2021

Transnational Threats to Maritime Systems and Seaport Security

Eric L. Hampton
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Eric L. Hampton, Sr.

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Ian Cole, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Olivia Yu, Committee Member,
Public Policy and Administration Faculty

Dr. Victoria Landu-Adams, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2021

Abstract

Transnational Threats to Maritime Systems and Seaport Security

by

Eric L. Hampton, Sr.

MS, Kennesaw State University, 2015

MPA, Columbus State University, 2011

BS, Thomas University, 2010

AS, Armstrong Atlantic State University, 2007

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2021

Abstract

An assessment of a 16-year period since the 9/11 attacks indicated that more than 14,000 security breaches in which security measures at seaports were circumvented due to vulnerabilities occurred and more than 24,000 suspicious activity reports were made. The susceptibility of United States' seaports to groups engaged in criminal activities, including drug trafficking, cargo theft, and smuggling of contraband and people undermines security practices and renders the nation vulnerable to acts of terrorism. The purpose of this qualitative study was to explore seaport security measures to identify and understand internal and external factors that may impact protection practices at U.S. seaports, including those that inadvertently contribute to unauthorized access to restricted facilities and cargo. von Bertalanffy's general systems theory was used to conceptualize and analyze seaports as complex systems, comprised of independent subsystems working together. Data for the study were collected through Zoom audio recorded interviews conducted with 10 security officials from seaports in the United States. These data were subjected to open and thematic coding, followed by rigorous qualitative analysis and interpretation. Collaboration was identified as a critical element to accomplishing security objectives, some SSOs described a lack of prioritization of security, lack of awareness and understanding of transnational threats as being major risk factors to the security culture. Findings from this study may be used for positive social change by local, state, and federal policy makers, law enforcement executives, industry leaders, academic scholars, and the public to cultivate a contemporary understanding of transnational threats to maritime systems.

Transnational Threats to Maritime Systems and Seaport Security

by

Eric L. Hampton, Sr.

MS, Kennesaw State University, 2015

MPA, Columbus State University, 2011

BS, Thomas University, 2010

AS, Armstrong Atlantic State University, 2007

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2021

Dedication

"And in thy seed shall all the nations of the earth be blessed, because thou hast obeyed my voice" (King James Version).

Therefore, I dedicate this work to my amazing parents Earnest and Emma Hampton. I could not have reached this milestone without your sacrifices, encouragement, and unwavering support. Your love, and guidance through action made me the man I am today. Also, I dedicate this work to my wonderful children, Eric Jr., Elisabeth, Olivia, Amanda, and Kevin, who are the source of my passion and purpose. I am forever, grateful that God blessed me with such amazing and loving children. You have made me so proud as a father.

Acknowledgments

With great humility, and appreciation I acknowledge all whom made this doctoral degree possible. First and foremost, I give honor and thanks to my Lord and Savior Jesus Christ, for his grace, mercy, and favor despite my unworthiness. Next, I am thankful and indebted to my beautiful wife and best friend Ramona who has been my greatest advocate, confidant, and inspiration. Words are incapable of adequately expressing my true gratitude for her patience, love, and support, allowing me to work on this doctorate, while she stood steadfast in her support of me and my ambitions. Finally, I am forever grateful to my Committee Chair, Dr. Ian Cole, Dr. Olivia Yu, and Dr. Victoria Landu-Adams, who provided me with expert guidance and support throughout this process.

Table of Contents

List of Tables....v

List of Figures....vi

Chapter 1: Introduction to the Study....1

Background....2

Problem Statement....4

Purpose....5

Research Questions....6

Theoretical Framework....6

Nature of Study....8

Definition of Terms....10

Assumptions....12

Scope and Delimitations....13

Limitations....14

Significance....15

Summary....16

Chapter 2: Literature Review....18

Introduction....18

Literature Search Strategy....19

Theoretical Foundation....20

Literature Review Related to Key Variables and/or Concepts....29

The International Ship and Ports Facility Security Code....31

The Maritime Transportation Security Act 34
The Security and Accountability for Every Port Act 37
Case Study: Maritime Security and European Seaports 41
Seaport Exploitation for Narcotics Smuggling and Terrorism 46
Suspicious Activity and Breach of Security Reports 61
Summary and Conclusion 65
Chapter 3: Research Method 68
Introduction 68
Research Design and Rationale 69
Role of the Researcher 70
Methodology 71
Instrumentation 75
Data Analysis Plan 76
Issues of Trustworthiness 77
Credibility 78
Transferability 79
Dependability 80
Confirmability 80
Summary 81
Chapter 4: Results 82
Introduction 82
Setting 83

Demographic 84
Data Collection 85
Data Analysis 87
Evidence of Trustworthiness 90
Credibility 90
Transferability 91
Dependability 91
Confirmability 92
Results 92
Research Question 1 93
Theme 1: Social Systems 93
Theme 2: Threat Perceptions 97
Research Question 2 102
Theme 3: Regulatory Scope 103
Theme 4: Barriers and Facilitators 107
Leadership 107
MTSA limitations 108
Sharing 109
USCG Penalties 111
Port Security Grant 112
Summary 113
Chapter 5: Discussion, Conclusions, and Recommendations 116

Introduction 116
Interpretation of the Findings 117
Social Systems 117
Threat Perceptions 119
Regulatory Scope 121
Barriers and Facilitators 122
Limitations of the Study 123
Recommendations 125
Implications 127
Conclusion 128
References 132

List of Tables

Table 1 *Participant Demographics*.....85

List of Figures

Figure 1 *National Response Center Data Summary 2015* 36

Figure 2 *National Response Center & USCG Data Summary 2020* 64

Chapter 1: Introduction to the Study

Seaports, like some airports, are international ports of entry (POE) where commercial vessels arrive to load and discharge cargo and passengers. U.S. seaports facilitate the importation and exportation of essential foods, equipment, electronics, medicines, chemicals, automobiles, and exotic merchandise totaling over $700 billion annually (Downes et al. 2019; Knatz, 2017; Peckam, 2012). There are 361 U.S. seaports that facilitate the movement of more than 95% of overseas cargo by volume (Anand & Grainger, 2018; Bagchi & Paul, 2017) which presents an array of business and security challenges. With a majority of goods being transported onboard ships destined for seaports around the world, the risk of importing illicit drugs, dangerous weapons or people into the United States increases (Rana & Moditsi, 2017; Yagoub, 2016; Zaitch, 2002). Large volumes of cargo in transit and the role of seaports in facilitating economic growth and competitiveness makes them ideal systems for exploitation or terrorist targets (Bagchi & Paul, 2017). Further, these large volumes of legitimate cargo repeatedly render port security measures ineffective against transnational organized criminals (TOCs), who routinely exploit the maritime transportation system to smuggle dangerous drugs into seaports around the world and could one day act as a mechanism for terrorist to smuggle a weaponized device.

The aim of this study was to explore U.S. seaports to understand why illegitimate actors and illicit goods gain unauthorized access to restricted facilities and cargo. The exploitation of legitimate seaport operations undermines security practices and renders the nation vulnerable to acts of terrorism that could result in significant loss of life or

major economic disruptions (Maritime Transportation Security Act, 2002). This study included an exploration of governmental reports and data, criminal trends, an analysis of seaport security measures, and participant interviews. In this study, I examined information using case studies of transnational criminal organizations to understand their frequently used methods of exploitation targeting seaports. This information provided interrelated insights into transnational organized criminals and terrorist groups.

In addition to the background, this chapter includes the problem statement, purpose of the study, research questions, theoretical foundation, nature of the study, and definitions of key terms. Additionally, I identify the gap in the literature that led to this study, as well as discuss the assumptions, scope and delimitations, limitations, and significance of the study. I summarize key points in the chapter's conclusions.

Background

Researchers have recognized the susceptibility of U.S. seaports to groups engaged in illicit activity including drug trafficking, cargo theft, and smuggling of contraband and people. The smuggling techniques used by traffickers to ship narcotics through U.S. seaports undermines legitimate business practices, contributes to a national opioid crisis, and exposes the nation to potential threats of terrorism. Terrorism on seaports can cause risk to life, and the economy (Chang & Thai, 2016; Maritime Transportation Security Act, 2002). It is estimated that a disruption resulting in the closing of a major U.S. seaport could cost the nation more than $1 billion dollars per day (Bagchi & Paul, 2017; Leonard et al., 2015). Further, the economic impact of a nuclear terrorist attack on a

major U.S. seaport and city would be catastrophic, resulting in disruption of U.S. trade between $100-200 billion and 50,000 to 100,000 deaths (Abt, 2003).

Data indicates that out of 40,126 recorded terrorist attacks between 1968 and 2007, only 136 were against the maritime industry (Eski, 2016); however, transnational criminal operations expose seaport vulnerabilities. There is also historical evidence of terrorist interest in maritime targets. For example, in 2000, members of the Al-Qaeda network attacked the USS Cole while it was docked in Aden, Yemen, killing 17 American sailors and injuring 42 others (Prodan, 2017). In 2002, Al-Qaeda, attacked the MV Limburg (157,000-ton crude oil tanker) in Yemen (Prodan, 2017). These attacks have exposed major vulnerabilities on international waterways linking commercial and military vessels to seaport facilities. For instance, plausible threat scenarios regarding the nation's major seaports involve concerns of a deliberate attempt to smuggle a weapon of mass destruction (WMD) inside of a cargo shipping container. WMDs are any destructive device designed or intended to cause death, or serious bodily injury through explosion or the release of toxins, poisonous chemicals, or their precursors (Department of Homeland Security, 2018), which terrorist groups have declared their intention to acquire and use (Maras & Miranda, 2016). Though lessons learned from the September 11, 2001, attacks have enabled security officials to better conceptualize and anticipate the dangerous consequences of a compromised aviation system, the maritime sector of the transportation network has not been fully examined.

Despite the threat of potential attacks, maritime security measures have not adequately secured seaports against unauthorized access to restricted port facilities and

cargo. There is also gap in the literature on the possible factors that allow individuals and illicit goods entry into U.S. seaports. Although a modest body of scholarship exists on protecting critical infrastructure, there is limited research specific to U.S. seaport security. The lack of research on U.S. seaports, coupled with increasing exploitation of legitimate cargo to smuggle illicit goods and increasing interactions between transnational criminal organizations, compelled this examination of maritime security measures. Findings from this study provides local, state, and federal authorities, including U.S. policy makers with additional knowledge they can use towards future efforts to secure U.S. seaports against organized crime and terrorism.

Problem Statement

Smuggling techniques used by traffickers to ship narcotics through U.S. seaports impacts business, fuels the opioid crisis and exposes vulnerabilities that criminal organizations or terrorist groups may further exploit to funnel illicit items, launder money, or potentially deliver a weaponized device into the United States (Shapiro et al, 2018). Ineffective security measures at U.S. seaports exposes both industry and the nation to substantial economic risk (Chang & Thai, 2016). It is estimated that a disruption resulting in the closing of a major U.S. seaport could cost the nation more than $1 billion dollars per day (Bagchi & Paul, 2017; Leonard et al., 2015). But there is limited research specific to U.S. seaport security. Literature reviewed offers only a cursory examination of maritime laws governing seaports and port security funding as a component of security cost benefit analysis (Knatz, 2017; Romero-Faz & Camarero, 2017). None of the studies reviewed examined the security of seaports from the perspective of U.S. security officials

or sought to identify factors that impact the effectiveness of seaport security measures or those institutional factors inadvertently contributing to security vulnerabilities. This study provides insight into why existing maritime security measures have not adequately secured seaports against unauthorized access to restricted port facilities and cargo.

Purpose

The purpose of this qualitative case study was to explore seaport security measures to understand internal and external factors that impact protection practices at U.S. seaports. This study sought to collect data primarily through document analysis and from participant interviews with individuals who are responsible for implementing security practices required by the Maritime Transportation Security Act of 2002 (MTSA). History has demonstrated an advanced level of sophistication and complexity rooted within the operational practices of transnational criminal organizations and terrorist networks. Transnational criminal organizations and terrorist groups are organized and well equipped with modern communications, weapons, and watercrafts to "conduct smuggling of people, drugs, weapons, and other contraband" (Department of Homeland Security, 2005, p. 5). The demonstrated ability and willingness of these groups to exploit archaic or passive security measures to conduct illicit activities must not be underestimated. Maritime drug smuggling routes and methods highlight the plausibility of transporting and introducing foreign extremists or a weaponized device into a U.S. seaport.

Research Questions

Research Question 1: What are the meanings, structures, and essence of lived experience of seaport security officials, in terms of instituting security measures required by the Maritime Transportation Security Act of 2002?

Research Question 2: What do seaport security officials perceive as barriers and facilitators to implementing security practices at U.S. seaports?

Theoretical Framework

Seaport operations involve arrangements between separate interrelated elements functioning together. Like living organisms that are sustained by synchronized organ functions in which the actions of one effect the performance of others, seaports are isomorphic systems found among the social and economic sciences. Seaport vulnerabilities and exploitation are likely outcomes attributed to host miscalculations, misalignments, errors, misdiagnosis, and mistreatments, allowing for invasion of criminal organizations. In the context of this study, “seaport security” is theorized as being a social construct requiring consistent practical application to be successful. Seaports are governed geographic boundaries, acting as host to various interdependent elements responsible for the facilitation of global trade. The U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), Port Authority Police Departments, and other local, and state agencies work semi-harmoniously to create a layer of security, protecting the system from disruption and exploitation by criminal and terrorist organizations. Seaport operations share homologous structures with those found in numerous complex sciences such as physics, biology, engineering, and law. They share similarities in

principles that govern the behaviors and interactions of entities, and actors working in U.S. seaports and are subject to invasion from rational criminal actors who seek to exploit them. Therefore, Ludwig von Bertalanffy's (1968) general systems theory (GST), which is applicable to exploring the nature of complex systems, helped to analyze the complex nature of seaports. General systems theory can be described as a science of wholeness offering a universal set of principles that apply to any system in general (von Bertalanffy, 1968). GST is a logico-mathematical discipline applicable to all sciences that explore the nature of complex systems (von Bertalanffy, 2008). Like weakened biological systems, the open, competitive, and porous nature of seaports makes them susceptible to invasion from transnational criminal organization elements. As complex systems, seaport inputs and outputs are driven by open trade markets, consumer demand, intermodal and logistical capabilities, and storage spaces that support the interactions of diverse organic elements operating within the maritime environment.

I conceptualized seaports as a unique individual system within a larger global maritime transportation system. Seaports are interconnected by waterways, vessels, vehicles, internal and external system users. As a homologous match to biological, psychological, mechanical, and social sciences, seaports depend on internal and external resources to function, and to produce its projected outputs (Perry, 1972). Seaports also share unique principles that govern interactions, and behaviors between various interconnected elements. Seaports operate within specific boundaries and retain unique cultural norms, structures, models, laws, language, processes, goals, and challenges. Seaports are governmental, political, and corporate bodies with overlapping authorities

and responsibilities. Therefore, there exists various sources of motivation among people, groups, entities, and industries interacting in seaports (Peery, 1972). Individual motivations likely influence perceptions, methods, and the subsequent outcomes of seaport security measures. Von Bertalanffy (1972) asserted that the main characteristics of living things are found in their organization; therefore, important phenomena are best understood through investigation of systems. Security measures in use at U.S. seaports establishes required processes and procedures to restrict infiltration of unauthorized people and illicit goods. However, despite the implementation of security countermeasures, the system remains weakened by corrupt users. Seaport smuggling occurs when rational actors circumvent system laws by acquiring host elements to facilitate illicit shipments among legitimate cargo. General systems theory is useful in studying complex organizational systems; it guided my research and aided in answering the study's research questions.

Nature of Study

The nature of this study is founded in qualitative research. Qualitative research is exploratory in nature and therefore ideal for systematically collecting data relevant to understanding why maritime security regimes have not adequately secured seaports against unauthorized access to restricted port facilities and cargo. Qualitative research offers flexibility and typically is not intended to prove or test a theory; however, applicable theories emerged once the data was collected and analyzed (O'Sullivan et al., 2017). Further, a case study design was appropriate for this study, as case studies are a qualitative approach to explore real-life systems (Creswell & Poth, 2018), which is used

to examine people, decisions, programs, and entities with unique characteristics relevant to a researcher's interest (O'Sullivan et al., 2017). Documents and unclassified records were obtained from the U.S. Department of Homeland Security (DHS) and used to conduct an in-depth analysis of the nature and number of incidents involving security and smuggling at U.S. seaports. The DHS reports were analyzed to determine what common themes emerge as indicators of contributing factors to circumvention of security measures and smuggling. Based on my findings, I delineated seaports as individual cases in the study.

In addition to analyzing documents using publicly available information, I identified current security officials, including chiefs of police, security directors, facility security officers (FSOs), federal officers, and other homeland security leaders who were contacted and invited to participate in an audio recorded Zoom interview. Nonprobability purposeful sampling was used to recruit experienced participants. A sample population of 10 participants were interviewed from U.S. seaports. Using an interview guide, questions were posed to participants; each question was open-ended and focused on beliefs, perceptions, and opinions of institutional influences on seaport security measures and proposed solutions to improve security practices. Responses were documented using both detailed notes and digital audio recordings. Participants' responses were collected, analyzed, and verified using member checking prior to the application of open coding and thematic coding, followed by a secondary inquiry for emergent themes using computer assisted qualitative data analysis (Saldana, 2016). This combined approach supported

validation, corroboration, triangulation and produced a more holistic understanding of this participant responses and the issue under study.

Definition of Terms

The terminology used in this research are common within maritime communities and derived from the Code of Federal Regulations (CFR) and the American Association Port Authorities (AAPA). The proceeding definitions are provided for the purpose of clarifying terminology and supporting contextual meaning throughout this study.

Breach of security: An incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated (33 CFR §101.105).

Container: A box made of aluminum, steel or fiberglass used to transport cargo by ship, rail, truck, or barge. The common dimensions of a container are 20 x 8 x 8 (called a TEU or 20-foot equivalent unit) or 40 x 8 x 8, (called an FEU, or 40 ft. equivalent unit). In the container industry, containers are usually simply called boxes (AAPA, n.d.).

Declaration of security (DOS): An agreement executed between the responsible vessel and facility security officer, or between vessel security officers in the case of a vessel-to-vessel activity, that provides a means for ensuring that all shared security concerns are properly addressed, and security will remain in place throughout the time a vessel is moored to the facility or for the duration of the vessel-to-vessel activity, respectively (33 CFR §101.105).

Exploitation: The act of taking advantage of something; the act of taking unjust advantage of another for one's own benefit (Black's Law Dictionary, 2009).

Facility security assessment (FSA): An analysis that examines and evaluates the infrastructure and operations of the facility taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures, and operations (33 CFR §101.105).

Facility security officer (FSO): The person designated as responsible for the development, implementation, revision and maintenance of the facility security plan and for liaison with the COTP and Company and Vessel Security Officers (33 CFR §101.105).

Facility security plan (FSP): The plan developed to ensure the application of security measures designed to protect the facility and its servicing vessels or those vessels interfacing with the facility, their cargoes, and persons on board at the respective MARSEC Levels (33 CFR §101.105).

Maritime security (MARSEC): The security level set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S (33 CFR §101.105).

MARSEC Level 1: The level for which minimum appropriate security measures shall be maintained at all times (33 CFR §101.105).

MARSEC Level 2: The level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident (33 CFR §101.105).

MARSEC Level 3: The level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable, imminent, or has occurred, although it may not be possible to identify the specific target of the threat (33 CFR §101.105).

Terrorism: The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives (28 C.F.R. § 0.85).

Transportation security incident (TSI): A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in an area (33 CFR §101.105).

Assumptions

In this study, I assumed that there is a need to better understand what, if any, impact does policy, economic practices, or politics have on security practices as U.S. seaports. It was furthermore assumed that ongoing exploitation of the global supply chain by transnational criminal organizations jeopardizes security at U.S. seaports, allowing for terrorist targeting to be directed to economic infrastructure. I assumed that individuals are willing participants in this study and that they would provide responses only based on factual knowledge obtained through experiences and observations of the phenomenon under study.

I also assumed that the promise of confidentiality and anonymity would result in participants being truthful and forthcoming in sharing of information related to seaport security within their respective geography and professional experience. All sources, documents, and literature that were a part of this research were free of biases and were objective and accurate. It is assumed that the information derived from secondary data sources were thoroughly evaluated, assessed, and accurately reported based on acceptable research and legal collection methods. It is also contended that this study's sample size is adequate to fulfil its stated purpose of exploring security measures at U.S. seaports. This study adheres with research ethical guidelines; therefore, I assumed that the use of secondary information did not skew the results of the study.

Scope and Delimitations

This study was focused on security measures in use at U.S. seaports. The study explored maritime security measures instituted under the Maritime Transportation Security of 2002 and other legal regimes acting in concert to prevent unauthorized entry into regulated facilities and cargo. I was unable to conduct field observations or in person interviews as part of this study due to geographical restraints and limited resources to support extensive travel and basic accommodations. Moreover, the method and design of this study inevitably led to encounters with security sensitive information that restricted its incorporation into my findings.

I included the use network sampling, which is more respondent driven, as an alternate strategy. Network sampling originates from a small group of initial participants from the study population who are asked to recruit up to three new contacts from within

their network (Patton, 2015). No participants were required to participate. All participants were adults, and no minors or members of vulnerable populations were included in this study. Recruiting and selection of participants was fair and impartial; gender, race, age and/or nationality were not relevant factors or of interest to this study, so participants were not be asked to disclose such. Due to legal limitations in investigating security sensitive measures at seaports, ports being spaced geographically, distinctions in cargo commodities, and diffusion of authorities of the sample population, the findings from this study should be considered exploratory and not to be generalized to other populations.

Limitations

Limitations of this study includes encounters with information that is designated as Sensitive Security Information (SSI) or classified under 49 Code of Federal Regulation, Part 1520.5(b). Additional potential barriers or challenges include my professional affiliation and experience as a law enforcement practitioner. Recruiting participants for interviews and objective separation of my role as a law enforcement officer from my role as researcher required constant evaluation and accountability. Challenges further included limiting or restricting access to data that is available through personal and professional relations with intended sample populations. Additionally, monitoring confidentiality or anonymity related to actual participants or seaport location of the individuals who participated could influence the outcomes of this study. Lastly, qualitative data cannot be generalized, so the perceptions and experiences of participants only represents those who participate in the study.

Significance

Researchers have supported the reality of convergence between drug traffickers and terrorist organizations (Bartrell & Gray, 2012; Brown, 2017; Drug Enforcement Agency, 2020). Both transnational organized criminals and terrorists perceive global trade as suited to meet demands for illicit drugs and transportation of illegal weapons (Leuprecht et al., 2015). This study makes an original contribution by filling a gap in literature, through the exploration of seaport security practices and incidents in which individuals gained unauthorized access to port facilities and cargo. This study seeks to increase understanding of internal and external institutional factors at seaports that may be in contention with existing security measures.

The results of this study are intended to provide essential insights into the perceptions of security officials and practices in existence at U.S. seaports. The 9/11 Commission's (2004) findings included warnings that terrorist organizations are not limited to targeting the aviation sector, but opportunities for terrorists to do harm are equally "as great, or greater in maritime or surface transportation" (p. 392). This study acknowledges the commission's findings and therefore provides a more in-depth look at security practices at seaports. Insights from this study furthers the goal of improving security practices at U.S. seaports and contributes to the foundation of knowledge available to policymakers, thereby supporting broader U.S. homeland security strategies.

The positive social change implication for this study provides policy makers, industry leaders and the public with information related to seaport exploitation such that the maritime system and communities are better protected against attacks. Through its

strategic focus on system thinking as a method for examining causes, contributing factors and solutions to addressing complex homeland security problems, this study dissected and explored the structures and cultures of seaports. This study's implication for social change is multifaceted. This study provides an increased understanding of seaport threats and vulnerabilities through an exploration of common methods used by traffickers to exploit legitimate cargo operations. This study is intended to intervene in the pathway of cultural complacency, to redirect and encourage a unified approach to safeguarding U.S. seaports. This study also provides a tool for organizational and systemic change through comprehension of maritime threats posed to public safety and national security. This study provides for the enhancement of knowledge for policy makers, industry leaders and public policy awareness for local communities. Lastly, this study creates a cultural change mechanism for stimulating social change in the general perception of seaport security importance. As a result of this study, risk of a terrorist attack against a U.S. seaport is mitigated.

