2015

Port Security: The Terrorist Naval Mine/ Underwater Improvised Explosive Device Threat

Peter von Bleichert
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Peter von Bleichert

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. Karen Shafer, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Gregory Dixon, Committee Member,
Public Policy and Administration Faculty

Dr. Anne Fetter, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2015

Abstract

Port Security: The Terrorist Naval Mine/Underwater Improvised Explosive Device Threat

by

Peter A. von Bleichert

MA, Schiller International University (London), 1992

BA, American College of Greece, 1991

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

June 2015

Abstract

Terrorist naval mines/underwater improvised explosive devices (M/UWIEDs) are a threat to U.S. maritime ports, and could cause economic damage, panic, and mass casualties. The purpose of this case study was to examine this threat and propose reforms that improve port security management. The study aligned with the mission area analysis objective of identifying and assessing potential terrorist threats in order to preempt and prevent attacks. Von Bertalanffy's general systems theory was the framework for research questions, which focused on improvements in port security management to mitigate the threat of terrorist M/UWIEDs. Data collection included a document content analysis of open source/nonclassified crime reports, government threat assessments, and legislation; physical artifacts (port infrastructure) information; policy papers; maps, satellite imagery, and navigational charts; peer-reviewed academic literature; and direct observation of 2 California-based maritime ports and an inspection of their physical artifacts. Data were organized by general themes; coded axially and selectively; and analyzed by phrases, topics, and words associated with minelaying, mine countermeasures, and port security. Key findings were that, since 9/11, overall port security has improved, although there has been little progress in countering the threat presented by M/UWIEDs. Further, vulnerabilities exist that terrorists who seek to commit an M/UWIED attack or campaign could misuse. The findings from this study contribute to positive social change by providing data to key stakeholders responsible for counterterrorism, mine warfare, and port security, thereby contributing to overall U.S. homeland security.

Port Security: The Terrorist Naval Mine/Underwater Improvised Explosive Device Threat

by

Peter A. von Bleichert

MA, Schiller International University (London), 1992

BA, American College of Greece, 1991

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

June 2015

Dedication

For my daughter, Elizabeth Anne: The countless hours are for you. I pray for you to have a long, happy, healthy, peaceful, and prosperous life, and can only hope I impart one lesson with this work: You can do anything if you never give up!

Acknowledgments

To my dissertation committee chair, Dr. Karen Shafer: Thank you for stepping up and sticking with me, and for guidance, patience, and professionalism. I could not have done this without you. I am forever grateful.

To my dissertation committee members, Dr. Gregory Dixon and Dr. Anne Fetter: Thank you for joining my team. It was a pleasure to work with you both.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

On September 11, 2001 (9/11), al-Qaeda—Arabic for *The Base*, the strong part of a pillar—an international terrorist network (Bajoria & Bruno, 2012), attacked the World Trade Center in New York City, attacked the Pentagon in Virginia, and targeted the White House in Washington, DC. These terrorists sought to inflict damage upon U.S. centers of economic, military, and government power, and to make clear that the nation, despite its superpower status, was highly vulnerable to asymmetric attack. Al-Qaeda and its splinter organizations have specifically stated that their goal is to further exploit this vulnerability by inflicting economic damage, panic, and mass casualties (Griset & Mahan, 2003) upon the United States.

The United States is reliant upon massive public and private infrastructure and, as a continental nation, is tied deeply to the planet's oceans and seas for both commerce and defense. The country operates an intricate network of intermodal landside connections, ports (lake-, river-, and sea-based), and waterways that represent critical nodes of its marine transportation system (MTS). The MTS is a gate to world markets, a critical facet of military mobilization, and a transportation network for goods and people; it creates commercial and recreational jobs, generates revenue through taxes and fees, and supports public recreation (U.S. Department of Homeland Security [DHS], 2005, p. ii). The MTS is served by 361 ports composed of approximately 3,200 facilities that handle cargo and passengers (American Association of Port Authorities [AAPA], 2013b), and, depending on the respective individual facility, it accommodates a spectrum of vessel types: barges, ferries, ocean-going cargo and passenger ships, and recreational watercrafts.

MTS ports are governed by various state and local public entities including port authorities, port navigation districts, and municipal port departments (AAPA, 2013b). These ports are located among the United States' vast seaboards and waterways along the Atlantic, Pacific, Gulf, and Great Lakes coasts, as well as in Alaska, Guam, Hawai'i, Puerto Rico, Saipan, and the U.S. Virgin Islands. Of the 361 United States maritime ports, the Port of South Louisiana is the largest, and the Port of Monroe, Michigan, the smallest (AAPA, 2013b). One hundred fifty of these ports are deep draft, accommodate ocean-going vessels (able to operate in deep open water), and are managed by 126 public seaport agencies (AAPA, 2013b). Regardless of size, however, all 361 facilities are essential to maritime commerce, are proximate to population centers, handle highly hazardous materials, and are entered by approximately 7,500 foreign ships every year (Evans & Stutin, 2006, p. 26). U.S. ports remain enticing and vulnerable terrorist targets.

Falling under the aegis of the DHS mission—defined by the National Strategy for Homeland Security as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur" (DHS, 2007, p. 11)—the need to secure America's ports is a pressing one.

The U.S. government has sponsored multiple critical infrastructure and key resource (CIKR) threat assessments regarding port security (Government Accountability Office [GAO], 2002, p. 6). These CIKR assessments addressed threat vectors—paths or tools that a threat actor uses to attack a target (Withers, n.d., p. 3)—that included human infiltration (frogmen, submersibles, and suicide teams, such as those that, in 2000,

crippled the U.S.S. *Cole* in Aden, Yemen, whereby terrorists piloted a small explosive laden boat—a water-borne improvised explosive device—up to the warship's hull and detonated it); delivery of chemical, biological, radiological, nuclear, and high yield explosive (CBRNE) weapons by commercial vessel; and the use of vessels themselves as weapons, such as the use of vessels to ram other vessels or fixed port infrastructure such as docks and bridges (Evans & Stutin, 2006). These threat assessments have concentrated on the so-called *megaports*—large deepwater facilities that experience the majority of trade by tonnage—and have neglected myriad medium to small facilities that represent the majority of U.S. maritime ports (Evans & Stutin, 2006). Therefore, those charged with port security have focused attention and resources on such facilities and CBRNEs smuggled among the hundreds of thousands of shipping containers that U.S. maritime ports handle each year. This is despite the fact that CBRNEs are difficult to acquire, handle, and deliver, especially now that port security vis-à-vis this attack vector has been hardened. It is thus likely that those who seek to harm the MTS will target smaller ports and use threat vectors that are more likely to succeed (Flynn, 2004, p. 92), the so-called *path of least resistance*. One such vector is that of terrorist naval mines/underwater improvised explosive devices (M/UWIEDs).

The inventories of more than 50 world navies contain more than 250,000 naval mines representing more than 300 types. Over 30 countries manufacture naval mines, and at least 20 countries sell them (U.S. Navy [USN], 2009, p. 7). Naval mines are quintessential asymmetric weapons, and weak naval powers have used them against the strong for over 200 years by (Truver, 2008, p. 107). When laid in the water, these

weapons can inflict major, long-term damage on shipping while allowing little or no chance for retaliatory action against the laying force and can impart the advantage of covertness and surprise (USN, 1996, Chapter 2.1.1). Ranging from simplistic to highly complex weapons, naval mines are available to terrorists on the international arms market, and, within the capabilities of their networks, terrorists can design and build improvised equivalents.

Such underwater improvised explosive devices can be made from a multitude of items, including bladder tanks, barrels, and old appliances, and explosive material is readily available in commercial form or from synthesized agricultural and industrial components (USN, 2009, p. 8). Without doubt, terrorist M/UWIEDs laid in one or more ports would have immediate and lasting effects on the economy and security of the United States (Sparks, 2005, p. 15), and their use is clearly aligned with terrorist goals of inflicting economic damage, panic, and, potentially, mass casualties. Admiral Allen, 23rd Commandant of the U.S. Coast Guard (USCG) stated, "What keeps me up at night? The threat of … improvised explosive devices" (USN, 2009, p. 13).

According to the National Infrastructure Protection Plan (NIPP), academia has an essential part in supporting U.S. CIKR security by studying, developing, and distributing best methods for ranking priorities and developing efforts for CIKR protection and by providing creative thinking and viewpoints on dangers (DHS, 2014a, pp. 25-26).

This qualitative case study broadens the current understanding of the threat of terrorist M/UWIEDs to U.S. maritime ports, and the findings may contribute to positive

social change by assisting stakeholders responsible for securing the MTS, thereby increasing protection of the homeland.

In Chapter 1, I provide further background on the threat of terrorist M/UWIEDs to U.S. maritime ports and delineate this study's problem statement, purpose, research questions, theoretical framework, nature, definitions, assumptions, scope and delimitations, limitations, and significance.

