010a) found that, “Based on our review of the 100 percent scanning requirement, scanning containers with RPMs instead of in combination with other NII equipment may be more achievable from a technology, logistics, political, and cost standpoint” (p. 15).

However, there are limitations associated with RPM. Most notably, scanning containers with RPMs alone introduces the vulnerability of not detecting shielded nuclear material. However, if customs officials believe based on targeting data that further inspections are necessary, they can have a container scanned by NII equipment (GAO, 2010b). In addition, foreign government officials stated that they are generally not opposed to the use of radiation detection equipment, as opposed to the use of NII equipment because it could hinder trade and reduce security by consuming a large amount of scarce resources (GAO, 2010b). The aforementioned statement reveals the most significant obstacle facing 100% scans. The inherent tension between the flow of commerce and the level security makes finding a viable equilibrium very challenging.

However, given the significant cut-backs and the current direction of our economy, cost has become an emerging qualifier as well. Simply put, RPMs are cheaper than NII equipment. GAO (2010b) found, the price for polyvinyl toluene monitors—the most common RPM used at U.S. seaports—is \$425,000 per unit. In contrast, the purchase price for large-scale NII systems used by CBP at U.S. seaports is approximately \$3 million per system.

Finding a way to finance sophisticated equipment such as the gamma-ray and x-ray imaging technologies remains a concern. Nevertheless, identifying a solution that requires a collective effort could prove to be the best alternative. Comparatively, GAO (2010b) found that CBP and DOE have paid the majority of SFI costs for operating the SFI program. Further yet,

the SAFE Port Act does not address the issue of who is expected to pay the cost of developing, maintaining, and using the infrastructure, equipment, and people needed for the 100 percent scanning requirement (GAO, 2010c). But implementing the requirement would entail costs beyond U.S. government program costs, including those incurred by foreign governments and private terminal operators, and could result in higher prices for American consumers (GAO, 2010a). Stipulations such as the previous emphasize the importance of global favor. Unless foreign ports want to contribute, it will be impossible to sustain a security strategy on such a larger scale. Furthermore, CBP has not estimated these additional economic costs, though they are relevant in assessing the balance between improving security and maintaining trade capacity and the flow of cargo (GAO, 2010c).

Recognizing the challenges to meeting the legislative requirement, DHS expects to grant a blanket extension to all foreign ports pursuant to the statute, thus extending the target date for compliance with this requirement by 2 years, to July 2014 (GAO, 2011). However, it should be noted that the DHS Secretary, Janet Napolitano, announced that the United States is no longer going to screen every cargo container before it enters the United States (Homeland Security News Wire, 2011).

Byrd (2008) found:

CBP has decided to focus on high-risk trade corridors in order to maximize the security benefit given the limited resources available to all governmental and private sector operators in the international supply chain as the most effective strategy to initiate 100% scanning. (p. 3)

Comparatively, GAO (2010c) stated that the Secretary of Homeland Security approved the “strategic trade corridor strategy,” an initiative to scan 100 percent of U.S.-bound containers at selected foreign ports where CBP believes it will mitigate the greatest risk of WMD entering the

United States. In particular, Byrd (2008) claimed that Singapore will not participate in the SFI tutorial but they are willing to work together to explore alternative approaches to container security. Reluctance to cooperate continues to be container security's greatest detriment.

Although, this strategy is relatively new, progress should be able to be documented and utilized in the future. GAO (2010a) stated, "CBP plans to evaluate the usefulness of these security measures and consider whether the continuation of scanning operations adds value in each of these locations, and potential additional locations that would strategically enhance CBP efforts." However, Assistant Deputy Administrator of the U.S. Department of Energy, David Huizenga noted, the SFI deployments in Honduras, the United Kingdom, and Pakistan indicate that scanning US-bound maritime containers is possible on a limited scale (U.S. Department of Energy, 2008). Furthermore, it has been proven that we can effectively integrate data from radiation detection equipment and non-intrusive imaging equipment to improve our overall detection capability, and that we can take this large amount of data and transmit it near real-time to the United States for analysis (U.S. Department of Energy, 2008).

With all the advantages that SFI established, acquiring 100% container cargo scans maintains a challenging task. Therefore, port officials decided to identify high risk areas and deploy resources in a strategic manner in order to maximize their efforts. In addition, two initiatives were created as auxiliary components for SFI: 1) the Strategic Trade Corridor Strategy and 2) Importer Security Filing (10+2).

Strategic Trade Corridor Strategy

The Strategic Trade Corridor Strategy is one of the two initiatives added to the layered maritime security approach in order to specifically augment SFI. That being said, the Strategic Trade Corridor advancement has become one of the newest additions to the layered approach to

container security. In April 2009, the Secretary of DHS endorsed the Strategic Trade Corridor Strategy as the path forward for implementing the SFI program (GAO, 2009a). This strategy attempts to mitigate the challenges regarding the implementation of 100% scans in the global supply chain. The Secretary was presented with three options ranging from implementing SFI at 70 ports that account for shipping over 90 percent of U.S.-bound containers to seeking repeal of the 100 percent scanning requirement (GAO, 2009a). Further, the Strategic Trade Corridor Strategy selected by the Secretary focuses cargo container scanning efforts on a limited number of ports where CBP has determined SFI will help mitigate the greatest risk of potential WMD from entering the United States (GAO, 2009a). Because negotiations are ongoing, details on the number of ports involved are not yet finalized (GAO, 2009a).

Collaborative efforts made this strategy possible. GAO (2009a) explained, “CBP determined which ports were strategic by working with DOE to develop a joint analysis of the potential risk of cargo containers from all foreign seaports that ship directly and indirectly to the United States.” More specifically, GAO (2009a) added, this analysis focused on issues such as known smuggling routes, volume of container traffic, proximity to special nuclear material sources, and known presence of terrorist cells operating in the country.

As stated previously, the approach to effective container security involves a layered strategy. There is no panacea that will single-handedly guarantee the absolute security of containerized cargo. GAO (2009b) stated, “It is unclear whether DHS intends for the Strategic Trade Corridor Strategy to be implemented in lieu of the 100 percent scanning requirement or whether it is an initial step towards full implementation at all ports.” However, GAO (2010b) explained this strategy may improve container security, but it does not achieve the legislative requirement to scan 100 percent of U.S.-bound containers. Furthermore, a plan for full-scale

implementation of the statutory requirement by July 2012 is absent because of challenges encountered thus far in implementing the SFI program (GAO, 2010b).

Importer Security Filing (ISF) aka 10+2

The second addition to the SFI program was the Importer Security Filing more commonly known as 10+2, which was implemented in 2008. The SAFE Port Act further instructed DHS to obtain better data from U.S. importers for container security screening and targeting efforts. CBP believes the additional data provided through 10+2 will enhance security by improving the targeting process used to identify containers that may pose a risk for terrorism (GAO, 2009b). In comparison, the GAO (2010a) explained this program seeks data on U.S. imported containerized cargo (prior to the loading of this cargo on ships at foreign ports) for 10 additional variables and information on ship stowage plans and container status messages from shipping lines. Furthermore, Blegen (2009) stated, “This regulation contains what is likely to represent the single most significant change in the U.S. import process in at least 15 years. In addition, Blegen (2009) noted CBP’s official rationale for the ISF regulation was the information required is that which is reasonably necessary to enable high-risk shipments to be identified so as to prevent smuggling and ensure cargo safety and security.

However, it should be noted that although the effective date of the 10+2 rule was January 26, 2009, the rule allowed for a 1-year flexible enforcement period (GAO, 2010a). Currently, ISF is being utilized at seaports throughout the U.S. January 26, 2010 marked the end of the flexible enforcement period and with that CBP plans to focus on importers who have not filed ISFs for shipments by issuing warning letters and possibly subjecting some of these shipments to nonintrusive inspections (GAO, 2010a).

GAO (2010a) listed the 10 required ISF data elements for U.S. bound cargo as:

- 1) Seller: Entity selling or agreeing to sell the goods.
- 2) Buyer: Entity to whom the goods are sold or agreed to be sold.
- 3) Importer of record number: Assigned number of the entity liable for payment of all duties and responsible for meeting all statutory and regulatory requirements incurred as a result of importation.
- 4) Consignee number: Number assigned to the individual(s) or firm(s) in the United States on whose account the merchandise is shipped.
- 5) Manufacturer: Entity that last manufactures, assembles, produces, or grows the commodity.
- 6) Ship to party: First deliver-to party scheduled to physically receive the goods after the goods have been released from customs custody.
- 7) Country of origin: Country of manufacture, production, or growth of the article.
- 8) Commodity Harmonized Tariff Schedule of the United States number: Category for type of merchandise, as defined by the Harmonized Tariff Schedule, being imported into the United States.
- 9) Container stuffing location: Physical location(s) where the goods were packed or loaded into the container.
- 10) Consolidator: Entity who loaded the container or arranged for the loading of the container. (p. 11)

The aforementioned criteria are specific for commercial shipping lines which import to the U.S. Importers are responsible for submitting data elements for the ISF, and the required data

elements differ depending on the cargo's destination (GAO, 2010a). This inconsistency can lead to unfavorable criticism within the supply chain.

For cargo containers that are transiting the United States but for which the United States is not the final destination, the rule requires importers to submit 5 data elements to CBP prior to loading (GAO, 2010a). In order for security initiatives to work properly, uniformity must be satisfied. Requiring more information from importers inbound to the U.S. as opposed to other countries could generate disobedience.

GAO (2010a) listed the 5 required ISF data variables for in-transit cargo:

- 1) Booking party: Entity who initiates the reservation of the cargo space for the shipment.
- 2) Foreign port of unloading: Port code for the foreign port of unloading at the intended final destination.
- 3) Place of delivery: Foreign location where the carrier's responsibility for the transport of the goods terminates.
- 4) Ship to party: First deliver-to party scheduled to physically receive the goods after the goods have been released from customs custody.
- 5) Commodity Harmonized Tariff Schedule of the United States number: Category for type of merchandise, as defined by the Harmonized Tariff Schedule, being imported into the United States. (p. 11)

A similar view has been adopted concerning the use of flexibilities within the administration of 10+2. GAO (2010a) defines flexibility as a provision (s) that allow importers flexibility in the timing and content of submission for certain data elements. This process created additional obstacles that CBP was unprepared to sustain. GAO (2010a) found CBP officials stated that the decrease in flexibility usage can be primarily attributed to the trade industry's

determination that flexibility use is unnecessary due to the existence of CBP's standard amendment process, which allows filers to update ISF information.

Under this standard amendment process, the importer is obligated to provide an amended ISF as soon as additional information is discovered or if there are changes to the shipment (GAO, 2010a). Nevertheless, providing a single standardized list of ISF variables for U.S. and foreign cargo decrease additional paper work and increase the amount of time allotted to personnel targeting high risk cargo while encouraging global support.

However, CBP is cognizant that global cooperation is the critical factor in order to achieve success with initiatives such as 10+2. Nonetheless, permitting importers to utilize flexibilities is proof CBP is attempting to alleviate the strain associated with diligent cooperation. GAO (2010a) found since the end of the flexible enforcement period, CBP has stated that it has been applying a "measured, common sense approach" to enforcement. In addition, CBP collects daily information on the ISF compliance of importers' shipments at each U.S. port to monitor the status of ISF implementation, as well as data on vessels arriving in U.S. ports for which carriers did not file vessel stow plans (GAO, 2010a). As a result, CBP's data indicate that in July 2010, approximately 80 percent of shipments were ISF compliant, and CBP officials said most carriers have submitted vessel stow plans (GAO, 2010a).

Attaining global compliance would significantly contribute to effective implementation. Some countries are realizing the need for establishing an efficient level of security. In some instances countries are beginning to replicate certain characteristics associated with American container security strategies. Blegen (2009) stated the European Union (EU), Japan, and other countries are in the process of formulating advance data-related regulatory requirements, with implementation dates in some cases already set.

In terms of timing, submission of the ISF to CBP, via one of the two authorized electronic systems (Automated Broker Interface or Automated Manifest System), must be done no later than 24 hours before the cargo is laden aboard a vessel destined to the US (Blegen, 2009). Blegen (2009) explained, “The manifest data is submitted to the US Government’s Automated Manifest System (AMS), where it is used to target shipments for inspection by CBP. The Automated Broker Interface (ABI) is a component of the U.S. Customs Service's Automated Commercial System that permits qualified participants to electronically file required import data with Customs (“Automated Broker Interface,” 2009). With the exception of the use of international standards-based messaging on a portion of the carrier ISF filings made in the AMS system, it appears that ISF messaging is to be based primarily on ABI-specific requirements and protocols (Blegen, 2009). Currently, over 96% of all entries filed with Customs are filed through ABI (“Automated Broker Interface,” 2009).

In general, it should be noted that the progression of security initiatives will be consistently modified in order to meet the mutable demands of the seaport security environment. There is no doubt that the next year of phased enforcement of the ISF requirements will lead to many lessons learned, and continued close scrutiny by international policymakers of the U.S. ISF (Blegen, 2009).

Collection of the additional cargo information and their incorporation into CBP’s Automated Targeting System (ATS) are intended to enhance CBP’s ability to identify high-risk shipments and prevent the transportation of potential terrorist weapons into the United States (GAO, 2010c). With the advent of more detailed information, personnel will be more capable to identify high risk cargo. Specifically, GAO (2010a) noted within ATS, CBP develops combinations, or sets, of two rules and assigns numerical weights to the rules in a set to determine overall risk scores for particular threats. The proficiency of separate security

mechanisms to interconnect information makes overall seaport security more impenetrable. More specifically, this strengthens container security. With most of the immediate attention being directed at the possibility of containers secreting a WMD, the seaport community is constantly preventing other threats. Threats such as piracy, organized crime, and drug-trafficking are just a few variables that must be calculated into the overall seaport security equation.

MegaPorts Initiative/Second Line of Defense

The Megaports Initiative reinforces SFI in the overall maritime security approach. U.S. Department of Energy (DOE) in cooperation with the National Nuclear Security Administration (NNSA) elaborated by stating, the Megaports Initiative is a key component of a multi-agency, multilayered, defensive network that strengthens the overall capability of partner countries to deter, detect, and interdict illicit trafficking in special nuclear and other radioactive materials at key international seaports. Furthermore, this program is part of the Office of International Material Protection and Cooperation in the U.S. DOE/NNSA (U.S. Department of Energy, 2010).

Since the start of the Megaports Initiative in fiscal year 2003, NNSA has completed installations of RPM equipment at 27 foreign ports, and implementation is under way at an additional 16 foreign ports (GAO, 2010c). In addition, the Megaports Initiative seeks to equip 100 ports with radiation detection systems by 2016, scanning approximately 50% global maritime containerized cargo and over 80% of U.S.-bound container traffic (GAO, 2010b). However, the success of this initiative, like the aforementioned initiatives, depends significantly on global cooperation. To select key ports for engagement, a Maritime Prioritization Model (MPM) was developed to consider both the volume of container traffic at the port and the threat level and/or strategic location of the port (U.S. Department of Energy, 2010). The initiative

currently extends to 34 ports around the world with work underway at 18 additional ports in Asia, Latin America and the Caribbean, the Middle East, Europe, and Africa (U.S. Department of State, 2010).