Summary

Although the United States has taken substantial steps in increasing the nation's security posture at seaports, many challenges and vulnerabilities remain (Leonard et al., 2015). Additionally, though, several Homeland Security studies have assessed how successful seaport security officials have been in instituting strategic screening practices, their evaluative criterion is lacking. Seaport security screening effectiveness and the institutional frameworks that support them is therefore analyzed under scrutiny of their failures. The enormous amount of cargo transiting U.S. seaports annually often renders

security screenings ineffective against transnational organized criminals who routinely exploit the maritime system to smuggle dangerous drugs and other contraband. Smuggling organizations pattern their criminal operations around the legitimate and porous cargo routes, mirroring multinational business functionality in a manner that disguises large shipments of drugs. This presents an array of challenges and concerns both to public safety and national security. Further, terrorists, like transnational criminals are assumed to be rational actors who also assess risk when making determination as to what transportation systems to exploit. Therefore, I conducted this qualitative study to explore security measures at U.S. seaports to gain a better understanding why individuals and groups gain unauthorized access to restricted facilities and cargo.

Chapter 2: Literature Review

Introduction

Smuggling techniques used by transnational criminal organizations to ship dangerous drugs, weapons and other contraband through U.S. seaports undermines security measures, nullifies responsible business practices, and threatens national security. The gap in literature is that U.S. seaport security has not been evaluated in relation to exploitation by transnational criminal organizations and terrorist groups. An in-depth review of academic literature, governmental records, and reports provided valuable insight that allowed me to contextualize the phenomenon and make an appropriate selection of method to further the study. The literature inquiry divulged evidence indicating an active expansion of terrorist group involvement in the illicit drug trade, creating and irrefutable means in which a weaponized device can be smuggled into the United States through a seaport. A qualitative study conducted by Leuprecht et al. (2015) observed that both transnational organized criminals and terrorists perceive the global economy as being ideally equipped to meet demands for illegal goods and services. The literature indicates the occurrence of a troubling convergence between drug traffickers and terrorist organizations in relation to tactics and economic motives. A study conducted by Levitt (2013) observed that more than 19 U.S. designated foreign terrorist organizations are known to be involved in the global drug trade. This phenomenon was further noted by Dishman (2016) who wrote that observable growth of the illicit economy, and the rise of segmented markets and networks have “major implication for terrorist and criminal collaboration” (p. 147). The purpose of this qualitative study was to

explore seaport security measures to identify factors that may adversely impact security measures at U.S. seaports. The objective of this comprehensive literature review was to research, collect, analyze, and fuse the literature related to maritime security, terrorism, and drug trafficking methods used to exploit major seaports. In studying the phenomenon of maritime drug trafficking using seaports as a conduit, contributors to failed security measures are identified. The chapter offers an inclusive review of the theoretical and conceptual bases of seaport security. The chapter also includes sections on my literature search strategy and theoretical framework, followed by a review of the literature. The chapter ends with a summary and conclusion section.

Literature Search Strategy

The literature search strategy for this study included the use of books, peer-reviewed journals from the Walden University Library, governmental and nongovernmental documents, reports, and articles relevant to seaport security and drug trafficking. The selected literature aided me in developing the theoretical framework for this qualitative study. The following is a list of key terms used to review relevant literature: *seaport security, homeland and maritime security, drug smuggling, transnational organized crime, drug cartel and terrorist convergence, narcoterrorism, shipping container security, port governance, Rational Choice, Game Theory* and *General Systems Theory (GST).* The primary databases for this study were *Taylor and Francis, ScienceDirect, and SAGE Journals, Thoreau, Google Scholar and Homeland Security Digital Library.* The literature search focused on retrieving peer-reviewed journals within 5 years of publication. However, extending the literature search beyond 5

years was necessary for a more wholistic overview and understanding of seaport security and threats posed against U.S. seaports.

Theoretical Foundation

The GST (von Bertalanffy, 1968) grounded this study and provided specific tenets for distinguishing maritime system structures, components, and functions both individually and holistically. Ludwig von Bertanlanffy (1968) posited that systems are composed of individual elements that interact with each other and the environment. In examining the interactions of maritime system components individually, I developed a better understanding of how unauthorized individuals and goods may gain unauthorized access to secure seaport facilities and cargo. GST asserts that all systems have common characteristics regardless of their internal nature (Skyttner, 2006). In the context of this study, GST allowed for the identification, and uncoupling of system components, to support objective examination of them individually. In examining maritime system components individually, this study revealed characteristics that are both similar and different. However, it is the distinguishing features of motives, functions and priorities observed between individual elements where research uncovers potential sources of system points of failure and literature gaps.

Developing an understanding of seaport security culture and logistical processes supported conceptualizations and analysis, of inadvertent contributors to unauthorized access to maritime environments. Bernard et al. (2005) noted that GST application to social organizations focused on the nature of openness and interactions within environments of various inputs and outputs. Maritime imports and exports represent

system inputs and outputs that replicates natural “feedback loops” in which they continuously adapt to changes in external environments (Bernard, 2005). Seaports are fast-paced environments where logistical operations are driven by consumer demand and just-in-time supply business models. The Federal Maritime Commission (2015) noted that future expansion of international trade is inevitable, and future demands on the U.S. intermodal system will be considerable.

Although security regulations are implemented at U.S. seaports, they contend with the financial and operational stresses of global trade. The Federal Maritime Commission (2015) observed that increases in transportation costs caused by seaport congestion harms the U.S. economy and adversely impacts the nation’s international competitiveness. Bernard et al. (2005) concluded that system malfunctions affect system inputs and outputs both directly and indirectly. In studying seaports as system components, cultural dynamics revealed potential areas of contention between security officials and port management responsible for logistical operations. Immediately observable in the literature review is that container volumes (inputs) entering seaports exceed security processing capacities, resulting in temporary security system overload (Hutchins, 2016; Johnson, 2013; U.S. Government Accountability Office, 2016). Only a limited number of product inputs can be inspected while entering seaports without adversely impacting logistical outputs. Researchers (e.g., Chang & Thai, 2016; Flynn, 2006; Shapiro, 2018; UNODC, 2016; Willis, 2016) indicated that while strong performance and growth indicates a properly functioning system, the growing presence of contraband amongst legitimate cargo demonstrates that seaport security measures are

insufficient. Illicit goods move from one environment to another environment through input to output processes facilitated through the maritime system.

Seaport operations involve arrangements between separate interrelated elements functioning together as a whole. Like living organisms that are sustained by synchronized organ functions in which the actions of one effect the performance of others, seaports are isomorphic systems found amongst the social and economic sciences. In applying GST, seaport vulnerabilities and exploitation are perceived as outcomes attributed to host miscalculations, misalignments, errors, misdiagnosis, and mistreatments; consequently, allowing for invasion of criminal organizations. In the context of this study, seaport security is analyzed both physically and socially. Bertalanffy's exploration of systems theory finds application across a range of complex fields in which the emergence of isomorphism clearly exists, including seaports. Bertalanffy's systems theory is rooted in the study of health and human systems in which physicians commonly perform diagnostic examinations of the body (system whole) and organs (parts) individually (Tretter, 2019). Physicians attempt to confirm the presence of disease in symptomatic patients to formulate effective treatment strategies; likewise, an evaluation of seaport health should include a thorough diagnostic, security examination of the maritime system as a whole and in part. Like viruses, illicit goods pose no imminent threat to society if they do not enter living functioning systems. However, when systems are infiltrated by illegitimate groups, they soon replicate or expand illicit activities. Legitimate systems that have been compromised eventually become enslaved and used for transnational organized criminal purposes. The maritime system and global supply chain, like groups

of interlinked cells have been routinely highjacked and made to work on behalf of criminal and terrorist networks. Viruses need host cells to replicate and expand, so they breach legitimate cell walls, deposit, and reprogram them for expansion, then remain within the host cell, making them impervious to medical treatment (Ruth, 2019). Similar to complex technological systems infected by malicious software (malware), drug trafficking organizations disguised as legitimate enterprises (shell companies) share the maritime transportation system with legitimate members who depend on seaports to facilitate the movement of essential goods. The frequent complex interactions between system components are not always understood or what they appear to be. Business practices are routinely exploited when they are lured by sophisticated trafficking and laundering schemes in which they are deceived to believe they are dealing with a trusted agent or source. Criminal networks behave similarly to malicious software. The most common type of malware are worms, viruses and trojan horses, each of which exploit system vulnerabilities for nefarious purposes. Worms exploit system vulnerabilities, taking over a host and manipulating its own controls to launch attacks against system networks (Brody et al., 2018; Williamson, 2004).

Seaport similarities are also found in complex ecosystems. Within ecosystems, ecologists study behaviors and nonlinear interactions between living organisms to gain understanding of environments, including cyclic predator and prey encounters, a potential parallel or bridge with game theory (Tretter, 2019). Seaport security measures are important processes in border security; however, they tend to create delays, increase congestion, and are detested as associated or cause for inconvenience. The goal of

security measures at seaports is to detect, deter and prevent the introduction of dangerous devices, substances, and people from gaining access to the United States. While safety and security are important objectives, the mission of seaport organizations requires a commitment to providing a positive customer experience and the promotion of transportation efficiency (City of Los Angeles, 2018; City of Portsmouth, 2018; Port Authority of New York and New Jersey, 2020). The goal of drug trafficking organizations (including terrorist organizations) is to observe, develop and employ sophisticated strategies to exploit transportation processes to introduce dangerous and illicit items into the United States. The main motivators of these groups center around profitability and power. One kilogram of cocaine purchased in Colombia is estimated to range between $1800 to $7000 per kilogram; the same amount would retail for between $27000 to $35000 in the United States and could be sold for about $160 per gram (Benitez, 2019; Stewart, 2016; U.S. Department of Justice, 2018). This complex interaction of competing and coalescing priorities evolves into a dangerous positive-sum game with drug trafficking organizations but may evolve into a zero-sum game with terrorist organizations (Tala & Zhuang, 2018; Song et al, 2016). Systematic social interactions between workers at seaports leads to development of both harmonious and conflictive relationships over security and logistical priorities. While security regulations are applicable to each component of seaport system environments, they must contend with logistical demands. A lack of integration or system synchronization between the two creates subsequent opportunities for criminal exploitation. The literature inquiry revealed key concepts that focused and guided this study.

Seaports are geographic boundaries, acting as host to various interdependent industries responsible for the facilitation of global trade. Seaports themselves are subsystem components of the global supply chain. As subsystems, seaports share unique vernacular or terminology to communicate processes and to convey meaning. One commonly used term in the maritime domain and common to both the shipping and logistical industries, and applicable to this research study is *intermodal*. Intermodal refers to the transportation of goods in shipping containers by more than one mode of transportation (Intermodal Association of North America, 2019). Intermodal transportation is a dynamic and complex system that involves multiple actors and decision makers. Intermodal local drayage operations involve the pickup and delivery of loaded inbound and outbound containers in a service region of an intermodal terminal within a specific time window (Macharis & Bontekoning, 2004).

Intermodal containers (commonly referred to as *box, container or TEU*) are moved through seaports by way of commercial trucks and rail. Container cargo operations typically involve an international freight forwarder. A freight forwarder is an individual or business that specializes in facilitating maritime cargo shipments and storage arrangements on behalf of a shipper (U.S. Department of Commerce, 2020). Freight forwarders serve as an intermediate between customers and final points of destination, and assists exporters in preparing price quotations, recommended packing methods, preparing the bill of lading and special submission using the Automated Export System (U.S. Department of Commerce, 2020). A freight forwarder arranges both vessel and terminal storage space and secures cargo shipping orders. Shipping orders are

documents used to specify what items are being transferred from an originating storage location to a new location. Shipping orders are sent to a pre-designated trucking company that uses the shipping orders to obtain an Equipment Interchange Receipt (EIR) from a port terminal facility. Local and over-the-road truck drivers arrive at seaports to pick-up or deliver containers that are either empty or loaded. While seaport logistical procedures may vary, most share similar processes for obtaining security clearance.

Security measures implemented with the passage of the MTSA, requires presentation of proper credentials (Transportation Worker Identification Credential) for authorization to access to a U.S. seaport. Truckers arriving at U.S. seaports interface with either a security official or security technologies that verifies authenticity of credentials presented by anyone attempting access to a restricted facility. Mandatory security credential requirements managed by the Transportation Security Administration (TSA) have restricted many people from obtaining access to U.S. seaports, including truck drivers. However, drivers who are unable to access a restricted port facility will often sub-contract container pick-ups and deliveries to a qualified driver or firm with a legal tractor and a TWIC equipped driver. These TWIC equipped drivers perform the actual drayage service, by delivering import loads retrieved from seaports to local yards, pre-designated warehouses, or other locations (National Academies of Science, 2011). Trucking companies typically experience high turnover of both employee drivers and owner subcontractors, so there is often a constant turnover, and new drivers entering seaports. Belzer and Swan (2011) noted that although the Customs-Trade Partnership Against Terrorism (CTPAT) program, relies on importers to know their supply chain

partners and to manage risk responsibly, low-paid supply-chain workers in the United States and abroad may provide an exploitable opening for criminal organizations. In a study conducted by Flynn (2006), he noted that C-TPAT member companies are publicly advertised, and their membership used as an economic marketing tool; however, interested partners not only include legitimate businesses, but they also include transnational criminal organizations. A drug trafficking or terrorist group would likely target a legitimate C-TPAT member company with a trusted brand name, because its cargo shipments would likely be less scrutinized by security officials when entering the United States. A terrorist organization need only commit resources to exploiting weak security measures within a trusted shipper's company, targeting its susceptible workers to gain unfettered access to container goods and seaports (Flynn, 2006).

Johnson (2013) explored the topic of transnational terrorism, globalization, voluntary compliance, and U.S. ports security. Johnson used a qualitative case study design to examine trade and terrorist interactions, as well as impacts of trade policy on terrorist opportunities, and homeland security measures. Johnson found that the United States is the primary target country for transnational terrorism, and voluntary compliance programs and low container inspection rates (3%-5%) at U.S. seaports is inadequate to protect the nation.

In a qualitative case study, Eski and Buijt (2016) explored corruption at the Port of Rotterdam to gain insight into why port workers help in the facilitation of illegal drug shipments. Eski and Buijt focused on the "rip-off" tactics used by drug trafficking organizations to smuggle contraband inside of shipping containers without the knowledge

of shippers or consignees. Rip-offs involve loading cocaine or other contraband inside a container of legal goods from a country of origin, then recovering them once the illicit goods arrive at the port of disembarkation. The study included an analysis of rip-off cases at the Port of Rotterdam, using files from closed criminal investigations conducted by port police and customs agencies. The study also used transcripts from police interviews, court records and interviews with former convicted port employees.

Eski and Buijt (2016) explained that port workers are crucial components of criminal networks because of their ability to move around within a busy seaport without drawing suspicion from security officials or other employees. Port workers are also able to provide confidential information about facility layouts, container stack locations, vessel origins, arrival, and departure times (Eski & Buijt, 2016). Corrupt port workers at Rotterdam were found to routinely assist criminal networks in gaining access to shipping containers by breaching security seals, deliberately positioning containers for ease of access, or by allowing use of employee access credentials (Eski & Buijt, 2016).

As noted in the theoretical framework of this study, GST allowed for observation of system components separate from the system wholes. This allowed me to focus on the individual functions, motivations, and priorities of these individual elements, to look for areas of contention that leads to gaps creating system vulnerabilities. Eski and Buijt (2016) uncovered several key findings that informed my study, particularly in relation to my research questions. Strategies used by transnational criminal networks to recruit port workers are barriers to the implementation and effectiveness of security measures at seaports. Some observed reasons uncovered by Eski and Buijt as to why port employees

become involved in trafficking drugs at seaports is personal cocaine and alcohol addiction, financial hardship, gambling problems, greed, persuasion, blackmail, and intimidation.

Sophisticated recruitment, manipulation and the threat of violence posed by drug trafficking organizations as an instrument for infiltrating seaports should not be dismissed or underestimated. Traffickers are known to target employees with drug addictions and financial hardships associated with gambling; offering susceptible workers money and drugs to lure them into their criminal networks. Traffickers and corrupt port employees were found to target vulnerable employees with solicitations and promises of debt relief and easy wealth (Eski & Buijt, 2016).

Perhaps more concerning is a qualitative case study conducted by Bloom (2017) uncovered similarities in the recruiting cycles, priorities, and approaches of terrorist groups, including Al Qaeda, and the Islamic State in Iraq and Syria (ISIS). Terrorist recruiting responds to changes in the external environment influencing decisions of target recruitment that are based on human asset availability, education, or training most beneficial to the organization (Bloom, 2017). Collectively, researchers have suggested that behavioral characteristics of insider threats includes vulnerability to blackmail, greed, and financial need (Bloom, 2017, Branker, 2016; Eski & Buijt, 2016).

Literature Review Related to Key Variables and/or Concepts

Through an in-depth analysis conducted with focus on macro, meso and micro system levels, I sought to uncover maritime enablers adversely impacting security practices at U.S. seaports. My objective was to understand how individuals or groups

circumvented security measures and gain unauthorized access to secure seaport facilities and containerized cargo to conduct smuggling operations. Seaports are by nature both quasi-government institutions and highly competitive multinational corporations. While they create opportunities for growth and development, they present significant challenges to policing them. According to the U.S. Government Accountability Office (2015), the risk of security breaches increases during the transitions and exchange of containerized cargo between ports and distribution centers.

Sergi (2020) expounded on seaport and cargo vulnerabilities by explaining that drug trafficking involves a multilateral exchange between multiple criminal actors including negotiators, producers, brokers, importers, distributors, and consumers. Drug trafficking operations and methods include the use of cars, trucks, shipping containers, cargo ships, and small boats interfacing with ports. The intersection of cargo transition points within the global supply chain increases risk of exploitation, allowing for dangerous drugs or weapons to be placed into a shipping container destined for the United States. There was a gap in current research literature regarding understanding the experiences implementing security measures at U.S. seaports. My research did, however, reveal an abundance of literature originating in European countries related to seaports security and included various methodologies applied by researchers to explore the full scope of issues relevant to this topic. Most studies conducted were qualitative in nature and included phenomenological, ethnography, and case study approaches. Several researchers (e.g., Bagchi & Paul, 2017, Eski, 2016, Eski, 2019, Leuprecht et al., 2015,

Sergi, 2020) addressed seaport security vulnerabilities through a multitude of qualitative methodologies and each case provided insight into the literature gaps under study.

When discussing seaport security, a review of the governing bodies and laws exercising overlapping authority in maritime domains is essential. I discovered that the implementation of security rules under domestic and international law, following the September 11, 2001, attacks provided an incomplete framework for maritime security. This study explored the International Ship and Ports Facility Security Code, Maritime Transportation Security Act of 2002, and the Security and Accountability For Every Port Act of 2006. I began with an inquiry into the International Maritime Organization, a specialized agency within the United Nations.

The International Ship and Ports Facility Security Code

The focus of the literature inquiry was on the experiences, perceived barriers, and facilitators to seaport security measures. Security measures in use at seaports are based on both domestic and international law, therefore, filling the knowledge gap required understanding the maritime regulatory framework. The International Maritime Organization (IMO) is a regulatory body of the United Nations (UN) responsible for the institution of global standards for safety, security, and environmental performance. The IMO implemented international maritime security measures following the September 11, 2001, terrorist attacks against the United States. The IMO emphasized that the threat of terrorist acts against the shipping and port industry are real and not imaginary; and therefore, decided that the organization should take measures to prevent acts of terrorism

which threaten the security of passengers, crew and the safety of ships (International Maritime Organization, 2004).

While the al-Qaeda network targeted and exploited the aviation sector to carry out the 9/11 attacks, the level of sophistication of the group, highlighted susceptibilities of the maritime transportation system to acts of terrorism. At its 22nd session, on November 2001, the IMO adopted Resolution A.924 (22) to evaluate maritime security measures, while focusing specifically on preventing acts of terrorism that threatened the security of passengers, crewmembers, and the safety of ships (IMO, 2008; Trelawny, 2008). The IMO subsequently adopted the International Ship and Port Facility Security (ISPS) Code as an amendment to the 1974 Safety of Life at Sea Convention (SOLAS) (United Nations, 2004). The regulatory framework outlined within the ISPS are binding on Contracting Governments, cargo ships, passenger vessels, and port facilities servicing ships engaged in the transport of international commerce (International Maritime Organization, 2004).

The IMO addressed security threats to the maritime transportation systems by dividing the 1974 SOLAS Chapter XI into two parts. Chapter XI-1 for Special Measures to Enhance Maritime Safety and a new Chapter XI-2 for Special Measures to Enhance Maritime Security which established the International Ship and Port Facility Security (ISPS) Code (United Nations, 2006). The Code consists of two parts: Part A which imposes mandatory requirements, and Part B which consists of recommendations detailing procedures to be undertaken when implementing the provisions of Part A (United Nations, 2006). The code established three maritime security (MARSEC) levels

designed to depict incidents and security threat levels ranging from low to high (MARSEC 1,2, and 3). MARSEC level l is required and is covered under ISPS Code section A. MARSEC level 2 indicates a heightened threat of security incident, while MARSEC level 3 refers to a probable or imminent threat of a security incident (International Maritime Organization, 2004).

The ISPS Code was adopted in 2002 and entered into force on July 1, 2004 (United Nations, 2006). The ISPS Code enhanced maritime security on board ships and at port facilities where the vessel interface occurs. The ISPS Code provided a standardized framework for evaluating and countering risks. Among the main objectives of the code was to establish an international framework involving cooperation between contracting governments, government agencies, local administrations and the shipping and port industries. The objectives of the ISPS Code focused on the detection of security threats against ships and port facilities engaged in international trade and the establishment of respective roles and responsibilities of the parties involved (International Maritime Organization, 2003). While individually comprehensive, the Code required Contracting Governments to enact the new security standards in their respective countries. Under the ISPS Code, Contracting Governments are responsible for ensuring the completion of Facility Security Assessments (FSA) and Facility Security Plans (FSP) for seaport facilities within their respective jurisdictions. These assessments were required to be undertaken by either the Contracting Government, or a designated authority. FSA findings require the approval of the Contracting Government or designated authority and

are used to support development of the FSP and to determine which facilities require appointment of a designated Facility Security Officer (FSO).

The FSO is responsible for the development of an FSP and oversees all aspects of facility security for the assigned facilities. The FSP requires security levels to reflect actions to address prevailing threat conditions impacting maritime facilities. Level 1 indicates minimum operational and physical security measures; level 2 indicates additional security measures implemented to address elevated threats; and level 3 outlines further specific actions required to support response efforts to imminent threats to a maritime facility (International Maritime Organization, 2020). The FSO also ensures that security provisions are implemented and monitors the continuing effectiveness and relevance of an approved plan, including conducting internal audits of the application of the plan. The effectiveness of a security plan is required to be tested by governing authorities. A facility's FSA in which an FSP is based and developed must also be reviewed every 5 years. Major amendments to an approved plan require submission and approval of governing authorities. International agreements require ratification to become legally binding domestically, therefore, a detailed inquiry of U.S. maritime laws was necessary.

The Maritime Transportation Security Act

The United States, as a Contracting Government member of the United Nations, implemented the ISPS, through the Maritime Transportation Security Act (MTSA) of 2002. The MTSA was signed into law on November 25, 2002, by President George W. Bush (Maritime Transportation Security Act, 2002). The MTSA was purposed to protect

the nation's ports and waterways from acts of terrorism. MTSA regulations are applicable to vessels and facilities operating on or adjacent to waters subject to the jurisdiction of the United States. The MTSA directed the U.S. Coast Guard (USCG) to assess the effectiveness of antiterrorism measures implemented in foreign ports from which U.S. documented vessels and foreign vessels depart on a voyage to the U.S. and any other foreign ports the USCG believes poses a security risk to international maritime commerce. According to the National Response Center (NRC) approximately 157 suspicious activity reports and more than 300 security breaches were reported to have occurred at U.S. maritime facilities in 2015; 500 breaches of security were reported in 2014; and more than 400 breaches were reported in 2013 (National Response Center, 2015). (See Figure 1 for reporting trends of incidents involving suspicious activity and breaches of security at U.S. seaports).