Background

By volume, over 90% of U.S. exports and imports move through the country's maritime ports (USN, 2009, p. 11). These facilities are integral to the safe movement of coastal, inland, and foreign commerce, making them vital to the U.S. economy (USN, 2009, p. 11). Ports represent potential terrorist targets, as they are sprawling, often close to urban areas, and accessible by both land and water (Caldwell, 2007, p. 3). In the aftermath of the 9/11 attacks, the Maritime Transportation Security Act (MTSA) of 2002 established a new framework for port security in the age of terror.

MTSA (2002) was intended to safeguard U.S. ports and waterways from the terror threat. MTSA legislated a wide range of security enhancements, including weakness calculations for port facilities and vessels; expansion of security strategies to mitigate risks for the MTS; establishment of the Transportation Worker Identification Credential (TWIC); and security assessments of foreign ports from where vessels sail on trips to the United States (Caldwell, 2007, pp. 3-4). However, MTSA focused on the threat of cargo, the vessels that deliver it to U.S. shores, and those that work in port facilities, and it failed to contend with the threat of terrorist M/UWIEDs.

The Security and Accountability for Every Port Act (SAFE Port Act, 2006, § 205) amended the original provisions of MTSA and added provisions: the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). Both the CSI and C-TPAT are administered by U.S. Customs and Border Protection (CBP) and are designed to reduce threats inherent with cargo containers. These programs also set up port security interagency operational centers at high-risk ports, set fee restrictions and a schedule for the TWIC program, required that all containers entering the United States be scanned for radiation, and provided data to CBP in order to target cargo containers for inspection (Caldwell, 2007, p. 4). Again, the SAFE Port Act focused on the threat of CBRNEs delivered by vessels and/or vessel-borne containers (GAO, 2012) and the companies and personnel that handle them and did not recognize the threat from terrorist M/UWIEDs. Exacerbating this blind spot, even the *U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship* did not once mention the threat (USCG, 2007). It was this lack of recognition, this research gap, which drove the purpose of my study.

This gap in the empirical literature base needed addressing. M/UWIEDs are the quintessential maritime weapons of terror: M/UWIEDs are cheap, can be easily acquired and deployed; and are problematic to counter (U.S. Department of Defense [DOD] & DHS, 2005, p. 4); are capable of economic disruption; and inflict fear and uncertainty (Hartmann, 1991, p. 5). When used in conjunction with other forces, M/UWIEDs also serve as a force multiplier (USN, 1996, Chapter 2.1.1). In other words, these weapons could be used in conjunction with air and land attacks against port facilities, distracting

and dividing responders, or could be an adjunct to a suicide mission, delaying, deterring, or destroying responders and maximizing the confusion and destruction created by the main attack (Dowd, 2004, p. 14). Furthermore, these weapons offer the terrorist operational security and the potential for interference/interdiction of U.S. naval deployments and operations (Truver, 2008, p. 107).

At a minimum, a terrorist M/UWIED could severely damage or sink a ship in a channel and disrupt port traffic. At most, such an attack could impart psychological effects by implying that a large minefield was present in one or more ports, thereby bringing MTS traffic to a complete standstill. Such effects would be multiplied by the lack of readily available mine countermeasure (MCM) assets at the attack site (Rodeman, 2003, p. 7). The impacts of a terrorist M/UWIED attack could be of a military nature as well, as such weapons laid in critical waterways would retard the flow of military shipments during times of conflict and hamper military sealift, a strategic element that forms the basis of U.S. wartime deployment for heavy equipment and stores (Truver, 2008, p. 108). As alluded, such weapons are readily available for purchase, or can be easily fashioned.

M/UWIEDs are cheap—costing from about $30 to approximately $30,000 for an advanced, multiple influence weapon (Truver, 2007, p. 46). Older weapons can be refitted with modern, sophisticated components, as well as counter countermeasures—such as building them from fiberglass or plastic and installing booby traps. Such counter countermeasures can make detecting and/or disabling them highly problematic (Truver, 2008, pp. 108-109). Terrorists can also acquire naval mines from the inventories of rogue

states (Truver, 2008, p. 109). For example, a U.S. Air Force reconnaissance aircraft found that acoustic naval mines had disappeared from a North Korean naval base in 2002, and U.S. intelligence has stated they believe that al-Qaeda is now is in possession of them (English, 2003). Intelligence agencies also reported that al-Qaeda has ties to the Iranian Revolutionary Guard's (IRG) Islamist militant training branch (English, 2003). The IRG had mined the Persian Gulf during the 1980s (Priest & Farah, 2003), making it another likely source for al-Qaeda to acquire naval mines (Dowd, 2004, p. 8). Furthermore, there have been reports that al-Qaeda hired a maritime security expert in 2004 ("The Secret World of Cargo Ships," 2013). According to Truver (2008), terrorist M/UWIEDs could "constitute an Achilles heel" (p. 107) for U.S. homeland security.

The economic impacts and effects on the MTS and the private companies that rely upon it are dependent on how severe an attack was, what the imparted casualties and damage were, as well as the reaction of the government and public. However, a successful attack on the MTS would likely have a far greater effect than the actual damage (Watts, 2005, p. 4). An example of such an impact can be gauged by the U.S. west coast port lockout.

In October 2002, as a result of a dispute between management and unions, all 29 U.S. west coast ports shut down for some 2 weeks (Richardson, 2004, p. 67). At the time, these ports represented 42% of U.S. maritime import-exports by value, and the shutdown resulted in the delay of 200 ships and 300,000 containers (Richardson, 2004, p. 67). This had a ripple effect that parked intermodal shipments across the country and piled up products in foreign warehouses, forcing vessels to make costly diversions to alternate

ports and companies to lay off employees and cut productivity, in addition to the loss of perishable/time sensitive cargoes (Richardson, 2004, p. 67). One estimate of the total cost of the west coast port lockout to U.S.-based business was $467 million (Richardson, 2004, p. 67). This number, however, did not reflect the fact that shippers foresaw the closure of these ports and therefore allowed dependent companies to mitigate impacts (Richardson, 2004, p. 67). Thus, one could argue that this estimate is on the low end of what an M/UWIED event in one or more ports would cost the economy. In addition, this half-billion-dollar estimate did not account for the long-term financial cost associated with increased insurance rates (Richardson, 2004, p. 67).

Insurance is vital to the global economy and specifically sea-borne trade. The Strikes, Riots and Civil Commotion (SRCC) category of marine insurance covers maritime acts of terror, adding a significant premium to base policies (Richardson, 2004, p. 69). Based on risk assessments, this SRCC premium is certain to escalate in the wake of an M/UWIED attack, adding to shipping costs and to the final cost paid by consumers for products (Richardson, 2004, p. 69). An example of this comes from the late 1980s, when Iraq and Iran were at war with each other and threatened and damaged oil tankers transiting the Persian Gulf (Watts, 2005, p. 4). A Cato Institute analysis of the conflict (as cited in Watts, 2005) showed that the greatest impact was not the damage to tankers, or an increase in oil prices, but the increased insurance rates paid by shippers plying these waters (p. 2).

Besides such commercial impacts, terrorist M/UWIEDs have the potential to inflict physical damage. Such damage could include crippling cruise ships, detonating

liquid natural gas carriers or the myriad other specialized vessels that transport explosive and/or hazardous materials, and sinking ferries full of civilians (Truver, 2007, p. 46).

According to Homeland Security Strategic Planning, a key function of DHS is preventing attacks by detecting threats (Homeland Security Studies and Analysis Institute [HSSAI], 2007, p. 11), safeguarding the United States by assessing CIKR and implementing protective programs for assets and systems (HSSAI, 2007, pp. 20-24). Despite a large number of government specialists focused on homeland security, the leaders of the NIPP have viewed academia as integral to understanding the terrorist threat spectrum, analyzing threat vectors, and making recommendations for mitigating such threats (DHS, 2009, p. 28). This case increases the understanding of the threat of terrorist M/UWIEDs to U.S. maritime ports, thereby furthering overall homeland security.

Problem Statement

The research problem concerns the threat of terrorist M/UWIEDs to U.S. maritime ports. This problem gives rise to the question of what steps relevant U.S. government agencies should take to reform or supplement security management to improve general MTS operations.

Since the attacks of 9/11, the United States has been engaged in an asymmetric conflict that is unlike any other one the nation has previously experienced (Renuart & Egli, 2008, p. 16). The terrorist enemy has transformed, and has forced U.S. security managers to revisit security weaknesses in all domains: air, land, and maritime (Renuart & Egli, 2008, p. 16). The 9/11 attacks exploited aviation, and there have been multiple incidents of land-based attacks (such as truck bombings), resulting in increased security

awareness for these domains and making commercial shipping and the maritime domain more attractive targets to terrorists (Rodeman, 2003, p. 6). The continuation of the trend of globalization and projected population growth will increase commercial and passenger maritime transportation, and, therefore, threats to the U.S. maritime domain will only increase (Neffenger, 2013, p. 21).