The NNSA has completed installation and testing of radiation detection systems at four new ports: Ashdod, Israel; Lisbon, Portugal; Kaohsiung, Taiwan; and Port Klang, Malaysia (“Nnsa Megaports Initiative,” 2009). While the deployment of these RPMs to overseas affiliates has yet to detect any significant nuclear smuggling activity, there have been other instances which presented customs officials with actionable data. Huizenga’s (2008) research concluded that in 2003, Georgian border guards, using US-provided portal monitoring equipment at the Sadakhlo border crossing with Armenia, detected and seized approximately 173 grams of highly enriched uranium (HEU) carried by an Armenian national. More recently, a Megaports RPM targeted several Cesium-137 sources which were detected in a container of scrap metal leaving Honduras bound for a smelting facility in the Far East (U.S. Department of Energy, 2008). The comments made by Huzienga (2008) are proof that the detection devices responsible for interdicting nuclear materials are effective in locating minute quantities. Therefore, similar technology could be utilized to target more specific areas of concern within seaports.

Furthermore, U.S. Department of Energy (2010) found that, “Because of shorter dwell times for containers, space constraints, availability of shipping data, and the difficulty of identifying chokepoints within the container terminals, capturing transshipments without seriously impacting port operations requires new and creative solutions.” Evans (2004) supported by explaining that transshipment creates difficulty in commercial cargo tracking, as cargo containers may be routed through hubs and then on via spokes to other destination prior to their final arrival point. The aforementioned statements, further, emphasizes the need to utilize intelligence by proactively collaborating with global affiliates.

Nevertheless, the U.S. Department of Energy (2008) noted the first mobile detection platform, a straddle carrier, was deployed at the Port of Freeport in the Bahamas in June 2006 using both plastic Polyvinyl Toluene (PVT) for primary detection and a spectroscopic detector for secondary isotopic identification. More specifically, NNSA, working in conjunction with the terminal operator, Hutchison Port Holdings, has successfully scanned over 730,000 containers at Freeport Container Terminal (Huzienga, 2008). Additionally, U.S. Department of Energy (2010) stated NNSA is also evaluating a new mobile platform for scanning transshipped containers on the quay at the Port of Salalah, Oman. Furthermore, the mobile system will increase the number of transshipped containers that can be scanned as well as improve the effectiveness and efficiency of the scanning process of transshipped containers with the same efficiency as fixed monitors (U.S. Department of Energy, 2010).

However, U.S. Department of Energy (2008) noted that if technology is developed to scan 100% of US-bound containers with the detection and imaging systems without impacting port operations, still, it may not necessarily be a cost-effective risk management strategy to equip the 700+ ports that ship directly to the U.S. This is where the multi-layered approach resurfaces. The Megaports Initiative collaborates with CBP where Megaports and CSI overlap to improve CSI inspection teams' ability to identify high-risk U.S.-bound containers (U.S. Department of Energy, 2010). Yet, identifying a suitable approach to negate or, at least, reduce the cost of such an initiative maintains a primary concern. Without bridging the gap between funding and initiation, supply chain security will continue to suffer.

Nevertheless, U.S. Department of Energy (2008) mentioned one obvious way to address the cost of overseas scanning is to encourage cost-sharing with host governments and with private industry. Furthermore, under the Megaports program, we are finding ways to do this where we provide equipment and training and the host government is responsible for design,

construction and installation costs (U.S. Department of Energy, 2008). Without doubt, one of the most significant obstacles associated with garnering global support is the cost to start and maintain such systems. U.S. Department of Energy (2008) further stated, “I cannot underscore enough that SFI or Megaports Initiative implementation cannot be successful without the partnership of the host nation, port authority, terminal operators, and other key stakeholders at the port” (p.1). In some instances, this means creating an entirely new platform for port authorities which entails significant labor and costs.

In addition, U.S. Department of Energy (2010) explained the Megaports Initiative should employ cost sharing in the Megaports implementation process. The primary dividend of cost sharing is buy-in from the host government and terminal operator. Furthermore, although no set formula for cost-sharing is available, the terminal operator or port authority often pays for design, construction, engineering, installation, or a combination of those costs. Cost-sharing arrangements are site-specific and negotiated differently for each port (U.S. Department of Energy, 2010).

However, U.S. Department of Energy (2010) did state that, under most Megaports agreements, DOE/NNSA commits to providing maintenance and training support for three years, after which time the partner country takes full responsibility for operating and maintaining the systems. This type of unilateral commitment effectively encourages participation. Moreover, the Megaports Initiative hosts regional Megaports workshops with partner nations annually or as needed to encourage information sharing between regional partners and to exchange lessons learned (U.S. Department of Energy, 2010). Inevitably, the success of any single initiative requires a cohesive and collaborative framework which promotes information sharing. By garnering a favorable relationship with all actors in the global supply chain, the United States and contributing nations will be able to effectively establish and maintain adequate container

security. Nonetheless, the U.S. has recognized a collective effort between all maritime affiliates is mandatory in the overall maritime security framework. Therefore, establishing partnerships accordingly can promote a more effective approach.

Customs-Trade Partnership Against Terrorism (C-TPAT).

Unilateral agreements are significant to ensure adequate security. By initiating a trustworthy bond with all associates involved in maritime security, port officials and personnel will be more capable of enforcing container security mechanisms. CBP has taken a lead role in working with foreign customs administrations on approaches to standardizing supply chain security worldwide (GAO, 2009b). Comparatively, Cheney (2003) announced the U.S. government would be, “Enrolling thousands of commercial importers in the Customs-Trade Partnership Against Terrorism program (C-TPAT) to secure the entire supply chain. Under C-TPAT, private industry partners providing verifiable security information receive preferential treatment during the shipping process. In return, C-TPAT members are entitled to various benefits—chief among them, a reduced likelihood of scrutiny of their cargo (GAO, 2008b). However, Roach (2003) explained, “I should state up front that it is not designed to, nor does it in fact, give any particular set of ports exclusive rights to ship containers to US ports” (p. 345). Nevertheless, benefits such as the latter are real factors that weigh on the minds of shipping companies and any other key stakeholder within the global supply chain.

Further, GAO, (2008b) noted that prior work on C-TPAT has acknowledged that while the C-TPAT program holds promise as part of a maritime security strategy, it has faced management and operational challenges. These challenges can equate to secondary and tertiary repercussions. However, weaknesses have been identified with C-TPAT and those companies attempting to reap the benefits of this program. Moreover, GAO (2008b) added that there are

problems with the portable, personal computer-based data-gathering instruments CBP has provided to its security specialists to help ensure that validation information is consistently collected, documented, and applied to decisions regarding the awarding of benefits to C-TPAT members.

If initiatives such as C-TPAT are to become universally adopted, they must be able to satisfy time constraints. Furthermore, this success must be predicated on the initiative and personnel's ability to recognize areas where time management can be improved and execute accordingly. The inability to make such adjustments widens the gap in effective container security. GAO (2008b) concluded while the validation instrument allows specialists an opportunity to collect data on the results of members' audits and inspections of their supply chain security practices, CBP does not require security specialists to use these data in validating members' security practices.

In effect, by not allowing these validation instruments the opportunity to replace direct testing, security specialists are wasting valuable time. When CBP encounters such inconsistencies, immediate action should result in order to avoid any further discrepancies. Until these collective challenges are corrected, CBP will be unable to assure Congress and others that C-TPAT member companies that have been granted reduced scrutiny of their U.S.-bound containerized shipments actually employ adequate security practices (GAO, 2008b).

Unanticipated container delays can cause costly supply-chain disruptions. For example, Martonosi et al. (2006) estimates the cost of delay per day to approach 0.5% of the value of a container. In comparison to Martonosi et al., Bakshi and Gans's (2007) claim that when inspection-induced delays can be anticipated, the extra pipeline inventory required to accommodate delays can be costly. For example, given an annual flow of \$423 billion in goods, a day of pipeline inventory will, inevitably, be worth only \$1.16 billion. Additionally, Bakshi

and Gans, (2007) stated improving the risk profile of these containers, CBP can reduce the number of containers it needs to inspect and, simultaneously, reduce the overall level of terrorism-related risks associated with containers entering the U.S.

Nevertheless, GAO (2008b) stated that these weaknesses compromised CBP's ability to verify that supply chain security measures, described in security information submitted by program members, were accurately reported and followed. In addition, other challenges with C-TPAT were identified, including that the program lacked adequate performance measures and a human capital plan indicating how CBP intended to develop new staff to meet the program's growing demands (GAO, 2008b).

As stated previously, if CBP is unable to ensure that shipping companies are actually updating and enforcing implemented security plans, then Congress and other contributors will stop allocating support. Therefore, CBP has acted on recommendations to strengthen the security validation process by establishing minimum security criteria for the majority of C-TPAT members (GAO, 2008b). These criteria are supposed to replace the general security guidelines that have contributed to unreliable information. The minimum security criteria for foreign manufacturers now state that foreign manufacturers must have written and verifiable processes for the selection of business partners including, carriers, other manufacturers, product suppliers (GAO, 2008b). C-TPAT and others must garner favorable support from their key stakeholders, most notably, the shipping companies and foreign seaports. For many companies, the program's benefits appear to outweigh its costs, and more than 7,000 companies have joined C-TPAT since its inception in November, 2001 (Basham 2007).

To strengthen C-TPAT program management, CBP, among other things, developed a human capital plan, implemented a records management system for documenting program decisions, and put additional performance measures in place (GAO, 2008b). More specifically,

the SAFE Port Act (2006) has mandated a pilot for a third-party audit program. Under this scheme, CBP-authorized third-party auditors (with appropriate access rights and training) conduct the audit, while the C-TPAT participant itself pays for the audit (Bakshi & Gans, 2007). Bakshi and Gans (2007) explained this plan is attractive to CBP for two reasons: 1) CBP is falling short of staff required to effectively validate the membership and later audit firms and 2) CBP auditors do not have access to certain trade lanes in the international supply chain.

Firms decide whether or not to join C-TPAT based on their respective costs of compliance and the expected congestion costs due to secondary inspection (Bakshi & Gans, 2007). The latter plays an integral factor in the overall equilibrium of effective security without hindering commerce. At the port of debarkation, all containers undergo some form of “passive” screening, a non-intrusive inspection which may include neutron and gamma-ray radiation monitoring. This is referred to as the primary inspection (Bakshi & Gans, 2007). Any further inspection, or secondary inspection, can include active tests, such as gamma and x-ray radiography, and possible devanning of the container for a comprehensive manual inspection (Bakshi & Gans, 2007).

Secondary inspection is widely considered the obstacle that puts the most strain on the equilibrium between security and commerce. A secondary inspection is considered any further inspection of the containers cargo after the initial or primary inspection (Bakshi & Gans, 2007). The cost to perform secondary screening is a deterministic value based on information collected and analyzed by DHS and CBP. It is in part based on salaries paid to the employees hired to perform secondary screening (McLay, Lloyd & Niman, 2008).

In most cases, the proficiency of detecting WMDs and other forms of contraband can be directly related to the personnel operating the equipment. More specifically, maintaining an environment that facilitates proper and ethical performance is critical to effective container

security. The maritime community has found that monitoring all personnel is challenging. However, through the implementation of the Transportation Worker Identification Credentials (TWIC) the maritime community has been able to make progress in assuring their personnel are among the most qualified.

Transportation Worker Identification Credentials (TWIC).

As defined by DHS, the purpose of the TWIC program is to design and field a common credential for all transportation workers across the United States who requires unescorted access to secure areas at MTSA-regulated maritime facilities and vessels (GAO, 2011). There is legitimate concern that transportation workers will exploit discrepancies within the seaport community. The U.S. Immigration and Customs Enforcement (ICE) (2010) found in July 2007 that longshoremen were actively involved in an international conspiracy that involved the importation of multiple kilograms and millions of dollars worth of cocaine, heroin, and marijuana through the Port of Miami and Port Everglades. Furthermore, the investigation revealed six members of the International Longshoremen's Association were taking cash payoffs to smuggle shipments of drugs into South Florida (ICE, 2010).

Additionally, Shifrel (2010) found, eight New Jersey longshoremen were busted for helping Panamanian drug dealers smuggle more than a ton of cocaine into the country - getting \$50,000 to \$100,000 apiece for their work. Also, The Waterfront Commission of New York Harbor (2011) stated on September 13, 2011, former longshoreman Anthony Bell was arrested by Detectives from the Waterfront Commission and the Manhattan District Attorney's Detective Squad after presenting forged documents to the Commission in an attempt to be re-instated as a longshoreman.

With activity such as the previous occurring on a consistent basis, there is, undoubtedly, a real concern that seaport personnel could allow a WMD to penetrate security. In most instances, the cash payoffs that seaport personnel accept to smuggle contraband, is a guarantee that the contents of the packages are not known. Therefore, seaport personnel could unknowingly transport the components capable of manufacturing a WMD, dirty bomb, etc. Most importantly, the probability that a cargo container is a threat is assessed by these personnel and within the DHS based on the perceived threat level. (McLay et al., 2008).

As mentioned throughout this research, personnel are inherently connected with technology and the process of container security. If either is absent, security will be ineffective. Potential for infiltration into the seaport through more direct means also poses a problem. In Close's (2009) study she explained, "Biometric identification procedures for individuals having access to secure areas in port facilities are important tools to deter and prevent port cargo crimes, smuggling, and terrorist actions" (p. 1). This factor is significant. In comparison, Lake et al. (2005) said, "Intermediaries such as buying agents and freight forwarders are the most frequently utilized intermediaries between the originating shipper and the ocean carrier" (p. 13). In Close's (2009) study she further stated, "An individual who does not hold a TWIC must obtain permission from the owner or operator to gain escorted access to secure areas" (p. 17).

The constant distribution and transfer of cargo containers makes this process susceptible to tampering. Lake et al. (2005) explained it is important to note that there are in reality two sets of actors involved: those who hold what could be termed as *documentary* custody, the people in the offices who handle the paperwork side of the transaction; and those actors who have *physical* custody. Unethical behavior in either position can have detrimental effect.

TWIC holder eligibility consists of two key components: 1) enrollment and 2) background checking. GAO (2011) stated, "Transportation workers are enrolled by providing

biographic information, such as name, date of birth, and address, and proof of identity documents, and then being photographed and fingerprinted at enrollment centers by trusted agents.” In addition, GAO (2011) noted TSA conducts background checks on each worker who applies for a TWIC to ensure that individuals who enroll do not pose a security risk to the United States. Moreover, a worker’s potential link to terrorism, criminal history, immigration status, and mental capacity are considered as part of the security threat assessment. Further, these background checks are broken down into two levels: 1) first level: initial automated background checking and 2) second level review: TSA adjudication center review. As a result of these checks the Maritime Security Council stated that 1,158 applicants were denied cards because of their criminal histories or immigration status. In addition, several were disqualified because they were on terror watch lists (“Hundreds of Millions,” 2011).

However, GAO (2011) found the number of TWICs provided to applicants with specific criminal offenses not defined as disqualifying offenses, as of September 8, 2010, the agency reported 460,786 cases where the applicant was approved, but had a criminal record based on the results from the FBI. More specifically, this statistic represented approximately 27 percent of individuals approved for a TWIC at the time (GAO, 2011).

When enforcing the use of TWICs there must be a system in place that will validate proper administration. The Maritime Security Council found that, undercover government investigators were able to get into major U.S. seaports — at one point driving a vehicle containing a simulated explosive — by flashing counterfeit or fraudulently obtained port “credentials” to security officials (“Hundreds of Millions,” 2011). Gaining access to fake credentials is a relatively simple task. Approaches for inspecting TWICs using biometric readers at individual facilities and vessels across the nation are being considered as part of a pilot but are not yet required (GAO, 2011). Nevertheless, the aforementioned evidence is proof of a necessary

and hasty solution. However, this weakness has been targeted by CBP and USCG and appropriate action is underway.