Figure 1

National Response Center Data Summary 2015

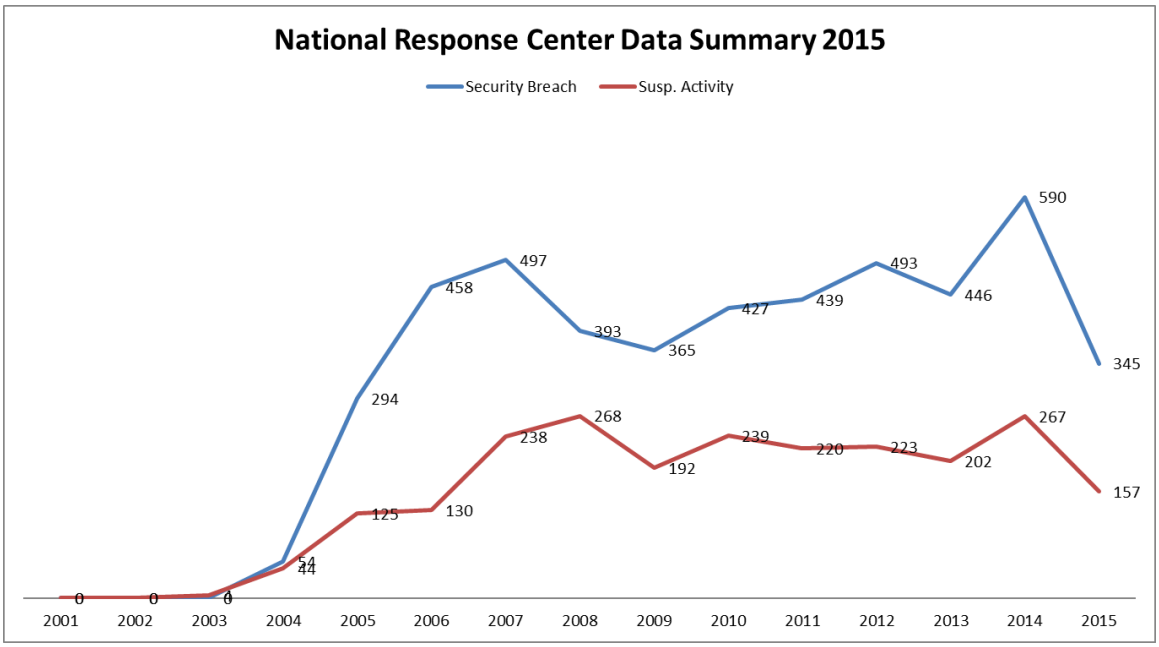


Figure 1. National Response Center Data Summary from 2001 to 2015 (does not include information from all sources). Hampton, E. (2015). An Analysis of the International Ship and Port Facility Security (ISPS) Code: A Multilateral Agreement to Secure the Global Supply Chain.

Lloyds of London estimated that approximately 112,000 merchant vessels link the world's 11,892 international port facilities in 155 coastal nations (Cox, 2013). About half a billion containers move throughout international waterways each year, and one out of nine containers are destined for U.S. shores (Cox, 2013). U.S. seaports handle more than 50,000 international vessels receiving more than 10,000,000 containers by ship annually (Cox, 2013). The sheer volume of container traffic into the United States annually clearly indicates a need for greater scrutiny of maritime security measures. Cox (2013) also noted that both the Transportation Security Administration (TSA) and the Federal Bureau

of Investigation (FBI) have recognized the global shipping network as the most viable and logistically feasible conduit for terrorist groups to maneuver weapons and operatives. The MTSA was followed by a host of new amendments and programs to strengthen maritime security, including the Security and Accountability For Every Port Act.

The Security and Accountability for Every Port Act

On October 13, 2006, the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) was signed into law, creating, and codifying new security programs and initiatives, and amending portions of the original provisions of the MTSA. The SAFE Port Act established new standards and was a catalyst for the implementation of radiation scanning of all imported containers entering the United States. The SAFE Port Act included new requirements for emergency response protocols, and encouraged cooperation between local, state, federal government, and the private sector. The SAFE Port Act required the inspection of "high-risk containers" before their arrival to the U.S., and implementation of the Customs-Trade Partnership Against Terrorism program (GAO, 2007). Enacted in October 2006, as an amendment to the MTSA 2002, the SAFE Port Act instituted several programs within the supply chain security framework. The SAFE Port Act (2006) amended portions of the MTSA, requiring area maritime transportation security plans that focus on swift restorations of trade operations following a Transportation Security Incident (TSI). A TSI is an incident or event that results in significant loss of life, environmental damage, transportation system disruption or economic disruption in a geographic area (U.S. Congress, 2006).

The SAFE Port Act requires that both vessel and facility security plans regulate access control measures of persons engaged in surface transportation or intermodal containers operations. The Act imposed requirements for the issuance of secure transportation security cards, commonly referred to as Transportation Worker Identification Credential (TWIC). The SAFE Port Act required the Secretary of Homeland Security (Secretary) to institute and make available risk assessment tools to be used for updating maritime security plans and allocated funding resources to support the development of plans, under the port security grant program (U.S. Congress, 2006).

The SAFE Port Act directed the Secretary to develop and implement strategic plans to enhance the security of the international supply chain and to "establish minimum standards and procedures for securing containers in transit to the United States" (U.S. Congress, 2006, Sec. 204). The Act directed the Secretary to establish and implement a Container Security Initiative (CSI) that identifies and "examines or search maritime containers that pose a security risk before loading in a foreign port for shipment to the United States" (U.S. Congress, 2006, Sec. 205). The SAFE Port Act included provisions that (a) codified the CSI and the C-TPAT; (b) required interagency operational centers where agencies organize to fit the security needs of selected ports; (c) set an implementation schedule and fee restrictions for the TWIC; (d) required that 100% of the containers entering high volume U.S. ports be scanned for radiation sources by December 31, 2007; and (e) required additional data be made available to CBP for targeting inbound cargo containers for inspection (GAO, 2013).

The C-TPAT is a voluntary government initiative that established a program of shared responsibility based on cooperation between CBP and trusted importers. Businesses who partner by signing program agreements are required to comply with specific terms and conditions in exchange for certain cargo benefits. Business partners who implement specific security measures to protect the global supply chain are less likely to face strict examination by the CBP, saving members valuable time and cost (Bagchi & Paul, 2017).

Nearly $750 billion of the U.S. Gross Domestic Product (GDP) is attributed to the Marine Transportation System (MTS). The MTS facilitates the transportation of global commerce and enables the projection of U.S. military forces around the world in defense against and in pursuit of foreign enemies. The MTS is one in which, its necessary complexities essentially render it, its own *Achilles Heel.* The system's porous nature and operational characteristics presents many challenges for seaport security officials who are responsible for its protection (U.S. Department of Homeland Security, 2005). Maritime operations comprise multiple distinct and independent components working synchronously: seaports, vessels, waterways, facilities, intermodal (rail) and users (U.S. Department of Homeland Security, 2005). U.S. seaport security has evolved as an area of interest and concern of the country since the signing of the Tariff Act of July 4, 1789.

Bagchi and Paul (2017) explained that seaports have many characteristics that make them ideal targets of terrorist, because their operations are essential to the vitality and competitiveness of national economies. An imbalance between seaport security and the facilitations of global goods creates logistical and security challenges, that when

mismanaged may result in both direct and indirect consequences. Inspecting container cargo is time consuming, burdening on security resources, and likely disruptive to the global supply chain.

One security measure in place to balance security and facilitation is the use of advance tracking systems. Under CBP regulations, importers are required to submit an Importer Security Filing (ISF), that includes information about any cargo destined for the United States before it is loaded on a vessel. CBP operates Automated Targeting Systems (ATS) to review container shipments destined for U.S. seaports to identify cargo that may be at risk for containing terrorist weapons or other contraband prior to being loaded on a commercial vessel. The frequency wherein transnational criminal organizations have successfully smuggled large quantities of illicit drugs amongst legitimate goods onboard commercial vessels remains a major concern for seaport security officials. The ability of these groups to move enormous amounts of dangerous narcotics from source countries, across international borders and into local communities, presents an imminent threat to public safety and health.

The security requirements imposed under SAFE Port Act of 2006, provided a cursory glance into the vulnerability concerns at U.S. seaports, including their susceptibility to drug trafficking organizations. The Act required the CBP Commissioner to establish performance indicators related to the seizure of methamphetamine and precursor chemicals and to extensively study the movement of drugs into the United States on an ongoing basis. A comprehensive summary report is required to be submitted to the U.S. Congress outlining measures for “targeting high risk drug smuggling

operations or circumvention of the Combat Methamphetamine Epidemic Act of 2005" (U.S. Congress, 2006, Sec. 707).

Case Study: Maritime Security and European Seaports

In an ethnographic study, Eski (2016) scrutinized port security by focusing on micro-level, occupational identities of frontline security officials at the port of Rotterdam and Hamburg. The study included explication of port security governance and conceptualization of port security. The strengths of this study center on the in-person experiences and insight gleaned from the researcher's ability to walk, drive, sail, and perform administrative duties alongside seaport security officials. This study is significant to my research of seaport security measures and factors inadvertently contributing to security vulnerabilities, principally indicating social dynamics that were present and important factors relevant for academic scrutinization. Eski explored seaports as an ethnographic study of social spaces, networks, cultures, and practices which facilitated a better understanding of interrelationships within the global maritime transportation system. Eski (2016) participated in the daily activities of 85 participants in Rotterdam (N = 52) and Hamburg (N = 33), consisting of 30 operational port police officers, 31 security officers, 10 customs officers and 14 others who were involved in port security-related matters" (p. 3).

Eski (2016) found noteworthy thematic responses amongst some participants that informed my qualitative study of U.S. seaport security. Local law enforcement and security officials without access to intelligence information were limited in their perception of threats posed to the Port of Rotterdam and Hamburg. This suggestion is

consistent with barriers identified by Frittelli (2005) who found that while effective intelligence sharing with local port authorities is important to port security, state and local officials may not have the required security clearances. While participants in Eski's study acknowledged the reality of terrorism, their ability to conceptualize active threats posed to the Port of Rotterdam or Hamburg were dismissed as being unlikely. Several participants noted that their cognitive construction of terrorism is primarily based on media depictions of the September 11, 2001 attacks, Osama bin Laden, Al-Qaeda in Afghanistan, and images of beheadings (Eski, 2016). The absence of encounters with individuals and incidents at seaports that meet the 9/11 terrorist criteria likely contributes to a distorted view of what terrorist attack planning or covert surveillance operations look like. Some participants however, perceived their ports to be ideal targets for an attack, and routinely engaged in scripted scenarios that created tangibility in seaport security measures and their contribution to the global war on terrorism. This literature inquiry suggests the absence of consistency amongst security officials in relation to terrorist threat perceptions. The study suggests that the absence of effective information and intelligence sharing amongst security officials creates perceptions of exclusion and may be a factor or barrier to the implementation of security measures at seaports.

The ports of Rotterdam and Hamburg was described as physically closed-off corporate domains where one small disruption caused by policing initiatives significantly impacts business operations (Eski, 2019). A disturbing finding of Eski (2019) revealed that security officials contend that internal cultures within the port of Rotterdam and Hamburg, has resulted in the commercialism of policing, rendering protective measures

secondary to logistical operations. Eski uncovered the existence of a highly contentious environment where management is perceived by line officers as market-oriented, power hungry and inept. Eski identified important social dynamics in existence at Rotterdam and Hamburg, whereas the decisions and actions of management potentially serves as an inhibitor to effective security measures. Security duties within the ports are shared amongst groups with varying levels of authorities including private security officers, police officers and customs officers. Participants indicated that low morale and inside quarrels are potential barriers in existence inside seaport environments (Eski, 2019).

Participants almost uniformly condemned management and managerial rationalities in commercializing policing and security practices. Eski (2019) also revealed internal division amongst the ranks of line officers at lower levels. Participants explained that they are compelled to adopt a commercial outlook of policing within the ports, particularly when interacting with port officials, shipping companies, truckers, dockworkers, and vessel crewmembers. This was an important discovery as it highlighted similarities and distinctions between the perceptions of port police officers and customs officers. This study aided in identifying key factors for further analysis comparatively against U.S. seaports. Some participants (port police and security officers) perceived the ports as "safe havens for drug trafficking," but perceived policing of drug trafficking not their responsibility, instead, viewed it as strictly a customs agency task and responsibility (Eski, 2019, p.10). While ports of entry are considered secure when security officials interdict (seize) contraband before it makes entry into a country, security measures are

often perceived as a burgeoning cost and not as a resource for businesses (Malcom, 2016; Sergi, 2020).

Findings from Eski (2016) postulated that while seaports are vital transportation hubs instrumental in the global movement of goods, they may lack terrorist allure, because they do not align with the reality of the threats posed by terrorist groups. This contrary opinion is divergent from a Congressional briefing prepared by Parfomak and Frittelli (2007) who stated that information recovered from an Al Qaeda suspect suggests that terrorist groups have indeed targeted and planned attacks against a "wide range of Western maritime targets" (p.23). Historical data indicates that out of 40,126 recorded terrorist attacks between 1968 and 2007, only 136 were against the maritime industry (Eski, 2016). These totals suggest that history contradicts those who perceives seaports as target locations prone to terrorist attacks. Eski (2018) argued that declaring seaports as alluring targets fails to contribute to global efforts to prevent acts of terrorism in maritime, instead only serving occupational meaninglessness. This assumption is based solely on the absence or limited data of historical incidents of terrorist attempts to target seaports and ignores the well documented convergence of terrorist and transnational drug trafficking organization's activities and their imperial capacity to exploit seaports worldwide. The 9/11 Commission pointedly noted historical lessons from Pearl Harbor; it underscored that although the U.S. government had intelligence of an impending Japanese attack in 1941, it failed to anticipate or prevent it from happening. The Commission cited historians who observed that despite evident warning, alert measures bowed to routine assumptions and practices (9/11 Commission, 2004). Any assumptions,

that dismisses U.S. seaports as conduits or targets to transnational criminal and hybrid terrorist organizations, breeds cultural barriers of complacency. These assumptions automatically instill perceptions of “low risk” assertion despite clear indicators of threats and vulnerabilities. The social, bureaucratic, corporate, and political nature of seaports complicates routine decision-making in relation to maintaining a balance between security and logistics. Maritime smuggling methods highly resembles a game of “Pac-Man” in which obstacles and open doors shape the operating system environment (Sergi, 2020). The ability of criminal organizations to successfully import-export contraband is highly influenced by both the rules of global trade and maritime security practices instituted at seaports.

Terrorist groups, like more common transnational criminal organizations are rational actors who assess risk when making decisions as to what transportation systems to exploit. The effectiveness of any security measures in countering threats of U.S. seaport exploitation, is conditional, based immensely on the ability of security officials to anticipate, prepare, and adapt tactical responses. Institutional culture, directs proactive measures, including investments in infrastructure, and technology and prioritizing the implementation of security practices into routine business and social practices (Malcom, 2016). The methods used by drug trafficking organizations to smuggle large quantities of illicit narcotics are the same likely methods that will be used by groups who are terrorist oriented. Zaitch (2002) described cocaine traffickers as illegal entrepreneurs who are innovative and constantly exploring means in which to maximize profits. Terrorist organizations too, share a need for financial resources to support future operations. This

entrepreneurial point of view influences the business models and strategies of criminal networks and encourages continued exploitation of seaport vulnerabilities. Zaitch asserted that traffickers preferred to conduct operations at port facilities where the likelihood of detection is low. Traffickers avoid hanging around port facilities, instead, preferring to send representatives to negotiate with harbor personnel; make pickup or monitor shipments (Zaitch, 2002). The researchers (Eski, 2016; Eski, 2019; Sergi, 2020; Zaitch, 2002) found security gaps that may have disastrous effects on the United States and the global supply chain. Some of the seaport security concerns raised by the researchers include cultures of complacency, internal contention between national counterterrorism strategies, maritime security, and supply chain priorities. There is an ongoing knowledge gap in understanding the impacts of security official's perceptions of terrorist targeting, from a nontraditional viewpoint of physical attacks to exploitation for indirect support of attacks.

Seaport Exploitation for Narcotics Smuggling and Terrorism

The multilateral application of GST contributed to this study. The isomorphic nature of GST assisted in understanding that much like the human body does not always display indicators of underlying health conditions, the vibrancy of transportation systems may not exhibit indicators of imminent threats. Instead, infiltration of criminal or terrorist organizations may be gradually realized, overshadowed, intoxicated by the economic successes of industry. The U.S. Department of Transportation (2005) observed that in the months preceding the 9/11 attacks, the airline industry experienced record highs in the number of airline passengers for a given month with 65.4 million travelers. After the

attacks, the airline industry experienced dramatic decline that took nearly 3 years to recover. As U.S. seaports experience unprecedent growth, the tendency to dismiss symptoms of exploitation and imminent threats are likely to occur, resulting in a public safety and public health crisis.

The National Drug Control Strategy observed that between 2014 and 2017, U.S. death rates attributed to synthetic opioids like fentanyl increased 413 percent (U.S. White House, 2019). This is particularly noteworthy as U.S. overdose rates rose to a record level in 2017 with more than half of the 72,000 overdose deaths being correlated with Mexican Drug Trafficking Organizations (DTOs) expansion into the opioid markets (Drug Enforcement Agency, 2017). The Drug Enforcement Agency (2017) emphasized that Mexican, Columbian, Dominican, Venezuelan, and Puerto Rican trafficking organizations are becoming more sophisticated and are major facilitators of maritime drug shipments to the United States. The Drug Enforcement Agency (2017) openly noted that methods employed by TCOs to smuggle dangerous drugs into the United States includes the use of U.S. ports of entry (POEs).

In this study, I addressed important gaps in the literature by utilizing governmental reports to develop an understanding of the complexities of drug trafficking at seaports and to identify common methods used to gain unauthorized access to ports and cargo. On June 19, 2019, CBP announced the seizure of 17.5 tons of cocaine at the Port of Philadelphia. CBP officials, along with Homeland Security Investigations (HSI), and U.S. Coast Guard detected anomalies while examining shipping containers aboard the MSC Gayane, a Liberian-flagged container ship, transiting from South American and

Caribbean ports. Security officials recovered a total of 15,582 bricks, totaling 35,000 pounds of cocaine (U.S. Customs and Border Protection, 2019; U.S. Department of Justice, 2020). The subsequent investigation revealed that on multiple occasions crew members helped load bulk cocaine onto the vessel from speedboats that approached during the night. Crew members used the vessel's crane to hoist cargo nets full of cocaine onto the vessel and then stashed the drugs in various shipping containers (Department of Justice, 2020). This literature filled a significant portion of the gap by suggesting that illicit drugs are loaded directly from speed boats on waterways, bypassing security procedures required for entry into seaports. This method suggests that legitimate cargo may enter a seaport, be loaded onto a commercial vessel, then later compromised onboard a commercial ship with the assistance of corrupt vessel crew. This exploitation strategy would further indicate that container seal tampering is an issue requiring further exploration.

Another example: February 22, 2019, CBP in Savannah, Georgia announced the seizure of 450 packages of cocaine with an estimated street value of $19 million. The illicit drugs were concealed inside shipments of pineapples that originated in Cartagena, Columbia (U.S. Customs and Border Protection, 2019). Then, on June 11, 2019, the Drug Enforcement Agency announced the arrest of two individuals in Augusta, Georgia, on charges of conspiracy to possess with intent to distribute cocaine. The arrest included the seizure of 20 kilograms of cocaine shipped through the port that was recovered after it was delivered to an Augusta warehouse (Drug Enforcement Agency, 2019).

Another example occurred in June 2020, when law enforcement officials investigating contraband shipped from the Dominican Republic, seized 50 kilograms of cocaine, with an estimated street value of 1.75 million, shipped through a seaport in Savannah, Georgia (Drug Enforcement Agency, 2020). Law enforcement officials arrested three men after the container was picked up and delivered to a local warehouse, where three men from Florida opened the container and began to unload boxes (Drug Enforcement Agency, 2020). This literature contributed to filling the gap by implying that illicit drugs are smuggled from U.S. seaports by criminal networks who infiltrated a restricted facility using legitimate credentials.

Further contributing to fulfilment of the gap is a March 2010 arrest at a southeast seaport. Port Authority police officers became aware that three men disguised as dockworkers had boarded a taxicab and were attempted to exit the seaport facility. As the three men approached the terminal exit gate they jumped out of the taxi and ran from police. The three men were arrested after a brief chase and charged with smuggling about $500,000 worth of heroin and cocaine (U.S. Department of Homeland Security, 2010). The subsequent investigation revealed that the men were stowaways from South America, who dressed in safety equipment meant to impersonate authorized vessel crewmembers, carrying illicit drugs hidden under their clothes. The men reportedly ferried from a beach in Panama, to the commercial vessel. The group conspired with a sophisticated network in the United States who planned to pick them up, conceal them and transport them once outside of the seaport. This literature contributed to filling the

gap by implying that illicit drugs are smuggled from U.S. seaports by vessel stowaways who gain access to restricted facilities from commercial vessels.

The threat of drug trafficking as a conduit for smuggling a weaponized device through a U.S. seaport was substantiated in the literature. The literature inquiry confirmed the need to further study and understand how individuals gain unauthorized access to seaports and cargo. This literature inquiry validated the legitimacy of concern and urgency to fill gaps regarding seaport security, as terrorist organizations have now expanded their involvement of transnational organized crime. Illicit drugs follow the pathways of legal trade, so it is the demand, business models and flow of commerce that determines, unwillingly, the course of illicit shipments. This study, therefore, did not focus on distinctions between TOC groups and terrorists, but instead focused on their shared motives and methods of operation as a means of exploring seaport security capabilities and vulnerabilities. Eski (2011) contended that globalization has created ideal trans-ocean pathways to support the international drug trade. Smuggling organizations pattern their criminal operations around legitimate cargo routes, mimicking business functionality in a manner that disguises large shipments of drugs. Transnational criminals are "well organized, well equipped, often possessing advanced communications, weapons, and high-speed craft to conduct smuggling of people, drugs, weapons, and other contraband" (Department of Homeland Security, 2005, p. 5).

Lichtenwald et al. (2012) warned against assumptions of an absence of evidence of cooperation between drug trafficking organizations and terrorist. Lichtenwald et al. (2012) instead, argued that interrelationships between the two groups can be seen in their

shared motives and common methods of operation. While several terrorist organizations could potentially provide valuable insight for this study, Hezbollah (Party of God) is the central focus, as its current activities most appropriately aligned with the purpose of this study. Members of Hezbollah, the Lebanon-based Shia Islamist political party and militant group is a designated foreign terrorist organization that engages in amongst other illegal activities, drug trafficking and counterintelligence operations targeting maritime interests. Levitt (2016) explained that Hezbollah's expansion into the South American area narcotics industry has grown significantly, particularly the *Tri-State Border* areas. Hezbollah collaborates with drug cartels, producing substantial revenue streams, facilitating money laundering and drug shipments into the United States and Europe. In 2017, the U.S. Department of Justice announced the arrest of Ali Kourani and Samer Eldebek, in acting as agents of Hezbollah; they were convicted in 2019 for committing acts in support of terrorism. According to the DOJ, the two men are members of the Islamic Jihad Organization (IJO) and conducted intelligence gathering operation of security procedures at U.S. airports, the Panama Canal and transiting commercial ships (Department of Justice, 2017). The Panama Canal was built in 1914 to shorten navigation between the Atlantic and Pacific oceans; and was widened in 2016 to accommodate large ships carrying containers to U.S. seaports. The Panama Canal Authority’s decision to invest more than $5 billion in improvements, widening the Canal shifted the pathways of trade between Asian ports, Mexico ports, West Coast ports, Gulf Coast ports and East Coast ports. As Park, Richardson & Park (2020) explained, an increasing flow of container trade between Asian countries and the U.S. will continue for the foreseeable

future as shippers seek to avoid West Coast port congestion. This changing dynamic highlights an urgency to broaden U.S. seaport security measures and capabilities, to investigate, detect, and disrupt acts supporting and facilitating terrorism against maritime targets. The emergence of convergence establishes an urgent need to understand how, with the institution of mandatory security measures in place, do rogue TOCs undermine legitimate seaport security practices. Literature supports the existence of convergence between drug traffickers and terrorist organizations.