By volume, upwards of 90% of U.S. exports and imports move through maritime ports (Caldwell, 2007, p. 3). Maritime ports are sprawling, often close to urban areas, are accessible by air, land, and water (Caldwell, 2007, p. 3), and are integral to the safe movement of coastal, inland, and foreign commerce, making them vital to the U.S. economy (USN, 2009, p. 11).

The current threat of terrorist M/UWIEDs is highly relevant to both homeland security and general infrastructure policy. This case study built upon current research in the area of port security (Bennett, 2008; Caldwell, 2007; Clark, Nincic, & Fidler, 2007; Dowd, 2004; Evans & Stutin, 2006; Frittelli, 2004; Lyons, Baker, Edlow, & Perrin, 1993; Rios, 2005; Rodeman, 2003; Truver, 2008; 2012; Watts, 2005) by expanding its scope to include the threat of terrorist M/UWIEDs.

Purpose of the Study

The purpose of this case study was to examine the areas of modern naval mine warfare and terrorism as they are related to the CIKR of U.S. maritime ports. The intent was to discover implemented port security management improvements relevant to the threat of terrorist M/UWIEDs; to examine this threat from an adversarial position; and to explore means of mitigating this threat with the development of proposed

recommendations for bureaucratic and policy reform. The case study focused on two ports in California: Oakland and Stockton.

Research Questions

1. Since 9/11, what port security management improvements have been implemented that mitigate the M/UWIED threat?
2. How could terrorists use M/UWIEDs to attack U.S. maritime ports?
3. What additional port security management improvements should be implemented to further mitigate the M/UWIED threat?

Theoretical Framework

In von Bertalanffy's (1969) general systems theory (GST), systems are complexes of elements standing in interaction (p. 33). Von Bertalanffy examined "the working of the world reflected in a cleverly designed, abstract game" (p. 11) and provided a structure by which researchers can investigate the interaction of multiple groups, organizations, or units working together to improve outcomes. GST allowed me to rise above linear cause-and-effect chains to observe interrelationships and processes of change (Senge, 1990, p. 73). A systems viewpoint is usually qualitative and, as stated by Patton (2002), helps researchers "view things as whole entities embedded in context and still larger wholes… [and that] …holistic thinking is central to a systems perspective" (p. 120). The holistic thinking that GST imparted benefited this study and allowed me to examine and interpret the complexities inherent to California port security and, ideally, to generalize them to U.S. maritime ports.

GST is relevant to security, especially the layered systems instituted for homeland security, and specifically port security. Using GST permitted me to delineate security management stakeholder responsibilities, and I applied it to my observation of relationships between bureaucracies responsible for port security and MCM in California. GST allows researchers to examine problems for generality versus the analytical-summative approach of classical science (von Bertalanffy, 1969, p. 19). I used the GST framework—discussed further in Chapter 2—to approach and answer my research questions.

In Research Question 1, I examined interacting and interrelated systemic elements established by national legislation and policy since 9/11 to protect U.S. maritime ports from potential terrorist threat vectors, specifically that of mine warfare. In Research Question 2, I examined two specific ports in California: the Port of Oakland and the Port of Stockton. Oakland is a physically large facility that handles a high volume of containers, and Stockton is smaller in size and handles primarily unpackaged bulk shipments. Each facility presents unique location, physical layout, and water depth. I constructed said examination around the systems found in Research Question 1 and used the unique features of these real world ports, as well as standard minelaying (MIL) tactics, to show how terrorists could attack port facilities using M/UWIEDs. Using the results from both Research Questions 1 and 2, I examined Research Question 3 and explored systemic inefficiencies, extrapolating these to make specific recommendations for national systemic reform.

Nature of the Study

This qualitative study concerned the Critical Infrastructure and Key Resources that comprise the U.S. Marine Transportation System and the threat of terrorist M/UWIEDs to two ports in California (one large, and one small). I used the framework of GST to examine existing documents and legislation enacted since 9/11 and then used holistic case studies of the ports of Oakland and Stockton. These two sample ports were selected due to geographic proximity to my home (convenience) and their representation of both ends of the port size/type spectrum (large bayside container-borne cargo facility versus small riverside bulk cargo facility).

Corbin and Strauss (2009) defined qualitative study as "a process of examining and interpreting data in order to elicit meaning, gain understanding, and develop empirical knowledge" (p. 1). This tradition is embodied in the framework of GST and applicable to my study's purpose to discover port security management inefficiencies and extrapolate these improvements to mitigate the threat of terrorist M/UWIEDs. The framework of GST aligns with HSSAI mission area analysis (MAA) (HSSAI, 2007).

MAA is a homeland security strategic analysis method that seeks to preempt and prevent attacks by identifying and assessing threats, with subordinate missions to prevent, protect, respond, and recover (HSSAI, 2007, p. 9). MAA is composed of a goal, missions, objectives, and functions, and it involves the collection, review, and analysis of qualitative information, including legislation, policy statements, and threat assessments.

MAA supports an objective of implementing protective programs for assets and systems by protecting CIKR through deterrence and mitigation of terrorist attacks. This is

accomplished by the following: (a) managing risk by finding the most cost effective and sensible group of countermeasures to reduce strategic, tactical, and operational risk; (b) defending the CIKR by securing resources through mitigation, delay, or prevention of the actual attack; and (c) devaluing potential targets by reducing the effectiveness of a target by lessening potential consequences (HSSAI, 2007, p. 27).

The MAA used in this study addressed the objective of identifying and assessing threats in order to obstruct and thwart attacks whereby I examined legislation, policy statements, and threat assessments from DOD, DHS and the U.S. Department of Transportation (DOT) as well as various public and private academic and security institutions. Furthermore, my MAA used a case study of two California ports. Case study research allows the examination of phenomena in actuality and has a long history in research that can be applied broadly. The strength of qualitative methodology resides in producing insights stemming from specific findings in context (Hoon, 2013, p. 522). By evaluating a particular phenomenon through case studies, I sought to understand the phenomenon in its totality (Hoon, 2013, p. 527). My case study included an examination of port channels, infrastructure, and water depth, whereby I applied standard MIL tactics and technology, and made conclusions as to how terrorists could lay M/UWIEDs to further their objectives.

Definitions

Anchorage: The approved site within a harbor or port that a vessel has been assigned and where said vessel drops anchor or attaches to a mooring (AAPA, 2013b).

Bathymetry: Submarine topography, or the depths and shapes of underwater terrain (National Oceanic & Atmospheric Administration [NOAA], 2014a).

Berth: A position on a wharf where a vessel secures itself by ropes attached to cleats in order to prevent uncommanded movement due to currents, tides, or wind (AAPA, 2013b).

Container: An enclosure made of aluminum, fiberglass, or steel that is usually rectangular in shape, and is used to carry and protect cargo. Such containers can be hauled by barge, ship, rail, or truck. Commonly called a *20-foot equivalent unit* or *TEU*, the containers dimensions are 7 meters x 2.5 meters x 2.5 meters for a total volume of 975 square meters. Containers also come in 40-foot equivalent units—FEUs—that double these dimensions. Containers can vary in configuration, whereby they can be collapsible, be cylindrically tank shaped for transport of liquids, have *rag tops* (open-topped containers that are covered by a tarpaulin), and are used to transport irregular cargo that juts from the top of a standard enclosed type (AAPA, 2013b).

Container terminal: A facility within a port's perimeter that is specialized to handle container-bearing vessels, whereby said vessels berth to discharge and/or take aboard containers. Such terminals are usually equipped with cranes that can safely lift up to 36 metric tons and have booms that can reach up some 37 meters, enabling them to reach the outer cells of vessels (AAPA, 2013b).

Draft: A measurement from the waterline of a fully loaded vessel to the lowest point of its hull (AAPA, 2013a).

Jihadi (or Jihadist): The belief that an Islamic state must be created that governs the entire community of Muslims, and that this creation justifies violent conflict and/or the use of violence (Zalman, 2014).

Manifest: A list of goods that have been loaded aboard a vessel and are approved and monitored by the captain. Also referred to as the respective vessel's cargo (AAPA, 2013b).

Maritime ports (ports): Commercial facilities where ships can dock and transfer people or cargo to or from land (AAPA, 2013b).

Maritime terrorism: Deeds and acts of terror undertaken within the maritime domain, with such deeds and acts exploiting or targeted versus vessels or facilities that are located within a harbor, port, adjacent to, or upon the water (Chalk, 2008, p. 3).

Mine countermeasures (MCM): The hunting and sweeping of mines from vital waterways (USN, 1996).