GAO's (2011) research found the Coast Guard's primary means of verification is shifting toward the use of biometric handheld readers with the continued deployment of readers to each of its sectors. In addition, as of December 21, 2010, the Coast Guard reports to have deployed biometric handheld readers to all of its 35 Sectors and 16 Marine Safety Units (GAO, 2011). Yet, this attention still renders concern. The Maritime Security Council stated the Government Accountability Office (GAO) mentioned the program does not provide reasonable assurance that only qualified people get the credentials ("Hundreds of Millions," 2011). In tests, investigators got into ports using counterfeit TWICs or authentic TWICs acquired through fraudulent means, and by stating false reasons for needing access. Further, GAO's (2011) research stated even if an individual presents an authentic TWIC acquired through fraudulent means, the cardholder is deemed not to be a security threat to the maritime environment because the cardholder is presumed to have met TWIC-related qualifications during a background check.

As stated throughout this research, personnel are responsible for the ultimate decision to stop and administer secondary inspections. Publicover (1999) found, "The majority of cargo loss claims involve cargo taken from transportation facilities by personnel authorized to be there and on vehicles controlled or similarly authorized by management. If the seaport community is dependent on untrustworthy and unqualified candidates to provide essential security procedures, then the multi-layered security framework can't be expected to operate effectively.

The Consumer and Security

Thibault *et al.* (2006) stated that, "Terrorists, if successful in these types of [seaport] attacks, could claim a major victory as their efforts would not only harm the U.S. but also disrupt

the global economy”(p. 1). However, the price of security has begun to take its toll. Maritime security and, more specifically, container security have prompted the transfer of security expenses to the consumer. This transfer is directly related to the level of security being enforced upon the majority stakeholders (i.e. commercial shipping companies, seaports, insurance companies, etc.). Extraneous but necessary fees incurred through security initiatives have encouraged majority stakeholders to raise the cost of shipping. Respectively, compiled cost figures from industry and press reports suggest an average security charge of \$6 per shipped container, as opposed to \$40 per bill of lading for the 24-hour rule (Bichou, 2008).

Further complicating issues is the desire to attain 100% scans on all containers entering the U.S. This issue, while significant, has been viewed as unachievable. Alternative methods must be emplaced if consumers desire to resist increasing distributor pricing. Validating this point, in 2011, DHS Secretary Janet Napolitano announced that the United States is no longer going to screen every cargo container before it enters the United States (Homeland Security News, 2011). Efficient container security will depend on several security initiatives as well as cooperation throughout the global supply chain. Napolitano noted that rather than scanning all cargo containers, DHS prefers a “layered approach” that includes increased cooperation between countries and better intelligence sharing and analysis in addition to screening some containers (Homeland Security News, 2011). Furthermore, she explained, “I think what we have learnt over time is that there are many different ways to achieve a security objective, you have to have multiple layers that operate effectively” (p. 1).

Without proper action consumer pricing will continue to increase. Furthermore, certain areas have been targeted that would augment security while decreasing risk to the consumer. Bakshi et al. (2007) found if there is limited scanning and radiation detection capacity, the delays resulting from waiting in inspection queues could require containers to sit idle at ports for

durations that are longer than required in the absence of inspections. More specifically, these extra delays would lead to increases in transportation lead times, resulting in higher inventory levels in supply chains, and ultimately in higher cost for consumers (Bakshi et al., 2007).

Another area of concern is the off-loading process from ship to terminal. The need to divert containers from their usual movements within port terminals, redirecting them through a centrally-managed government inspection facility, has the potential to engender significant terminal congestion (Bakshi et al., 2007). Decreases in terminal efficiency, along with increased lead times, would lead to higher consumer costs. (Bakshi et al., 2007). In addition, Erik Rabjerg Nielsen, the director and head of operations and deployment for Maersk Line, announced in May 2011 that the company will add further surcharges to cover increased security costs (Pelton, 2011). Reason being, the Maersk Line expected its piracy-related costs to double in 2011 to \$200 million in order to cover insurance premiums, hardship allowances and the rerouting of vessels away from high-risk zones in the region (Pelton, 2011).

In order for majority stakeholders to compensate for the fees accumulated through the shipping process, higher pricing is eminent. However, in a highly disintegrated and fragmented maritime and logistics industry, there is no guarantee that additional security charges accurately reflect the true incremental costs incurred by each operator, including ports (Bichou, 2008). Standard practices in the industry suggest that market players try to generate extra profits by transferring costs to each other (Evers and Johnson, 2000; Fung et. al, 2003), and there is already evidence of similar practices in the recovering of security costs by the port industry (Bichou, 2008). Finding a solution that promotes effective security, while decreasing pricing would be beneficial to all parties involved.

Summary

Understanding the threats that affect the seaport community and, more specifically, containerized cargo provide seaport officials with knowledge that will make it possible to improve current security limitations. The effects of current implemented security measures are difficult to gauge. There have been numerous qualitative and quantitative studies conducted on single aspects concerning the maritime industry. Nevertheless, there seems to be a lack of research relating to the perception of effectiveness in the maritime security industry as observed by deputy port directors and their designees.

Understanding the successes and faults of security measures utilized by various seaports could enable port deputy directors of operations and security to analyze and assess cargo more effectively. Research has determined several security techniques: 1) Container Security Initiative, 2) Transportation Worker Information Credentials, 3) Customs Trade Partnership Against Terrorism, 4) Automated Targeting System, 5) Secure Freight Initiative, 6) Megaports Initiative, 7) Importer Security Filing (10+2), 8) 24 hour rule and the 9) Strategic Trade Corridor Strategy. In addition, this research has targeted several threats including: 1) piracy, 2) container theft, 3) stowaways and 4) terrorism.

Piracy has emerged and maintained its role as a significant threat to maritime transport. While most publicized attacks have occurred in the vicinity of the Gulf of Aden, there has been an increasing presence off the coasts of Nigeria, Indonesia and South America. In addition, container theft and stowaways remain a concern. However, the responsible authorities have proven effective in locating and deterring these threats. Nevertheless, while all the threats identified in this research pose a maritime transportation security risk, terrorism and the potential for containers to secrete a WMD pose the most dangerous threat. If CBP and the USCG are

unable to identify containers that pose a risk to U.S. national security, then the threat for a terrorist attack will increase significantly.

The management and facilitation of the security techniques discussed above pose difficult challenges for the population in this study. Therefore, it is essential to gain pertinent information regarding the techniques. The more information obtained from the participants, the more likely this study will reach a level of saturation that is sufficient.

Chapter 3 contains the methodological design to be implemented and descriptions of the subjects, instruments, and procedures. The researcher's rationale for selecting a qualitative method is to gather pertinent information by personally interviewing port officials in regards to container security. Further, the study's purpose and research questions are clearly provided for the reader.

CHAPTER 3: RESEARCH DESIGN AND METHODOLOGY

Introduction

The literature concerning the perceptions of deputy port directors or their designee is relatively new. This study contributed to the research describing the perceptions of deputy directors concerning container security techniques. This chapter includes discussion: (a) population and sample, (b) methodology, (c) data collection and instrumentation, and (d) data analysis.

The purpose of this qualitative study was to analyze and assess maritime security and the perceptions of selected officials and personnel as it pertained to the use of implemented container security measures at United States seaports along the Gulf Coast. The limited research required more attention to produce a more detailed analysis and subsequent understanding of the effectiveness of implemented security measures at seaports. The research questions guiding this study were as follows:

1. What are the main threats to seaports along the Gulf Coast?
2. What is the main threat to containers?
3. How do port security administrators and the USCG perceive containerized cargo threats?

Method

This study utilized a qualitative approach to interview deputy port directors or designees in their natural setting in order to examine their perceptions and that of their designees. The deputy directors and designees were selected by contacting seaports of Houston, TX; Corpus Christi, TX; Galveston, TX; New Orleans, LA; Gulfport, MS; Mobile, AL; Tampa, FL; and Miami, FL via telephone/email. Given the sensitivity of this research, contact was attempted at the soonest possible time in order to build rapport with the subjects. These subjects have been targeted given their first hand knowledge and potential for a conscientious perspective. Their perceptions gave the researcher an alternative viewpoint which will be helpful in analyzing the complexities of container security.

The data was collected by conducting in-depth telephonic interviews. This technique was chosen given the geographic limitations presented to the researcher. Nevertheless, the researcher was prepared to conduct face to face in-depth interviews had it been more convenient for the subjects identified in this study. In addition, some interviews were conducted via email if directed to do so by the selected individual.

Population and Sample

The participants of this qualitative study were selected by non-probability sampling. Non-probability sampling methods can be useful when descriptive comments about the sample itself are desired. Additionally, it is quick, inexpensive and convenient (Berg, 2007). The participants were identified utilizing a snow-ball sampling technique. A snow-ball sampling technique “Is a non-probability sampling technique that is used by researchers to identify potential subjects in studies where subjects are hard to locate” (Bernard & Ryan, 2010). The focus of a snow-ball approach is to reach little known or hard to obtain subjects. Further, Bernard and Ryan (2010)

indicated the strength of the snow ball approach to be, “The chain referral process allows the researcher to reach populations that are difficult to sample when using other sampling methods.”

Participants were selected from one population: seaport deputy directors, assistant deputy directors, directors of security or their designee from the seaports of Galveston, Miami, Corpus Christi, Houston, New Orleans, Gulfport, Mobile, and Tampa. The sample of port officials were selected by contacting the Ports of Galveston, Corpus Christi, Houston, Miami, New Orleans, Gulfport, Mobile, and Tampa who gave the names of employees currently working during December 2011-February 2012. The subjects in this study were preferred given their particular knowledge and experience within the seaport community. In some instances the subjects have gathered experiences they encountered while serving in or working with the USCG, as well as, the CBP or other forms of law enforcement. Generally, there is one deputy director of operations/security or designee per seaport. In all there was an anticipated population sample amounting to eight individuals. Of those eight individuals, six decided to participate in this study. Although, this population is small in number, the background of each participant supplied sufficient and detailed data which gave this research and the researcher a thorough and accurate context for subsequent analysis.

The identified subjects provided the researcher with perceptions that were extremely particular. The subjects’ work experience gave the researcher and subsequent research a level of authenticity which has yet to be studied. All potential participants were selected equitably and in accordance with proper procedure. In addition, the risks and benefits were justly distributed in order to confirm the participant’s responses without damage or impairment to their credibility. When the potential participants were identified, the researcher sent a letter (See Appendix B) designed to establish the willingness of the participants to participate in the study. The letter asked, “Would you be willing to participate in an interview designed to explore the perceptions

of the effectiveness of implemented container security measures at your seaport”. Individuals who returned the letters with affirmative responses were contacted to schedule a date, time, and location to participate in an open-ended interview (See Appendix C).

Due to geographical limitations, the researcher conducted telephonic interviews. However, if necessary the researcher would have visited selected seaports in order to accommodate the sample population. Telephonic interviews were chosen as the primary interview technique based largely on the geographic limitations. However, telephonic interviews have other significant advantages. Hagan (2006) stated telephonic interviews can be recorded via an inexpensive patch between the telephone and the recording instrument. Furthermore, if a digital recorder is used, the interview can later be transcribed in the traditional fashion or downloaded into a computer and converted to text (Hagan, 2006). Nevertheless, there are disadvantages associated with telephonic interviews. For example, some people have no telephone, and others unlisted numbers. In addition, current telephone technology hinders the ability for the interviewer and interviewee to use full channels of communication (Hagan, 2006). However, the aforementioned disadvantages did not discredit the validity of the responses in this research.

The sample size in this qualitative study was dictated by very specific criteria. Therefore, the sample size was small. In all, eight participants were eligible given the concerns mentioned above. Merriam (1998) stated that sample size depends on the questions to be presented, the intended data, the analysis, and the available resources to support the study. Further, Lincoln and Guba (1985) suggested sampling until the point of saturation. Bernard and Ryan (2010) stated that when a model ceases to provide sufficient incremental improvement within the data gathering process, the research has reached a point of saturation. Prior to the interview, an IRB approved Informed Consent Form (See Appendix D) was signed digitally and emailed to the

researcher by five of the six participants indicating the voluntariness, confidentiality, and risks associated with the interview. In the event that a participant was unable to receive an informed consent form, the researcher articulated the form verbatim and secured the participant's approval to notarize the form. The remaining participant gave verbal permission indicating his approval to take part in this research.

Data Collection and Instrumentation

All data were collected by the researcher. The researcher has been trained in the ethical principles and institutional policies governing human subject research in accordance with the Collaborative Institutional Training Initiative (CITI). Merriam (1998) indicated that in all forms of qualitative research, "The researcher is the primary instrument for data collection and analysis... Data is mediated through the human instrument, the researcher, rather than through some inanimate inventory, questionnaire, or computer" (p.7). Furthermore, the researcher remained objective in order to minimize any attempt to indirectly manipulate the responses. Interview guides were developed to explore the seaport deputy director's perceptions of the effectiveness of implemented container security measures at the ports of Galveston, Corpus Christi, Houston, Miami, New Orleans, Gulfport, Mobile, and Tampa. For instance, "What, if any, factors hinder your seaport's ability to maintain 100% scans of containerized cargo?" The aforementioned question is representative of the type of question that was asked to the participant.

All participating seaport deputy director's interviews followed a semi-structured guide (See Appendix C) designed to ascertain the perceptions of seaport deputy directors or their designees regarding the effectiveness of implemented container security measures. The interviewer asked for interviewees to elaborate on certain responses in order to obtain more

detailed information. Probing questions, or simply probes, provide interviewers with a way to draw out more complete stories from subjects (Berg, 2007). Furthermore, probes frequently ask subjects to elaborate on what they have already answered in response to a given question (Berg, 2007). The telephonic interviews were tape recorded and lasted approximately 30 minutes. The recordings were kept in a secure location in order to prevent any outside tampering. The recordings were transcribed into a document and formatted accordingly. Additionally, once the recordings were transcribed, the recordings were erased as mentioned in the informed consent form.

Data Analysis

The research consisted of a qualitative method design to explore the perceptions of seaport deputy directors or their designees pertaining to the perceived effectiveness of implemented security measures at the ports of Galveston, Corpus Christi, Houston, Miami, New Orleans, Gulfport, Mobile, and Tampa. Initially, all the relative forms were completed by the researcher and sent to the Institutional Review Board (IRB) to locate certain risks that could have been associated with this study. Further, the IRB was provided with information describing how confidentiality would be maintained and with a copy of the Informed Consent Form.

Approval from Institutional Review Board was received (See Appendix E). Each interview, except for interviews via email, was tape recorded and, then, transcribed verbatim by the researcher and was checked multiple times to ensure correctness, which provided “the best database for analysis” (Merriam, 1998, p.88). The researcher identified the common themes which emerged from the data. Further, to ensure consistency of analyzing the data, the findings were imported into a Microsoft Word document to locate commonalities. The Word document enabled the researcher to organize the transcriptions and locate patterns and commonalities. The

researcher utilized two observational coding techniques. The first technique, repetitions, identified themes by taking notice to the number of times a question reveals a recurrence of similar terminology (Berg, 2007). The second technique, similarities and differences, exposed themes by comparing how responses are alike or different from preceding or following statements (Berg, 2007).

Summary

The purpose of this qualitative study was to explore the perceptions of seaport deputy directors regarding the perceived effectiveness of implemented container security measures at the ports Galveston, Corpus Christi, Houston, Miami, New Orleans, Gulfport, Mobile, and Tampa. Subsequent to securing the participants, open-ended interviews were conducted, tape recorded and transcribed verbatim. Then the data was imported into a Microsoft Word document to organize and easily identify emerging themes. The collected data revealed the perceptions of seaport deputy directors regarding the perceived effectiveness of implemented container security measures.

While there is significant research concerning the different techniques, there is a lack of research as it relates to the perceived effectiveness pertaining to seaport deputy directors and their designees. This study represented the first time this sample group has been investigated.