Exploitation of U.S. seaports requires traffickers to first, connect with a criminal broker within a source country and to secure sufficient funding to pay the broker's fee. The drug broker will likely liaise with drug cartel or clan members to facilitate arrangements of drug shipments. The illicit drug operation will involve secondary sourcing between the broker, Mexican drug cartel and Colombian drug producers or depending on the type drugs being smuggled, may involve Australian brokers in Myanmar for shipments moving through Thailand (Sergi, 2020). Traffickers who utilized the services of a drug broker often pay more; however, their risk of arrest is minimized with this method (Sergi, 2020). The broker is knowledgeable of seaport operations and oversees the shipment's logistical details, including terminal facility details, and shipping containers manifest information. Drug trafficking brokers contract with criminal networks or individuals working inside the exporting seaport. These individuals provide logistical and human support for the drug shipment while in port and may involve external freight forwarders who help to ensure that the illicit cargo is successfully loaded onboard a ship in port. Once loaded on board a container vessel the illicit drugs then

travel amongst legitimate cargo bound for markets or a target location within the United States, Europe, or other destinations.

Once the illicit drug shipment arrives at a U.S. port of call the shipment is then offloaded along with other legitimate goods. The drug shipment maybe removed from the container while inside the port, however this method increases risk of arrest and is potentially more expensive, often requiring the assistance of a local criminal network or individual working within the local port (Sergi, 2020).

One example was highlighted in a June 8, 2020 press release from the United States Attorney's Office for the Middle District of Florida announcing the arrest of three individual working for a Mexican drug trafficking organization. Members of a criminal network operating in Florida and Georgia pled guilty to conspiracy to distribute methamphetamine and heroin, and attempted possession with intent to distribute methamphetamine and heroin. According to the plea agreement, between October 2018 and March 2019, members of the drug trafficking organization organized and coordinated the shipment of numerous containers of methamphetamine and heroin aboard a cargo ship (Department of Justice, 2020, para. 1).

This domestic network (broker and co-conspirators) arranged arrivals and pickups of illicit drug shipments from a seaport in Tampa, Florida using a rental truck, then transported the illicit cargo to a residence in Atlanta, Georgia. (Department of Justice, 2020). This case underscores the sophistication of transnational criminal networks and the threats they pose to seaports, local communities, and the nation. This group infiltrated and exploited an otherwise secure system to facilitate movement of illicit items. The

global supply chain is composed of active interconnected subsystems that link communities and commodities from around the world; however, its reliance on open access and speed creates ideal conditions for criminal exploitation.

A product manufactured in one country may be composed of multiple components outsourced by another manufacturing factory in the same country or one from outside the country. Once assembly of the product is complete, a manufacturer would then load the product into a shipping container at an inland facility, after which it likely will travel by truck or rail to a major deep-water seaport in the region. In many instances, due partially to constant changes in freight handling, shipping containers are subject to tampering before its arrival at the seaport. Belzer and Swan (2011) noted that gaps in supply chain security increases risk of freight tampering the further inland it originates. Twenty-four hours before being loaded and departing on a commercial vessel, operators must notify U.S. authorities of the nature of the freight being shipped in each container, to receive authorization for loading onto a ship.

Belzer and Swan (2011) noted that although most containers will safely travel unimpeded, threats of piracy or a terrorist group gaining access to containers are increasing. A study conducted by Frittelli (2005) concluded that security initiatives implemented after 9/11 have not changed the intermodal transportation environment sufficiently to fundamentally reduce vulnerability to cargo containers, as a means of facilitating terrorism. Frittelli (2005) asserted that major credibility problems associated with shipping container loading and screening processes exits overseas, primarily in ensuring the integrity of cargo as it transits to the United States from its overseas origin.

Effective port security measure at point of origin is necessary, as inspecting cargo on the once it is loaded onboard commercial vessels is practically impossible and inspecting cargo upon its arrival at a U.S. seaport "could be too late to prevent a terrorist event" (Fittelli, 2005, p. 17).

In March 2006 retired U.S. Coast Guard Commander Stephen Flynn, testified before the Senate Homeland Security and Governmental Affairs Subcommittee. As part of his testimony, Flynn outlined a plausible terrorist smuggling scenario in which a U.S. seaport might be used to introduce a radiological device into the country, while hidden amongst a container shipment of shoes made in Indonesia. Flynn explained that a local truck driver sympathetic to al Qaeda, would be a participant actor who transported a legitimate sealed loaded container of sneakers to a bogus warehouse location. Though the container is sealed when it departs from the manufacturer, a trusted C-TPAT member, the seal is removed by the terrorist operatives and later replaced with a clone. Terrorist operatives would remove some of the legitimate commodities from the container, then load a radiological device, shielded in lead wrapping (Flynn, 2006). The sympathetic co-conspiring driver would then drive the loaded container to the Port of Surabaya, Indonesia, gain access, make the delivery to handlers who would load the concealed bomb onto a smaller feeder ship destined for Jakarta, Indonesia (Flynn, 2006). The container could then be loaded onto a larger container ship destined for the Port of Hong Kong. Once at the Port of Hong Kong, the container would be offloaded and then loaded onto a new Panamax container ship destined for Vancouver, British Columbia. Once in Canada, the container would be off loaded and placed onto a railcar bound for Chicago,

IL (Flynn, 2006). The container would then arrive at its destination; when opened by unwittingly cargo handlers, a triggering device attached to the door could detonate the bomb in the American heartland (Flynn, 2006).

In May 2020, the Drug Enforcement Agency (DEA) and the United States Attorney for the Southern District of New York, announced that a former member of the Venezuelan National Assembly was criminally charged with narcoterrorism, drug trafficking and other weapons offenses. According to officials, Adel El Zabayar conspired and participated in the illegal importation and exportation of cocaine to the U.S. with members of the Venezuelan Cartel de Los Soles, Foreign Terrorist Organization Revolutionary Armed Forces of Columbia (FARC), Hezbollah and Hamas (Drug Enforcement Agency, 2020). Hezbollah's expanding convergence with drug traffickers poses an imminent threat to the United States and the global supply chain; it is a dangerous communal relationship. Bartrell and Gray (2012) described networks of drug cartels as force multipliers for Hezbollah, instrumental in facilitating their acquisition and smuggling of weapons, weapon components and even operatives into the United States. Conversely, *Cartel de Los Soles* for example is believed to have directly recruited terrorists from Hezbollah and Hamas to assist in planning attacks against the United States (Drug Enforcement Agency, 2020).

On January 2, 2020, the United States killed Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) Commander Qasem Soleimani in a targeted drone strike. Iran's Supreme Leader Khamenei and President Hassan Rouhani both have "vowed revenge" for Soleimani's killing (Congressional Research Service, 2020, p. 3). This is noteworthy,

as Iran's primary terrorist proxy group is Hezbollah; it provides Hezbollah with thousands of rockets, shortrange missiles, and small arms, and has trained "thousands" of Hezbollah fighters at camps in Iran (Congressional Research Service, 2020, p. 6). Hezbollah's expanding ability to facilitate large drug shipments in convergence with transnational criminal organizations onto vessels and into U.S. seaports presents an urgent need for attention to maritime vulnerabilities.

Yagoub (2016) declared Columbia, Brazil, and Venezuela as significant departure points for enormous quantities of drugs being shipped onboard commercial vessels that are bound for European and likely U.S. markets. According to Yagoub, maritime smuggling using shipping containers onboard commercial vessels is the preferred options for narcotic traffickers. The European Monitoring Centre for Drugs and Drug Addition (EMCDDA) noted a significant increase in the use of shipping containers to smuggle large quantities of drugs into major seaports, accounting for over two-thirds of European Union seizures between 2011-2013 (EMCDDA, 2016). According to Insight Crime (2019) authorities in the Netherlands seized more than 73 metric tons of cocaine in 2018 at both the Port of Rotterdam and the Port of Antwerp, a 35 percent increase from 54 metric tons seized in 2017. These accusations highlight an urgency for seaport security officials to explore and understand the nature and methods of narcotics traffickers in undermining security practices at U.S. seaports. In 2016, the DEA announced the arrest of members of the Lebanese Hezbollah's External Security Organization Business Affairs (BAC), for its involvement in international criminal activities such as drug trafficking and money laundering in which proceeds were used to purchase weapons for Hezbollah

(U.S. Drug Enforcement Agency, 2016). The group was targeted as part of Project Cassandra, an international enforcement operation focused on dismantling global networks responsible for the movement of large quantities of cocaine into the United States and Europe (U.S. Drug Enforcement Agency, 2016). In 2016, former DEA Operations Chief, Michael Braun testified before the Committee on Financial Services of the House of Representatives. Braun reported that Hezbollah and South American drug trafficking organizations have moved, "hundreds of tons of cocaine, over a 15-year period and have moved massive amounts of currency, hundreds of, millions, perhaps billions of dollars in currency around the world in the most sophisticated money laundering scheme that we have ever witnessed" (United States, 2018).

The United Nations Office on Drugs and Crime (2018) estimates that more than 750 million TEUs are moved at seaports worldwide each year; and approximately 5% are physically inspected. Dishman (2016) noted that the "growth of the illicit economy, coupled with the rise of segmented markets and networks, has significant implication for terrorist and criminal collaboration" (p. 147). Dishman expressed concerns that since the 20th century, relationships between Transnational Criminal Organization (TCO) leaders and terrorist groups have evolved to support network operational and logistical needs. Criminal organizations have acquired "explosives and weapons training, assassination, and other services, while terrorist organizations obtain fraud and smuggling services" from transnational criminal organizations (Dishman, 2016, p. 147).

The U.S. Department of State (2020) noted the exploitation of seaports in countries such as China, Jamaica, Pakistan, Europe, and Brazil as facilitators in "the

movement of drug shipments across borders" (p. 174). The U.S. Department of State (2020) emphasized that Brazil "remains a major transit route for cocaine from the source countries of Bolivia, Colombia, and Peru" (p. 110). Seaports in Pakistan act as one of the world's top transit corridors for illicit drugs, allowing for the illicit distribution of drugs globally (U.S. Department of State, 2020). According to the U.S. Department of State (2020) the Philippines is also a regional transshipment and destination point for illicit drug trafficking in Southeast Asia. While its airports and vast coastlines are exploited, transnational criminal organizations continue to exploit the Philippine seaports for major drug shipments (U.S. Department of State, 2016).

Another example of seaport vulnerability is found in a May 2020, seizure by Customs officials at the port of Havre, France, of 1.4 tons of cocaine that was hidden inside of a shipping container loaded with coffee. The dangerous drugs were loaded onboard a commercial vessel in the port of Puerto Cortes, Honduras. The illicit shipment was then swapped to another vessel in the Dominican Republic, before departing for its destination in France. The estimated street value was $110 million (Papadovassilakis, 2020). The United States is an allied partner with Honduras, and routinely works together to fight against transnational criminal networks engaged on narcotics trafficking, money laundering and trafficking of persons (U.S. Department of State, 2020, para. 1). In 2019, during a routine inspection onboard a commercial vessel docked at Port Newark, security officials discovered a shipping container with indicators of tampering. Officials noticed that the doors of the shipping containers, manifested with dry fruit, appeared to have been manipulated. A search of the container led to the discovery of 3200 pounds of cocaine,

with an estimated street value of $77 million (Watson, 2019). This illicit shipment of drugs arrived from Columbia.

Drug trafficking and organized crime funds terrorist groups such as al-Qaeda and FARC, providing the necessary financial resources to purchase weapons and pay the salaries of fighters (Thachuk & Lal, 2017). The cross pollination of terrorism and drug trafficking reveals a dangerous convergence that demands a change in maritime counterterrorism strategy. Seaport security measures appear to be inadequately equipped to detect, deter, or prevent exploitation of transnational criminal organization or terrorists. The shared financial motives, structures and criminal tactics represents a dangerous fusion in which convergence has happened. Thachuk and Lal (2017) cautioned it is increasingly difficult and arguably fruitless to continue to classify terrorism and organized crime separately. According to Shelly and Picarelli (2005) regions such as the Tri-Border area of Paraguay, Brazil, and Argentina are saturated with organized crime and terrorist activity and it "is often difficult, not to say meaningless, to draw a distinction between groups. Many individuals belong to both terror and organized crime groups and conduct a variety of tasks for both" (p. 5).

In the 1970s and 1980s, the Revolutionary Armed Forces of Columbia – People's Army (FARC) for example, became involved in the cocaine supply chain following the toppling of the Medellin and Cali cartels. By the 2000s, the FARC, an antigovernment guerrilla group formed in 1964, was identified as the largest supplier of cocaine in Latin America (Thachuk & Lal, 2017). While the group has undergone transition into a political party, the appetite of ex-guerilla members (dissidents) still engaged in organized

crime has led to expansion of the FARC's trafficking enterprise. The group has expanded its criminal enterprise and altered many of its drug trafficking routes to include routine shipments to West African seaports. In 2013, the DEA arrested members of al-Qaeda in the Islamic Maghreb (AQIM) and FARC involved in an elaborate scheme whereas cocaine was exchanged for drugs and weapons. The smuggling operation involved the use of fake export licenses for commercial ships used to traffic large quantities of drugs to major West African ports (Thachuk & Lal, 2017). Shelley & Picarelli (2005) noted that an increasing number of criminal organizations are serving the financial or logistical ends of terror groups and thus serve as nodes of interaction. By analyzing criminal penetration of seaports, research may provide "an important tool for assessing terrorist risk, both from the perspective of straight piracy, and because of the larger problem of penetration of ports by terrorists" (Shelly & Picarelli, 2005, p. 47).

Suspicious Activity and Breach of Security Reports

I gathered existing records of seaport security activity from the USCG, to support the methodology of this research study. Due to the sensitive nature of this research, and potential restriction in the sharing of information by security officials, I obtained the data using a Freedom of Information Act (FOIA) request. The data assisted in appraising and evaluating U.S. seaport security cultures prior to conducting interviews with security officials. Under federal law (33 CFR § 101.305) U.S. seaports are required to report breaches of security to the National Response Center (NRC) without delay; and are required to report suspicious activities that may result in a Transportation Security Incident (TSI).

The objective of this data analysis was to identify patterns in security threat activities, pinpoint incident locations and to help guide the development interview questions. I gathered unclassified information by submitting a FOIA request to the NRC (United States Coast Guard). The FOIA provides access to federal agency records or information that are not exempted from disclosure due to a governmental need for protective measures related to national defense and security (U.S. Department of Justice, 2020; 5 U.S.C. § 552). I formally requested all data explicit to maritime border security, specifically focusing my request on seaport security. I requested that the NRC compile and provide the annual total number of security breaches and suspicious activity incidents reported to the U.S. Department of Homeland Security (NRC/USCG) from seaport officials. My request included specific dates encompassing periods beginning July 1, 2001 to the date of request, April 21, 2020.

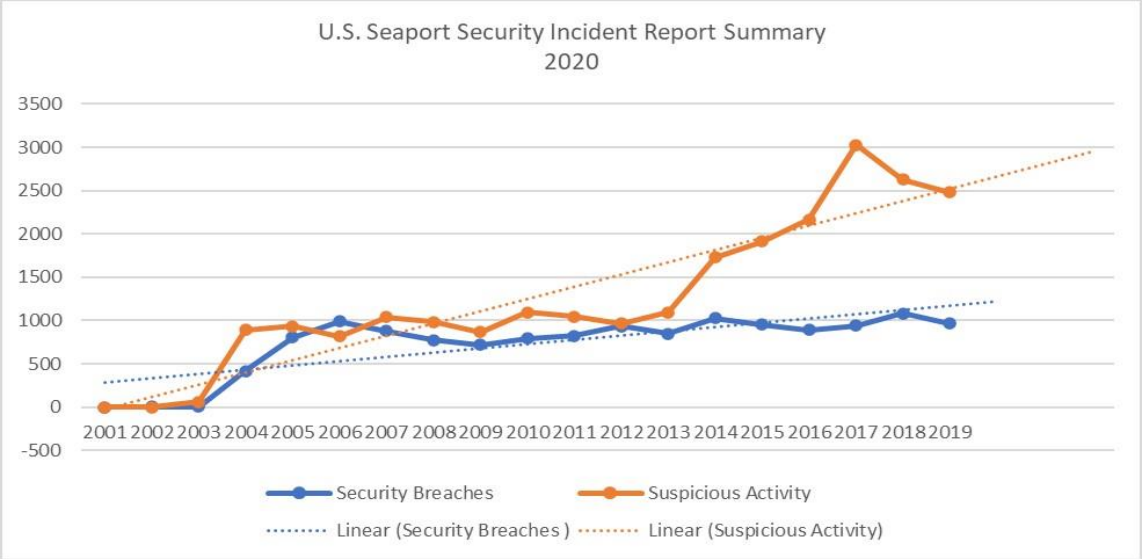
I included a formal inquiry into the actual nature of each reported incident, and the actual incident locations by zip code from which each report generated. My request included a statement of purpose for my request, and a general explanation of my intent to satisfy a research gap as part of academic doctoral studies at Walden University. Recognizing the sensitive nature of my request, I clarified my intent was not to acquire information protected or classified as Sensitive Security Information (SSI) under 49 Code of Federal Regulation, Part 1520. After several follow up requests, I received the needed records to conduct my analysis and to gain additional understanding of the phenomenon under study. However, while the records were sufficient for my study, I was not provided any information specific to the nature or actual locations of these incidents. I sought to

explore, collect, and analyze the data relevant to seaport threats, security activities and behaviors of security officials.

Through this collection of governmental records and analysis of the data, I made several important observations. The first observation I made was that an earlier study (Hampton, 2015) presented data indicating that incidents and activities were significantly lower than data currently being reported in this study for the same evaluation periods. A comparative analysis of both studies discovered the difference in data collection methods. The original 2015 FOIA request, limited the search criteria by only seeking data from the NRC database instead of records of all archived data recording breaches of security and suspicious activity as seaports. The second observation was that on July 1, 2004, both the ISPS Code and the MTSA became effective. In that same year (2004) there were a total of 418 incidents reported by U.S. seaports, in which security measures were circumvented, eluded, or violated. In 2005 the number of reports nearly doubled to a total of 803 security breaches that were reported to have occurred at U.S. seaports, followed by 991 in 2006; 880 in 2007; then averaging 868 incidents annually through 2015. Annual averages from 2016 to 2019, increased to 969 incidents annually. Third, I found that suspicious activity reporting steadily increased from 62 incidents in 2003 to 2482 incidents in 2019. The data records for periods beginning in 2016 and ending in 2019, were most notable with a peak of 3026 suspicious activity incidents at U.S. seaports being recorded (See Figure 2).

Figure 2

National Response Center & USCG Data Summary 2020



This data validated the rational for studying the effectiveness of security measures instituted at U.S. seaports, and warranted pursuit of qualitative interviews. The data informed this study by proposing that measures implemented at U.S. seaports since July 1, 2004 have not been effective in eliminating unauthorized access to restricted facilities. There has been no notable decline in security breaches since 2003, when reporting was not mandatory. Also noted was a significant increase (3026) in suspicious activity occurring at U.S. seaports between 2014 and 2017. The collective findings supported the rationale for this study, guided this research and supported the selection of its methodology.

Summary and Conclusion

In this chapter, I reviewed literature pertaining to seaport security, maritime drug trafficking and terrorism convergence. I also reviewed literature about transnational organized crime and maritime laws instituted in response to acts of terrorism committed against the United States. This study was not overly concerned with the collection of empirical data related to cargo volumes or number of security incidents occurring at seaports, but rather, I focused on exploring factors that allowed authorized people and illicit goods access to restricted facilities and cargo. In this qualitative analysis the focus of my study was on understanding why security measures failed to adequately secure U.S. seaports against smuggling and to explore the risk of a weaponized device being introduced through a port of entry. The literature illustrated that vulnerabilities do exists within cargo import and export processes that allows criminal organizations to successfully smuggle large quantities of drugs through seaports. The literature also illustrates that the intercoupled nature of the maritime transportation system renders current seaport security measures futile against criminal infiltration. Literature also revealed a lack of uniformity in terrorist threat perceptions amongst security officials at European ports; resulting in contentious interactions that contributed to know morale. Lastly, the literature illustrated an expanding convergence of DTO and terrorist organizations in international drug trafficking. The major theme in the literature encompassed the urgent need to prioritize and synchronize seaport security measures across all system components.

U.S. seaports directly support over 23 million American jobs and 4.6 trillion in economic activity. Seaports facilitate the movements of goods totaling approximately 26% of the U.S. economy, and anticipates trade volumes to quadruple by 2030 (United States, 2018). Acknowledging threats posed to U.S. seaports, in a 2017, Homeland Security Committee Hearing, Chairman Michael T. McCaul publicly emphasized that the security of U.S. seaports and cargo containers is vital to homeland security and the nation's financial health (United States, 2018). The Committee noted that security threats have evolved from piracy to complex smuggling operations, transnational organized crime, and terrorism (United States, 2018). While terrorist organizations are ideological, their reliance on illegal activities to fund attacks and support operational expenses has led to transformation into transnational criminal organizations (Thachuk & Lal, 2017). A false dichotomy of terrorism and organized crime as separate phenomena threatens the evolution of U.S. seaport security and the global supply chain.

The emergence of evidence indicating a correlation between counter-drug and counter-terrorism measures demonstrates that policy and practical countermeasures must also evolve and overlap to adequately eliminate seaport security vulnerabilities. The U.S. Coast Guard is touted as the first line of defense against drug traffickers seeking to smuggle illicit substances into the United States through seaports and waterways. The USCG coordinates with other federal agencies and countries to disrupt and deter the flow of illegal drugs and accounts for more than half of all U.S. government seizures of cocaine each year (USCG, 2020). U.S. CBP is responsible for more than 11 million maritime containers arriving at U.S. seaports annually, and is responsible for knowing

what is inside, or whether they pose a risk to national security (U.S. Customs and Border Protection, 2019). Port Authority police departments in the U.S. are specialized local and state law enforcement agencies responsible for protecting seaport from all threats whether by land, sea, or air (GPAPD, 2020; LAPP, 2020; PANYNJ[PAPD], 2020). Recognizing that narcoterrorism "embodies the merger of two phenomena, an even actual cooperation between two criminal networks, can make security theories more encompassing and more relevant and useful for policy making" (Bjornehed, 2004, p. 315).

The literature review included the collections of data from an in-depth research of academic literature; an analysis of archival records, governmental reports, and documents; and concluded with a series of open-ended interviews with seaport security officials. The combination of data collection methods used in this study supports triangulation, in which verification and corroboration of my findings is objectively accomplished. Additionally, data source triangulation used in this study strengthens its credibility (Yin, 2016). Although the literature on port operations is comprehensive, few studies pertain to seaport security measures and their capacity to prevent unauthorized access to restricted facilities and cargo. The lack of research presents a serious gap within the literature. In Chapter 3, I discuss the methodology used to determine the best course of action for securing U.S. seaports against transnational criminal and terrorist groups.