Naval mine: These weapons can be deployed in the surf zone (water that is less than 3 meters deep) to deep water (that which is deeper than 60 meters), and have high explosive payloads ranging from a few kilograms pounds to several metric tons. There are four main types of naval mines: (a) bottom; (b) buoyant moored; (c) drifting; and (d) limpet (mines attached directly to the target, such as the hull of a ship or submerged infrastructure like docks or bridge footings). These naval mines can be deployed by aircraft, boats, divers, submarines, ships, or personnel/vehicles, such as from a dock or bridges crossing waterways (USN, 2009, p. 9).

New Panamax ship: A vessel that transports containers that is designed to precisely fit the locks that comprise the expanded Panama Canal. New Panamax ships—also referred to as *NPXs*—have a capacity of about 12,500 TEUs ("The geography of transport systems," 2015, para. 5). The expanded Panama Canal locks are to be 427 meters in length, 55 meters in width, and 18.3 meters in depth, demanding that a New Panamax ship not exceed the dimensional limit of 364 meters in length, 49 meters in width, and 17.3 meters in draft (Canal de Panamá, 2014). As of 2013, 16% of container ships were classified as New Panamax (Modernization of the Panama Canal, 2015).

Panamax ship: A container ship capable of transiting the Panama Canal's lock chambers and fitting beneath the Bridge of the Americas at Balboa, Panama. The canal's locks are 320 meters in length, 34 meters in width, and 13 meters in depth, demanding that a Panamax ship not exceed the dimensional limit of 294 meters in length, 32 meters in width, and 12 meters in draft (Maritime Connector, 2014). Panamax ships have been in operation since the opening of the Panama Canal in 1914 (Maritime Connector, 2014). As of 2013, 84% of container ships are classified as Panamax (Goforth, 2015, para. 8).

Port authority: An administrative agency that manages port facilities and property, including wharves and other infrastructure (AAPA, 2013b).

Port of call: A port where a cruise ship stops. This stop can be transitory or be the vessel's final destination (AAPA, 2013b).

Sonar: An acronym for *sound navigation and ranging*. Sonar is used to find and localize objects upon or beneath the water, and is either active—whereby sound waves

are generated and transmitted into the water—or passive—whereby ambient sounds are collected and analyzed (NOAA, 2014b).

Terminal: A location within a port for the handling of bulk or containerized cargo. Can also be referred to as a wharf (AAPA, 2013b).

Terrorism: "Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents" (22 United States Code [USC] § 2656 f (d) (2)).

TEU: See *container*.

Triple-E ship: A container ship class designed by Maersk shipping lines, an acronym for *economy of scale, energy efficiency and environmental improvement*, and capable of carrying 18,000 TEUs ("Triple-E: The world's largest ship," 2013). These vessels are also referred to as "Post New Panamax" ("The geography of transport systems," 2015, para. 6).

Assumptions

Assumptions of this study included that past cases of MCM and terrorist M/UWIED employment are relevant to future MCM and future terrorist M/UWIED attacks. Also, despite the wide variety in size and type, I assumed that all U.S. ports were likely targets of terrorist M/UWIEDs and that a coordinated attack could occur that would span the size/type spectrum. These assumptions were made in order to apply past lessons and were aligned with past terrorist attacks that sought to simultaneously hit multiple targets to maximize effect as related to their goal of inflicting economic damage, panic, and mass casualties.

Scope and Delimitations

The scope of this research included an examination of post-9/11 port security management as related to preventing terrorist mine warfare attacks. This case study encompassed port security management; organizations—public and private—responsible for port security as related to MCM; employment of MCM and terrorist M/UWIED attacks since the Second World War (WWII); current MCM tactics and technologies; and GST. Furthermore, drawn from the population of 361 U.S. maritime ports, the scope of the study included a nonrandom sample of convenience of two ports in California.

The scope of this study did not include intelligence gathering methods, and the assumptions of this study included that all terrorist groups seek ways to attack the United States; that the M/UWIEDs threat vector falls within the means of terrorist organizations; and that there is a generalized threat to U.S. maritime ports from terrorist M/UWIEDs.

The scope of this case study included only current MCM tactics and technologies. Any classified technologies and the new tactics they may impose in the future are likely to fall in the realm of unmanned underwater vehicles (UUVs). Such systems exist and their tactics are known, and classified systems are likely to only improve existing capabilities, not establish paradigm shifts in either minehunting or minesweeping.

The case study's delimiter—the boundary between separate, independent regions of data—was to not examine port security related to military vessel anchorages/wharfage due to restricted classification of such information. Though U.S. commercial maritime ports often host military vessels, this study focused on the commercial vessels that utilize

such shared facilities. Despite said delimiter, the study was not limited in its relevance, and the findings are readily transferable.

This research—though relevant to U.S. homeland port security policy, the nation's expeditionary forces engaged in capturing, securing, or defending foreign ports, or its allies and friends abroad—is transferable to littoral (coastal environment) and open ocean MCM. Despite this relevance, the research had certain limitations.

Limitations

This study used data and studies available to the public, and I could not use those of a classified nature. The Homeland Security Act and MTSA created safeguards for sensitive security information. Information may be designated as sensitive when a release would be harmful to security; expose private, confidential, or trade specific information; or would represent an unjustified invasion of privacy (DHS, 2009, p. 77).

This limitation, however, did not impede the relevance of this case study as classified information likely regarded (a) intelligence gathering methods, and/or intelligence regarding the threat level of terrorism to ports, and/or the specific goals of a group of terrorist regarding use of M/UWIEDs within U.S. maritime ports; and (b) so-called *black* MCM technologies (those not yet revealed to the public realm).

I had no relevant biases/conflicts of interests that would affect my role as an independent observer.

Significance

This case study is important as the findings will further academic literature by filling an existing research gap regarding port security management. MTSA and the

SAFE Port Act were both written and enacted to enhance port security in the aftershock of the 9/11 terrorist attacks. Bennett (2008) and Caldwell (2012) summarized these two acts and the subsequent policy they provided. Clark et al. (2007) examined the state of port security and found that, despite improvements, port security management still lacked in several areas and that U.S. maritime ports remained vulnerable to terrorism. Dowd (2004) and Evans and Stutin (2006) discussed the threat of mines to U.S. naval forces operating within the homeland's maritime domain or deployed abroad. This focus on military ports and warships resulted from the U.S.S. *Cole* attack. For this case study, however, I examined the threat of terrorist M/UWIEDs to MTS. Furthermore, by outlining port security management improvements implemented since 9/11 and extrapolating areas for potential reform of port security management related to terrorist M/UWIEDs, this case study added to the foundation of knowledge upon which key policy makers and stakeholders base decisions and policy. The findings of this study will contribute to positive social change by advancing efficacy of U.S. counterterrorism, mine warfare, and port security, thereby contributing to overall homeland security.

This study rests upon the goal of positive social change. Due to societal reliance upon maritime trade for economic wellbeing and maintenance of the standard of living, port security is a major issue in the United States. Because maritime transport is the foundation upon which modern globalized society rests, it is essential that the entire spectrum of threats to the MTS be recognized, that security of the system be enhanced and maintained, and that security measures not become burdensome by impeding commerce and increasing costs of goods.

Summary

The United States is a target of terrorism. Terrorists seek to inflict economic damage, panic, and mass casualties. Designated as CIKR, U.S. maritime ports are vulnerable to a spectrum of terrorist threats that include containers loaded with CBRNEs, vessels that seek to ram other ships or infrastructure, and water-borne improvised explosive devices—the dreaded small boat suicide attack. Though these threat vectors receive the majority of attention, funding, and security management policy, they are not the only means by which terror could be brought to U.S. maritime ports (Caldwell, 2007; Renuart & Egli, 2008; Rodeman, 2003; Neffenger, 2013; USN, 2009).

I outlined in Chapter 1 the threat to U.S. maritime ports from terrorist M/UWIEDs. The purpose of my case study was to explore mitigation of this threat and to discover steps to take in order to reform or supplement security management, thereby advancing overall operations within the MTS, as well as the development of recommendations for bureaucratic and policy reform. Furthermore, in Chapter 1, I outlined the three research questions of the study and the use of GST as a framework, as well as the nature, definitions, assumptions, delimitations, limitations, and significance of the study. In Chapter 2, I present a comprehensive review of the literature; in Chapter 3: the research methodology; in Chapter 4: results; and in Chapter 5: interpretations, implications, and recommendations.

Chapter 2: Literature Review

Introduction

This case study concerned the threat of terrorist M/UWIEDs to U.S. maritime ports and potential steps that policy maker and stakeholders should take to reform or supplement security management with a view towards advancing operations within the MTS. The purpose of my case study was to examine areas of modern naval mine warfare and terrorism as related to the CIKR of U.S. maritime ports to increase understanding of the terrorist M/UWIED threat to U.S. maritime ports, to explore means of mitigating this threat, and to develop recommendations for bureaucratic and policy reform.