Chapter 4 will provide answers to the research questions and interview schedule. Furthermore, the answers given by the participants will be interpreted at length in order to give the reader a clear and thorough observation of the problems associated with cargo container security as well as other obstacles currently hindering total port security.

CHAPTER 4: ANALYSIS OF RESULTS

Restatement of the Research Questions

The researcher determined four research questions that would identify the perceived effectiveness of containerized cargo security. First, what are the main threats to seaports along the Gulf Coast? By targeting the main threats as determined by the selected officials, the researcher would be able to better understand how container security was ultimately affected. Secondly, what is the main threat to containers? By specifically identifying the main threat to containers the researcher would be able to focus and elaborate on the single most important aspect that was and is currently hindering container security. Thirdly, how do port security administrators and the USCG perceive containerized cargo threats? By gathering the perceptions of port security administrators and the USCG, the researcher ascertained the opinions and viewpoints of those individuals most involved in facilitating and administering seaport security. Moreover, the pertinent literature in Chapter 2 has placed emphasis on the significance of intelligence in regards to container security. Therefore, this final question is vital to improving container security.

Interpretation of Results & Statements of Significance

In all, only six seaport deputy directors or their designees across five states (Texas, Louisiana, Mississippi, Alabama, and Florida) accepted the researcher's invitation to participate in this study. This sample size can be interpreted as being rather small and insignificant. However, these six participants equate to a sample size that is sufficient given that the

researcher's original projected sample size was eight, amounting to a response rate of 75%. Most importantly, 100% of the Gulf Coast states were able to participate in this study and give their opinions regarding the perceived effectiveness of container security at their respective ports. Therefore, with a representation and subsequent interview from all states bordering the Gulf Coast, this research study was successful in acquiring the data required to reach a point of saturation. The results were extracted from the interview questions by identifying common themes. As mentioned in Chapter 3 the two observational coding techniques utilized to extract the results were: repetitions and similarities and differences.

As previously mentioned, two of the seaports that were identified in previous chapters respectfully declined to participate in this research project. The Port of Corpus Christi, TX, deals primarily with oil tankers. Initially, the researcher believed that the security techniques at such a port would still be beneficial to this research. However, after much deliberation, the researcher determined that the insignificant number of containers being transported offered little to the research associated with this study. The researcher would still like to state that the deputy director at Galveston and the surrounding staff were very accommodating and helpful when contacted. Also, the Port of Houston, TX was unable to submit to an interview for legal reasons, for further details see the attached email in Appendix F. Nonetheless, the researcher would like to state that the initial process leading up to the inability to submit to an interview was very accommodating and their demeanor was extremely professional. In addition, one of the participants had referred the researcher to a CBP contact affiliated with their respective port. However, after exhausting several lines of communication, the CBP official informed me via email that he would not be able to participate, for further details see the attached email in Appendix G.

Taking into consideration the limitations that were mentioned previously in Chapter 3, the researcher would like to add that in exactly one instance the questionnaire template was emailed to a participant instead of conducting a telephonic interview. The participant requested to participate via email. Therefore, the researcher emailed the interview schedule to the participant's designated email address. This did not affect the validity or quality of the answers. Moreover, the participants that submitted to answering the interview schedule via telephone indicated they were more than willing to participate.

Interview Question #1: In your opinion, what is the biggest threat(s) facing container security?

First and foremost, it is significant to mention that most of the participants agreed that multiple threats were present. However, discerning which threats were more impending than the others could be determined based on their knowledge and experience at their respective port. For example, one participant stated that, "The biggest threat is "not knowing" what exactly is in the contents of a container upon arrival". The author informed the participant of initiatives such as Importer Security Filing, which are utilized to validate a containers contents throughout the transportation process. The trepidation of the participant could be interpreted as doubt in the security framework. Further, the participant mentioned that "It is extremely difficult to open every single container". Therefore, the ability to be certain of a container's contents is crucial to the overall security process. Another participant stated that, "The possibility of a terrorist secreting a weapon of mass destruction (WMD) is the biggest threat".

Ultimately, five out of the six (approximately 83%) participants answered that the biggest threat facing containers was their ability to be exploited for smuggling purposes. If that statistic is coupled with the previous statement concerning the validation of a container's contents, it

should be considered a significant concern. Additionally, three out of the six participants (50%) specifically mentioned a concern that a WMD within a container could be successfully smuggled into the country. Moreover, another participant stated that, “Securing the supply chain is the biggest threat.” If the security of the supply chain itself is seen as a threat, then the ability to successfully detect the smuggling of contraband or a WMD becomes less likely. Furthermore, one participant (approximately 17%) answered that container theft was the biggest threat facing container security.

Interview Question #2: What security techniques/methods are employed at your seaport to accommodate container security?

Six out of the six participants (100%) answered that their seaports employed a layered approach to security. As previously stated in Chapter 2, a layered security approach has been determined by numerous security experts to be the most successful security technique. For example, participants mentioned the use of background checks of new shipping companies, automated manifest systems checks, the deployment of radiation portal monitors (RPMs) at the exit gates, security cameras, and port security plans. A participant at one of the larger ports specifically mentioned that there was an absence of equipment capable of scanning containers upon being offloaded directly from the container ship. This participant stated that, “Now, if CBP or DHS had put these devices on the spreader bars of the gantry cranes that off-load the cargo, then the crane operator scans a container and gets a reading... he can immediately put the container back on the vessel.” Certainly, this would be a significant deterrent, however, there would need to be a considerable number of these devices and the need for personnel in order to keep this technique from diminishing the efficiency of the container terminal and the eventual flow of goods.

If a container terminal at a seaport is unable to offload and distribute containers in a timely manner, serious monetary repercussions can result. One participant stated that, “If containers get held up at your port they can start charging a fee known as demurrage, which means I [commercial shipping vessel] came into your port and only expected to be here a day and you [the port] did something or failed to do something that kept me here longer.”

Additionally, the participant stated that, “The shipper can charge the port for keeping them there longer than their expected departure time and charges can be significant. We are talking about tens of thousands of dollars depending on the size of the ship and the cargo.” Therefore, without the appropriate number of devices and personnel it can be inferred that security will be compromised at major seaports in order to maintain an efficient and timely distribution process. This can diminish the effectiveness of subsequent security and a solution should be identified.

Four out of the six participants (approximately 67%) specifically stated that the majority of these security techniques/methods are the responsibility of the CBP and USCG. Knowing this, it should be possible to establish a more cohesive and enthusiastic security relationship between seaport security administrators and CBP and USCG. More specifically, this relationship could give seaport security administrators the opportunity to offer their particular knowledge and recommend specific areas for security enhancement. In fact, two of the larger ports mentioned that they have the cooperation of surrounding local and federal law enforcement agencies. This type of collaboration only improves the communication which is necessary to validate the subsequent intelligence.

Interview Question #3: On average, how many inbound containers receive some form of scan/inspection before arrival?

Five out of the six participants (approximately 83%) agreed that the number of containers being scanned before they arrive at their port was not significant enough to impact security in a favorable manner. The other participant (approximately 17%) did not feel comfortable answering the question. In addition, two of the six participants (approximately 33%) agreed that the number of inbound containers that receive some form of scan/inspection before arrival could easily be determined as less than 10-20%, depending on their location and the host country from which they receive the majority of their containers. For example, one participant mentioned that the majority of the containers at his terminal “Are shipped from Jamaica before arriving at his particular port.” At this port, he knows that they have sufficient nonintrusive inspection resources capable of sustaining a consistent rate of scan/inspection. Additionally, three out of the six participants (50%) did state that this question was better suited for CBP. However, upon contact with a CBP affiliate with one these six ports, a decision was made to neglect answering such questions. Nevertheless, this affiliate was extremely professional and cooperative.

Interview Question #4: Where do the majority of containers receive inspection (i.e. at your port or before arrival to your port)?

Given the figures associated with the previous question, the subsequent statistics should be expected. Nevertheless, six of the six participants (100%) answered that the majority of their containers receive inspection after arrival at their port. This statistic reveals that there is a significant gap in security. Waiting to inspect containers at their destination, even with enough state of the art technology, is too late in the supply chain process. Furthermore, this viewpoint is shared unanimously by every security expert on the subject. Improving security abroad and,

more specifically, the validation of security at the host port would significantly benefit not only container security but also total supply chain security in general.

Interview Question #5: Are you able to scan/inspect all containers upon arrival at your seaport? Yes or no? If not, why?

Five out of the six participants (approximately 83%) answered that they were not able to scan /inspect all of the containers upon arrival at their seaport. One participant (approximately 17%) stated that he was able to scan all of the incoming containers at his respective port. It is significant to mention that the one participant that indicated their port's ability to conduct 100% inspection of all containers was at a considerably smaller port with a significantly smaller number of containers. Nevertheless, it has long been known and understood that acquiring 100% scans is a formidable challenge. Moreover, without complete and resolute global cooperation, such a goal was even more challenging. Five out of the six participants (approximately 83%) did indicate that their ports utilized techniques that attempted to mitigate these challenges. One example is the use of the ISF also known as 10+2. ISF requires the shipper to provide the port of destination with 10 additional variables pertaining to the ship's stowage plan, container contents, etc., that the destination port can use in order to determine the validity and threat of incoming containers.

In addition, two out of the six participants (approximately 33%) did mention that there are two different types of scan: (a) VACIS (gamma ray) and (b) RPM. The other four participants (approximately 67%) did not specify the technology that was utilized at their ports. Moreover, the participants stated that all containers at their ports are sent through RPMs at the exit gates of the port. Yet, the location of the RPMs seems counter-intuitive. If the containers are

receiving preliminary security scans at the exit gates, it has become too late to successfully deter any threat. One participant indicated that this type of inspection needs to be conducted when the containers are being off-loaded rather than at the exit gates. The participant stated that, “The captain of the port could order the offending vessel 25 miles out until they mitigate the problem.” However, the participant also mentioned that, “You will get a reading from clay tile, from bananas, and you know there are different things where you will get a reading (false positive).” These types of readings can be frequent in port and, consequently, strict security decisions could cause more harm than good.

Interview Question #6: Do you believe container security has reached its pinnacle? Yes or no?

Six out of the six participants (100%) answered that container security still had room for improvement. Furthermore, they indicated that the current security framework was headed in the right direction.

Interview Question #7: What, if any, factors hinder your seaport’s ability to maintain 100% scans of containerized cargo?

Four out of the six participants (approximately 67%) stated that the misuse of technology hinders 100% scans of containerized cargo. For example, a participant stated that, “Had the RPMs been attached to the spreaders of the crane that actually off-load the vessels, the process would be more effective.”

Additionally, two of the six participants (approximately 33%) answered that lack of equipment was the main factor hindering security at their seaport. One of the participants explained, “One main problem is the lack of equipment and then the people who are needed to

operate it. U.S. Customs does not have an unlimited budget and the mandate required to constitute 100% screening, they have to meet a happy medium there.” In comparison the other participant stated that, “What hinders most ports is that there is a fixed amount of resources and container volume goes up and down.”

However, technological inspection/scanning resources, by themselves, will never be able to match the volume of containers. Therefore, it is critical to maintain a layered approach, which can mitigate the inabilities of a single approach. One participant stated that, “Scanning is only a part of the investigative process. The ability to get 100% is an impractical number. Scanning is only a part of the tools in their arsenal.” Furthermore, he mentioned that it is the investigative and intelligence work at the port of origin which can make sure that the container doesn’t even get put on the ship. More specifically, these investigations occur before the ships even leave the port of origin. Nevertheless, there are multiple working parts that interdependently determine the success of such an approach. Keeping open lines of communication will encourage collaboration.

Interview Question #8: Would you consider technology to be your greatest asset in your ability to maintain efficient container security? If so, which technological advancements (i.e. nonintrusive imaging, gamma ray inspection) play a significant role? If not, why?

Six of the six participants (100%) answered that technology was the most significant asset to maintaining efficient container security. One participant explained that, “The physical inspection [of a container] and the teams tasked with this, consisted of about four guys and pretty much spending the better part of the day going through the container.” Furthermore, this same participant explained, “You can either go four people for every one container or one individual per RPM or other mechanisms with ability to screen containers in so many minutes or seconds, etc.”

In regards to the types of technological advancements, six out of the six participants (100%) stated that their ports utilized RPMs and the majority of these are positioned at the exit gates of the port. One participant stated that, “CBP and DHS put out an advisement called a radiation portal monitor (RPM) and sometimes where and how these things are set up causes me a little bit of worry.” As previously stated, in reference to the seventh interview question, positioning these devices in an alternative location could improve the effectiveness of container inspection. In addition, one participant explained, “The RPM is most prevalent because it’s 100%, so from there other methods of screening descend from that. If a container went through the portal and an indication of a radiation agent was received the next step would be for someone to actually go out to the container and physically inspect it with other scanning instruments.” In addition, five out of the six participants (approximately 83%) stated that their port did utilize x-ray technology in order to scan containers. Yet, one participant did mention that, “They [containers] do not all get x-rayed but they are scanned for radiation.” Furthermore, only two of the six participants (approximately 33%) specifically preferred to utilize some form of gamma ray imaging systems like VACIS. However, other participants did mention that CBP would be more qualified to answer questions regarding technology employed at the port.

Two of the six participants (approximately 33%) mentioned that technology was not the only factor to consider. For example, one participant declared, “I believe technology is probably the majority of it. Let’s say 60-75% of it. The human element has to click in there too. It’s a combination of having the technology and the personnel that know what the technology means.” Another participant stated that, “I think technology is a significant part of it, but I also think and I’m pretty sure they [CBP] would agree with me, is that intelligence gathering is the most significant part in the fight against terrorism.” Another participant explained that, “Technology

such as nonintrusive imaging and gamma ray inspections are an efficient way of maintaining container security but human intervention is a valuable tool.”

Interview Question #9: What is the most significant factor you consider when adopting/endorsing a security technique (i.e. Secure Freight Initiative, Container Security Initiative, TWIC)?

Five out of the six participants (approximately 83%) indicated that they had no power to adopt a security technique. One of the six participants (approximately 17%) indicated that he did not feel comfortable answering this question. Furthermore, the five participants explained that the aforementioned security techniques are mandated by CBP, USCG or TSA. One participant acknowledged, “Basically, we are being told by Customs, ‘we are putting this equipment at your port, help us find a place that makes sense’.” The previous statement does reveal that Customs is willing to work with and accommodate the seaports in a way that can benefit both parties. However, that same participant stated that, “We weren’t given much of a choice and the same thing had to do with TWIC, which is really more of a way of identifying these people you are allowing into the port.” On the other hand, it seems that the opinion of the participants in this case could benefit CBP.

In regards to the effectiveness of security techniques and initiatives one participant explained that, “I don’t think a “single” initiative is most successful. The initiatives, whether it is TWIC, Radiation Portal Monitor initiatives or deployment of additional x-ray machines, they all work together to make a more secure environment.” Furthermore, the participant clarified, “You can’t pick one and say that it is the most effective. What you’re trying to create is multiple opportunities to locate a threat.”

In regards to TWIC, five out of the six participants (approximately 83%) indicated that improvement was needed. One participant acknowledged that these concerns were rooted in the inability to confirm the authenticity of the TWIC card. One participant explained that, “One of the problems is the card reader itself. There were five pilot ports with these card readers. A lot of these machines are not holding up in the maritime environment.” Another participant explained that, “The real part of the TWIC card is the reader. And what they want you to be able to do is have this reader and the reader gets updated weekly or daily or monthly. I’m not sure if they’ve figured that out. They have not got the TWIC reader part figured out yet.” On a different note, one participant stated that, “TWIC, on the other hand, looked at terrorism, they didn’t care if you were a drug dealer. As a result, fifty-four convicted criminals came back to work at the port again.”