Chapter 3: Research Method

Introduction

The purpose of this qualitative study was to explore seaport security to understand what internal and external factors impact protection measures. Qualitative research is exploratory in nature, focused on meaning and understanding; therefore, it is ideal for gaining an understanding of existing maritime security measures and the phenomenon of unauthorized access to restricted port facilities and cargo. I used a qualitative research design because it offers flexibility and typically is not intended to prove or test a theory; however, elements of established theories did emerge during the literature review and may be observed during collection and analysis of the data (O'Sullivan et al., 2017). I used variants of a case study design to focus the study on the examination of seaport security measures as an individual function in a system with unique characteristics relevant to my research interest (O'Sullivan et al., 2017).

Transnational criminal networks routinely exploit the maritime transportation system to smuggle illicit goods into seaports around the world. Smugglers routinely infiltrate legitimate export processes to hide dangerous drugs, weapons, and other contraband inside of shipping containers from source countries, then retrieve them by exploiting import cargo processes at a port of destination. To explore and understand why seaport security measures have not adequately prevented unauthorized people and cargo from gaining access, I examined the maritime system as a whole and its subsystems individually, with strategic focus on seaports. Chapter 3 includes an overview of the research methods I used in conducting my investigation. In the research design and

rationale sections, I discussed the use of a case study approach and explained why it was important to this study. The research questions are also restated, and the role of the researcher is discussed. Lastly, the chapter includes the methodology that I followed in collecting and analyzing the study's primary data source.

Research Design and Rationale

The following research questions guided this study:

Research Question 1: What are the meanings, structures, and essence of lived experience of seaport security officials, in terms of instituting security measures required by the Maritime Transportation Security Act of 2002?

Research Question 2: What do seaport security officials perceive as barriers and facilitators to implementing security practices at U.S. seaports?

The complexity of seaport security, terrorism, crime, public policy, and global trade requires an approach, and strategy that offers both sufficient latitude, and capacity for understanding processes, people, events, and experiences (Yin, 2016). By conceptualizing U.S. seaports as both a system whole and subsystem component, I was able to explore with specificity, individual components and functions interacting in the maritime environment to identify barriers and facilitators. Seaports are social organizations that employ highly technological systems to facilitate the movement of goods and people. Therefore, human factors and processes were analyzed as part of this study because they influence overall system performance (Caws; 2015; Tin, 2016). The literature and secondary data sources indicated the prioritization of seaport security diverges dramatically amongst system components who rely upon each other to ensure

system efficiency. Accordingly, it was logical and necessary to pursue insight through the primary data source, participant interviews. Seaports are diverse in nature and vary significantly across geographical and political spheres, so findings from individual participants vacillated significantly; so, insight may not be generalizable and but may support theoretical propositions (Yin, 2018).

Role of the Researcher

As the inquirer, and primary research instrument, I was responsible for designing the interview protocol, interview guide, selecting participants, and conducting interviews with seaport security officials. I was responsible for the interview questions and disseminating consent forms to each participant. My role further included answering questions, addressing concerns of the participants, and transcribing all the data. While I had no personal relationships with any of the participants, careful consideration was given to my professional affiliations. One important task for the study was to bracket myself by acknowledging my personal and professional experiences as a law enforcement official. It was important to ensure that my relationships, knowledge, and experiences do not influence or interfere with reality expressed through study participants. The study did not include anyone in my direct chain of command. There were no power based supervisory, differential or instructor relationships involved in this study. Lastly, I had no recruitment interactions with the intended study pool prior to initiating contact for this study, nor were incentives offered as a condition for participation.

As an actively serving senior law enforcement officer (with over 20 years of experience) specializing in areas of maritime security, antiterrorism, investigations, and emergency management, I had preconceived ideas about my topic. To avoid bias, and to ensure consistency, I used a standardized set of questions for each interview. I used a digital audio recorder to record all interviews, took detailed notes, and provided each participant an electronic copy of their responses (within 72 hours of the interview). As an important mechanism to support and preserve the ethical values of this study, data exclusion was strictly scrutinized, and participant responses were verified using member checking. Member checks are procedures whereby a study's findings are shared with participants to ensure the accuracy of a study and reinforce ethical and collaborative relationships (Yin, 2016). Participants were asked to review their responses and to confirm that they were accurately transcribed before beginning analysis. Finally, there were no monetary incentives for participants to avoid the appearance of response influence or bias during interviews.

Methodology

This qualitative research study was conducted to explore and understand factors that adversely impact seaport security measures. The research used case study variants as an analysis approach for corroborating findings from multiple sources (Yin, 2016). The literature review of academic journals, articles and governmental reports led to findings indicating that U.S. seaports are at risk to exploitation by transnational criminal organizations, including hybrid terrorist organizations. An in-depth review of governmental records validated the academic literature findings, expanded my

understanding, and increased my intellectual interest in perceived barriers and facilitators to seaport security. Both the literature and secondary data sources confirms the existence of the problem and the existence of a literary gap.

To help in identifying concepts, and relationships existing in seaports, I used general systems theory. The theoretical framework is instrumental in allowing me to conceptualize seaports as complex systems, comprised of various independent components working together to sustain the viability of global commerce. The theoretical framework provides a mechanism from which I observed isomorphism between the maritime transportation system and other areas of science. This is critical, as it allowed me to focus and evaluate the relationships in existence between seaport components to uncover conflicts, weaknesses in processes, barriers, and to identify inadvertent contributors to unauthorized access.

According to Yin (2016) qualitative research is conducive for exploring social, institutional, cultural, and environmental conditions that influences perceptions, and actions of people. This study aimed to capture those experiences and perceptions from frontline security officials responsible for seaport security. Qualitative research samples (or instances) are chosen in a deliberate manner to yield both sufficient and relevant data specific to the topic under study (Yin, 2016). Qualitative studies seek to obtain maximum variations through broad ranges of information derived from samples with different viewpoints and perspectives on topics under study. The literature review (Chapter 2) indicates the existence of potential opposing viewpoint amongst line officers and management, regarding security threats and practices at seaports. Therefore, this study

included participant interviews with various levels of authority, ranks, and seniority, to facilitate the collection of potential opposing experiences and perspectives (Yin, 2016). According to Yin (2016) data collected as part of qualitative research is more vastly compiled from conversational interviews, as opposed to by use of classic instruments. My goal was to capture the objective (untainted) experiences and perspectives of security officials most knowledgeable of barriers and facilitators to security at U.S. seaports. An important component to the methodology is the development of a robust protocol; therefore, I examined the number of security incidents occurring at U.S. seaports between 2001 and 2019. My findings from that examination assisted in determining my line of inquiry for participant interviews.

The primary data collection method was participant interviews. Participants included U.S. seaport security professionals in current or former positions of subject matter authority. Participant selection criteria included a mandatory minimum combination of 2 years law enforcement and/or security experience in a maritime jurisdiction. First, using public information sources, I identified top ranked U.S. seaports by container volume, cross referenced them, and identified security professionals with current or former security (law enforcement) responsibilities within them. The target sample population included various levels of authorities amongst *Chiefs of Police*, *Security Directors*, *Facility Security Officers (FSOs)*, *first line officers* and other *homeland security professionals*. As a contingency plan, I used the social media platform, LinkedIn, to identify participants and to solicit participation. This study used nonprobability purposeful sampling to recruit experienced participants who could provide

a broad range of information and perspectives. Prior to conducting interviews, I obtained approval from Walden's University Institutional Review Board (IRB).

After obtaining IRB approval, using public sources, I identified and contacted participants from the sample population by email (or second email as needed). Participants received a consent form (see Appendix B) by email for their review; an email reply indicating their willingness to voluntarily participate in the interview was required. The informed consent form detailed the study's nature, and purpose, my contact information, potential risks to participants, and methods of confidentiality between the participants and the researcher. The privacy and confidentiality of participants was prioritized in this study. Therefore, no real names were used, and each participant was assigned an alphanumeric number to protect their privacy and for de-identification purposes. Participation in this study was voluntary, therefore, contributors were not required to participate, and each were consenting adults; no minors or members of vulnerable populations were included in this study.

This research applied the redundancy (saturation) principle in sample estimates for this study. Redundancy refers to qualitative data collection focused on maximizing information, whereas little or no new information is forthcoming (Patton, 2015; Yin, 2016). Yin (2016) stated that the purpose of data collection is to maximize information, therefore, the study concluded when no new information was provided by the participants.

Instrumentation

The qualitative interview protocol was produced by me and adhered to Walden's University interview guidelines. The qualitative interview questions (see Appendix A) were based on information obtained through literature sources and governmental archival records reviewed as part of this study. A series of structured but open-ended questions related to the central research questions were used to better understand security measures from the perspective of security officials. The interview questions were arranged in a semi-structured manner, and probes and follow-up questions were used to stimulate participant response, when elaboration to comments were necessary (Rubin & Rubin, 2012; Yin, 2016). Each interview lasted approximately 1 hour and 45 minutes, and written notes were taken throughout each session to assist in illuminating insight and summarizing the study's findings.

Potential issues that might arise when using interviews as a data collection method, included insufficient sampling of a population, sampling bias and errors due to convenience, and purposive sampling. Convenience sampling was deemed inappropriate for generalizing with any degree of certainty and therefore, not used as part of this research study (O'Sullivan et al., 2017; Yin, 2016). While it was important that the number of participants in this study reach a point of sufficiency, participants were not selected based on convenience. Lincoln and Guba (1985) asserted that in contrast to traditional sampling, redundancy is the primary criterion for purposive studies. Yin (2016) noted that a researcher may be able to estimate and state, ahead a likely range of sample for a study. Therefore, I estimated that a sample of 10 – 18 participant responses

may result in maximization of information, sufficient for answering the research questions.

Data Analysis Plan

The study's data analysis included a combination of open codes (level 1) and category codes (level 2), followed by an inquiry for emergent themes using computer assisted qualitative data analysis (Saldana, 2016). The study followed five qualitative analytical phases: they included compiling, disassembling, reassembling, interpreting, and concluding (Yin, 2016). The analysis plan was based on an immersion into each of the participant's responses (Rudestam & Newton, 2015). Informal analysis was performed during the initial collection to assist in assessing the adequacy of participant responses and overall data obtained. Notes and transcriptions from each interview were formally arranged and sorted (Yin, 2016). The compiled data was then disassembled and further arranged with level 1 codes being assigned. The data was then subjected to level 2 coding, then later followed by an inquiry for emergent themes using computer assisted qualitative data analysis software (Saldana, 2016). The data was then reanalyzed, interpreted, and used to create a summarized narrative of my findings, before drawing my conclusion (Yin, 2016).

I used NVivo, to assist in managing data and to support the prioritization and honoring of participant voices (Saldana, 2016). The use of NVivo, allowed me to transfer documents, and audio files from secondary analysis and information management. The pre-coded data from the interview transcriptions were uploaded into NVivo software and a systematic query was performed to assist in identifying emergent themes. The

combined analysis approach assisted in establishing and maintaining validity, rigor, trustworthiness, and dependability in my findings. My observations and interpretation were subjected to the scrutiny of expert review by assigned research committee members and external audit by knowledgeable consultants who has no relation to this study (Rudestam & Newton, 2015). To manage data, I stored interview data in a password protected external hard drive. As a contingency plan in case data is loss, I stored an additional copy of data in an encrypted format on a password protected USB Flash drive. Both devices were secured in a safe location and kept for at least five years as proposed by Walden University's Research Ethics guidelines.

Issues of Trustworthiness

The trustworthiness and validity of this study was prioritized throughout its components, including topic selection, literature review, approach, data collection, and is strictly maintained to its conclusion. This study's trustworthiness is based and reflected on four major components: credibility, transferability, dependability, and confirmability (Lincoln & Guba, 1985). I explicitly, and methodically convey the challenges in collecting data relevant to topic, and techniques that I used for overcoming them. Patton (2015) stated that reflexivity reminds the qualitative researcher be attentive, conscious of one's own perspectives, and to undertake in an ongoing examination of what is known and how it is known. Reflexivity necessitates in-depth introspection of individual thinking patterns and exploring our understanding interpretations (Patton, 2015). Reflexivity requires self-awareness and actively monitoring of the role and influence a researcher may on a study's outcomes (Ravitch & Carl, 2016). It necessitates and

assessment of a researcher's positionality and subjectivities as they relate to a research topic (Ravitch & Carl, 2016). Recruiting and selection of participants was fair and impartial; gender, race, age and/or nationality was not relevant factors or of interest to this study; therefore, participants were not asked to disclose such. To minimize the potential of overlooking risks, overestimating benefits, or assuming consent is informed and voluntary, I followed the advice and guidance of the Institutional Review Board (O'Sullivan et al., 2017). The trustworthiness of this study is central to its research design, methods, and findings; therefore, deliberate attention and strategic measures were taken for its assurance.

Credibility

Qualitative research produces highly creditable results when incorporated into a study's design (Rubin & Rubin, 2012; Shenton, 2004). This study disclosed its use of thick rich descriptions to report participant responses, implements the use of triangulation, and member checks. This study incorporates measure to acquire familiarity with the culture of each participant by consultation, a review of appropriate documents and through the researcher's own experiences (Shenton, 2004). I devoted substantial time, energy and focus on becoming oriented with the phenomenon under study. Through comprehensive academic research and practical experience, prolonged engagement is accomplished and contributes to the credibility of this study (Lincoln & Guba, 1985). Rubin and Rubin (2012) noted that credibility is strengthened in part when a researcher demonstrates that findings are based on information obtained from people knowledgeable about the study topic. A person's formal position is not always a good representation of

their knowledge of a research topic; therefore, I determined the sufficiency of each interviewee's experience based on the selection criteria. Rubin and Rubin (2012) also noted the importance of transparency, and its role in allowing a reader to see the processes used for data collection and analysis. This study was careful and intentional in instituting measures to encourage honesty. Participants were given the opportunity to refuse to participate in the study, as a mechanism for vetting and retaining willing samples (Shenton, 2004).

Transferability

Transferability references the ability of results to be applied to a wider population. The goal of qualitative research is to develop descriptive relevant statements that may be applicable or transferable to broader context while maintaining its original context-specific richness (Ravitch & Carl, 2016; Rubin & Rubin, 2012; Yin, 2016). The application of GST as the theoretical framework and the triangulated findings from collected data uncovered potential replicable findings that may be extrapolated to other areas of study. In conceptualizing seaports as both complex systems and subcomponents of a larger maritime system, the study's finding are comparable and potentially applicable to various other systems. As Shenton (2004) noted however, transferability inference should be made readers of the work. This study used sufficient thick description of the phenomenon under investigation to provide its readers proper understanding, thereby enabling them to make appropriate comparison (Lincoln & Guba, 1985; Shenton, 2004).

Dependability

Qualitative research is considered dependable when it is consistent and stable over time (Ravitch & Carl, 2016). Dependability is established through detailed reporting of the study's processes. This study outlined its processes for collecting, analyzing, and reporting its findings. The study's data collection and management techniques remained robust throughout a logical, and traceable process. The appropriateness of my chosen methods to answer the core constructs and concepts of the study supported the trustworthiness of this study (Ravitch & Carl, 2016).

Confirmability

Confirmability refers to the neutrality or the degree findings are consistent and repeatable (Connelly, 2016). Qualitative researchers acknowledge that the world is a subjective place; therefore, its goal is to ensure its findings can be confirmed (Ravitch & Carl, 2016). Confirmability aims to ensure a study's findings are the result of experiences and responses of participants and not characteristics and preferences of the researcher (Shenton, 2004). Therefore, confirmability was established in this study by maintaining a robust audit trail, in which the details of data collections, data analysis, and interpretation were clearly outlined. Throughout this research study, I maintained detailed records of documents, electronic recordings, observations, and process notes (Lincoln & Guba, 1985). Confirmability was supported using triangulation to address potential biases that are likely to subconsciously influence my beliefs, and directing underlying decision making, including the selection of methods. Lastly, confirmability was further established and maintained through reflexivity. I included reflexive analysis to supplement

interviews, observations, and analytical notes, as a technique for maintaining awareness of my own influence on the data.

Summary

This chapter presented the research design and rationale, methodology for the discovery and analysis of data. It discussed the collection and management of data, codification, method of analysis, and outlined ethical considerations. The rationale and methodology described in this chapter summarized the design and research steps used for data collection, organization, analysis, and protection. Through this qualitative study I investigated seaport security measures to understand why individuals continue to gain unauthorized access two seaports and cargo. In Chapter 4, I discuss the findings of the research, emergent themes, and the implications from the analysis.

Chapter 4: Results

Introduction

In chapter 4, I present the findings of my research. This qualitative study was focused on the effectiveness of seaport security measures in preventing unauthorized access, and countering transnational threats posed to maritime systems. Scholarly research into the phenomenon under study is limited, therefore, I sought to make an original contribution to knowledge by bridging the gap in literature. Through research of seaport security and data collection, I gained an understanding of the phenomenon under study, potential factors that inadvertently allow unauthorized access to restricted seaport facilities and containerized cargo. The study was guided by two central research questions:

Research Question 1: What are the meanings, structures, and essence of lived experience of seaport security officials, in terms of instituting security measures required by the Maritime Transportation Security Act of 2002?

Research Question 2: What do seaport security officials perceive as barriers and facilitators to implementing security practices at U.S. seaports?

Data was collected for this study through 10, Zoom audio interviews that were digitally recorded. The chapter includes a general description of participant demographics and includes articulation of the interview setting. The chapter includes a presentation of the data, data analysis, and highlights of observed patterns and themes amongst participant responses. The chapter concludes by outlining the study's findings in relation to my research questions.

Setting

The study population consisted of seaport security officials (SSOs) representing geographical areas from across the United States. Interviews were conducted on dates and times chosen by participants, which supported and promoted sharing of personal, and professional experiences, observations, and perceptions relevant to the study. Some of the challenges that I experienced during this study on seaport security were locating participants who were willing to speak openly about security practices (successes or failures) and balancing the use of probes to reveal information likely to be deemed as security sensitive, personally, or professionally embarrassing.

As I discussed in Chapter 2, a significant number of security breaches were reported to have occurred at U.S. seaports since the implementation of the MTSA. While specific facilities are not disclosed in this study, fear of criticism may have also deterred some security officials from participating in this study. Rubin and Rubin (2012) explained that a potential participant must trust that a researcher will not make public what could be embarrassing or harmful to an interviewee. Creswell and Poth (2018) explained that potential participants are often fearful that their issues may be exposed to people outside their communities. I addressed and mitigated these challenges through several actions. My background in law enforcement and seaport security helped to establish and maintain trust with potential and actual participants. I alleviated concerns about the intentions of this project and stimulated interest of potential participants, by providing a thorough description of the study and the research process during initial communication with participants. Lastly, by providing participants with official consent

forms, I validated the legitimacy of the study and encouraged participation. There was no indication that the study participants felt pressured, concerned, or other negative feelings during the collection phase.

Demographic

My target sample population involved SSOs representing geographic areas from each maritime border region of the United States, including northeast, southeast, southwest, and western borders. Participants were identified using open-source information (public records) and professional networks. I used Zoom audio to conduct the study because of the geospatial location of participants. A comprehensive description, including positions of the study's participants cannot be divulged because it may lead to their identification. The participants included senior SSOs, comprising local, state, and federal levels of government. I used pseudonyms to identify each participant listed in Table 1, based on the invitation dissemination order sequence; 10 of the 44 invited SSOs agreed to participate. For example, an invitation was sent first to SSO 1, who agreed to participate. SSO 2, and SSO 3, were invited, but did not participate. SSO 4 and SSO 5 were invited and did participate. SSO 6, SSO 7, and SSO 8 were invited, but did not participate; SSO 9 was invited and did participate. This continued until saturation was achieved. See *Table 1* (on the next page) for participant demographics.

Table 1

Participant Demographics

Participant	Gender	Length of Employment	U.S. Region	Representative Level
SSO 1	Male	33 Years	Southeast	Federal
SSO 4	Male	20 Years	Southeast	Local
SSO 5	Male	30 Years	Northeast	State
SSO 9	Male	20 Years	West	Local
SSO 13	Male	24 Years	Northeast	State
SSO 16	Male	27 Years	Southeast	Local
SSO 17	Male	29 Years	Southeast	Federal
SSO 37	Male	17 Years	West	Local
SSO 38	Male	38 Years	Southwest	Local
SSO 41	Male	20 Years	Southwest	Local

Data Collection

After receiving Walden University IRB approval (No. 12-07-20-0344611), I began participant recruitment by searching and identifying potential participants using open public sources, including seaport websites, maritime port directories and the professional network, LinkedIn. Qualitative data were collected from 10 participant interviews; and while this was slightly fewer than initial estimates, the sample size proved to be more than sufficient to achieve data saturation. Based on data acquired from the U.S. Department of Transportation (2020) my sample population represented 40% of the top 25 U.S. seaports responsible for 96% of all loaded TEUs. In addition, my study's sample population represented the collective experiences of officials working at facilities

that accounted for 47.7% of 55.5 million TEUs handled by the top 25 U.S. seaports in 2019. The sample population was therefore, more than adequate to contribute rich insight into the phenomenon under study.

Yin (2016) explained that saturation occurs when themes are repeated from participant's interviews. After completing 10 interviews, I observed redundancy in participant responses. I reached a point of data saturation when no new information was being generated. To recruit participants, I extended research invitations by email correspondence. I sent a total of 44 invitations to potential participants who possessed a job title with responsibilities for seaport security. Of the 44 invited recipients, 10 individuals (22.7%) responded as interested participants for the study.

Data collection was conducted over the course of 60 days, beginning in December 2020, and continued through February 2021, with weekly interviews being conducted with on average 1 - 2 consenting participants. The IRB authorized research collection method I used was audio recorded interviews; with reflective journaling being used as a bracketing strategy throughout the interview sessions. Before the start of each interview, I expressed appreciation for their participation and provided a brief overview of my study. The consent form was briefly discussed, and I reemphasized the right to withdraw from the study at any time without negative consequences. After obtaining assurance from each participant of their willingness to participate and their consent to be audio recorded, I initiated the interview, each of which lasted approximately 90 minutes. Interview questions were open ended and designed to invoke replies, while allowing for use of probes to solicit expanded information specific to the research design and focus of the

study. I used Zoom as the primary recording device and a Sony PX Series Digital Voice Recorder as a secondary (backup) device. Zoom allowed me to schedule meeting times, control access to each interview and allowed me to record my conversations with participants. Zoom also provided participants the ability to call in using a telephone or computer. During each interview, I made handwritten notes of significant and most notable responses from each participant. The participants were informed that the interviews would be confidential and, to ensure confidentiality, their names were replaced with alphanumeric characters in all transcription documents and within the findings of this study. There was no variation in data collection from what was presented in chapter 3.

Data Analysis

After completing the participant interviews, I transcribed the recordings using both manual methods and Otter.ai transcription software. I employed a careful and intense analysis strategy involving reading and re-reading the transcripts and listening to the interview recordings, to gain understanding of participant feedback relevant to their experiences and perceptions and to ensure attentiveness to prevailing themes. I then initiated member checking by sending a copy of the individual participant transcript to their preferred email for review. The interview transcriptions were redacted of participant names and supplemented with alphanumeric characters randomly assigned to each participant. Once transcription accuracy was determined, I compiled the data (audio and notes) together identified only by the assigned alphanumeric characters. I then disassembled the data, reading each transcript and applying open-coding (level 1)

methods to assist in developing initial codes from the written text with specific focus on relating data amongst each participant.

I emersed myself in the data collected from each transcription and audio recording and created additional handwritten notes of significant or repetitive words or phrases used by participants. I then reassembled the data using substantive themes that were created based on the combinations of disassembled items that I coded. This second application of coding allowed me to better understand how the data from each participant related to broader conceptual issues expressed by all participants. I further analyzed the data, using the most frequently found themes amongst participants responses, that enabled me to better conceptualize and contextualize commonalities. I then reanalyzed and interpreted the reassembled data, obtaining a more holistic understanding of the shared participant experiences.