The acts of terror perpetrated on 9/11 by the militant Islamic fundamentalist group al-Qaeda were a hard lesson for the United States. Since the 1990s, al-Qaeda has been the predominant terrorist threat to the United States, its allies, friends, and forces abroad (White House National Security Council [NSC], 2006, p. 1). “Al-Qaeda is a transnational movement fueled by a radical ideology of hatred, oppression, and murder, in concert with increased technology and globalization” (NSC, 2006, p. 1). Al-Qaeda and its network have been responsible for planning and executing multiple terrorist attacks, including those perpetrated on 9/11. "Organizations that employ terrorism as their principle means of action lack the capability to persist in open armed contest with regular government forces" (Project on Defense Alternatives, 2002, p. 1). Although terrorism is a tactic, terrorist organizations use this tactic to realize strategic aims. Maritime ports happen to be soft (unarmored/undefended) high value (strategic) targets.

Maritime ports are among U.S. infrastructure and resources deemed critical under the NIPP. The United States is part of a globalized economic system that requires just-in-time supply, and ships that pass through maritime ports move most—over 90%—of the nation's vast amount of trade (USN, 2009, p. 25). The 9/11 attacks showed that terrorists could exploit vulnerabilities in the United States' vast transportation systems. Maritime ports are part of this system, and their vulnerabilities are ripe for misuse. A spectrum of potential threats faces those responsible for port security management. One of these is the terrorist M/UWIED.

The potential consequences of a terrorist M/UWIED attack upon the United States are enormous (Dowd, 2004, p. 3). By using or threatening the use of M/UWIEDs, terrorists could advance their economic, military, or political ends, including accompanying psychological effects (Truver, 2007, p.46). The laying of terrorist M/UWIEDs in U.S. channels and harbors would accomplish profound effects, especially considering the transit of cruise ships or ferries transporting thousands of people, as well as USCG or USN vessels. If used as part of an expansive campaign across multiple locations and facilities, a terrorist M/UWIED attack could have disastrous economic and psychological impact. The DHS (as cited in DOD, 2009) recently expressed:

> We are increasingly concerned with terrorists using [naval] mines or underwater improvised explosive devices in domestic U.S. ports and waterways.
>
> …[T]errorists can use these weapons for military effects and psychological terror—with the potential for significant harm to the global economy. (p. 3)

When considering defense from terrorist naval mining of U.S. maritime ports, the central problem is one of imparting security while minimizing impact upon commerce. The impediment of commerce is the greatest threat posed by terrorist M/UWIEDs and is why these weapons have the potential to deal a massive blow to the U.S. economy, perhaps even crippling it (Truver, 2007, p. 46). Many ports are strategic sealift ports, whereby the United States relies upon their infrastructure to send and receive by sea forces and materiel essential to the defense of the nation. Therefore, maritime ports are critical infrastructure whose accessibility must remain uninterrupted (Evans & Stutin, 2006, p. 26). This means that examination of the terrorist M/UWIED threat is highly relevant to both homeland security and general infrastructure policy.

In Chapter 2, I iterate the case study's framework and provide a literature review related to key concepts. This next section of Chapter 2 outlines the literature search—exhaustive in breadth and depth—followed by the theoretical framework of the study, as well as a literature review focused on the concepts of naval mine warfare, port security, and terrorism.

Literature Search Strategy

Multiple databases were used for this study, including: EBSCO; Google Scholar (retrieving only peer-reviewed scholarly works from this search engine); Homeland Security Digital Library; International Security & Counter Terrorism Reference Center; LexisNexis Academic; Military and Government Collection; ProQuest Central and Dissertations; Political Science Complete; Political Science: A SAGE Full-text

Collection; U.S. Naval Institute Archives; and, Walden University's Academic Complete and Thoreau.

Search words and terms included *asymmetric threat*; *bureaucracy*; *case study*; *coast guard*; *general systems theory*; *maritime security*; *maritime terrorism*; *mines*; *mine countermeasures*; *MCM*; *mine warfare*; *naval warfare*; *port security*; *qualitative study*; *terrorism*; and, *underwater improvised explosive devices*. For germane scholarship across the searchable databases, different Boolean combinations of terms were used to yield the broadest number of relevant and current sources.

For all searches, I used the earliest available start points and terminated with September 11, 2014, and I emphasized peer-reviewed and scholarly sources produced within the last decade, especially those conducted within the last 5 years. The scope of the literature included peer-reviewed articles; books; journals; theses; and, U.S. government-published assessments, legislation, and policy statements.

I found few examples of peer-reviewed scholarly work regarding the threat from terrorist M/UWIEDs to U.S. maritime ports, and government data covering this threat vector were scant. Though I used the full range of databases and search words/terms, results were still limited, and this therefore further justified this topic as worthy of doctoral research. All scholarly literature that I retrieved from the aforementioned search was combined with that of general homeland and port security for review.

Theoretical Framework

This study used GST (von Bertalanffy, 1969) to make distinctions and organize ideas. GST seeks to understand the interaction of multiple elements, aims to understand

this interaction from multiple perspectives, and uses an approach that is holistic in outlook (Skyttner, 2006, p. 3). Holistic thinking seeks universality (a universal worldview).

Said universality is expressed in mechanistic terms and finds internal structure and causal laws. "Just as one cogwheel drives and influences the other in a rational way, a measurable cause always produces a measurable effect in any rational system" (Skyttner, 2006, p. 14). Von Bertalanffy (1969) also recognized that views and data are prejudiced by time-dependent models (Skyttner, 2006, p. 5) and that a system progresses from the whole to its parts. This deconstruction—called *synthesis* in GST—first identifies the overall system (in the case of this study: homeland security) of which the unit in focus (port security) is a part. Properties or behavior of the system are explained and, finally, the properties or behavior of the unit in focus as a part or function of the system. Therefore, GST seeks to explain versus simply describe (Skyttner, 2006, p. 34), thereby expanding the focus of the observer, and, in doing so, the theory attempted to resolve a crisis of classical science.

This crisis arose when attempts at explaining biological and social phenomena fell short. Recognition of emergent properties of living organisms in the 1920s, and the failure of scientific analysis to explain such phenomena, demanded a new approach (Skyttner, 2006, pp. 35-36). During the 1930s, von Bertalanffy formulated ideas, and then went on to found the American Association for the Advancement of Science with Miller in 1956.

Conceived at the Stanford Center for Advanced Study in the Behavioral Sciences by von Bertalanffy, Boulding, Gerard, and Rapoport (International Society for the Systems Sciences [ISSS], 2014), GST came into its own during the 1950s with the decade's plunge into the atomic, computer, and space ages. Von Bertalanffy's (1969) paper on GST appeared in the journal Science, and the work became a classic in the school of thought (Skyttner, 2006, pp. 35-36). With this recognition and an administrative reorganization, the American Association for the Advancement of Science became the ISSS in 1988 (ISSS, 2014).

Von Bertalanffy's (1969) paper espoused that systems had general features that operate independently of the scientific disciplines to which they belonged. In his paper, and working with Boulding, von Bertalanffy sought to create a universal science, and to link splintered areas of study with a *law of laws*. To accomplish this, von Bertalanffy proposed integrating associations and parallels within science; promoting communication across disciplines; and, establishing a theoretical foundation for broad scientific education (Skyttner, 2006, p. 39). Within this framework, GST had been established.

GST deals with features of systems on a nonrepresentational level. The theory can be applied regardless of domain or physical form of a system. The theory recognizes that all systems—abstract, concrete, conceptual, manmade, or natural—share common characteristics, and that they all help us describe human existence. With this premise, GST cut across disciplines, and recognized that emergence—the birth of complex patterns (systems) by a collection of comparatively simple collaborations—resulted from

the interaction of independent parts (Skyttner, 2006, p. 40). U.S. port security is such a system; primarily one of organizations.

According to GST, organizations are produced by the society that surrounds them and the needs they serve (Skyttner, 2006, p. 352). Organizations have become "the most characteristic and powerful human system of our time" (Skyttner, 2006, p. 353). Organizations are human creations, fragile yet robust. Ironically, though created by biological beings, organizations often outlive them. However, they can also be undermined or destroyed by the behavior of a single biological being (Skyttner, 2006, p. 354). In GST, an organization has units; makes choices, and attempts to apply and enhance them; regulates internal organization and subsystems; has an internal control system; and—perhaps most importantly—*seeks to ensure its continued existence and means of flourishing* (my italics emphasis; Skyttner, 2006, p. 355). GST employs myriad methodologies to analyze organizations and handles sweeping interweaved complex systems. GST assumes that systemic problems are similar in nature, regardless of the system from within which they originate (Skyttner, 2006, p. 457).