The inconsistencies associated with TWIC seem perpetual in nature. For example, one participant detailed a specific occasion. The participant stated that, “The Master of the vessel had an unlimited tonnage master’s license, he had been a U.S. mariner for thirty years, he had a top secret clearance from the Navy, he had a military ID card, a TWIC card, merchant mariner’s credentials, etc.” The participant went on to explain that, “He wanted to bring his wife on ship with him.... according to the Coast Guard rules, we could not let her onto the property without a TWIC card.” Furthermore, “The master of the vessel wanted to be able to escort his wife from the main gate to the ship and we couldn’t let him do it unless he was designated a TWIC escort. It’s harder to get onto a U.S. port facility than it is to get on to a U.S. military base.”

Interview Question #10: Would you consider global cooperation essential to improving container security? Yes or no?

Six out of the six participants (100%) agreed that global cooperation was essential to improving the current container security paradigm. One participant explained that, “Yes, absolutely and again that is not a call of the port. That is more of a governmental decision. I know that the government and DHS are trying to work with these foreign ports and countries in order to get the screening done.” That same participant stated that, “They obviously like for the foreign ports to say that they have screened 100% of containers but that hasn’t happened yet and probably not going to happen. Some foreign entities don’t want to allow inspectors to come over.” Furthermore, he mentioned, “That would be a good place to research, ‘why this global cooperation is so difficult to achieve’.” Another participant indicated that Customs would be the resource to contact, if they would be willing to address this question. On the other hand, one participant did offer some insight explaining that, “First of all you have to get the shippers and the port to understand what you are trying to accomplish and you have to relate to them what you are trying to accomplish, while you are asking them to do what you need to do.” Furthermore, this participant elaborated stating, “The next thing is you need interagency cooperation...the people on the ground and the people above them need to understand what each one brings to the table in regards to assets and resources and use those to the greatest benefit possible.” Additionally, the participant explained, “Certainly CBP is the lead on this stuff but they wouldn’t be as nearly as successful if they ignored the resources and people that are around them.”

Interview Question #11: What agencies (USCG, CBP, local/state authorities) are responsible for the majority of your container security?

All six participants (100%) indicated that CBP was responsible for the majority, if not all, of the container security within their seaports. Furthermore, one participant affirmed that, “They [CBP] are the ones scanning the containers, they are the ones targeting containers. They are the ones with boots on the ground looking at containers.” However, another participant did indicate that the USCG works with CBP in specific instances. For example, the participant referenced in question eight pertaining to the use of teams to physically search containers suspected of transporting contraband elaborated on his opinion of the level of cooperation exhibited between CBP and USCG. He stated that, “These [physical] inspection teams are either USCG or CBP and sometimes both”. Additionally, the participant stated that, “If for some reason intelligence indicated drugs were coming in on some of these banana ships, the USCG would probably send a team down here and work with CBP.” In regards to the intelligence being shared the participant also mentioned, “There were issues with the intelligence, there were separate agencies that didn’t want to share intelligence.”

Also, another participant explained, “If you are a TWIC program and you follow under that federal regulation, you have to be TWIC compliant because the USCG will inspect you for that.”

Emergent Themes

Three themes emerged: 1) technology, 2) cargo theft, and 3) the Panama Canal. As stated previously, the participants believed technology was a significant aspect of container security. In most cases they agreed that technology must be constantly critiqued and improved. One participant explained, “Technology is a game changer, I’m talking with you now and its 2012, in

2015 security can be changed with one advancement in technology. There are “sniffers” that sniff the air within a container for contraband, chemicals and compounds.” Advancements such as these “sniffers” could improve container inspection times, especially secondary inspections. In question eight, one participant stated that physical inspection could “take four agents the better part of a day” to inspect and repack a container. With advancements such as an “air sniffer”, inspection times could be drastically reduced. Furthermore, this same participant declared, “I think as science advances that type of technology becomes more advanced and sniffers could have the ability to identify and wider spectrum of materials within a container.” Future research should focus on technological advancements. Technology is one of the most significant factors to consider when scrutinizing future techniques and, when combined with competent and cooperative operators, it can become a true force multiplier.

Cargo theft continues to plague the container supply chain industry. One participant mentioned, “The port is a highly regulated restricted area, a lot of theft of whole containers or part of containers occurs outside the port unless in restricted or secure areas.” Another participant agreed and explained that the volume of containers and traffic at his port made container theft a significant threat. These statements reveal the need to focus on total supply chain security. In addition, maintaining a multi-layered security approach would diminish this threat. However, the complications associated with foreign/global cooperation should be considered the main topic of discussion in future research. Without complete cooperation such a security technique will inevitably be futile.

Two of the six participants (approximately 33%) mentioned that the future of the Panama Canal should be considered when developing any security recommendations. One participant explained that, “The expansion of the Panama Canal in 2014 could have a huge impact on Gulf ports. There will be much larger ships moving through the canal. That will have impact on cargo

moving into the gulf.” Specifically, this expansion will generate a significant increase in the volume of containers being imported to Gulf Coast ports.

Additionally, one out of the six participants specifically brought to the researcher’s attention the use of the railroad within the seaport environment. The participant stated, “With regard to rail at our port we have short rail, in other words, we are called class I carriers and the Union Pacific brings rail down to yards outside the port...the short line brings cargo into the port.” Elaborating further, the participant explained, “There is a couple things that happen here, firstly, we have identified the engineers on these trains, so we know them visually. We have a cadre of police officers and they know them that way or they can show us their card from the cab.” More specifically, the participant stated, “My concern with the railroad was that there was no way I wanted a police officer having to go over to a train and actually inspect the [TWIC] card of the engineer before we let him inside the port.” The participant proposed, “We have to do some kind of inspection ahead of time so we know these personnel before opening the gate. That’s how it works at these various ports. It is not a good thing for these officers to physically inspect cards.”

Summary

The research questions presented in Chapter 3 were answered indirectly through the participants’ responses to the interview schedule. The comments and answers, both, provided compelling interpretations. The first research question asked “What are the main threats to seaports along the Gulf Coast?” The research showed that the main threats were dictated by the sheer volume of containers that are imported to seaports along the Gulf Coast and how this magnitude hinders the level of container scan and inspection required. The second research question asked, “What is the main threat to containers?” The research showed that the main threat was a combination of contraband smuggling via cargo containers and container theft. The

final research question asked, “How do port security administrators and the USCG perceive containerized cargo threats?” The research showed that, both, the administrators and USCG share similar perceptions. Their viewpoints endorse the need for more global cooperation and the advantages of technology regarding enhanced container security.

The interview questions and subsequent answers revealed several distinctions and areas that could be targeted to improve the current status of container security. First, the interviews identified the susceptibility of cargo containers in regards to the smuggling of contraband and theft. More specifically, contraband smuggling and theft were viewed to be the biggest threats facing container security. Second, the participants confirmed that a layered security approach was currently being utilized at their respective ports. However, they indicated that this approach could be more efficient. Third, the number of containers being scanned before arrival to the respective Gulf Coast ports was insignificant. Additionally, two of the participants indicated that the number was somewhere between 10-20%. Fourth, the interviews indicated that the majority of containers were not inspected or scanned until arrival to their respective ports. Fifth, in almost all cases it is not possible to scan or inspect 100% of containers. The interviews did reveal that one port was capable of attaining 100%. However, this port was considerably smaller than the rest of the Gulf Coast ports in this study. Sixthly, the participants specified that the current container security paradigm could be improved.

The major factor hindering the efficiency of container security is the limited amount of resources. Investigative work and intelligence play an integral role in mitigating the challenges of limited equipment and personnel. The role of technology is regarded as the greatest asset in a seaport’s ability to maintain efficient container security. However, the interviews indicated that technology alone was insufficient. More specifically, the participants discerned that competent personnel were necessary in order to maximize the benefits of technology. The endorsement and

adoption of security initiatives is not determined by the seaport. These security decisions are mandated by CBP. Furthermore, the interviews indicated that the current status of TWIC needs to be improved. Global cooperation is vital to the overall effectiveness of container security. Moreover, the advancements in technology such as “air sniffers” could give security facilitators an added edge. In conclusion, three themes also emerged: 1) the role of technology, 2) cargo theft, and 3) the expansion of the Panama Canal.

Chapter 5 will analyze the data collected in Chapter 4. Furthermore, Chapter Five will construct conclusions on the current status of container security and make policy recommendations that will supplement the deficiencies identified through the interpretation of results and, subsequent, analysis.

CHAPTER 5: CONCLUSIONS, DISCUSSIONS & RECOMMENDATIONS

Summary and Conclusions

There is a wealth of literature concerning the evolution of the shipping container and the subsequent revolution that the modern shipping container created for the intermodal supply chain. The modern cargo container has cemented itself as the single most advancement responsible for the efficiency and increased flow of commerce to date. It is evident, through researching the pertinent literature, that the cargo container was innovative and revolutionary for commerce and the flow of goods. However, it has also proven to be just as appealing and beneficial to those wishing to exploit them in order to cause harm to the United States. Criminals and terrorists alike don't necessarily need to destroy or cripple a U.S. seaport to accomplish this. Instead, they could attempt to exploit the integrity of a cargo container and smuggle the components capable of improvising a WMD into the U.S.

With all the added benefits that the cargo container has generated, the possibility of exploitation for smuggling, theft and other criminal activities has become more of a concern. While the security initiatives associated with container security have been well documented, the views and perceptions of deputy directors of security and their designees in regards to the perceived effectiveness of these initiatives have been overlooked.

The research literature for the topics discussed in Chapter 2, indicates that the deputy directors are knowledgeable and aware of the problems they might encounter while securing our nation's seaports. The research revealed that many of the participants were retired from the

USCG, law enforcement, or had several tours as the Captain at a U.S. seaport. That being said, the majority of this population had been working within the time periods before and after the initiation of the container security programs and initiatives discussed in Chapter 2. Their professional experience gave the researcher an accurate and honest portrayal of the perceived effectiveness of container security and its progress over the years. In addition, they were well qualified to clarify and elaborate on any inconsistencies the researcher identified.

In order to obtain the results, an interview schedule was developed. The interview questions attempted to gather responses that would rate the level of perceived effectiveness of current container security as seen by deputy port directors of security or their designee at the ports of Houston, TX, Galveston, TX, Corpus Christi, TX, New Orleans, LA, Gulfport, MS, Mobile, AL, Tampa, FL, and Miami, FL. This would be achieved through asking basic questions concerning the perceived threats to containers, the location of primary inspections, a port's ability to sustain a high rate of container inspections, factors hindering inspection, the role of technology, the role of global cooperation, the agencies primarily responsible for container security and the factors considered when endorsing a particular security technique. When combined, the answers to these questions gave the researcher an accurate assessment of the overall perceived effectiveness of container security. Following the completion of the interviews it was discovered that containers were threatened by theft, smuggling of contraband such as drugs and weapons, and the integrity of a container's contents.

The results from this research revealed that the majority of containers are not inspected or scanned until they reach U.S. seaports. Also, it was confirmed by the population sample that a consistent high rate of container inspections was unattainable. All of the participants confirmed the inability of attaining a consistent high rate of scan. Furthermore, it was perceived that the misuse of technology could account for the incapability of sustaining a high rate of container

inspections, and it was perceived that both technology and global cooperation were essential to improving container security. In addition, it was learned that CBP was the primary agency responsible for container security and it was perceived that deputy directors of security or their designees had little to no influence in the adoption or endorsement of a security initiative. According to the findings of the study, deputy directors/designees believe that container security could be more effective than it is presently. In other words, these port security officials believe container security is inadequate.

As mentioned earlier, the study determined that current container security techniques could be more effective. However, one participant offered a contrary viewpoint. He explained, “This may be a crazy way to measure it, but there has not been an incident in the United States, container cargo related.” The participant indicated that the type of incident he was referring to would be the use of a container as a vehicle for a WMD or dirty bomb. Nevertheless, there have been numerous incidents where containers have been used to transport drugs, weapons, and other forms of contraband. For example, In February of 2011, at the port of Miami, customs officials targeted a container using x-ray scanning which led to the discovery of nearly two tons of marijuana, valued at \$7.6 million (Kriel, 2011).

It is the author’s opinion that examples such as the one mentioned above solidify the point that a container could be compromised in the same fashion to secrete a WMD. In addition to the information referenced in Chapter 2, as little as four kilograms of plutonium – about the size of a soda can – or three times that amount of highly enriched uranium (HEU) can potentially be enough for a bomb (Bunn, 2006). Such a small object could easily be shielded making it invisible to X-ray, radiation, or gamma ray inspection.

Moreover, it has been proven that criminals target the container transport system. As mentioned in earlier chapters, criminals have been utilizing containers since its inception to

transport contraband and turn a profit. Therefore, it should be mentioned that a terrorist organization may place the same value on the container and subsequent transport. The literature along with this study indicates that containers would be an ideal method to facilitate the smuggling of a WMD into the U.S.

Discussion of Implications & Recommendations for Future Research

In order to determine the perceived effectiveness of cargo container security an interview schedule was generated to satisfy the qualitative nature of this study. Among the twelve interview questions considering the effectiveness of container security, the questions concerning the amount of containers scanned prior to and upon arrival at U.S. seaports, the role of technology, the need for global cooperation, and whether container security had reached its pinnacle all acted as significant predictors of the feelings shared by the population sample. The answers given by the participants revealed several areas for improvement and recommendations for future research.

It is also the author's opinion that global cooperation and the correct use of technology play an important role in improving the effectiveness of container security and act as a deterrent to a cargo container being utilized in a terrorist attack upon the U.S. Six out of the six participants agreed that if containers were not pre-inspected or scanned until they reached U.S. ports it would, essentially, be too late. Moreover, security initiatives such as CSI were specifically created to mitigate these types of challenges. However, without the cooperation of the global shipping and port community, container security and subsequent initiatives will be less effective.

The role of technology is vital for container security to be successful. Specifically, the participants claimed that the relationship between technology and port personnel was significant.

In some cases, the participants mentioned that even if more scanning instruments were procured, competent and highly trained technicians would be required to operate the instruments. When probed further regarding the ability to establish more instruments and technicians, the participants stated that funding was the main reason for the absence of action. Furthermore, given the current status of the economy and the ever increasing debt, it is no surprise that such improvements have been neglected. It does seem, however, that in an attempt to mitigate this absence, CBP and DHS must do more with fewer resources. It is in the author's opinion that the previous statement explains the placement of RPMs at the exit gates of U.S. seaports. A new solution is needed.

One suggestion for future research would be to investigate the inherent relationship between technology and the operator. More specifically, determine what factors during port personnel training could be manipulated in order to alleviate or eliminate the strain associated with this relationship. In addition, explore whether it is possible for technology to accomplish more.

Incorporating nanotechnology into the current container security paradigm could prove to be valuable. The use of nanotechnology in the maritime environment isn't new. Dr. Morton Wallach of PEL Associates has developed technology which can readily achieve the goal of container security at a low cost. The method is based on smart sensors, a version of which is being developed for DARPA (Defense Advanced Research Project Agency) (Direnzo & Doane, 2007). Furthermore, in this approach micro-sensors are designed with surface groups reactive with chemicals and biological hazards. On reaction the sensors emit an agent specific color or IR signal wirelessly to a control system (Direnzo & Doane, 2007).

Furthermore, Dorenzo and Doane (2007) stated:

In the case of a dirty bomb or WMD the sensors are designed with a conductive coating. In the presence of such hazards which characteristically emit energetic particles the air in the container becomes ionized and on contact with the sensors the conductivity is changed in a characteristic manner which is picked up wirelessly by central control systems.