Although initial conclusions could be drawn from this iterative analysis, I followed up by recompiling the coded data and further analyzing them using NVivo software. I selected this software to assist in managing the large amounts of data, support primary analysis, assist in characterizing themes and revealing patterns that emerged from the collective responses to the interview questions. Using the software, I was able to visualize frequently used words, phrases, and concepts to identify and extract the most common themes and explore their associated meanings. Through this in-depth evaluation of the themes collected from participant responses to the semistructured interview questions, I was able to uncover common patterns and expand the themes more broadly, contributing to a more refined understanding of seaport culture, facilitators, barriers, and

challenges to maritime security. This study was based on qualitative research and presents the collected data using direct quotes from participants to support the identified and observed themes. Quotes are recognized as the primary way to bring participants' voices into written reports (Ravitch & Mittenfelner, 2016; Yin, 2016). This study incorporated use of direct quotes to provide rich descriptions when discussing this complex phenomenon; this was to ensure readers are provided clear and insightful descriptions of participants' actual experiences and perceptions (Creswell & Poth, 2018).

Yin (2016) explained that all qualitative studies contain information about the actions and voices of individual participants. This study conveys the perceptions, beliefs, and observed behaviors of seaport security officials. Therefore, it was important and necessary to accurately portray the real-world events and participant perspectives about the phenomenon under study. The organization of the study's findings are presented in a cross-case presentation manner, in which interspersing quotes from participants were intended to use their voices to draw attention to the specific interview topics (Yin, 2016; Creswell & Poth, 2018).

There were four themes identified: (a) social systems (b) threat perception, (c) regulatory scope, and (d) barriers and facilitators. Social systems reference complex arrangements and interactions between separate but coalescing elements, including their individual beliefs and perceptions in relations to the whole. Threat perceptions are defined as the conscious and unconscious assessment of impending harm or disruption. Regulatory scope references the specific application, range, and authorities of a law.

Barriers are conceptualized as inhibitors to progress and facilitators are conceptualized as enablers of progressive actions. There were no discrepant cases.

Evidence of Trustworthiness

The trustworthiness and validity of this study was prioritized throughout each of its components, including topic selection, literature review, approach, data collection, and was strictly maintained to its conclusion. This study's trustworthiness is established on four major components: credibility, transferability, dependability, and confirmability. I communicated the challenges encountered in collecting data and outlined the techniques that I use to overcoming them. I utilized reflexivity to ensure attentiveness to personal biases and to undertake in an ongoing examination of what is known and how it is known (Patton, 2015). Reflexivity necessitates in-depth introspection of individual thinking patterns and exploring our understanding interpretations (Patton, 2015). Recruiting and selection of participants was fair and impartial; gender, race, age and/or nationality were not relevant factors or of interest to this study. To minimize the potential of overlooking risks, overestimating benefits, or assuming consent is informed and voluntary, I consulted and adhered to the guidance of Walden University's Institutional Review Board.

Credibility

Qualitative research produces highly creditable results when incorporated into a study's design (Rubin & Rubin, 2012; Shenton, 2004). I employed the use of thick rich descriptions to report participant responses and the findings of my study. Comprehensive academic research practical experience, and prolonged engagement with the data contributed to a more holistic understanding and credibility of this study (Lincoln &

Guba, 1985). The participant's time in employment ranged between 17-38 years. Rubin and Rubin (2012) noted that credibility is strengthened in part when a researcher demonstrates that findings are based on information obtained from people knowledgeable about the study topic. I was intentional in instilling confidence in the study and in encouraging honesty and transparency. Participants were given the opportunity to refuse to participate in the study, as a mechanism for retaining only willing participants (Shenton, 2004).

Transferability

Transferability references the ability of results to be applied to a wider population. The goal of qualitative research is to develop descriptive relevant statements that may be applicable or transferable to broader context while maintaining its original context-specific richness (Ravitch & Carl, 2016; Rubin & Rubin, 2012; Yin, 2016). This study used sufficient thick description of the phenomenon under investigation to provide readers proper understanding, thereby enabling them to make appropriate comparison (Lincoln & Guba, 1985; Shenton, 2004).

Dependability

Qualitative research is considered dependable when it is consistent and stable over time (Ravitch & Carl, 2016). Dependability was established through detailed reporting of the study's processes. I thoroughly explained the processes for collecting, analyzing, and reporting the study's findings. The study's data collection and management techniques remained robust throughout a logical, and traceable process.

Confirmability

Confirmability refers to the neutrality or the degree findings are consistent and repeatable (Connelly, 2016). Qualitative research acknowledges that the world is a subjective place; therefore, its goal is to ensure its findings can be confirmed (Ravitch & Carl, 2016). Confirmability aims to ensure a study's findings are the result of experiences and responses of participants and not characteristics and preferences of the researcher (Shenton, 2004). Therefore, confirmability was established in this study by maintaining a robust audit trail, in which the details of data collections, data analysis, and interpretation are preserved. Throughout this research study, I maintained detailed records of documents, electronic recordings, observations, and process notes (Lincoln & Guba, 1985).

Results

During interpretation, the four dominant concepts emerged from the participant responses and aided in delineating recurring themes: (a) social systems (b) threat perception, (c) regulatory scope, (d) barriers and facilitators. My analysis found seaport security officials to be highly motivated, passionate, and expressive in their commitments to the success of global commerce and U.S. seaports. Each participant communicated a desire to provide high level security services to their respective seaport and perceived their work as a critical element of homeland security service to their communities and the nation. The participant's backgrounds were extraordinary, including some who have military, intelligence and counter-terrorism work experience obtained globally. An average of 26 years of service (experience) exists amongst the 10 participants. Participant

responses included rich, in-depth descriptions of observations and their perceptions of risk and threats posed to U.S. seaports. Participants were forthcoming in sharing their experiences in relation to challenges associated with integrating security practices into organizations with logistical and operational missions and priorities.

Research Question 1

The meanings, structures, and essence conveyed by participants encompassed their personal observations, encounters, and assessments, all of which contributed to responses that provided a more holistic understanding of their perceptions and formulated opinions. RQ1 focused on the meanings, structures, and essence of lived experience of seaport security officials, in terms of instituting security measures required by the MTSA. To explore and answer this question, the semi-structured interview questions were designed to explore internal cultural phenomena, to elicit natural responses in which participants expound on their individual realities derived from personal experiences. A series of associated probes also focused on threat perceptions of security officials including the smuggling of illicit items through seaports. Lastly, probes were used to explore the perceptions of information sharing amongst local, state, and federal officials since the implementation of MTSA.

Theme 1: Social Systems

The overarching research question investigated the meanings of lived experiences of SSOs who are responsible for implementation of security measures mandated by MTSA. These officials lived experiences are unique because they occur in the context of a securitized maritime work environment positioned within national ports of entry, where

their security obligations consume significant time and personal resources. Understanding the experiences of SSOs as a process of understanding the phenomenon under study was consistent with the framework inclusive of concepts of self, relationships, and observations of institutional climate (Ravitch & Mittenfelner, 2016).

Participants were asked to describe the security culture of their seaports, and its impact on how they exercise security measures. Participants were also asked to describe the internal relationships between SSOs and port management in relation to the balancing of security and operational priorities, and to describe their perception of threats to U.S. seaports. Participant data suggested that the lived experiences of SSOs includes a shared interest in cargo security and facilitation. Six participants (SSO 1, SSO 4, SSO 5, SSO 17, SSO 38 and SSO 41) described cultures of collaboration and collective security consciousness. For example, SSO 5 described his facility's security cultures as robust, and credits its success in achieving security objectives, to the support of managerial leadership who have direct access to the State's Governor's Office. He also attributed success to a highly trained nationally accredited police force and engaged contract security services. SSO 4 described his facility's security culture favorably, explaining that the complexities of balancing security practices with enterprise priorities is challenging. He stated:

> I would say security is embraced. You know, especially with the port director, he's got two job functions. One, he runs an enterprise, so he's got to carefully weigh security with not disrupting the flow of commerce. So, he has to tread that

> very, very lightly. But here culture is very good when it comes to security. We work hand in hand with our civilian security partners.

SSO 17, described his seaport as having a culture that reflects strong partnerships and collaboration with port authority police, and operations. He stated:

> I hate to keep patting ourselves on the back, but, you know, we've kind of become a model port partnership across the board, up to the point where it has recognition all the way up to our headquarters. People from our top are reaching down, you know, asking how are you doing, what you're doing, and what's the best way to go about doing that.

While participants shared similar beliefs that their facilities do a "good job" in maintaining secure facilities, four participants (SSO 9, SSO 13, SSO 16 & SSO 37) diverged by explaining their perception of security as being a tolerant measure that is strictly compliance focused. SSO 16 explained that security staff are constantly pressured not to hold up cargo operations and are regularly asked to accommodate customers and clients. SSO 15 explained, "we are business driven, so much that we are very business conscious, and it's harder on security forces to accommodate sometimes."

Another participant (SSO 9) described a culture that strictly compliance focused and void of motivation or desire to engaged in proactive security operations. SSO 9 described the security culture and his relationship with the operational workforce as good; however, he elaborated by explaining, "as far as facility security goes, I do believe the terminals are not motivated to do a lot more than is required by the Coast Guard."

SSO 9 and SSO 13 both explained that while their port facilities effectively prioritize security, they have witnessed port officials whose actions demonstrate that they simply want to satisfy basic USCG requirements. SSO 13 explained, “they are not interested in doing real security.” Participants explained that security practices at seaports are viewed as too costly and adversely impactful to business. For example, SSO 37 said, “they are only focused on their bottom line, and most cargo operations and financial services personnel negatively view security as a threat to their budgets.” SSO 37 further described seaports as organizations that “embraces security only to the extent that it benefits them financially. They are looking at the bottom line, and almost everyone looks at security as a hit to that bottom line; we are not revenue generating.”

SSO 37 further elaborated by explaining that the security profession as a whole is not view favorably and described the differences in hiring practices and pay disparities with other professions. He explained:

> The problem I think, in corporate America and in governmental systems is we do not trust the professionalism of our security professionals. In the medical profession, you are going to get your checkups. You hire people who are experienced, have education in doing what they do, and you trust their advice, and you support them. You may not want to pay the money to have, you know, whatever surgery it is, in order to keep you going, but you pay it because you want to have that quality of life or improve your quality of life.

After exploring the social system interactions between SSOs and operations personnel at U.S. seaports, I developed a better understanding of the SSO lived

experiences. I then turned my focus to the motivations and perceptions of threats as perceived by SSOs.

Theme 2: Threat Perceptions

One of the core responsibilities of seaport security personnel is to screen people, vehicles, and cargo. The main objective of this practice is to prevent the introduction of dangerous devices and substances that are potentially concealed and smuggled, from gaining access into a seaport facility or onto a vessel. All participants demonstrated strong familiarity, and an in-depth comprehension of the sophisticated techniques used by transnational criminal organizations in smuggling illicit items through the maritime system. Security officials assess the illicit activities of TCOs as a tangible variable of risk. Bullock et al. (2016) posited that, "the uncertainty component of risk, contained within the probability of disastrous event occurrences place is the greatest burden on those who are treating a full portfolio of risks that must be compared in relation to each other" (p. 510). The risk perception of SSOs was based on perceived vulnerabilities and potential consequence of exploitation for transnational illicit smuggling.

Seven participants (SSO 5, SSO 9, SSO 13, SSO 16, SSO 17, SSO 37 and SSO 41) described their perceptions and experiences with smuggling and the perceived implications to seaport security. For example, SSO 17 explained that while his observations of large-scale drug trafficking originating from high-risk countries have typically targeted European seaports, he explained that eventually, those same drugs and methods are used in the return of illicit drugs back to the United States. SSO 17 further explained that:

> Drug organizations can get more money for the narcotics in Europe, they can get it for twice the price tag of what they can get in the U.S., but, as always, those narcotics going to Europe are eventually going to find its way back to the US., because not all narcotics are coming across the southern border; you're still going to have that come back through the seaport in some way shape or form.

Participants explained that both foreign and domestic intelligence suggests that terrorist organizations have shifted to the drug trade to support their operations. Seven participants (SSO 5, SSO 9, SSO 13, SSO 16, SSO 17, SSO 37 and SSO 41) perceived the potential manipulation (conversion) of common smuggling methods used by drug trafficking organizations, to exploit and conceal a weapon of mass destruction as the greatest threat to seaports.

When asked to describe perceived risk associated with drug smuggling at seaports, SSO 5 explained that federal agencies (CBP and USCG) do a great job overall, but they are "terribly understaffed," and over the past five years, most newly hired CBP officers have been sent to the southern border versus seaports. Participants (e.g., SSO 5, SSO 9, SSO 13, SSO 16, SSO 17, SSO 37, SSO 38 and SSO 41) explained that the plausibility of drug trafficking methods and routes being exploited poses a major risk to seaports. For example, SSO 5 even cautioned that foreign governments, intelligence agencies, and terrorist organizations, "know how to get a nuke into the country."

SSO 5 provided a plausible strategy that may be used by a terrorist group seeking to exploit smuggling methods and routes. SSO 5 explained:

> When China and Russia, tried to or did steal technology from the U.S. military they used to always go after, this was long time back in the 50s and 60s, they'd go after the whole kit and caboodle. What they smartly began to do is take one bolt, one spring, one gasket at a time, then put it together later. I'm afraid they have the same mentality with a nuclear weapon.

This data suggests the perceived potential for transnational criminal organizations to gradually smuggle items through legitimate transportation systems is a major concern of some SSOs. This response also highlights the enormous challenges confronting SSOs in detecting illicit items from amongst legitimate goods. When asked what he perceived as the greatest threat posed to a U.S. seaport, SSO 9 explained:

> If you can move drugs and people, which we know they do on the west coast here in pangas and yachts and sailboats from Mexico; the government's getting better at detecting them; there's more radar stations, but if you can bring that, you could, you know, in a worst-case scenario, you could bring an explosive device or a nuke in to.

Data collected from other participants suggested agreement that legitimate cargo operations may be exploited to import a dangerous device, or to launder money associated with criminal and terrorist activities. For example, SSO 13 stated:

> The other thing that's not really addressed is what's going out. You know, if drugs are coming in, there's probably money going out. And matter of fact, we know there's money going out. Certainly, some ports, more than others. We know there's weapons going out as well.

When asked to describe risk associated with drug smuggling as seaports, SSO 16 suggested that no difference exists between drug smuggling and weapons smuggling. He explained:

> Smuggling routes have been around for hundreds of years and they've smuggled everything from donkeys to gold, to cocaine to weapons. I think, though, that part of it is knowing that the commodity could change. It’s not like I am not worried about drugs, I mean, I spent most of my career doing drug interdiction, but I think just whatever method you're using, if you're successful bringing drugs in, just change the commodity and that's what scares me the most about the drug smuggling piece.

When asked to describe risk associated with drug smuggling as seaports, SSO 37 described an incident in which weapons were smuggle on board a ship:

> In the 1980s, in Seattle, there was a parasitic element that had been welded to the side of a ship in Seattle, the welding was done offshore someplace else. But long and short of it was there was a very large cache of firearms that had been put into a fairly hydrodynamic shape and well into the hull. It was making its way eventually over to the Middle East. So, firearms are being smuggled from Far East, to the Middle East, the long way. That particular ship was eventually destined to go through the canal and get over into the Mediterranean. So you know, it's not unusual.

SSO 16 further elaborated by outlining a plausible strategy likely to be used by a group seeking to exploit smuggling methods and routes. He explained:

> From a practical standpoint, knowing that they're successful, moving narcotic products, and they could supplant that with anything else and get through, you know, they're honing their craft with drugs if you will, but they could put, and same with migrant smuggling, same thing. You could be putting, you know, 100 migrants through, and you're getting through every time, and then all of a sudden, four special interest aliens come over.

SSO 37 explained that he was not worried about a nuclear device being smuggled into a U.S. seaport, but expressed concern about organized crime, transnational threats, and radiological devices being used against a seaport. SSO 37 stated:

> I am concerned about what I would call normal, everyday crime. I'm concerned about organized crime, both by you know, gang type or organized gang, you know, mafia type things. And I'm also concerned about international crime, that's very well organized; that I'm concerned about. I am concerned about dirty bombs, or radiological dispersal devices, and biological and I am very concerned again about the normal everyday day to day crime of smuggling, because that's what nickels and dimes us to death.

All participants acknowledged and agreed that seaports may be exploited by terrorist organizations engaged in drug trafficking. While all participants agreed that smuggling is a major threat, three participants (SSO 4, SSO 13, and SSO 41) believe that cybersecurity threats pose the most immediate threat to a U.S. seaport. These participants suggested that U.S. seaport cargo manifests may be manipulated to facilitate illicit

shipments or technological systems may be compromised to facilitate an unintended closure.

While conducting the participant interviews, it became immediately evident that while all SSOs remained conscientious of the need to balance their duties with the facilitation of cargo, their coalescing responsibility to protect life and property seemed to create an occupational identity dilemma. SSOs seemed to genuinely value their relationships with port partners responsible for logistical operations; however, their responses seemed to express at least some frustration with what they perceived as complacency or dismissiveness of potential threats by port officials. After exploring SSO threat perceptions, I developed a more holistic understanding of SSO meanings, structures, and essence of lived experiences. I then turned my focus to the strengths and weakness of the MTSA, as perceived by SSOs.

Research Question 2

RQ 2 focused on the perceived barriers and facilitators of security practices at U.S. seaports. To explore and answer this question, participants were asked a series of questions to explore the perceived capabilities of security officials to institute mandates under the MTSA, and to describe their overall effectiveness in preventing unauthorized access to restricted facilities and containerized cargo. This series of questions also provided access to a more refined understanding of potential barriers and facilitators to security at U.S. seaports.

Theme 3: Regulatory Scope

All ten participants agreed that the MTSA has significantly strengthen the security of U.S. seaports, however, each participant noted some weaknesses within the Act that warrants immediate attention of policymakers. For example, SSO 13 stated:

> I think the system made huge strides after the implementation of MTSA and its pretty effective. I think there's issue still with TWIC readers. We, in fact have had issues with people using other people's work cards, or even a couple of guys trying to use, like paper versions.

When asked if the implementation of MTSA has made U.S. seaports more secure against unauthorized access, SSO 37 replied:

> No, I will tell you right now, I tell everybody the same thing; number one, I hate the TWIC program. I think it's a completely worthless waste of time and money. Number two, MTSA as a whole is security theater. It's a lot of legislation, written ultimately by lawyers, even though I had a lot of input to it, by the time the lawyers and legislators got ahold of it, it does nothing, or very, very little. It allows us to apply for grants. And I am tired of the grants, getting, you know, toys for boys, for who spent millions of dollars on buying things that never get used and just go away.

SSO 16, SSO 37 and SSO 38, explained that several weaknesses exist within the MTSA and TWIC program. One of the perceived problems with the law, is a lack of a comprehensive background checks associated with the TWIC program. SSO 37 and SSO 38 explained that TWIC does very little to enhance security measures at U.S. seaports

because backgrounds standards are inadequate to uncover and eliminate high risk applicants. For example, SSO 37 stated:

> Anybody can get a TWIC card. So, all of our 9/11 hijackers would have qualified for a TWIC card, even today, all right. They had no background, they have never gotten themselves into trouble, nothing is going to stick out on the radar and say, hey, will you take a look at this guy or this gal. I can live in the middle of Nevada and get a TWIC card. So, there is no correlation between having the credential and actually having access.

SSO 38 said, “unless an individual is on a terrorist list, they are going to get a TWIC.” SSO 38 further described an incident that occurred at his seaport facility in which an individual was arrested and convicted for stealing military equipment but was later issued a TWIC. This suggestion indicates the belief that possession of a valid TWIC, does not negate a potential insider threat to a U.S. seaport.

SSO 38 explained that the subjective nature of facility security plans and the absence of counter smuggling authority and capabilities restricts the ability of local security officials to prevent unauthorized access of people or illicit (dangerous) items. He explained:

> MTSA does nothing to address a narcotic or other illicit material threat. It's meant it's poised squarely at fences, gates, TWIC cards. I mean, when you look at all the stuff in there, and none of its prescriptive, for example, you know, you're just maintaining a secure perimeter. Well, what's a secure perimeter? define it? Well, it's whatever. It's whatever you put into your facility security plan.

SSO 16 and SSO 37 explained that some incidents in which individuals gained unauthorized access to the port were associated with long haul truckers, particularly in the summertime, “when children are out of school or their spouse, boyfriend, or girlfriend” were concealed inside the sleeper cab of a truck.

SSO 13 expressed concern that access control measures are tied to databases that can be manipulated by insider threats that allow access by unauthorized individuals. SSO 13 described one observation he made while working in a seaport outside of the United States, but warned the same may occur at U.S. seaports:

> A lot of it was access to databases, including the terminal operating system or cargo management system where all the important information about cargo was kept. They could even manipulate it to move the cargo around the terminal to areas. I had cases where they move the containers to areas where the camera coverage was poor so that they could access it, or where they got access to seal numbers on the computer system, so they could get the duplicates set up; there's tons of stuff going on.

SSO 37 explained that large volumes of trucks entering seaports daily, has led many ports to transition to automation. The participant explained that the access control process requires a presentation of a valid TWIC but explained that the truck cabs are not being inspected for other occupants. This participant further explained that even prior to the recent changes in processes associated with coronavirus disease (COVID-19), concerns of security screeners related to contagions from needles or dangerous objects, caused many to avoid detailed screening of truck cabs. SSO 37 explained by stating:

> I don't know anybody that's going to be asking to really do anything to get to the back part of a tractor trailer and the sleepers to see what's going on. And the probability of coming across something that is really going to be a major security risk factor versus the factor of being sued by your security guard that's injured, it's not worth it. So, to be honest, putting stuff out there, just the way I see it.

When asked to describe risk associated with drug smuggling as seaports, SSO 41 said the MTSA was effective in countering drug traffickers. SSO 41 explained his reasoning:

> I will say that MTSA helps that and I will give you an example of that. The drugs that we see here, wash up outside of the port, they don't come through the port. The reason is, because our screenings are so high with the interaction that we do with Customs, that, you know, the traffickers won't bring it to the port, they'll drop it outside the port, and somebody else will pick it up, if you understand what I'm saying. I attributed that to strong screening and customs interaction here at MTSA facilities.

Five participants (SSO 4, SSO 13, SSO 16, SSO 37 and SSO 38) noted that while access control measures are more robust, several reoccurring incidents involving undeclared passengers in trucks and porous perimeters undermines efforts to prevent unauthorized access to restricted facilities. "We still have our breaches, you know, its people walking in the wrong way where there is no security guard and he missed it. One guy actually jumped a barbed wire fence. I couldn't believe he actually did it" (SSO 4).

After exploring SSO perceptions of the MTSA, I developed a better understanding of the perceived strengths and weaknesses of seaport security regulation. I then turned my focus to the perceived barriers and facilitators of security, as perceived by SSOs.

Theme 4: Barriers and Facilitators

Participants were asked about relationships, resources and types of support received in keeping their facilities secure against unauthorized access, and to explain what they perceived as barriers and facilitators of security. Participant responses were concentrated around five main issues: (1) leadership engagement, (2) MTSA limitations, (3) information sharing, (4) civil penalties and (5) federal funding.

Leadership

Two participants (SSO 5 and SSO 13) emphasized the importance of the USCG and senior management as major facilitators in maintaining a culture of security within the ports.

SSO 5 described the role of the USCG, he explained:

> They take it extremely seriously. They do a great job, you know; the Coast Guard, they get a lot of things dropped in their lap, when things happen, you know, after 9/11, they got a lot of things placed on their table, including antiterrorism…The leadership of those ladies and gentlemen has been fantastic. So, they are the ones that set the initial posture.

SSO 13 explained the security must be prioritized amongst port management to be effective. SSO 13 elaborated by saying:

> Nothing will happen if the top folks don't buy into it. And the way they buy into it is by getting exposed to it, and the way to get exposed to it is by having security be something that's placed in front of them. So, the biggest thing is that is I guess, characterized as a seat at the table with the senior management.

SSO 5 suggested that the leadership and oversight of USCG contributes to accountability at the highest levels of port management. SSO 5 also emphasized the importance of "buy in" and support from executive management as being essential to the effectiveness of seaport security practices.

SSO 5, SSO 37, SSO 9 and SSO 16 also remarked that being vested with authorization to hire, contract, train, and develop collaborative partnerships between security and law enforcement personnel helps to creating a strong security culture.