GST methodology can be used to design a system or to refine one that already exists (Skyttner, 2006, p. 458). GST employs steps developed primarily for cybernetics. For designing a new system, the first step is articulation of what the system should do; second, registration of what the system has done; third, differences between the first and second steps are expressed; fourth, explanation of the causes of these differences; and, fifth, controlling the system to minimize these difference (Skyttner, 2006, p. 459). When seeking to refine an existing system, a researcher begins with the problem, asking: What

are the limitations of the present system? Next, alternative solutions are generated, asking: What alternative systems are possible? Finally, the generated alternatives are evaluated by asking: What are the costs of continuing the present system and of changing to alternative systems (Skyttner, 2006, pp. 470-471)? Within this framework, GST is effective for understanding complex systems.

Maritime ports are complex systems where civilians, government, and the private sector interact. Maritime ports contain myriad infrastructure, cater to multiple modes of transportation (rail, truck, and ships), are administered by multiple agencies, and operate under an aegis of varying security management, strategy, tactics, and techniques (Plant & Young, 2007, p. 17). From a GST perspective, the MTS is a system of maritime operations. These operations interface with landside ones, doing so at intermodal links to domestic commerce and global supply chains (DHS, 2005, p. 2). It would be a difficult if not impossible endeavor to physically secure all CIKR with barriers and policing (Plant & Young, 2007, p. 17). This inadequacy applies to the CIKR of maritime ports.

The majority of U.S. maritime infrastructure is managed and/or owned by local, state, and private maritime industry (Federal Emergency Management Agency [FEMA], 2013). Therefore, multiple government and private organizations share responsibility for securing ports (DHS, 2009). With these many partners involved, port security management requires a framework from within which to identify strengths and weaknesses.

"Systems thinking imparts a rich language for describing a vast array of interrelationships and patterns of change" (Senge, 1990, p. 73), and allowed me to

examine the system of port security as related to terrorist M/UWIEDs, determining "deeper patterns lying behind the events and the details" (Senge, 1990, p. 73). There are often holes in outcomes/outputs in security management, especially when programs overlap, as:

> Agencies are often unable to roll up the performance claims of their constituent programs, even if they are within the same area or portfolio, because the logic and measures for program components tend to be developed separately by different individuals and subunits. (Jordan & Reed, 2007, p. 169)

The following academic and government studies incorporate a GST framework, and provide examples of application to areas and issues of U.S. national security:

In 1996, the Marine Corps Combat Development Command tasked the Center for Naval Analyses (CNA) with assessment of the application of GST to land warfare, using the theory to study physical systems that exhibited complicated dynamics. Though the study covered land warfare, the methodology exhibited the potential of GST to understand complexity and highlight deficiencies by fundamentally altering understanding of complexity. The CNA's (1996) study contributed to the understanding of a new paradigm in land warfare by amphibious forces, and set a new tradition in coupling GST with general military theory (Ilachinski, 1996).

GST has also been used to formulate strategy and subordinate tactics, unifying uncoordinated compartmentalized functions, and aligning them with policy and goals. An example of this is Colonel Warden's Air Theory for the Twenty-first Century. This theory offered a "five ring system" that shepherded a new age of systematic wartime

aerial targeting by analyzing the theretofore haphazard system of target selection, and, discovering and highlighting deficiencies, established procedures that dramatically improved systems. Though Jackson (2000) found that the resultant system sidestepped legal and moral implications of aerial targeting, and the potential of tactics to conflict with international law, Warden's analysis did not include such factors, and the resultant "five ring system theory" encompassed a purely military design. Such a weakness, however, can be rectified in other studies that employ GST as a framework by including such considerations.

Schwan (2012) employed a GST framework to examine U.S. border security endeavors, and found them to be compartmentalized, fragmented, and poorly coordinated. Furthermore, Schwan (2012) found limited collaboration with international partners, and extrapolated that effective border control is reliant upon broad cooperation. This study addressed general border security management by using a systems approach by examining all borders (land and maritime) as well as associated border security institutions, and attempted to determine systemic reasons for ineffectiveness (Schwan, 2012).

GST is also applicable to understanding the terrorist adversary and the groups they represent. Larsen, Haugh, and Lichtblau (2006) employed the GST framework to find additional means of combating global terrorism by asking, how could terrorists be analyzed as complex adaptive systems; finding them to be just that. Larsen et al.'s (2006) study iterated the usefulness of GST as a method of analyzing terrorism and similar phenomena.

Literature Review Related to Key Concepts

In this section of Chapter 2 I begin with a review of the literature on terrorism, focusing on maritime terrorism. Then I review mine warfare—including the weapons, MIL, and, MCM—then; U.S. MCM operations in combat situations ranging from the Korean War (1950-1953) to the Libyan Civil War (2011). Further in Chapter 2 I then review U.S. MCM in counterterror operations; potential terrorist tactics employing M/UWIEDs; current MCM—the exercises, helicopters, ships, marine mammals, and people—and; future MCM—the ships and systems, including new unmanned ones. Finally, this section reviews port security: the facilities, legislation, and organizations.

Terrorism

The phenomenon of terrorism lies at the core of this study. I used the definition provided by Title 22 of the USC, as adopted by the National Counter Terrorism Center, in that terrorism is: “Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents” (22 USC § 2656 f (d) (2)). Terrorism is a tactic born of weakness. "[Terrorists] compensate for this weakness through stealth and by choosing soft, high value targets" (Project on Defense Alternatives, 2002, p. 1).

Since the 1990s, al-Qaeda has been the predominant terrorist threat to the United States, its allies, friends, and forces abroad. “…al-Qaeda is a transnational movement fueled by a radical ideology of hatred, oppression, and murder,” and abuses technology and globalization (NSC, 2006, p. 1). This militant Islamic organization and its network

have been responsible for planning and executing multiple terror attacks, including those devastating ones of 9/11.

Since the attacks of 9/11, al-Qaeda's nature has continued to evolve, and has changed dramatically specifically during the past decade, making the effort to interdict and dismantle the organization a fluid and unpredictable one (Renuart & Egli, 2008, p. 16). Though many al-Qaeda leaders have been captured or killed, and the organization's communications, finances, and training camps have been disrupted, a network of various militant groups has been established and link previously disparate groups. These groups all espouse a shared goal: to hurt the United States, its interests, and its people. Though al-Qaeda's role in leader-down planning of terror attacks has been diminished, it has franchised its brand of devastating and synchronized violence to groups around the globe. Ideology and religion, as well as a shared fanatical zealousness is the bond of this global web, making al-Qaeda stronger as an ideology than it is as an organization (Richardson, 2004, pp. 28-30). One of these al-Qaeda franchisees is the Khorasan Group.

Khorasan denotes greater Afghanistan, parts of central Asia, and the Xinjiang province of the People's Republic of China. Khorasan Group is unlike the Islamic State of Iraq and the Levant—known as ISIS or ISIL—, which wants to establish an Islamic kingdom that spans modern day Iraq and Syria by grabbing land and governing it. Instead, Khorasan instead seeks to attack the West in spectacular fashion (Levine, Gordon-Meek, Thomas, & Ferran, 2014). According to Levine et al.'s (2014), 50 hardened fighters, all sharing jihadist affiliations, comprise the Khorasan Group, and are

"plotting and planning imminent attacks against Western targets to include the U.S. homeland." (para. 21)

For the purposes of this study, besides such jihadi groups, terrorism included all "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents" (22 USC § 2656 f (d) (2)) as perpetrated by foreign national irregular forces/operatives, transnational organized crime networks that include drug, human and weapon smuggling, and environmental criminals (Neffenger, 2013, p. 18), as well as domestic individuals or groups. All such "terrorists" are relevant to the M/UWIED threat to ports.

Regarding the domestic threat, there were, prior to 9/11, several domestic terrorists that were active, including infamous persona such as the Oklahoma City Federal Building bombers McVeigh and Rudolph. Furthermore, one domestic terrorist was active post 9/11: the Beltway Sniper Williams, aka: Mohammad (Clark et al., 2007, p. 99). Such domestic terrorist have motivations that range from antigovernment, to religious convictions, and the imposition of anarchy. It is not beyond the imagination that, besides the substantial foreign threat, that domestic terrorists could seek to cause harm the United States, or create chaos within it by attacking maritime ports. However, attack scenarios are inevitably drawn back to those that have already occurred…

The 9/11 attacks exploited aviation and there have been multiple land-based attacks such as truck bombings—for example, the Oklahoma City Federal Building bombing perpetrated by McVeigh/Randolph. Because of the devastation associated with aviation and land-based attacks, security awareness has increased in these areas and

associated modes of transport hardened. Because of this fact, commercial shipping and the maritime domain has become a more attractive target to terrorists (Rodeman, 2003, p. 6). Over the next decade, globalization and population growth will expand maritime activity, and, therefore, threats to the U.S. maritime domain will increase, too (Neffenger, 2013, p. 21).