Regarding the physical application, these sensors would be impregnated on to the surface of a thin plastic film which is adhered to the wall of the container. In addition, the cost is “very small,” about 3-5 cents per sensor or five dollars per container (Dorenzo & Doane, 2007). In another application nanotechnology could be used to tag containers for tracking movement from truck to ship to dock to truck again, providing a constant “updated position” (Dorenzo & Doane, 2007).

Perhaps DHS funding could be granted in an attempt to further this research.

Nanotechnology could even be incorporated into buoy systems, allowing “smart buoys” the ability to scan cargo containers aboard commercial shipping vessels. DARPA has already provided funding to several organizations in 2012. This includes the Wyss Institute for Biologically Inspired Engineering at Harvard University which was granted a \$2.6 million contract to develop a smart suit that helps improve physical endurance for soldiers in the field (Mowatt, 2012). Also, researchers in the Department of Biological Engineering at MIT will receive up to \$32 million over the next five years to develop a technology platform that will mimic human physiological systems in the laboratory (Darpa and Nih, 2012).

Nanotechnology presents a great opposition to the myriad of threats converging with container security. DARPA funding could equip DHS with the finances required to advance technology to an unprecedented level. Futurist technology should be persistently researched and

explored in order to combat anticipated threats. More specifically, the advancement of technology is even more critical at Gulf Coast ports given the scheduled completion of the Panama Canal expansion. In 2014, more containers can be expected to arrive at these ports via commercial shipping. Therefore, a sufficient level of security is contingent on the ability of technology to accomplish more.

All participants emphasized the significance of global cooperation and suggested that CBP would be a good place to start for future research. As previously stated in Chapter 4, the author contacted a CBP liaison affiliated with one of the major seaports analyzed during this study. However, the liaison informed the author via email the unwillingness of his superiors to cooperate (See attached email Appendix G). Nevertheless, the participants unanimously stated that CBP is the primary government agency most responsible for container security. Therefore, CBP would undoubtedly hold the most pertinent information regarding several of the above questions.

A second suggestion for future research would be to establish a relationship that would encourage communication with CBP in regards to the unwillingness of global actors to cooperate. CBP could consider this information classified. However, it is the author's opinion that CBP's apprehension to elaborate on specific questions could lead to complications for future researchers. In facilitating the implementation of total port security and, more specifically, container security, it is imperative to obtain the perceptions of CBP. It is the author's opinion that applying these perceptions, in addition to the opinions of the participants of this research, could prove to be invaluable for further research of container security.

One out of the six participants informed the researcher that he would be unable to answer the question regarding the most significant factor when considering the endorsement of a security technique. So, a third suggestion for future research would be to target and explore the

reasoning for such apprehensions. It is possible that other officials share similar concerns. Their views are significant to the improvement of container security. Therefore, if similar viewpoints are sacrificed at this expense, competent and professional assessments could go unvoiced.

A fourth suggestion would be for future research to concentrate on the complications associated with interagency communications. If deputy directors and their designees fail in establishing an amicable and cooperative relationship with CBP and USCG, there could be a decline in the effectiveness of container security. This could possibly result in increased rates for the transportation of containers and, therefore, consumers would end up bearing the costs. It is in the author's opinion that the communication between the numerous authorities that operate within the seaport, especially in regards to container security, could be more efficient. The seaport security climate is constantly changing. Therefore, cohesive, dynamic and immediate communication must be achieved in order to diminish threats targeting the seaport environment.

Additionally, it is the author's opinion that intelligence plays a significant role in mitigating the challenges of acquiring a high rate of scan or inspection. One of the six participants declared that the process of gathering and disseminating actionable intelligence is critical to container security. Certainly, cooperation is imperative when attempting to exploit the benefits of intelligence. Moreover, cooperation must be attained on a global scale in order for this type of solution to function properly. For the abovementioned reasons, it is the author's opinion that global cooperation is the single most critical factor to consider when striving to improve container security.

With this in mind, a fifth suggestion would be to examine the reasoning behind the reluctance in global cooperation. But as one participant put it, "Now with Chavez down in Venezuela rattling his sabers as much as he is against the U.S., are the containers checked? No."

So, a simple answer could be that some countries have an unfavorable outlook on the U.S. With that being said, reconciling these relations may be the only way to encourage global cooperation.

A sixth suggestion would be to focus future research on the inherent tension between the level of container security and its influence on commerce. That means investigating how thorough security can be without negatively affecting the economy. As previously stated in Chapter 4, demurrage is a tax that shipping companies can charge a seaport for storing their cargo longer than anticipated. If that charge is executed, repercussions will be felt through the entire economic cycle. Undoubtedly, this type of action could intimidate the stakeholders tasked with administering container security. In order to avoid a significant charge, seaport security personnel may sacrifice the level of inspection to meet an expected time schedule. CBP would be the initial agency to contact in this regard.

The final suggestion for future researchers would be to obtain the opinions of terminal operators. Reason being, terminal operators are the individuals tasked with providing the physical security of containers once they have arrived at the seaport. The majority of seaports and, more specifically, some of the ports in this study, rent terminal space to terminal operators that load and unload large container ships. One participant stated, “We are a landlord port authority, we provide a rentable space to terminal operators that bring the ships in and they load the ships and put them into their terminals.” Therefore, examining the perceptions of these terminal operators would give future research another layer of representative information which could be compared with other populations.

Summary

In conclusion, while several areas of improvement have been identified, the author would like to acknowledge that the seaport community is a very difficult environment to secure. With

the multitude of threats that frequent this climate, it is important to recognize that all the actors associated with container security, especially, CBP have done fine work in diminishing the anticipated threat of container exploitation. Nevertheless, improvement should always be considered. Individuals wishing to exploit container transport are constantly examining the current state of security in an attempt to manipulate weaknesses into their favor. Therefore, investigating and critiquing container security from all angles is paramount to sustaining effective security.

REFERENCES

- Ackerman, K. (1997). *Mysterious disappearances*, Practical handbook of warehousing. 4th, New York, NY, Chapman and Hall.
- Ahern, J. P. (2009). Testimony of acting commissioner jayson p. ahern, u.s. *customs and border protection, before the house appropriations committee, subcommittee on homeland security, on cargo and container security*. Retrieved from website:
http://www.dhs.gov/ynews/testimony/testimony_1238603858577.shtm
- Alabama State Port Authority. (2011). Retrieved from <http://www.asdd.com/portfacts.html>
- Atkinson, W. (2001). "How to protect your goods from theft." *Logistics Management & Distribution Report*. Peerless Media. 2001. Retrieved December 13, 2011 from HighBeam Research:<http://www.highbeam.com/doc/1G1-72518496.html>
- Automated Broker Interface (abi). (2009). Retrieved from
http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/abi/
- Automated Targeting System. (2007). *The Electronic Privacy Information Center*, Retrieved from <http://epic.org/privacy/travel/ats/default.html>
- Babul, M. J. (2004). *No silver bullet managing the ways and means of container security*. (Master's thesis). Retrieved from <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA423690>.
- Bakshi, N., Flynn, S.E., & Gans, N. (2009). Estimating the operational impact of container inspections at international ports. Retrieved from
http://opim.wharton.upenn.edu/risk/library/WP20090501_NB,SF,NG_CSI.pdf.
doi:10.1287/mnsc.1100.1252

- Bakshi, N., & Gans, N. (2007). *Securing the containerized supply chain: an economic analysis of c-tpat*. Manuscript submitted for publication, The Wharton School, University of Pennsylvania, Philadelphia, Pennsylvania. Retrieved from http://opim.wharton.upenn.edu/risk/library/WP2007-11-19_NB,NG_ContainerSecurity.pdf. doi:10.1287/mnsc.1090.1105
- Banomyong, R. (2005). The Impact of port and trade security initiatives on maritime supply-chain management. *Maritime Policy and Management*, 32(1), 5. doi: 10.1080/0308883042000326102
- Basham, W. R. (2007). Remarks by CBP Commissioner W. Ralph Basham on Container Security at the Center for Strategic and International Studies. http://www.cbp.gov/xp/cgov/newsroom/speeches_statements/archives/2007/commish_remarks_sc.xml
- Berg, B. L. (2007). *Qualitative research methods for the social sciences*. (6th ed.). Boston, MA: Pearson Education, Inc.
- Bernard, H. R., & Ryan, G. W. (2010). *Analyzing qualitative data: Systematic approaches*. Thousand Oaks, CA: SAGE Publications, Inc.
- Bichou, K. (2008). *Security and risk-based models in shipping and ports: review and critical analysis*. (Master's thesis, Imperial College, London, England). Retrieved from <http://www.internationaltransportforum.org/jtrc/discussionpapers/DP200820.pdf>
- Blegen, B. C. (2009). U.s. importer security filing: advance electronic data under the safe framework meets the real world. *World Customs Journal*, 3(1), 73-86.
- Blumenthal, D. (2007). CBP kicks off secure freight initiative. *Office of Public Affairs*. Retrieved from http://www.cbp.gov/xp/CustomsToday/2007/apr_may/secure.xml

- Bohlman, M. (2001, September). Iso's container standards are nothing but good news: containers standards help remove technical barriers to trade. *ISO Bulletin*, 12-15. Retrieved from <http://www.iso.org/iso/container0109.pdf>
- Container Security Initiative (csi). (2006, April). *Global Security*. Retrieved from <http://www.globalsecurity.org/security/ops/csi.htm>
- Booth, F., & Altenbrun, L. (2002). Maritime and port security, piracy, and stowaways: renewed concerns over old problems. *15 University of San Francisco Maritime Law Journal* 1(47), 15-19.
- Boyce, C., & Neale, P. (2006). Conducting in-depth interviews: a guide for designing and conducting in-depth interviews for evaluation input. *Pathfinder International*, Retrieved from http://www.pathfind.org/site/DocServer/m_e_tool_series_indepth_interviews.pdf?doc ID=6301.
- Bridis, T. (2006, March 11). Government document shows u.s. port vulnerability. *Associated Press*. Retrieved from <http://www.foxnews.com/story/0,2933,187558,00.html>
- Bunn, M. (2006). Nti: Securing the bomb: Interdicting nuclear smuggling. *NTI*, Retrieved from http://www.nti.org/e_research/cnwm/interdicting/index.asp#_ftn2
- Cabrera, N. (2010, February 12). New cargo security 24 hour rule rattles carriers. *Lilly and Associates International*. Retrieved from <http://shiplilly.com/blog/2010/12/new-cargo-security-24-hour-rule-rattles-carriers/>
- Carafano, J. J., Weitz, R. & Andersen, M. E. (2009). *Maritime security: Fighting piracy in the Gulf of Aden and beyond*. Washington, DC: Heritage Foundation
- Cargo container vulnerabilities. (2005). *PJ Murray Associates, Inc*. Retrieved from http://www.sealock.com/pdf/PJMA.Cargo_Container_Vulnerabilities.ISO.7.05.pdf

- Chalk, P. (2008). *The maritime dimension of international security: terrorism, piracy, and challenges for the united states*. Retrieved from http://www.rand.org/pubs/monographs/2008/RAND_MG697.pdf
- Cirincione, R., Cosmas, A., Low, C., Peck, J., & Wilds, J. (2007). Barriers to the success of 100% maritime cargo container scanning. Retrieved from <http://esd.mit.edu/staging/WPS/2007/esd-wp-2007-05.pdf>
- Close, K. (2009). Twice as an access control at u.s. seaports. *Journal of Transportation Law, Logistics & Policy*, 76(1), 11-19. ISSN: 10785906
- Cohen, S. (2005). Boom boxes: Shipping containers and terrorists. *Berkeley Roundtable on the International Economy (BRIE)*, University of California, Berkeley. Retrieved from <http://brie.berkeley.edu/publications/RP7.pdf>
- Darpa and Nih. (2012, July 24). Retrieved from <http://web.mit.edu/newsoffice/2012/human-body-on-a-chip-research-funding-0724.html>
- Department of Homeland Security. (2005). Department of homeland security announces \$17.1 million award for operation safe commerce container cargo security program. Retrieved from http://www.dhs.gov/xnews/releases/press_release_0658.shtm
- Deputy Director. (2006). Retrieved from: www.sucss.state.il.us/documents/ClassSpecs/SPEC1035.pdf
- Dhs Announces New. (2007). *Electronic Privacy Information Center*, Retrieved from <http://epic.org/privacy/travel/ats/>
- Direnzo, J., & Doane, C. (2007). Nanotechnology: The next frontier for maritime security?. *Maritime Activity Reports*, Retrieved from <http://www.marinelink.com/news/article/nanotechnology-the-next-frontier-for-maritime/312785.aspx>

- Doyle, M. (2009, November 18). Hijacked tanker's captain dies. *British Broadcasting Company*. Retrieved from <http://news.bbc.co.uk/2/hi/africa/8366097.stm>
- Flynn, S. E. (2008). Overcoming the flaws in the U.S. government exports to improve container, cargo, and supply chain security. *Council on Foreign Relations*. Retrieved from http://opim.wharton.upenn.edu/risk/library/2008-04-02_Flynn_ImprovingContainerSecurity.pdf
- Former Longshoreman Arrested. (2011, September 13). *Waterfront Commission of New York Harbor*. Retrieved from <http://www.wcnyh.org/newspage62.html>
- Glesne, C. (2005). *Becoming qualitative researchers: An introduction*. Boston, MA: Allyn & Bacon.
- Hagan, J. E., (2006). *Research methods in criminal justice and criminology*. Boston, MA: Allyn and Bacon.
- Hall, M. (2006, March 14). Most of the containers moving through u.s. ports unchecked . *USA Today*, Retrieved from http://www.usatoday.com/news/washington/2006-03-14-ports-unchecked_x.htm
- Hundreds of Millions [Weblog message]. (2011, May 12). Retrieved from <http://maritimesecuritycouncil.wordpress.com/2011/05/12/gao-report-on-twic-where-are-the-scanners/>
- International Chamber of Commerce. (2011). *International Maritime Bureau*. Retrieved from <http://www.icc-ccs.org/home/imb>
- International convention for safe containers. (2011). *International Maritime Organization*. Retrieved from <http://www.imo.org/about/conventions/listofconventions/pages/international-convention-for-safe-containers-%28csc%29.aspx>

- Ituh, A. (2010). Port security technology for closed container inspection at united states seaports of entry. *Capstone Report*, Retrieved from: <https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/10209/Ituh-2010.pdf?sequence=1>
- Kaluza, P., Kolzsch, A., Gastner, M. T., & Blasius, B. (2010). The complex network of global cargo ship movements. *Journal of the Royal Society. Interface* 7, 1093-1103 doi: 10.1098/rsif.2009.0495
- Kriel, L. (2011, November 20). Nearly two tons of marijuana found at miami port. *The Miami Herald*. Retrieved from <http://www.miamiherald.com/2011/10/20/2463843/nearly-2-tons-of-marijuana-found.html>
- Lee, H. L. & Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management, *International Journal of Production Economics*, 96(3), 289–300. doi:10.1016/j.ijpe.2003.06.003
- Levinson, M. (2006). *The box: How the shipping container made the world smaller and the world economy bigger*. Princeton, NJ: Princeton University Press.
- Loh, L. & Venkatraman, N. (1992). Diffusion of information technology outsourcing: Influence sources and the Kodak effect, *Information Systems Research*, 3(4), pp. 334–358. doi: 10.1287/isre.3.4.334
- Lun, Y. H., Wong, C. W., Lai, K. H., & Cheng, T. C. (2008). Institutional perspective on the adoption of technology for the security enhancement of container transport. *Transport Reviews*, 28(1), 21-33. doi:10.1080/01441640701358804
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, CA: Sage Publications, Inc.
- Maersk a-class (2011). *Global Security*. Retrieved from <http://www.globalsecurity.org/military/systems/ship/maersk-a.htm>