MTSA limitations

All participants agreed that the MTSA does not adequately address and does not institutes sufficient measures to provide security officials the means to counter complex smuggling methods or defend against cyber threats potentially associated with or orchestrated by criminal or terrorist organizations. This is perceived as a barrier by some participants. For example, SSO 13 described the MTSA as follows:

> So, its focused-on terrorism and less focused on cargo and supply chain security, so less effective when you're talking about issues like trafficking and smuggling, more effective when you're talking about trying to stop attacks against ships and ports. So, the way I always describe it, is the MTSA is focused on ports and ships

as targets, but not as conduits of illicit activity, so, it has been very, very effective. But it's also, you know, limited in its scope.

SSO 16 identified language barriers between drivers and security personnel have often been factors associated with attempted access of undeclared passengers or weapons into the restricted port facilities.

Sharing

Six participants' (SSO 5, SSO 13, SSO 16, SSO 17, SSO 37, and SSO 41) responses were consistent with findings uncovered as part of this study's literature review, where indication of frustration exist because of a lack of access to adequate intelligence information for port directors. All participants noted that a lack of access to basic intelligence information hinders, depletes, or detracts from full capacity of port authority officials, police, and other security officials to conceptualize real threats to maritime. This concern is perceived by all (ten) SSOs as counterproductive to the objective of maritime domain awareness and was identified as a major barrier to seaport security.

Each participant noted the negative impact of poor information sharing as being a barrier to building trust. SSO 1 cautioned that building trust is a timely process that is complicated when agencies are territorial and do not share information. SSO 1 explained: "I'd say that probably the biggest barrier, both locally, statewide and nationally, is getting and continuing to foster relationships and that integration amongst the various groups."

The MTSA briefly addressed prevailing threats to seaports and emphasized the need for improvements in information sharing. "Criminal organizations are exploiting

weak security at ports to commit a wide range of cargo crimes. Intelligence and information sharing among law enforcement agencies needs to be improved and coordinated at many ports" (Maritime Transportation Security Act, 2002, sec. 101).

SSO 41 has observed improvements in information sharing; however, he said more improvements are needed from federal agencies to local and state agencies.

> Information sharing from the federal level to the state and local level, tends to be a large drop off; it has gotten better, especially in cybersecurity, but it could use a much stronger improvement. There is that disconnect between federal and state level with information sharing.

While all (ten) SSOs acknowledged and commended significant progress in strengthening of informal communication between local, state, and federal agencies since September 11, 2001, one dominant recuring theme is that sharing barriers, associated with unclassified information, and the need to broaden access to security clearances remains. SSO 5 emphasized that port directors should not be limited to a reliance on news media outlets to know what threats are posed to the United States. SSO 5 perceives the lack of secret clearances to port directors as, "a real failing of the federal government in taking security serious; how can you set up security landside, or waterside, to meet the threat, when you don't even know what the threat is."

This perspective, however, was not fully shared by all participants. Four SSOs (SSO 1, SSO 5, SSO 16, and SSO 17) perceived intelligence sharing as being significantly improved. However, good communication appears to be perceived and measured laterally amongst federal and state agencies only, and not factored with

inclusion of port authority officials and police agencies responsible for port security. SSO 1 acknowledged the existence of some concern regarding the legality of information sharing outside of federal jurisdictions, despite noting the need to maintain relationships of shared trust with local and state partners. SSO 17 explained that sharing information horizontally and vertically is imperative to countering criminal or terrorist exploitation of seaports. SSO 17 highlighted the effectiveness of local, state, and federal joint taskforces as a significant facilitator of information sharing and broader seaport security.

SSO 4 identified good communication with "port partners" as a significant facilitator of security, specifically crediting the DHS *See Something, Say Something* program as highly effective in facilitating the reporting of suspicious activity at the seaport.

USCG Penalties

Four participants (SSO 9, SSO 37, SSO 38, and SSO 41) perceived U.S. Coast Guard civil penalties as a barrier to security. SSO 37 explained:

> When some knucklehead hops a fence someplace and you call it into Coast Guard, depending on the Petty Officer responding they show up and they check it out. Some will write you a notice of violation; you're in violation for allowing someone to circumvent your security. Well, the reason we caught them is because we were paying attention and the person trespassed, they had to climb over a barbed wire fence or whatever the barriers are, circumvent those security measures. Why are you punishing me?

SSO 41 agreed and explained what he perceives as unfair civil action against seaports, and how it creates a barrier of trust that results in some officials refusing to report security breaches when they occur.

> You know if we report a violation to the NRC and then the NRC or the TSA or Coast Guard dubs us at fault, well it's an automatic fine. So, it stops ports from wanting to tell that they've had a violation, that violation could be a violation of information; let's say it happened at another port, it may be information that I need, well I'm not going to get that information because they don't want to tell on themselves and risk a fine.

Port Security Grant

Eight participants (SSO 4, SSO 5, SSO 9, SSO 13, SSO 16, SSO 37, SSO 38, and SSO 41) identified the Port Security Grant (PSG) as being a major facilitator of seaport security. “We are very fortunate down here to get funding through the port security grant. Without access to those funds, we would be very well under secured, that has been a huge benefit to us.”

SSO 5 agreed, and explained, “the federal ports security grant program is vital to my port and all ports in the United States in order to provide funding for certain projects.”

When discussing resources needed to strengthen seaport security, SSO 4 said, “there are a lot of gaps, a lot of gaps. I would like to see more federal funding for ports, even though we do get grants. I just don’t think it's enough.”

While all (ten) participants expressed enthusiasm and optimism about the current state and future state of seaport security, they conveyed four main issues relevant to the research questions: (a) 80% of participants relayed that security priorities are ambiguous and often secondary to cargo facilitation priorities; (b) 100% of all participants perceived the threat landscape of seaports as being multifaceted and in a constant state of change driven by the illicit activities of transnational criminal organizations; (c) 70% of participants perceived that the MTSA was too narrow in scope, and not adequate to posture seaports to counter exploitation; and (d) 80% of participants perceived the lack of intelligence sharing as a barrier, and multilateral communication and collaboration as a major facilitator to seaport security.

This was an exploratory study composed of a nonprobable, purposeful sample population. The main intent of the study was to explore and understand the experiences and perceptions of seaport security officials. Rival thinking was applied throughout the study process and involved a deliberate continuing application of skepticism to the data and my assumptions. There were no discrepant cases.

Summary

This chapter contained the results of the analysis, connected the analysis back to the research questions, and demonstrated the consistency of the thematic analysis with the qualitative case study methodology. I interviewed 10 participants for this qualitative study, using a self-developed interview guide designed to explore and understand SSOs perspectives of security measures. The results of this study were divided by two research questions and generated four major themes. In the first research question I explored the

meanings, structures and lived experiences of security officials by exploring their perceptions of seaport cultures. Participants expressed enthusiasm, support, and a balanced understanding of the function and importance of both seaport security and logistical operations. However, some officials perceived security measures to be a secondary priority to port logistical operations.

The lived experiences of SSOs encompasses dynamic cultures driven by customer demand. While collaboration was identified as a critical element to accomplishing security objectives, some SSOs described a lack of prioritization of security, lack of awareness and understanding of transnational threats as being major risk factors to the security culture. The internal culture relies on partnerships of collective vision for both logistics and security; however, a lack of intelligence sharing was found to restrict development of a shared vision and understanding of transnational threats.

Within the second research question I explored the perceived effectiveness of the MTSA, barriers and facilitators of security measures at seaports. Some participants perceived the limitation of authorities granted to owner operators as a barrier. These participants believe that the MTSA should be amended to expand the authorities of port security directors to empower them to legally, under CFR authority, to act against violators of their FSPs. Additionally, the current level of funding under the Port Security Grant (PSG) program ($100 million) is perceived as insufficient, and the overall award process is viewed as disproportionate, unfavorably to smaller (Tier II, III & IV) seaports.

Lastly, according to interviewed security officials, current security measures at U.S. seaports are inadequate to prevent or deter activities of transnational criminal

organizations, including those converged with or facilitated by terrorist groups. By exploring the recurring themes, I concluded that seaport security measures have enhanced seaport security from the pre 9/11 era, however, these measures are inadequate to eliminate security risks. Maritime security measures must evolve to focus not only on U.S. seaports as targets, but must focus more on supply chain security, and threats of exploitation by TCOs. In the next chapter the results are discussed in relation to the literature and its implications for improving security at U.S. seaports.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

The purpose of this qualitative case study was to explore the experiences and perceptions of SSOs, to understand what factors impact security measures, and inadvertently allows unauthorized access at U.S. seaports. The sophisticated networks of transnational criminal organizations and their demonstrated ability to smuggle illicit items creates new challenges to U.S. seaports. Maritime drug smuggling divulges transportation pathways and methods that may be used by extremists to exploit a U.S. seaport to introduce a dangerous device or substance into the country.

This study included the collection of data through participant interviews with individuals who are responsible for preventing unauthorized access of people and illicit items. I used an exploratory case study design to focus on the meanings and lived experiences of security officials to better understand existing maritime security measures and to identify barriers and facilitators of security. The interview questions provided detailed insight into the perceptions, observations, and experiences of security officials. I used a self-developed interview guide to obtained qualitative data through in-depth, semistructured individual interviews.

The results of the data from 10 SSOs supported previous research (Eski, 2016; Eski, 2019; Fritteli, 2005; Sergi, 2020; Zaitch, 2002) that suggested systematic social interactions between security and operations personnel results in the development of both harmonious and conflictive relationships over security and logistical priorities. The data also affirms the perceived existence of an evolving threat landscape within the maritime

domain. The data also suggests that despite its improvements to seaport security, the MTSA has not adequately equipped security officials to counter sophisticated smuggling operations orchestrated by TCOs and have not effectively implemented the TWIC program. Lastly, the study affirmed previous findings that gaps in intelligence and information sharing between local, state, and federal officials continue to be an obstacle to enhanced security effectiveness at seaports.

The results of the study provided new perspectives into the experiences of SSOs; however, further research should be conducted. In this chapter, I discussed the findings in relation to the literature review. Social change implications resulting from the study's findings are discussed. Lastly, this chapter presents my recommendations for further study and provides a conclusion to the study.

Interpretation of the Findings

Social Systems

This study's findings include important observations in maritime that parallels those observed in the aviation industry by the 9/11 Commission. The Commission (2004) noted that the Federal Aviation Administration (FAA), had been vested by Congress with dual and sometimes incongruent mandates: regulating safety and security and promoting the aviation industry. This study found a similar dynamic at play within the maritime transportation industry. The primary mission of SSOs, much like the FFA, is twofold, security and facilitation of global commerce. This study's participants uniformly described U.S. seaports as organizations with cultures in a constant pursuit of equilibrium. Although all participants identified collaboration as the most essential

element needed to balance operational and security objectives, some participants described a disproportionate balance between logistical priorities and security.

This study's data confirmed peer-reviewed literature findings outlined by Eski (2016) and Eski (2019) who identified important social dynamics in existence at the Port of Rotterdam and the Port of Hamburg, whereas the decisions and actions of management was perceived as an inhibitor to effective security measures. This data also confirmed findings of Malcom (2016) who identified institutional culture as a significant influencer in the prioritization of routine security practices. All participants described the importance of cooperation with various subgroups working within a seaport. Social relationships and interactions between port employees, employees of unions, tenants another industry partners, were identified as a central premise and major element of business productivity and security effectiveness. This study did not uncover any evidence or indicators of low morale amongst SSOs.

The 9/11 Commission (2004) testified that the Inspector General of Transportation told them of "great pressures from the air carriers to control security costs and to limit the impact of security requirements on aviation operations so that the industry could concentrate on its primary mission of moving passengers and aircraft" (p. 85). The study confirmed the literature findings of disparities in security and operational management. Participants noted the perceived burdening cost of security, as a factor resulting in port officials exploring ways to reduce security measures.

The theoretical framework provided by von Bertalanffy (1968) informed this study by postulating that the fundamental character of organizations that replicates

characteristics of living things, is understanding it as an isomorphic system. Von Bertalanffy (1968) explained that systems are readily distinguishable by their reliance and steady exchange with the external environment. Participant depictions of their respective seaports aligned with von Bertalanffy (1968); appropriately each participant described ports as open systems interacting with the environment and being comprised of various inputs, throughputs, and outputs. Investigations solely of individual parts and process, without an understanding of complex interactions does not sufficiently contribute to understanding phenomenon impacting a system. Therefore, this study used a holistic approach to explore, investigate, and discover all factors relevant to the phenomenon.

Threat Perceptions

SSOs are homeland security professionals whose knowledge and experiences inform their conscious and unconscious estimations of threats and risk posed to maritime. They are responsible for the anticipating, countering, preventing acts that may be orchestrated by domestic or international rational actors. SSOs are responsible for securing large open areas, designed to facilitate expedited movement of people and goods. These officials routinely encounter attempts to circumvent security measures at seaports, many of which are determined to lack a known terrorism nexus. While federal officials employ target analysis capabilities, credential authentication measures, random screenings, roving patrols, and CCTV are the predominant measures in use by local and state port officials to detect and deter the introduction of dangerous devices and substances into a seaport. Often with limited security staffing and intelligence resources,

port authorities are responsible for stopping threats that are not fully understood or even perceived.

Comparably, the Commission noted that in the years before 9/11, the FAA did not perceive hijacking as the prevailing threat to aviation, but instead sabotage was perceived as the greatest threat. The absence of domestic hijackings in the previous decades; and the perceived greater susceptibility to explosives than firearms led to miscalculations that created and environment conducive for exploitation. Security measure implemented after the 9/11 attacks effectively postured U.S. seaports to defend against a more traditional threat against critical infrastructure. However, while Vehicle-Borne Improvised Explosive Devices (VBIED) is certainly plausible, 21 century threats have evolved and become far more sophisticated and elusive.

Significant enhancements have been made through the installation of physical security measures such as access gates, cameras, fencing, and barricades; however, in most instances more must be done. Improvements are needed to secure dockside waterways surrounding seaports, airspace above seaports and network systems connecting them to the world. However, the greatest vulnerability confronting seaports to date, is their susceptibility to illicit use by transnational criminal organizations. The evolution of definition and conceptualization of maritime threats appears to lag in time, constrained by archaic comprehension of terrorist tactics used by the pre-9/11 al Qaeda network. While historical lessons are a cornerstone for future response preparedness, they must not stifle the ability of security officials to image, as noted by the 9/11 Commission.

Regulatory Scope

A distinct layer of security employed within U.S. seaports is administered under the USCG and TSA managed TWIC program. This study uncovered opposing viewpoints on the effectiveness of the TWIC program. The TWIC is perceived by some security officials as highly effective in establishing a standard framework for identifying port workers, however, card authentication and holder vetting remains a major challenge, particularly, in addressing potential insider threats.

Furthermore, passenger prescreening at airports, pre-9/11 failed to align FAA "no-fly" list with the government's broader watchlist of known and suspected terrorist. Likewise, this study's findings uncovered no reliable mechanism or resources that provides local and state level SSOs capabilities to screen entrants to restricted facilities who may pose a higher risk, except those on the Canceled Card List (CCL).

The Commission (2004) noted that several years prior to 9/11, FAA requirements for screeners to conduct continuous and random screenings had been replaced by explosive detection and even simply ignored by air carriers. This study observed a need to re-envision and redefine the definition of security breaches, including any attempts to smuggle "illicit" items, as acts in support of terrorism. The need to expand regulatory comprehension of convergence, and to expand the scope of the MTSA to better align with broader efforts at countering drug trafficking, human smuggling, money laundering and weapons smuggling, should be encompassed as a mandate for all seaport security plans.

Barriers and Facilitators

Both the literature and participant responses describe a "layered" approach to security at U.S. seaports, as being the most effective to protecting people, facilities, and vessels. A layered approach infers that a failure in one layer of security would not be fatal, because additional layers would provide backup security (Commission, 2004, p. 83). Seaport security was found to encompass multiple layers, including credential verification, random screenings, and inspections, roving patrols, CCTV, and some internal intelligence capabilities.

The levels of organizational structures, resources and motivations were found to fluctuate quite significantly. Most notable, were varying levels of subjectivity in interpretation of security effectiveness that appeared to influence objectives and intensity of efforts. Even with a robust security program, multiple layers in place at airports were insufficient to prevent the 9/11 hijackers from exploiting aviation by gaining access and weaponizing four commercial aircrafts. Like airports, seaports were found to focus resources and effort on access control measures. However, despite the thousands of vehicles and people entering the restricted areas of seaports daily, unlike aviation, X-ray technology is mostly nonexistent. Instead, seaports rely on randomized screenings conducted by humans who strengths and limitations are noted in chapter 4 of this study.

All participants acknowledged improvements in information sharing amongst security officials; however, most noted was a deficit in intelligence sharing between federal agencies and SSOs. Participants emphasized that a lack of information sharing diminishes security officials' capacity to accurately conceptualize the threat landscape.

This perspective confirms findings of Eski (2016) and Frittelli (2005) who postulated that a lack of sharing is a barrier to security.

In the months preceding the 9/11 attacks, the FAA's policy was to use intelligence to identify plots and threats posed the civil aviation. Unfortunately, most of the informational data received by the FAA contained little pertaining to presence and activities of terrorists in the United States (Commission, 2004). Intelligence was not prioritized amongst FAA leadership, so, the deployment of appropriate countermeasures was inadequate. Participants in this study noted that without sufficient intelligence information, protecting landside maritime assets and reducing exploitation vulnerabilities to smuggling is nearly impossible. SSOs at the local and state level often encounter information through field interviews and arrests, that may contribute significantly to the federal intelligence cycle and subsequent investigations; however, as noted by several participants in this study effective information and intelligence sharing must be mutually reciprocated, both horizontally and vertically.

Limitations of the Study

The purpose of this qualitative study was to explore seaport security measures to identify and understand factors that may impact security measures at U.S. seaports, including those that inadvertently contribute to unauthorized access to restricted facilities and cargo. It was my intent to interview participants who are security officials, working at local, state, and federal agencies within U.S. seaports. My intent was to interview participants from each U.S. maritime border, so I could collect and evaluate unique geographic (regional) experiences.

While my sample did represent each geographical area from across the United States, only 10 participants were interviewed. The sample size was small, as the pool of willing participants proved to be extremely difficult to access. I attributed this to the sensitivity of the study topic and the potential for unfavorable information to be disclosed by some potential participants. The question of whether the findings of my study could be extended across all U.S. seaports remains open and requires further research. The research was not large enough to represent all U.S. seaports; however, even in studies composed of large samples, it is impossible to include the entire target population. Therefore, research is always limited, and generalizations are not absolute. According to Yin (2016) the purpose of data collection is to maximize information, therefore, a study may conclude when little information is forthcoming.

All responses to the interview questions were similar in nature, and sufficiently detailed. The participant responses were collected until no new information was conveyed, and I was confident that saturation was achieved. The self-developed interview guide was robust and effective in facilitating open conversations. However, at the conclusion of the data collection, during transcription and analysis, I felt that too much data outside of scope and interest of the study was collected. Lastly, the study was further limited by my position as an instrument of data collection, analysis, and reporting. My position within the study subjected to findings vulnerable to the influence of my own biases and preconceptions on the findings.

Recommendations

The focal point of this study aimed to explore the experiences and perceptions of SSOs to gain an understanding of how individuals gain unauthorized access to restricted maritime facilities and cargo. Due to the study's exploratory nature, more research is needed to continue the growth of knowledge of seaport security. The findings from this study discovered several important factors requiring further study. Participant perceptions and experiences coupled with research data supported the notion that U.S. seaports may not be adequately secured against transnational threats. The data suggested that security measures instituted under the MTSA have made seaports more robust; however, they are inadequate to secure them against sophisticated exploitation tactics orchestrated by TCOs, including those who may be associated with terrorist groups.

Security measures currently in use account for differences in cargo import volumes and type cargo; however, the uniqueness of U.S. seaports is not limited to commodities and performance but encompasses far more complex issues. Unfortunately, current security measures do not account for likelihood of DTO and terrorism convergence. Therefore, based on the results of this study, I have several recommendations, each based on the proposed expansion of academic research to examine seaport security cultures, maritime threat perceptions, regulation effectiveness, and evaluation of security grant allocations.

My recommendations from this research study begin with proposing that further comprehensive academic research supported and funded by the U.S. government be conducted at all U.S. seaports. I recommend that future research be expanded to include a

sample population large enough to generalize its findings. It became apparent early in the study that the maritime culture is controlled by priorities that support its fundamental purpose to facilitate the movement of global commerce. However, participants conveyed an expectation of port management to prioritize security objectives uniformly with those of logistics priorities.

The study's findings suggest however, that nonsecurity personnel (including management, labor, and truckers) may lack full comprehension of the sophistication of maritime threats and risks, thereby subjecting their routine practices to potential exploitation. Some officials described a shared understanding between security staff and executive management of the importance of security whereas, others described an obliged relationship. Therefore, I recommend that future qualitative studies be conducted to collect additional data on the levels of domain awareness, and threat perceptions of both SSOs and nonsecurity personnel working in U.S. seaports. I recommend that future studies include an evaluation of the MTSA to determine if amendments are needed to strengthen the security posture of U.S. seaports. Future studies should include an evaluation of the TWIC program to determine if a need exists to institute greater accountability measures for individuals who violate security regulations at seaports.

Next, to address the perceived lack of information sharing, I recommend that mixed methodology research be conducted to explore and evaluate current practices of information sharing between local, state, and federal officials. Future research should capitalize on participant surveys and questionnaires to collect data in support of in-depth analysis of rates and direction of sharing, performance and to identify areas of potential

improvements in information sharing. I further recommend that academic research be governmentally funded and conducted to provide the U.S. Congress a comprehensive report evaluating the actual use of funds allocated under the Port Security Grant Program (PSGP), with specific attention being given to how funds are used by individual seaports.

Implications

U.S. seaports serve local communities, states, regions, and the nation by facilitating access to essential goods and services, including food, medicines, and other supplies, therefore, families, organizations, and society as a whole benefit from a more robust maritime system. Designated U.S. seaports also serve an integral role as part of the National Port Readiness Network (NPRN), acting as a critical link to the achievement of national security objectives by supporting military force deployments. Therefore, the implications of this study are not limited to focus on economic consequences of exploitation but may include broader societal ramifications is its findings are ignored.

There are many elements of this study that supports Walden University's vision of social change. Positive social change can be achieved through the rigors of academic research designed to identify and fill knowledge gaps through data collection on a topic of study. This study provided a comprehensive literature review that included background, and historical context that increased awareness of maritime threats and security challenges. The general systems theory guided this study by providing a robust theoretical framework from which I examined the phenomenon of seaport security. The framework challenged the conventional conceptualizations of systems analysis and provided a new perspective and approach for researching system wholes. The theory

offered valuable insight into the behaviors of isomorphic systems. This enabled me to identify parallels with other complex systems and provided a comprehensive avenue of approach for generating new ideas. The study findings determined that countering transnational threats posed to U.S. seaports and the maritime system requires a 21st century holistic approach between both government and the maritime industry. This study contributes to positive social change within the maritime industry by highlighting lessons learned from SSO experiences, observations, and perceptions.

The study findings increased comprehension of maritime threats, and identified security barriers, better preparing policymakers and practitioners to work concertedly in countering transnational threats and rectifying inadvertent barriers to security. Public policy directly impacts operational and security practices, influences behaviors and perspectives associated with public safety, homeland security, and civil liberty. This study may be used to direct organizational and systemic change in the perspectives and practices in use at U.S. seaports. This study findings may be leveraged to draw attention to seaport vulnerabilities and the importance of refocusing attention from 20th century to a 21st century conceptualization of terrorism. As a result of this study on seaport security, policy makers, and practitioners are better positioned to assess risk to the economy, public safety, public health, and national security.