Maritime terrorism. Maritime terrorism describes acts of violence upon or beneath water. These acts are carried out by terrorists to further their tactical or strategic goals (Nelson, 2012, p. 15). The Council for Security Cooperation in the Asia Pacific defines maritime terrorism as:

> The undertaking of terrorist acts and activities (1) within the maritime environment, (2) using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, (3) against coastal facilities or settlements, including tourist resorts, port areas, and port towns or cities. (Chalk, 2008, p. 3)

It is known that "transnational criminals, pirates, and *terrorists* [my italics emphasis] seek to exploit the complexity of the maritime domain and the vulnerabilities of the global supply system" (USCG, 2007, p. 5). Due to the organization's enmity to U.S. interests and responsibility for past attacks, national security policy has been focused on Al-Qaeda. However, individuals or organizations not associated with al-Qaeda could strike the United States (Parfomak & Frittelli, 2007, p. 2). According to the U.S. Department of State (2006), al-Qaeda is now "a more diffuse worldwide movement of like-minded individuals and small groups, sharing grievances and objectives, but that

are not necessarily organized formally" (p. 13). With this change from a relatively structured organization to a decentralized movement comprising multiple terrorist groups, maritime terrorism scenarios will need to contemplate a wide gamut of potential perpetrators.

Regardless of the perpetrating individual or group, terrorists choose maritime targets that are symbolic, and are of an economic, civilian, environmental, and/or military nature. Such targets could include oil tankers and oil platforms; cruise ships and ferries; hazardous/volatile carriers, such as chemical or liquid natural gas tankers; and, warships (Murphy, 2008, pp. 200-212).

Tactics employed by terrorists in the maritime domain fall into two categories: attacks upon ships while they are in port; and attacks upon ships while they are at sea (Rodeman, 2003, p. 7). Terrorists can place explosives aboard a ship and detonate them directly or remotely (Murphy, 2008, pp. 212-213); terrorists could use ships as weapons by piloting them into another ship—likely one carrying hazardous or volatile cargo—or into port infrastructure; or, terrorists could smuggle a CBRNE into a port and activate/detonate it (Chalk, 2008, p. 26).

There are several reasons why the maritime vector of attack is attractive to terrorists: (a) vulnerabilities permeate this domain. These vulnerabilities include poor surveillance, weak port security, an excess of targets, reliance on crowded chokepoints and waterways, and a tendency to crew vessels with minimal personnel; (b) enterprises specializing in water equipment and sports that provide terrorists with training and resources for operating at sea; (c) economic destabilization caused by the

blocking/shutting down of a port (Chalk, 2008, pp. 21-22); (d) mass coercion of enemy audiences—many people confined in a one space, such as a cruise ship or ferry; and (e) the pervasive cargo container system that gives terrorists a means to covertly move personnel and weapons (Chalk, 2008, pp. 25-26).

The nature of the terrorist threat to U.S. maritime ports is unique. Gone are the days of Nazi U-boats or Soviet submarines lurking off the national coast and ports. During WWII and the Cold War, the U.S. leaders knew the enemy, its capabilities, procedures, tactics, techniques, and weapon systems, and could make a reasonable assessment as to which axis of attack the threat would originate from. Today, the terrorist enemy cannot be expected to launch an attack from one direction, and, therefore, U.S. defensive forces cannot align towards a recognized threat direction to dissuade the threat. This makes the threat asymmetric, a threat that seeks to target not only the military of the United States, but its economy, ideology, and people. Terrorists also have at their disposal several means of attacking U.S. maritime ports. Among these are M/UWIEDs, a threat that, time after time, is given only cursory mention or neglected all together in threat assessments and policy formulations. However, before examining the threat of M/UWIEDs to U.S. maritime ports, a basic understanding of mine warfare was necessary.

Mine Warfare

The primary objective of a naval minefield is to prevent entry and use of an area, and is not specifically to damage, destroy, or sink a vessel. The presence of M/UWIED or uncertainty of their presence raises questions for the defender, such as: What weapons are

actually in the water; and, where are they? (Savitz, 2006). Mine warfare comprises the weapons themselves, as well as two categories of capabilities and operations: MIL and MCM.

The weapons. There are several types of naval mines and methods of detonation, with any improvised versions likely to fall into these general categories:

Bottom mines. These weapons rest proud on the seafloor, are immobilized by their own weight, and are often buried under sediment to thwart countermeasures. When meant to attack surface targets, bottom mines are most effective when laid in shallow water; that which is less than 60 meters in depth (Truver, 2012, p. 34).

Moored mines. These anchored weapons incorporate an air space that allows the mine case to become buoyant, floating at a respective depth in the water column, including those that float just above the sea floor, those that are *in volume*—floating midwater—, and, those floating near or just beneath the water's surface. There are moored mine types with torpedo or rocket payloads (USN, 2009, p. 9). The radius of damage from a moored mine tends to be less than that inflicted by a bottom mine (Truver, 2012, p. 34).

Floating mines. These weapons are neutrally or positively buoyant and float on or near the surface. As they are not anchored or tethered, floating mines drift with prevailing currents and tides. Some floating mines are of the oscillating type, in that, though adrift, rise and fall between two preset depths. These weapon types are addressed by international law, which stipulates that moored naval mines must deactivate or self-detonate within an hour of breaking free of their anchor, and places an outright ban on

freely drifting types. Despite this prohibition, most drifting mines continue to be available and used (USN, 2009, p. 10), and some might ignore international law and allow such mines to drift freely (Truver, 2012, p. 34).

Limpet mines. These weapons are directly placed upon and attached to a targeted surface, such as the hull of a ship or upon infrastructure, such as the submerged support structure of a rail or road bridge. Limpet mines have a timer and can be set to explode shortly after placement, or several days later (USN, 2009, p. 10). Limpet mines require a frogman or submersible to approach a vessel and physically attach the mine to the hull. Such underwater strikes are—according to professional divers with military experience—complicated at best due to poor visibility, and usually strong currents and tidal flows. For example, with Port of Rotterdam Police approval, professional divers executed an underwater approach to a moored vessel, finding the dark water and loud engine noise tough to overcome (Richardson, 2004, p. 22). However, despite such challenges and dependent on specific port conditions, such attacks are feasible.

Regardless of type, naval mines can be detonated by: (a) contact, when their casing or appendages contact a target; (b) influence, when sophisticated sensors—acoustic, magnetic, pressure, seismic, underwater electrical potential, and video –detect a target; or, (c) command, when the weapon is fired by direct order of the miner (Truver, 2012, pp. 35-36). According to Vice Admiral Connor, Commander, Submarine Forces: "The torpedo of the future and the offensive mine of the future will be hard to distinguish" (Edwards and Gallagher, 2014, p. 71).

MIL. The concept of the naval mine began with *Greek fire*, an incendiary weapon used to defend Constantinople in the year 673. Naval mines were first used by Americans in 1776. Called *torpedoes* at the time, the experimental submarine *Turtle* attempted to attach a limpet mine to the hull of HMS *Eagle*, a Royal Navy ship of the line anchored in the Hudson River. The first effective use of naval mines by the USN was during the War of 1812, denying entry to the Port of New York by British forces. The last time the USN used offensive mining was during the 1991 Gulf War when four A-6 Intruder bombers laid a field at the mouth of the Kwahr Az Zubayr River to thwart Iraqi freedom of navigation in the northern Persian Gulf (21st Century U.S. Navy mine warfare, 2012, p. 56).

In time of war, the primary goal of a naval minefield is to block access to a beach, coast, harbor, port, or waterway, and not to damage, destroy, or sink a vessel. However, M/UWIEDs may be specifically laid to damage or destroy. Naval mines, or the potential that mines have been laid, create psychological uncertainty that allows the weapons to impose effects, even without being fired (Truver, 2012, p. 35).

Naval mines are designed for operations in the spectrum of water depths. This ranges from the surf/craft landing zone—less than three meter water depth—to deep water—greater than 60 meters—, and can be used in defensive or offensive modes either to directly attack enemy vessels or to protect friendly vessels or a maritime area (Truver, 2012, p. 34). The deployment depths of these naval mine types are referred to in Figure 1.

SURF ZONE 0 m – 3 m	VERY SHALLOW WATER 3 m – 12 m	SHALLOW WATER 12 m– 60 m	DEEP WATER Over 60 m
Bottom			
Moored			
Floating			
		Rising	

Figure 1. Mine threat spectrum. Adapted from 21st Century U.S. Navy mine warfare: Ensuring global access and commerce (p. 9), by U.S. Navy, 2009. Program Executive Office Littoral and Mine Warfare/Expeditionary Warfare Directorate. Washington, DC: U.S. Department of Defense.

MCM. Countering mines that have been laid is a slow, tedious, and resource-intensive process that involves specialized personnel and equipment (Dowd, 2004, p. 6).