- Martin, J. (2011, February 21). The triple-e maersk container ship will be the world's largest ship and the most efficient. *Gizmag*, Retrieved from <http://www.gizmag.com/triple-e-maersk-worlds-largest-ship/17938/>
- Martonosi, S. E., Ortiz, D. S., & Willis, H. H. (2006). *Evaluating the viability of 100 percent container inspection at america's ports*. Retrieved from http://www.rand.org/pubs/reprints/2006/RAND_RP1220.pdf
- Mayhew, C. (2001). The detection and prevention of cargo theft. *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*, 214, 1-6. Retrieved from <http://www.aic.gov.au/documents/B/B/0/{BB0D4DB9-5290-46E5-8438-486632808090}ti214.pdf>
- McNicholas, M. (2008). *Maritime security: An introduction*. Oxford, UK: Elsevier.
- McLay, L. A., Lloyd, J. D., & Niman, E. (2008). Interdicting nuclear material on cargo containers using knapsack problem models. doi:10.1007/s10479-009-0667-4
- Merriam, S. B. (1998). *Qualitative research and case study applications in education*. Boston, MA: Jossey- Bass.
- Mississippi State Port Authority. (2011). Retrieved from <http://www.shipmspa.com/>
- Mowatt, T. (2012, July 19). *Harvard's wyss institute receives \$2.6 million in darpa funding to develop smart suit that improves physical endurance*. Retrieved from <http://wyss.harvard.edu/viewpressrelease/89/>
- Mullet, R., Palma, A., Seneviratne, A., & Rodriguez, M. (2004). *Intermodal container security in the post 9/11 era*. (Master's thesis) Virginia Polytechnic Institute and State University. Virginia. Retrieved from [http://marcorodriguez.net/Documents/International commerce post 911.pdf](http://marcorodriguez.net/Documents/International%20commerce%20post%20911.pdf)

- National Research Council. (2003). Cybersecurity of freight information systems: A scoping study -- Special Report 274. *The National Academies Press*. Retrieved from http://www.nap.edu/openbook.php?record_id=10730&page=69
- Operational Csi Ports. (2006). Retrieved from http://www.worldtraderef.com/wtr_nl/WTR_site/csi.asp
- Operation Safe Commerce. (2005). *Material Handling and Logistics*. Retrieved from http://mhlnews.com/global/outlog_story_7153/
- Pinto, C. A., & Rabadi, G. (2008). U.S. port security. In W. Talley (1st Ed.), *Maritime Safety Security and Piracy*. London, UK: Informa Law.
- Pelton, R. J. (2011). The other side of piracy: Should shipping companies lower surcharges to reflect lower threat? *Somalia Report*. Retrieved from: <http://www.somaliareport.com/index.php/post/1927>
- Port of Corpus Christi. (2009). Retrieved from <http://www.portofcorpuschristi.com/>
- Port of Galveston. (2011). Retrieved from <http://www.portofgalveston.com/>
- Port of Houston Authority. (2010). Retrieved from <http://www.portofhouston.com/>
- Port of Miami. (2010). Retrieved from <http://www.miamidade.gov/portofmiami/cargo.asp>
- Port of New Orleans. (2011). Retrieved from: <http://www.portno.com>
- Publicover, J. J. (1999). U.S. Department of Transportation, Research and Special Programs Administration. *Intermodal cargo transportation*. Retrieved from <http://ntl.bts.gov/lib/21000/21900/21982/PB99152761.pdf>
- Roach, A. (2003). Container and port security: A bilateral perspective. *International Journal Of Marine & Coastal Law*, 18(3), 341-361. doi:10.1163/092735203770223576
- Rogers, E. M. (1995). *Diffusion of innovations*. 4th ed. New York: Free.

- Scheiber, L. B. (2003). *Defender's edge: Utilizing intelligent agent technology to anticipate terrorist acts* (Master's thesis). Retrieved from Institute for Defense Analyses. (IDA Document D-2849)
- Schuler, M. (2008, September 2). Containerized: A brief history of container ships. *GCaptain*, Retrieved from <http://gcaptain.com/container-ships-a-brief-history?2241>
- Secure freight initiative. (2009, February 25). Retrieved from http://www.dhs.gov/files/programs/gc_1166037389664.shtm
- Shifrel, S. (2010, October 5). Longshoremen busted for helping push a ton of panamanian cocaine through ny, nj port. *New York Daily News*. Retrieved from http://articles.nydailynews.com/2010-10-05/news/27077233_1_longshoremen-cocaine-social-networking-sites
- Shipping Housing Container Guide. (2010). Retrieved from <http://www.shipping-container-housing.com/>
- Spittle , A. (2011, February 3). Piracy: No stopping them. *The Economist*, Retrieved from <http://www.economist.com/node/18061574>
- Standard shipping containers. (2009). *Container container*. Retrieved from http://www.containercontainer.com/about_containers.aspx
- Sweet, K. M. (2006). *Transportation and cargo security: Threats and solutions*. Upper Saddle River, NJ: Pearson Education, Inc.
- Thibault, M., Brooks, M. R., & Kenneth, J. B. (2006). The response of the U.S. maritime industry to the new container security initiatives. *Transportation Journal*, 45(1), 5-15. ISSN: 0041-1612
- Tampa Port Authority. (2009). Retrieved from <http://www.tampaport.com/>
- U.S. Congressional Research Service, Federation of American Scientists. (2005a) *Usa patriot act: Background and comparison of house- and senate-approved reauthorization and*

- related legislative action* (RL33027). Retrieved from <http://www.fas.org/sgp/crs/intel/RL33027.pdf>
- U.S. Congressional Research Service, Federation of American Scientists (2005b). *Terrorist nuclear attacks on seaports: threat and response*. (RS21293). Retrieved from <http://www.fas.org/irp/crs/RS21293.pdf>
- U.S. Congressional Research Service, Federation of American Scientists (2005c). *Border and transportation security: The complexity of the challenge* (RL32839). Retrieved from <http://www.fas.org/sgp/crs/homesecc/RL32839.pdf>
- U.S. Congressional Research Service, Federation of American Scientists (2005d). *Port and maritime security: Background and issues for congress* (RL31733). Retrieved from <http://www.fas.org/sgp/crs/homesecc/RL31733.pdf>
- U.S. Congressional Research Service, Federation of American Scientists (2007). *Maritime security: Potential terrorist attacks and protection priorities* (RL33787). Retrieved from <http://www.fas.org/sgp/crs/homesecc/RL33787.pdf>
- U.S. Congressional Research Service, Federation of American Scientists (2009a). *The global nuclear detection architecture: Issues for congress* (RL34574). Retrieved from <http://www.fas.org/sgp/crs/nuke/RL34574.pdf>
- U.S. Congressional Research Service, Federation of American Scientists (2009b). *Terrorist watchlist checks and air passenger prescreening* (RL33645). Retrieved from <http://www.fas.org/sgp/crs/homesecc/RL33645.pdf>
- U.S. Customs and Border Protection (2002, November 20). *Customs and border launch 'operation safe commerce' program*. Retrieved from <http://www.cbp.gov>
- U.S. Customs and Border Protection (2006, September 29). *Container security initiative strategic plan*. Retrieved from <http://www.cbp.gov>

- U.S. Customs and Border Protection (2007, January 4). *Maritime cargo security in the age of global terrorism*. Retrieved from <http://www.cbp.gov>
- U.S. Customs and Border Protection (2011, March 20). *Container security initiative fact sheet*. Retrieved from <http://www.cbp.gov>
- U.S. Department of Energy, National Nuclear Security Administration (2008). *Testimony on “nnsa’s megaports initiative and its role in the secure freight initiative (sfi)” before the senate commerce, science, and transportation subcommittee*. Retrieved from <http://nnsa.energy.gov/mediaroom/congressionaltestimony/06.12.08>
- U.S. Department of Energy, National Nuclear Security Administration (2009). *Nnsa megaports initiative expands to four new ports*. Retrieved from <http://geneva.usmission.gov/2009/09/30/nnsa-new-ports/>
- U.S. Department of Energy, National Nuclear Security Administration (2010). *The second line of defense: Megaports initiative*. Retrieved from http://nnsa.energy.gov/sites/default/files/nnsa/inlinefiles/singlepages_9-15-2010.pdf
- U.S. Department of State (2010). *Signing of the megaports initiative*. Retrieved from <http://www.state.gov/secretary/rm/2010/04/140130.htm>
- U.S. Department of Transportation, United States Coast Guard (2005). *Navigation and vessel inspection circular no. 9-02(P16700.4)*. Retrieved from <http://www.uscg.mil/hq/cg5/nvic/pdf/2002/9-02%20chg2.pdf>
- U.S. Government Accountability Office (July, 2003). *Container security: Expansion of key customs programs will require greater attention to critical success factors*. (Publication No. GAO-03-770). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d03770.pdf>

- U.S. Government Accountability Office (March, 2006). *Cargo container inspections: Preliminary observations on the status of efforts to improve the automated targeting system.* (Publication No. GAO-06-591T). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d06591t.pdf>
- U.S. Government Accountability Office (October, 2007a). *One year later: A progress report on the safe port act.* (Publication No. GAO-08-171). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d08171t.pdf>
- U.S. Government Accountability Office (December, 2007b). *Federal efforts needed to address challenges in preventing and responding to terrorist attacks on energy commodity tankers.* (Publication No. GAO-08-141). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d08141.pdf>
- U.S. Government Accountability Office (January, 2008a). *Supply chain security: Examinations of high-risk cargo at foreign seaports have increased, but improved data collection and performance measures are needed.* (Publication No. GAO-08-187). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d08187.pdf>
- U.S. Government Accountability Office (April, 2008b). *Supply chain security: U.s. customs and border protection has enhanced its partnership with import trade sectors but challenges remain in verifying security practices.* (Publication No. GAO-08-240). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d08240.pdf>
- U.S. Government Accountability Office (June, 2008c). *Supply chain security: Challenges to scanning 100 percent of u.s.-bound cargo containers.* (Publication No. GAO-08-533).

Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d08533t.pdf>

U.S. Government Accountability Office (October, 2009a). *Supply chain security: feasibility and cost-benefit analysis would assist dhs and congress in assessing and implementing the requirement to scan 100 percent of u.s.-bound containers.* (Publication No. GAO-10-12).

Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d1012.pdf>

U.S. Government Accountability Office. (December, 2009b). *Homeland security: Dhs's progress and challenges in key areas of maritime, aviation, and cybersecurity.*

(Publication No. GAO 10-106). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d10106.pdf>

U.S. Government Accountability Office (September, 2010a). *Supply chain security: Cbp has made progress in assisting the trade industry in implementing the new importer security filing requirements, but some challenges remain.* (Publication No. 10-841). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d10841.pdf>

U.S. Government Accountability Office (July, 2010b). *Dhs progress and challenges in key areas of port security.* (Publication No. GAO-10-940). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d10940t.pdf>

U.S. Government Accountability Office (October, 2010c). *Maritime security: Dhs progress and challenges in key areas of port security.* (Publication No. GAO-11-140). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d11140r.pdf>

U.S. Government Accountability Office (August, 2011). *Progress made but further actions needed to secure the maritime energy supply*. (Publication No. GAO-11-883). Retrieved from GAO Reports Main Page via GPO Access database: <http://www.gao.gov/new.items/d11883t.pdf>

U.S. Immigration and Customs Enforcement (2010). *Border enforcement security task force (best)*. Retrieved from <http://www.ice.gov/best/>

United Nations Convention on the Law of the Sea, Article 101 (1982). Retrieved from http://www.un.org/depts/los/convention_agreements/texts/unclos/part7.htm.

United States Code of 1948, 18 USCS § 1651 (2002). Retrieved from <http://law.justia.com/codes/us/title18/18usc1651.html>.

United States. Cong. House. 109th Congress, 1st Session. Pub. L. 109-347, *Safe Port Act of 2006* [introduced in the U.S. House; 13 October 2006]. *GPO Access*. Retrieved from <http://www.access.gpo.gov/congress/cong009.html>; DOCID: f:s608is.txt>.

van de Voort, M. O'Brien, K. Rahman, R., & Valeri, L. (2003). "*Seacurity*": *Improving the security of the global sea-container shipping system*. Retrieved from http://www.rand.org/pubs/monograph_reports/2005/MR1695.pdf

Walters, S. (2007). Contemporary maritime piracy. *Crime and Justice International*, 23(96), 10-16. Retrieved from <http://www.southchinasea.org/docs/walters-contemporary-maritime-piracy.pdf>

World shipping council (2011). Retrieved from <http://www.worldshipping.org/about-the-industry/containers>

Wright, C.L. (2007). Bridging the gap in port security: network centric theory applied to public/private collaboration. *Naval Post Graduate School*, Retrieved from

<http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA467714>

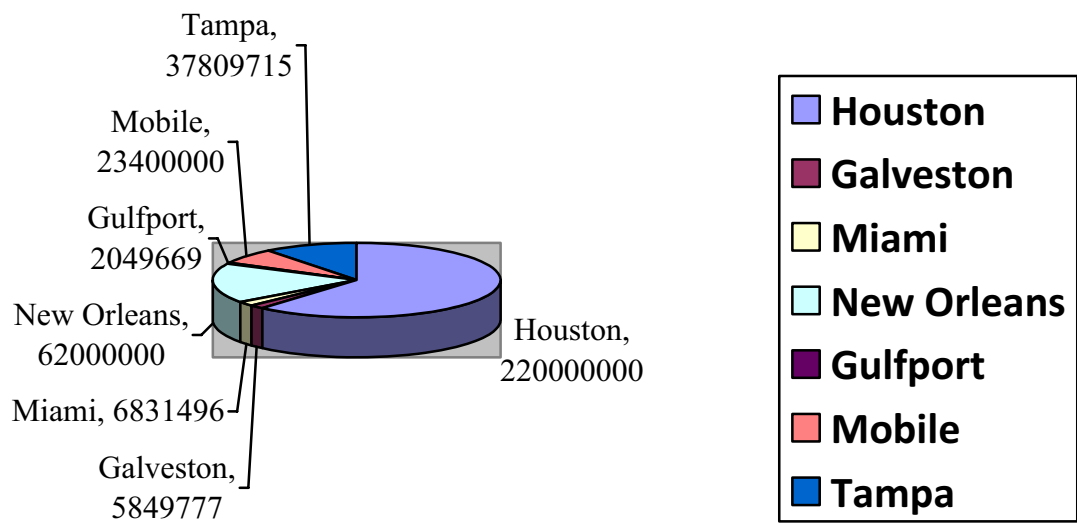
9/11 Commission (2007). *Implementing recommendations of the 9/11 commission act of 2007*.