Conclusion

History is embroidered with an incomputable number of examples of susceptibility within maritime to criminal and terrorist use. In 2017, USCG Vice Commandant, Admiral Charles W. Ray testified before a House Homeland Security

Subcommittee on Border and Maritime Security. Admiral Ray testified that while small in numbers, USCG has encountered special interest aliens, those from countries associated with terrorism (C-SPAN, 2017). Admiral Ray acknowledged and underscored his belief that transnational criminal organizations are capable and willing to smuggle special interest people into the United States for profit. Technological advancements (e.g., internet Wi-Fi, cellular, two-way radio, and satellite communications) have increased the speed of commerce and communications, empowering, and strengthening business models of not only legitimate businesses, but criminal and terrorist organizations also.

The world watched in horror as the 2008 Mumbai attackers who traveled by sea, sailing from Karachi, Pakistan on a cargo vessel, launched deadly attacks in Mumbai, India. The terrorist group hijacked an Indian fishing trawler, murdered its crew except for the captain, and then proceeded to Mumbai, where 164 people were killed and more than 300 were injured (Rabasa et al., 2009; Finseraas & Listhaug, 2013). The attackers used cell phones, blackberry devices, and satellite phones to maintain contact with their handlers located in Pakistan, during the attack (Rabasa et al., 2009).

U.S. seaports are irrefutably one of the nation's most important transportation resources, if not the most important. The reliance of U.S. seaports on speed has allowed them to remain competitive but has also inadvertently made them less safe. The maritime environment has become increasingly complex, altered by the adaptative nature of trade and global conflicts between rational actors, some of which are engaged in illicit activities that distort finite rules of trade with infinite greed.

The MTSA is unquestionably one of our nation's greatest legislative accomplishments, a culmination of strategic thinking and strongly rooted in lessons learned in combatting terrorism. The MTSA capsulates history's most horrific moment and provided a pathway for success based on 20th century threat behaviors. What is before us now, is a new 21st century threat, one that is unconventional, decentralized, and sophisticatedly positioned.

According to Maltz (2017), while conducting a large money laundering investigation involving a criminal group in Medellin, Colombia, DEA agents uncovered elements of the terrorist group Hezbollah who were being funded by worldwide cocaine sales. The Agent further explained that in 2016, DEA working with European law enforcement officials previously identified a massive Hezbollah drug and money laundering scheme, where the group was in fact involved in shipping multi-tons of cocaine around the world (Maltz, 2017). It is now necessary to unlearn some of what we have come to understand about terrorism and drug trafficking. The time is now to dissolve barriers, restructure security forces and adopt a shared consciousness of maritime threats before we are forced to accept that convergence is a *real thing.*

The 9/11 Commission report noted that the former Central Intelligence Agency Director, George Tenet, described pre 9/11 intelligence warnings as a system "blinking red." There is tendency amongst some in the maritime industry to underestimate or even dismiss what is perceived as minor, unfounded, or inconsequential violations; however, record drug seizures facilitated through the exploitation of commercial vessels, coupled

with the susceptibility of U.S. seaports, may represent significant system alerts, symptoms or underlying conditions associated with deadly impending acts of terrorism.

References

Abt, C. (2003). *The economic impact of nuclear terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability*. Cambridge, Massachusetts: Abt Associates for the U.S. Department of Transportation. Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability -- Executive Summary (abtassociates.com)

Alda, E., & Sala, J. L. (2014). Links between terrorism, organized crime, and crime: The case of the Sahel region. *International Journal of Security and Development, 3*(1), Art. 27. http://doi.org/10.5334/sta.ea

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity, 23*(3), 121–127.

Bagchi, A., & Paul, J. A. (2017). Espionage and the optimal standard of the Customs-Trade Partnership against Terrorism (C-TPAT) program in maritime security. *European Journal of Operational Research, 262(1)*, 89–107. https://doi.org/10.1016/j.ejor.2017.03.014

Bartell, D. L., & Gray, D. H. (2012). Hezbollah and Al Shabaab in Mexico and the terrorist threat to the United States. *Global Security Studies, 3(4)*, 100–114

Belzer, M. H., & Swan, P. F. (2011). Supply Chain Security: Agency Theory and Port Drayage Drivers. *The Economic and Labor Relations Review, 22*(1), 41–63. https://doi.org/10.1177/103530461102200103

Benítez, G. J., Chandra, S., Cuadros Veloza, T. C. L. W., & Díaz Cárdenas, I. J. D. (2019). Following the price: identifying cocaine trafficking networks in

Colombia. *Global Crime, 20*(2), 90–114. https://doi.org/10.1080/17440572.2019.1588116

Bernard, T. J., Paoline, E. A., III, & Pare, P.-P. (2005). General systems theory and criminal justice. *Journal of Criminal Justice, 33*(3), 203–211. https://doi.org/10.1016/j.jcrimjus.2005.02.00

Björnehed, E. (2004). Narco-Terrorism: The Merger of the War on Drugs and the War on Terror. *Global Crime, 6(3/4)*, 305–324. https://doi.org/10.1080/17440570500273440

Bloom, M. (2017). Constructing expertise: terrorist recruitment and talent spotting in the PIRA, Al Qaeda, and ISIS. *Studies in Conflict & Terrorism, 40(7)*, 603–623. https://doi.org/10.1080/1057610X.2016.1237219

Branker, J., Eveleigh, T., Holzer, T. H., & Sarkani, S. (2016). Access control, identity management and the insider threat. *Journal of Airport Management, 10(2),* 180–199.

Brown, K. (2017). Transnational terrorism. *E-International Relations.* https://www.e-ir.info/2017/01/19/transnational-terrorism/

Bullock, J., Haddow, G., and Coppola, D. (2016) *Introduction to homeland security*. Elsevier.

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

Collins, S. J., Newhouse, R., Porter, J., & Talsma, A. (2014). Effectiveness of the surgical safety checklist in correcting errors: A literature review applying Reason's swiss cheese model. *AORN Journal, 100(1*), 65–79. https://doi.org/10.1016/j.aorn.2013.07.024

Connelly, L. M. (2016). Understanding Research. Trustworthiness in Qualitative Research. *MEDSURG Nursing, 25(6)*, 435–436.

Corrigan, S., Kay, A., Ryan, M., Ward, M. E., & Brazil, B. (2019). Human factors and safety culture: Challenges and opportunities for the port environment. *Safety Science, 119*, 252–265. https://doi.org/10.1016/j.ssci.2018.03.008

Cox, L. Stephen. (2013). The advent and future of international port security law. *National Security Law Journal*. 77-124

C-SPAN. (2017). *Drug cartels and border security*. https://www.c-span.org/video/?424110-1/federal-officials-testify-drug-cartels-border-security

Dezem, V. (2019). Germany Has Biggest Ever Cocaine Seizure Totaling 1 Billion Euros. *Bloomberg.Com*, N.PAG.

Dishman, C. (2016). Terrorist and criminal dynamics: A look beyond the horizon. Beyond Convergence. https://cco.ndu.edu/Portals/96/Documents/books/Beyond%20Convergence/BEYOND%20CONVERGENCE%20%20World%20Without%20Order%20.pdf?ver=2016-10-25-125406-170

Downes, R., Hobbs, C., & Salisbury, D. (2019). Combating nuclear smuggling? Exploring drivers and challenges to detecting nuclear and radiological materials at

maritime facilities. *The Nonproliferation Review, 26:1-2,* 83-104. https://doi.org/10.1080/10736700.2019.1610256

Eski, Y. (2011). Port of call: Towards a criminology of port security. *Criminology & Criminal Justice, 11(5),* 415–431. https://doi.org/10.1177/1748895811414593

Eski, Y. (2016). The war on meaninglessness: A counter-terrorist self through an absent terrorist other. *Ethnography. 17(4),* 460–479. https://doi.org/10.1177/1466138116639984

Eski, Y. (2018). A fear of coercion and accountability? Security officers and the non-use of force. *Policing & Society*, 28(8), 985–998. https://doi.org/10.1080/10439463.2017.1340292

Eski, Y. (2020). Customer is king: promoting port policing, supporting hypercommercialism. *Policing & Society, 30(2),* 153–168. https://doi.org/10.1080/10439463.2019.1606808

European Monitoring Centre for Drugs and Drug Abuse. (2016). *Perspectives on drugs. Cocaine trafficking to Europe.* https://www.emcdda.europa.eu/system/files/attachments/2641/Cocaine%20trafficking_POD2016.pdf

Federal Maritime Commission. (2015). *Port congestion: causes, consequences & challenges.* Bureau of Trade Analysis. https://www.fmc.gov/wp-content/uploads/2019/04/PortForumReport_FINALwebAll.pdf

Finseraas, H., & Listhaug, O. (2013). It can happen here: the impact of the Mumbai terror attacks on public opinion in Western Europe. *Public Choice, 156(1/2),* 213–228. https://doi.org/10.1007/s11127-011-9895-7

Flynn, S. E. (2006). *Port security is still a house of cards.* Far Eastern Economic Review, 1, 5.

Frittelli, J. F. (2005). *Port and maritime security: Background and issues for Congress: RL31733*. Congressional Research Service: Report, 1–22.

Hampton, E. (2015). *An Analysis of the International Ship and Port Facility Security (ISPS) Code: A Multilateral Agreement to Secure the Global Supply Chain.* Kennesaw State University.

Hutchins, R. (2016). *100 percent fired up.* Journal of Commerce (1542-3867), 17(15), 26.

Intermodal Association of North America. (2019). *What is intermodal*. Resource Center. https://www.intermodal.org/what-intermodal

Johnson, B.-A. S. (2013). Transnational terrorism: globalization, voluntary compliance, and U.S. port security. *Global Studies Journal, 5(4),* 65–76. https://doi.org/10.18848/1835-4432/CGP/v05i04/40871

Klir, G. (1972). *Trends in General Systems Theory*. John Wiley. NY.

Knatz, G. (2017). How competition is driving change in port governance, strategic decision-making and government policy in the United States. *Research in Transportation Business & Management, 22*, 67–77. https://doi.org/10.1016/j.rtbm.2016.08.003

Leonard, T. J., Gallo, P., & Veronneau, S. (2015). Security challenges in United States sea ports: an overview. *Journal of Transportation Security, 8(1–2),* 41. https://doi.org/10.1007/s12198-015-0155-9

Leloup, P. (2019). Policing, port security and crime control: an ethnography of the port securityscape. *Policing & Society, 29(3),* 367–370. https://doi.org/10.1080/10439463.2019.1582652

Levitt, M. (2013). The global footprint of Lebanon's Party of God. *Georgetown University Press.*

Levitt, M. (2016). Hezbollah's growing threat against U.S. national security interests in the middle east. *Washington Institute.* https://docs.house.gov/meetings/FA/FA13/20160322/104719/HHRG-114-FA13-Wstate-LevittM-20160322.pdf

Levitt, M. (2016). Hezbollah's Transnational Organized Crime. *Washington Institute for Near East Policy:* Policy Watch, 1–2.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry.* Beverly Hills, CA: Sage Publications, Inc.

Leuprecht, C., Walther, O., Skillicorn, D. B., & Ryde-Collins, H. (2017). Hezbollah's global tentacles: A relational approach to convergence with transnational organized crime. *Terrorism and Political Violence*, *29*(5), 902–921. https://doi.org/10.1080/09546553.2015.1089863

Lichtenwald, T. G., Steinhour, M. H., and Perri, F. S. (2012). A maritime threat assessment of sea based criminal organizations and terrorist operations. *Homeland Security Affairs.* https://www.hsaj.org/articles/227

Macharis, C and Bontekoning, Y. (2004). Opportunities for OR in intermodal freight transport research: A review. *European Journal of Operational Research.* 153. Pp. 400-416.

Maltz, D. (2017). Attacking Hezbollah's financial network: Policy options. *United States House of Representatives House Committee on Foreign Affairs.* https://docs.house.gov/meetings/FA/FA00/20170608/106094/HHRG-115-FA00-Wstate-MaltzD-20170608.pdf

Marks, P. (2016). Policing the waterfront: networks, partnerships, and the governance of port security. *Global Crime, 17(2),* 221–224. https://doi.org/10.1080/17440572.2016.1148314

Miranda (2018). Understanding Human Error in Naval Aviation Mishaps. *Human Factors (6)*, 763. https://doi.org/10.1177/0018720818771904

National Academies of Sciences, Engineering, and Medicine. (2011). *Truck drayage productivity guide*. Washington, DC: The National Academies Press. https://doi.org/10.17226/14536

Ostrom, E. (1998). A behavioral approach to the rational choice theory of collective action: presidential address, American Political Science Association, 1997. *American Political Science Review*

Ostrom, E. (2011). Background on the Institutional Analysis and Development Framework. *Policy Studies Journal, 39(1),* 7–27. https://doi.org/10.1111/j.1541-0072.2010.00394.x

Ostrom, E. (2016). The Comparative Study of Public Economies. *American Economist, 61(1),* 91–107. https://doi.org/10.1177/0569434515626858

O'Sullivan, E., Rassel, G. R., Berner, M., & Taliaferro, J. D. (2017). *Research methods for public administrators* (6th ed.). New York, NY: Routledge.

Pala, A., & Zhuang, J. (2018). Security screening queues with impatient applicants: A new model with a case study. *European Journal of Operational Research, 265(3),* 919–930. https://doi.org/10.1016/j.ejor.2017.08.038

Papadovassilakis, A. (2020). *Cocaine seizures expose flaws at Guatemala, Honduras ports.* InSight Crime. https://insightcrime.org/news/analysis/cocaine-central-america-caribbean-ports/#:~:text=Cocaine%20Seizures%20Expose%20Flaws%20at%20Guatemala%2C%20Honduras%20Ports.,the%20northern%20stretch%20of%20Central%20America%E2%80%99s%20Caribbean%20coast.

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Thousand Oaks, CA: SAGE.

Peery Jr., N. (1972). General systems theory: An inquiry into its social philosophy. *Academy of Management Journal, 15(4),* 495. https://doi.org/10.2307/255144

Rabasa, A., Blackwill, R., Chalk, P. Cragin, K., Fair, C., Jackson, B., Jenkins B., Jones, S., Shestak, N., & Tellis, A. (2009). *Lessons of Mumbai.* Rand Corporation. https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf

Rana, R. and Moditsi, K. (2017). *The linkage between illicit drugs trafficking and terrorist groups*. Old Dominion University Model United Nations. https://www.odu.edu/content/dam/odu/offices/mun/2017/ib-2017-first-drugs-and-terrorism.pdf

Romero-Faz, D., & Camarero-Orive, A. (2017). Risk assessment of critical infrastructures – New parameters for commercial ports. *International Journal of Critical Infrastructure Protection, 18,* 50–57. https://doi.org/10.1016/j.ijcip.2017.07.001

Rousseau, D. (2015). General systems theory: Its present and potential. *Systems Research and Behavioral Science, 32,* 522– 533. https://doi.org/10.1002/sres.2354

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). Thousand Oaks, CA: Sage Publications

Rudestam, K. E., & Newton, R. R. (2015). *Surviving your dissertation: A comprehensive guide to content and process* (4th ed.). Thousand Oaks, CA: SAGE.

Saldana, J. (2016). *The coding manual for qualitative researchers*. The Oaks, CA: Sage.

Scholliers, J., Permala, A., Toivonen, S., & Salmela, H. (2016). Improving the security of containers in port related supply chains. *Transportation Research Procedia, 14,* 1374–1383. https://doi.org/10.1016/j.trpro.2016.05.210

Simon, M. K. (2011). *Validity and reliability in qualitative studies. In Dissertation and scholarly research: Recipes for success* (pp. 1–3). Seattle, WA: Dissertation Success. http://dissertationrecipes.com/wp-content/uploads/2011/04/Validity-and-Reliability-in-a-Qualitative-Study.pdf

Shapiro, L. R., Maras, M.-H., Velotti, L., Pickman, S., Wei, H.-L., & Till, R. (2018). Trojan horse risks in the maritime transportation systems sector. *Journal of Transportation Security, (3–4),* 65. https://doi.org/10.1007/s12198-018-0191-3

Shelley, L. I., & Picarelli, J. T. (2005). Methods and motives: exploring links between transnational organized crime and international terrorism. *Trends in Organized Crime, 9(2),* 52–67. https://doi.org/10.1007/s12117-005-1024-x

Shenton, A. K. (2004). *Strategies for ensuring trustworthiness in qualitative research projects.* Education for Information, 22(2), 63–75.

Skytter, L. (2006). *General systems theory: Problems, perspectives, practice*. http://ebookcentral.proquest.com

Song, L., Yang, D., Chin, A. T. H., Zhang, G., He, Z., Guan, W., & Mao, B. (2016). A game-theoretical approach for modeling competitions in a maritime supply chain. *Maritime Policy & Management, 43(8),* 976–991. https://doi.org/10.1080/03088839.2016.1231427

Stewart, S. (2016). *From Columbia to New York City: The narconomics of cocaine. Business Insider*. https://www.businessinsider.com/from-colombia-to-new-york-city-the-economics-of-cocaine-2015-7

Thachuk, K. L., & Lal, R. (2017). Terrorist Criminal Enterprises. *International Journal of Terrorism & Political Hot Spots, 12(2/3),* 101–117.

The 9/11 Commission Report. (2004). *Final report of the national commission on terrorist attacks upon the United States, official government edition.* https://fas.org/irp/offdocs/911comm.html

United Nations Conference on Trade and Development. (2018). *Review of maritime transport.* https://unctad.org/system/files/official-document/rmt2018_en.pdf

United Nations of Office on Drugs and Crime. (2020). *The UNODC-WCO Container Control Programme. Overview.* https://www.unodc.org/unodc/es/ccp/Overview.html

United Nations Office on Drugs and Crime. (2021). *UNODC-WCO global container control programme*. https://www.unodc.org/ropan/en/BorderControl/container-control/ccp.html

U.S. Customs and Border Protection. (2019). *U.S. Customs and Border Protection seizes over 17.5 tons of cocaine in Philadelphia.* https://www.cbp.gov/newsroom/national-media-release/us-customs-and-border-protection-seizes-over-175-tons-cocaine

U.S. Department of Commerce. (n.d.). *Make the export sale: Shipping basics.* International Trade Administration. https://www.export.gov/article2?id=Freight-Forwarders

U.S. Department of Justice, Drug Enforcement Administration. (2018). *2018 National Drug Threat Assessment*. https://www.dea.gov/sites/default/files/2018-11/DIR-032-18%202018%20NDTA%20%5Bfinal%5D%20low%20resolution11-20.pdf

U.S. Department of Justice. (2019*). Cocaine seizures bring recent port of Savannah totals to more than $53 million. Drug Enforcement Agency*. https://www.dea.gov/press-releases/2019/06/11/cocaine-seizures-bring-recent-port-savannah-totals-more-53-million

U.S. Department of Justice. (2020). *Hidden cocaine shipment seized from container. Drug Enforcement Agency*. https://www.dea.gov/press-releases/2020/06/03/hidden-cocaine-shipment-seized-container

U.S. Department of Justice. (2020). *MSC Gayane crew member pleads guilty to cocaine trafficking stemming from one of the largest drug seizures in U.S. history.* https://www.justice.gov/usao-edpa/pr/msc-gayane-crew-member-pleads-guilty-cocaine-trafficking-stemming-one-largest-drughttps://www.justice.gov/usao-edpa/pr/msc-gayane-crew-member-pleads-guilty-cocaine-trafficking-stemming-one-largest-drug

U.S. Department of Transportation. (2019). *National port readiness network.* Maritime Administration. https://www.maritime.dot.gov/ports/strong-ports/national-port-readiness-network-nprn#:~:text=The%20NPRN%20consists%20of%20the%20National%20Port%20Readiness,Sealift%20Command%20%28MSC%29%20U.S.%20Army%20Forces%20Command%20%28USFORSCOM%29

U.S. Department of Transportation. (2018). *Port performance freight statistics in 2018, annual report to congress.* Bureau of Transportation Statistics. https://www.bts.gov/sites/bts.dot.gov/files/docs/browse-statistical-products-and-data/port-performance/224751/ppfsp-annual-report2018.pdf

United States. (2018). *Examining physical security and cybersecurity at our nation's ports: Field hearing before the Committee on Homeland Security.* House of Representatives, One Hundred Fifteenth Congress, first session, October 30, 2017.

United States. (2018). *Exploring the financial nexus of terrorism, drug trafficking, and organized crime: Hearing before the Subcommittee on Terrorism and Illicit Finance of the Committee on Financial Services.* U.S. House of Representatives, One Hundred Fifteenth Congress, second session, March 20, 2018.

U.S. Government Accountability Office. (2016). *Maritime security: progress and challenges in implementing maritime cargo security programs.* https://www.gao.gov/products/gao-16-790t

U.S. White House. (2019). *National drug control strategy. Office of National Drug Control Policy.* https://www.whitehouse.gov/wp-content/uploads/2019/01/NDCS-Final.pdf

von Bertalanffy, L. (1968). *General System Theory: Foundations, Development, Applications.* New York: George Braziller.

von Bertalanffy, L. (1969). *General systems theory*. *Foundations, development, application*. George Braziller, Inc. New York, NY. (Original work published 1968)

von Bertalanffy, L. (1972). The History and Status of General Systems Theory. *Academy of Management Journal, 15(4),* 407–426.

von Bertalanffy, L. (2008). *An outline of General System Theory.* Emergence: Complexity & Organization, 10(2), 103–123.

Watkins, A. (2019). *At Newark, 3,200 pounds of cocaine*. New York Times, 168(58264), A20

Weible, C. M., Sabatier, P. A. (2018). *Theories of the policy process* (4th ed.). Boulder, CO: Westview Press

Wehner, P. (2014). *False sense of security?* Estates Gazette, 14.

Willis, H. (2016). *Ten years after the Safe Port Act, are America's ports secure?* Rand Corporation. https://www.rand.org/blog/2016/04/attractive-targets.html

Yin, R. K. (2016). *Qualitative research from start to finish*. (2nd Ed.). Sage.

Yin, R. K. (2018). *Case study research design and methods*. (6th Ed.). Sage.

Yagoub, M. (2016). *New report offers details on cocaine traffic to Europe.* InSight Crime. https://insightcrime.org/news/analysis/cocaine-trafficking-to-europe-explained-by-new-report/

Appendix A: Interview Questions and Corresponding Research Questions

Interview Question no.	Question	Corresponding RQ(s)
1	How long have you served in your current profession and what do you find most rewarding about your job?	1
2	What are your duties and responsibilities as a security official working within at a seaport?	1
3	What about your profession and function fulfill your sense of purpose most?	1
4	How would you describe the security culture at U.S. seaports and the impact it has on mandatory security practices?	1
5	Can you describe your experience in implementing and exercising security measures at your seaport?	1
6	What kinds of things help in facilitating security functions at your seaport?	1, 2
7	Can you tell me about the types and levels of support you receive in keeping your port secure against unauthorized access?	1
8	There is some belief and views that there is a lack of support for seaport security measures, in your opinion what constitutes barriers to security?	1
9	There is some belief and views that there is a lack of support for seaport security measures, in your opinion what constitutes support of security?	1
10	How would you describe the effectiveness of security practices at your seaport in preventing unauthorized access to the restricted facility?	1

11	How would you describe the effectiveness of security practices at your port in preventing unauthorized access to containerized cargo?	1
12	How would you describe the capabilities of security officials at your facility to institute all mandates under the Maritime Transportation Security Act of 2002?	1, 2
13	What do you perceive as the great threat to U.S. seaport security?	2
14	How would you describe the level of preparedness of seaport security officials to respond to an act of terrorism in port?	1, 2
15	How would you describe risks associated with drug smuggling at seaports?	1, 2
16	What do you believe is are the greatest facilitators to successful smuggling of illicit items through seaports?	2
17	How does information sharing amongst local, state, and federal officials impact your ability to institute effective security measures at seaports?	2
18	How does internal communication between line officers and management impact seaport security practices?	2
19	How would you describe current security practices at seaports in relation to terrorism prevention?	2
20	How would you describe current security practices at seaports in relation to counterdrug smuggling?	2
21	What kind of training do you believe is needed to equip security officials to protect seaports from transnational criminal organizations?	1, 2
22	What suggestions would you offer for improving security at U.S. seaports?	2