(PUBLIC LAW 110–53—AUG. 3, 2007). Government Printing Office. Retrieved from <http://intelligence.senate.gov/laws/pl11053.pdf>

LIST OF APPENDICES

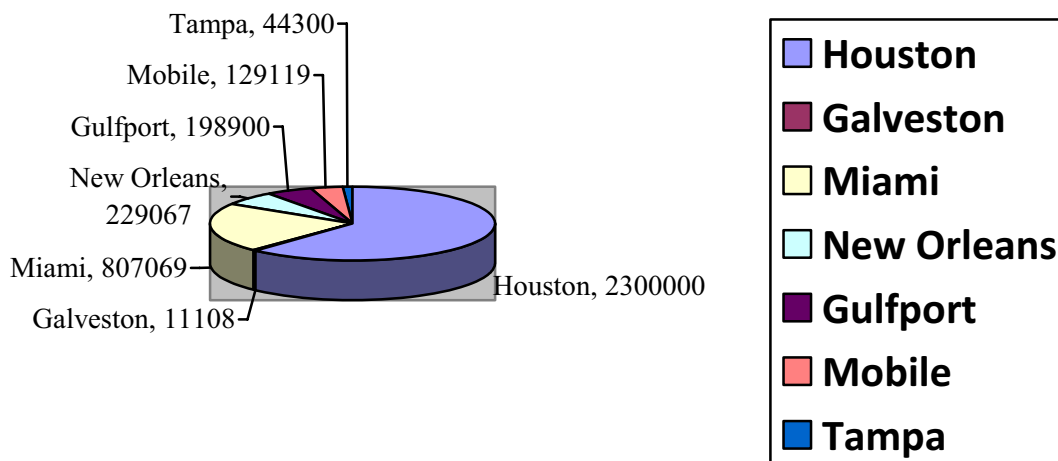
APPENDIX 1A: TONNAGE IN 2009

Table 1A. Tonnage in 2009 (in short tons)



APPENDIX 2A: NUMBER OF TEUs

Table 2A. Number of TEUs in 2009

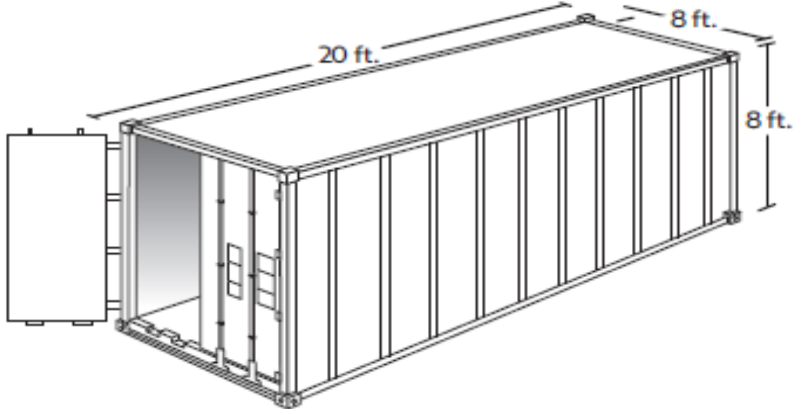


APPENDIX 3A: WHAT IS A TEU?


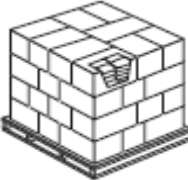
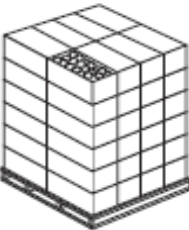
Table 3A: What is a TEU?

WHAT IS A TEU?

A TEU, or twenty-foot equivalent unit, is the basic container measurement used in the shipping industry. It is the equivalent of a container 20 feet long by 8 feet wide by 8 feet high. Typically, containers being transported on the road are 40 feet long, the equivalent of two TEUs.



What can a TEU hold?

		
Peaches	Pecans	Vidalia Onions
66 peaches per box 3,630 peaches/pallet 10 pallets per TEU	24 - 6-ounce bags of shelled pecans per box 36 boxes per pallet 324 pounds of pecans per pallet	48 - 40-pound boxes 1,920 pounds on pallet 10 pallets per TEU
36,300 peaches per TEU	3,240 pounds of shelled pecans per TEU	28,800 Vidalia onions (average onion = 1.5 pounds)

SOURCES: U.S. Dept of Transportation, wespak.com, diamondnuts.com, vidaliaorganics.com

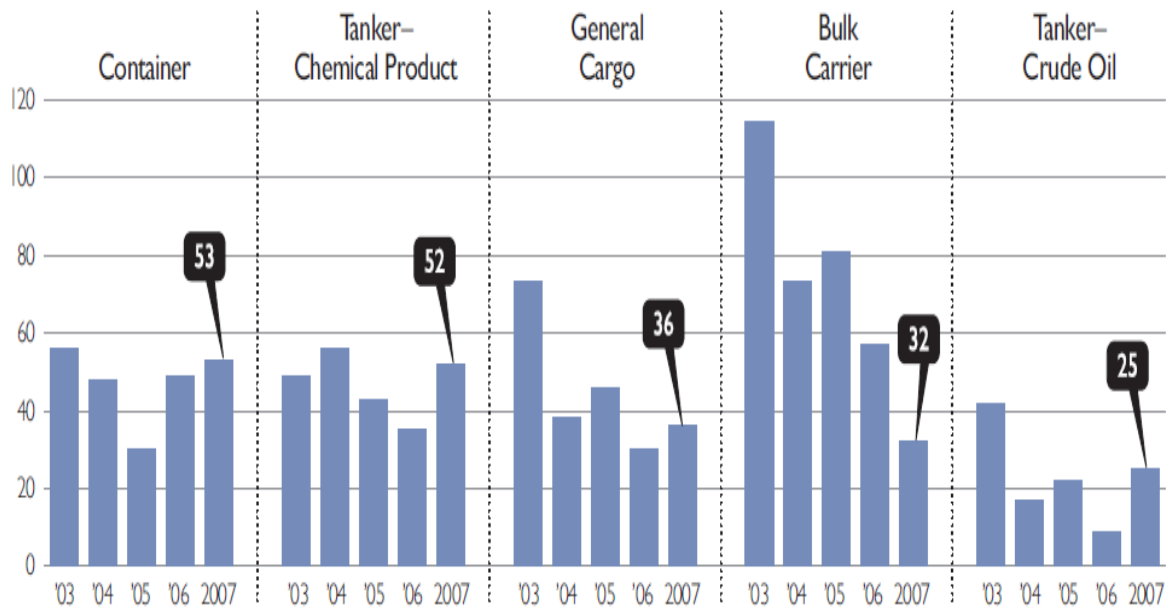
Todd M. Hagin/for Morris News Service

APPENDIX 4A: TYPES OF VESSELS TARGETED

Table 4A. Types of Vessels Targeted by Pirates

The Five Vessel Types Most Often Attacked by Pirates

Pirates have been targeting container ships and tankers in recent years. The charts below show pirate attacks per year, and are ordered, highest to lowest, by the number of attacks in 2007.



ICC International Maritime Bureau, (2007).

APPENDIX B: ENDORSEMENT LETTER

Appendix B: Endorsement Letter

Date: 12/28/11

Dear _____

The security of containerized cargo has remained a significant aspect in the overall maritime security perspective. Participation from key administrators would be a valuable addition to the enhancement of container security. As part of the continual efforts to advance container security, I want to interview security administrators/deputy directors at seaports along the Gulf Coast. I believe input from these selected individuals will provide my research with acute analysis and assessments. Further, your thoughts could significantly stimulate the progress of container security within the global supply chain.

Through the Legal Studies Department at the University of Mississippi, I have developed a set of questions that I believe will help assess the effectiveness of current containerized security techniques. With your cooperation and endorsement, I believe the future of containerized security will benefit significantly.

The interview process will take approximately 20-30 minutes. After the interview has been transcribed, I and my committee will compile the answers and introduce the responses into my study. Individual answers will remain confidential.

I would appreciate your assistance and cooperation. If you have any questions, feel free to contact me.

Sincerely and respectfully,
William A. Neely, III
2LT U.S. Army
University of Mississippi, M.C.J. candidate
(601)-941-7194
waneely@olemiss.edu

APPENDIX C: INTERVIEW SCHEDULE

Appendix C: Interview schedule

- 1) In your opinion, what is the biggest threat(s) facing container security?
- 2) What security techniques/methods are employed at your seaport to accommodate container security?
- 3) On average, how many inbound containers receive some form of scan/inspection before arrival?
- 4) Where do the majority of containers receive inspection (i.e. at your port or before arrival to your port)?
- 5) Are you able to scan/inspect all containers upon arrival at your seaport? Yes or no? If not, why?
- 6) Do you believe container security has reached its pinnacle? Yes or no?
- 7) What, if any, factors hinder your seaport's ability to maintain 100% scans of containerized cargo?
- 8) Would you consider technology to be your greatest asset in your ability to maintain efficient container security? If so, which technological advancements (i.e. nonintrusive imaging, gamma ray inspection) play a significant role? If not, why?
- 9) What is the most significant factor you consider when adopting/endorsing a security technique (i.e. Secure Freight Initiative, Container Security Initiative, TWIC)?
- 10) Would you consider global cooperation essential to improving container security? Yes or no?
- 11) What agencies (USCG, CBP, local/state authorities) are responsible for the majority of your container security?
- 12) Do you have any questions for me? Anything you want to discuss that I haven't covered in my questions?

APPENDIX D: INFORMED CONSENT

Protocol 12-147

Date Approved: October 20, 2011

MODEL CONSENT FORM

Consent to Participate in an Experimental Study

Title: Perceived Effectiveness of Container Security at Selected Seaports along the Gulf Coast

Investigator

William A. Neely, III
Department of Legal Studies
203 Odom Hall
The University of Mississippi
(662) 915-7902

Sponsor

Michael P. Wiggington, Ph.D.
Department of Legal Studies
203 Odom Hall
The University of Mississippi
(662) 915-7902

Description

We want to know whether container security at selected seaports is effective in deterring the smuggling of weapons of mass destruction (WMDs), materials to make a dirty bomb, drugs, weapons, etc. In order to answer our question, we are asking you to answer 10 questions. Each question will address a certain aspect of container security implemented at the selected seaport. The answers you provide will permit an accurate review of container security effectiveness. More specifically, your responses will potentially improve the container security implemented at United States seaports, and, ultimately, all ports within the global supply chain.

Risks and Benefits

We do not think that there are any risks. There is current research which evaluates the effectiveness of container security at seaports. However, research pertaining to your expertise/experience is lacking. By providing honest and accurate responses, the seaport community will be able to incorporate your answers into an improved security plan.

Cost and Payments

The interview will take about half an hour or 30 minutes to finish. There are no costs for helping us with this study.

Confidentiality

We will not mention your name at any time before, during, or after this study. Only the name of your seaport will be mentioned within this study. Therefore, we do not believe that you can be identified from or by personal responses attributed to this paper.

Right to Withdraw

You do not have to take part in this study. If you start the study and decide that you do not want to finish, all you have to do is to tell William A. Neely, III or Dr. Wiggington in person, by letter, or by telephone at the Department of Legal Studies, 203 Odom Hall, The University of Mississippi, University, MS 38677, or 915-7902. Whether or not you choose to participate or to withdraw will not affect your standing with the Department of Legal Studies, or with the University, and it will not cause you to lose any benefits to which you are entitled.

The researchers may terminate your participation in the study without regard to your consent and for any reason, such as protecting your safety and protecting the integrity of the research data.

IRB Approval

This study has been reviewed by The University of Mississippi's Institutional Review Board (IRB). If you have any questions, concerns, or reports regarding your rights as a participant of research, please contact the IRB at (662) 915-7482.

Statement of Consent

I have read the above information. I have been given a copy of this form. I have had an opportunity to ask questions, and I have received answers. I consent to participate in the study.

Signature of Parent/Guardian
[Remove if no minors are involved.]
Date

Signature of Investigator
Date

APPENDIX E: IRB APPROVAL



THE UNIVERSITY OF
MISSISSIPPI

Office of Research and Sponsored Programs

The University of Mississippi
100 Barr Hall
Post Office Box 907
University, MS 38677
(662) 915-7482
Fax: (662) 915-7577

October 20, 2011

Mr. William A. Neely, III
Legal Studies
University, MS 38677

Dr. Michael Wigginton
Legal Studies
University, MS 38677

Dear Mr. Neely and Dr. Wigginton:

This is to inform you that your application to conduct research with human participants, ***The Perceived Effectiveness of Containerized Cargo Security (Protocol 12-147)***, has been approved as Exempt under 45 CFR 46.101(b)(2).

Please remember that all of The University of Mississippi's human participant research activities, regardless of whether the research is subject to federal regulations, must be guided by the ethical principles in *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*.

It is especially important for you to keep these points in mind:

- You must protect the rights and welfare of human research participants.
- Any changes to your approved protocol must be reviewed and approved before initiating those changes.
- You must report promptly to the IRB any injuries or other unanticipated problems involving risks to participants or others.

If you have any questions, please feel free to call me at (662) 915-7482.

Sincerely,


Diane W. Lindley
Coordinator, Institutional Review Board

APPENDIX F: DISAPPROVAL TO PARTICIPATE IN INTERVIEW

Appendix F: Disapproval to participate in interview: Houston, TX

LT. Neely,

My apologies for the delay in response to your inquiry. Unfortunately, we will not be able to complete the "interview schedule" you sent due to the nature of the questions. The information you requested constitutes Sensitive Security Information and we are prohibited from divulging that information in accordance with 49 CFR Part 1520. Below I have provided a general response from the Port Security and Emergency Operations Department.

The Port of Houston Authority is committed to continually improving safety and security at our facilities and work with our local, state and federal partners to achieve our goals. These partners include the U.S. Coast Guard, U.S. Customs and Border Protection, FBI, JTTF and ICE to name but a few. The Port Authority's Port Security and Emergency Operations Department employs many different security initiatives and programs such as our Coast Guard approved Facility Security Plans, ISO 28000 certification for Security Management Systems, Customs -Trade Partnership Against Terrorism (CTPAT) as well as actively participating in numerous committees and associations. The Port Authority has representation in the Area Maritime Security Committee and many of its sub-committees, the American Association of Port Authorities (AAPA) and its Security Committee, as well as ASIS International. Utilizing all assets available, the Port Authority is constantly evaluating and striving to improve its security policies and procedures.

Please feel free to contact me should you have any further questions.

Respectfully,

[REDACTED]

Facility Security Officer
Port of Houston Authority
Turning Basin, Woodhouse and Manchester
[REDACTED] (office)
[REDACTED] (fax)

APPENDIX G: DISAPPROVAL TO PARTICIPATE IN INTERVIEW: CBP

Appendix G: Disapproval to participate in interview: CBP liaison (Mobile, AL)

Mr. Neely,

Unfortunately, I have not been granted permission to address your questions and my requests to our HQ have not been responded to favorably. I have exhausted several avenues within CBP to allow me to respond without success and as such will have to decline your request for assistance.

I do apologize for the delayed response but had hoped that I might persuade someone to allow me to respond.

I wish you the best with your project.

[REDACTED]
Acting Director, Business Operations Branch
OA, Asset and Administrative Management Division
[REDACTED] (Office)
[REDACTED] (Cell)
[REDACTED]@cbp.dhs.gov

VITA

William Augustus Neely, III was born to Bubba and Paula Neely on December 5, 1985 in Jackson, Mississippi. William received his high school diploma from Madison Central High School in Madison, Mississippi in May of 2004. From there William decided to further his education by enrolling in the University of Mississippi in the Fall of 2004. William's academic successes, particularly in Fall 2008, Spring 2009, and Fall 2009, placed him on the Dean's and Chancellor's Honor rolls. In December of 2009, William earned a Bachelor of Paralegal Studies with a minor in English. After graduation William decided to further his education by enrolling into the Master's of Criminal Justice program at the University of Mississippi.

During his tenure in the Master's of Criminal Justice program, Mr. Neely focused his coursework in homeland security, transportation security, trans-national organized crime, and criminal analysis. In the Spring of 2011, Mr. Neely received the Outstanding Graduate Student award for his diligence while participating in the MCJ program. Additionally, in the Spring of 2011, Mr. Neely received the Iron Mike award for outstanding leadership through the ROTC at the University of Mississippi. In the Fall of 2011 Mr. Neely was selected as a Distinguished Military Graduate (DMG) for ranking in the top 20% of cadets throughout the United States. In December of 2011, Mr. Neely was commissioned as a 2LT in the United States Army as an Infantry officer and will be attending the Infantry Basic Officer Leadership Course in November of 2012. In December of 2012, Mr. Neely will graduate with an overall 3.89 GPA and a Master's of Criminal Justice degree, emphasizing in Homeland Security.