The best MCM operations prevent minelayers from deploying their weapons, as, once laid, mines are hard to find, classify, and nullify (Truver, 2012, p. 36). Therefore, intelligence is the greatest MCM tool, and allows kinetic attack on assembly facilities, depots, and potential minelayers. Such preemptive attack is in line with the general counterterrorism strategy of the United States, whereby actionable intelligence is used to target attack aircraft, cruise missiles, naval fire, and special operations to interdict such threats. However, should terrorist M/UWIEDs be laid successfully, standard MCM operations are initiated. Such operations consist of minehunting and minesweeping.

Minehunting. Minehunting consists of detection, classification, localization, identification, and neutralization of the enemy weapon, with sonar representing the most effective method for detecting and classifying mine-like contacts. If a contact is determined to be mine-like, trained divers, marine mammals, or equipment such as video cameras and laser systems on UUVs can investigate the contact from beneath the surface, or by hull mounted or aerial-towed sonars that can be used from above the surface. Once

a mine-like object has been positively identified as a mine, it must be destroyed, isolated, neutralized, or rendered safe (Truver, 2012, p. 37). This process is called minesweeping.

Minesweeping. This involves trawling specific areas of water with mechanical or influence systems to destroy mines. Mechanical systems seek to cut the tether of moored mines, or physically damage the mines, such as dragging chains to cut control wires. Once mechanically swept, the mines must be destroyed or rendered safe. Influence systems seek to stimulate the acoustic, electrical, magnetic, or pressure detonator so that the mine fires harmlessly (Truver, 2012, p. 37).

MCM in combat operations. MCM figured prominently during WWII, Korea, and Vietnam, numerous crises of the Cold War, Operation Desert Storm and Operation Iraqi Freedom, as well as the recent Libyan Civil War intervention. These examples exhibit the difficulty of interdicting clandestine laying operations, primarily due to the ease by which vessels can be disguised and blend in with legitimate maritime traffic.

Korea. The Korean War was the first United States experience with naval mines after WWII. During this conflict, North Korea placed more than 3,000 mines off its east coast, deploying them in a matter of weeks. This deployment utterly frustrated a United Nations amphibious task force and its plan to assault the port city of Wonsan in October 1950. Commanding the 250 ship task force, Rear Admiral Smith stated: "We have lost control of the seas to a nation without a navy, using pre-World War I weapons, laid by vessels that were utilized at the time of the birth of Christ." During clearance operations, three coalition MCM vessels were sunk by mines, resulting in the death or wounding of more than 100 personnel. By July 1953—the end of the Korean War— though coalition

MCM forces represented just 2% of all United Nations's naval forces, they had suffered 20% of overall naval casualties (Truver, 2012, p. 31). This debacle spurred broad U.S. MCM research and development, experimentation, and procurement, with national shipyards delivering upwards of 250 surface MCM vessels for national and allied navies (USN, 2009, p. 5).

Vietnam. U.S. forces used aircraft to lay some 11,000 naval mines in Vietnamese coastal rivers and waters. This campaign virtually halted all North Vietnamese water-borne trade and operations, including the entrapment of multiple Soviet Bloc vessels in the ports of North Vietnam. The USN then mined Haiphong Harbor in May 1972, a campaign that many have credited with bringing North Vietnam to the Paris Peace Talks table.

Though the mining of Haiphong Harbor represented offensive mining, it is relevant to MCM and, therefore, this study, in that the resultant Paris Peace Accords stipulated that the United States agree to clear these naval mines. Said clearance was accomplished in a campaign called Operation End Sweep, a 7 month long operation that saw the first use of helicopter-borne MCM capabilities (USN, 2009, p. 5).

During the Vietnam War, the North Vietnam Army and Vietcong guerillas designed and laid a plethora of M/UWIEDs—from floating baskets full of explosives to 2,000 pound command detonated types—in the country's deltas and rivers. During the 2 decades of conflict, two U.S. warships struck M/UWIEDs (Truver, 2008, p. 110).

Arabian Gulf tanker wars. During the 1987 Operation Earnest Will, the United States had reflagged and began to escort Kuwaiti tankers through the Persian Gulf as they

were under threat of an Iranian naval mine campaign that promised to close the Straits of Hormuz; the spigot that flowed Middle Eastern oil to the world. The weapons—primarily floating types—provided an indirect means for Iran to punish conservative Gulf states for their support of Iraq during the first Gulf war, as well as claim that God supported the Islamic Republic's struggle by steering ships into the mines. Despite being escorted by the USN guided missile destroyer U.S.S. *Kidd*, on July 24, 1987, near Iran's Farsi Island, a mine blasted the reflagged and renamed Kuwaiti crude oil supertanker *Bridgeton*, formerly the *al-Rekkah* (Richey, 1987).

Hit on the port side about 60 meters from the bow, *Bridgeton* would have played a primary role in the U.S. escort operation by acting as a shuttle, carrying oil for transfer to other vessels waiting outside the gulf ("Reflagged tanker crippled by mine," 1987). With the prospect that more mines could have been laid along the 1,200 kilometer tanker convoy route, the United States had to ask its European allies for minesweeping help. Just days after the *Bridgeton* had been crippled a mine was sighted in waters some 257 kilometers ahead of another convoy of reflagged tankers. This brought the convoy to a standstill off the Saudi Arabian coast while, later that same day, the Panamanian tanker Texaco Caribbean struck a mine (Richey, 1987).

Both the USN and commercial shipping had been delivered a cold harsh message: Naval mines could circumvent the world's most powerful navy and threaten the global economy's energy supply. Several Soviet designed 242 pound mines were found to have been laid in the main deepwater shipping channel that led into Kuwait ("Reflagged tanker crippled by mine," 1987). On April 14, 1987, a U.S. guided missile frigate—the U.S.S.

Roberts—struck an Iranian mine. Though the mine blew a five meter hole in the hull, broke engine mounts, and cracked the ship's keel, the crew was able to fight the fires and keep the warship afloat. This encounter showed how a low tech, $1,500 mine could impede freedom of navigation and control of the sea, and inflict disproportionate damage—some $96 million worth—to a billion dollar vessel (USN, 2009, p. 5).

Desert Shield/Storm. The defensive operation that preceded the offensive one of Desert Storm was called Desert Shield. During this operational period the USN lost control of the northern Arabian Gulf to Iraq. This was not due to Iraq's superior naval forces, however. Though Iraq possessed a vastly inferior navy, they laid over 1,300 naval mines. Despite being under the surveillance of multinational coalition naval forces, these enemy minelaying operations succeeded and severely damage two USN warships, forcing coalition commanders to abandon a planned amphibious assault out of fear of more casualties (Truver, 2012, p. 30).

The abandoned amphibious assault left 30,000 U.S. Marines at sea on their ships, and checked the world's largest, most powerful amphibious force. Immediately following the conclusion of hostilities, operations were begun to clear these enemy naval mines. However, this effort took several years, even though facilitated by the use of captured minefield maps (USN, 2009, p. 6).

Operation Iraqi Freedom. As opposed to the campaigns of the 1980s and 1990s, the 2003 Iraq War represented a highly successful MCM effort. Wary of the frustrating mine warfare experience delivered by Baghdad during Operation Desert Storm, the United States assumed that the northern Arabian Gulf would be heavily mined. Though

Iraqi forces were able to lay several mines, coalition special operations forces seized numerous Iraqi improvised minelayers that included barges and tugboats, with each having more than 100 types of naval mines aboard. Despite this camouflaged enemy MIL activity, coalition teams were able to sweep those mines that had already been laid, allowing humanitarian aid ships to offload vital supplies in captured Iraqi ports (Paulsen, 2003; USN, 2009, p. 7).

Libya. On April 29, 2011, during the U.S.-led allied Operation Unified Protector, Libyan government forces attempted to close the Libyan port city of Misratah by laying moored contact mines outside the harbor entrance. The mines were deployed from rubber boats which were then sunk. Blocking aid and preventing the evacuation of foreigners and wounded from the besieged city was the objective of this MIL operation (Lekic, 2011). Despite a heavy North Atlantic Treaty Organization [NATO] naval presence, several mines were set and activated, though others broke free of their moorings and went adrift.

NATO warships that patrolled the area quickly discovered the minefield, and interdicted it prior to its completion ("Libyan government threatens aid," 2011). "It…shows his [Qaddafi's] complete disregard for international law and his willingness to attack humanitarian delivery efforts," said British Brigadier General Weighill, director of NATO operations in Libya. According to international law, any nation engaged in laying naval mines is to notify shipping to the general location of the minefield. NATO minesweepers moved in and swept the port's approaches, readily clearing those mines that threatened shipping (Lekic, 2011).

Past terrorist M/UWIED attacks. There have been several instances of terrorist bottom, moored, and floating M/UWIEDs.

In January of 1980, during the U.S. grain embargo of the Soviet Union, an unknown person telephoned a naval mine threat in to authorities, claiming to have laid M/UWIEDs in the channel of the Sacramento River using a self-contained underwater breathing apparatus (SCUBA). Called the *Patriotic Diver* by authorities, this act of terror shut down all shipping movements on the river, and forced the USN to deploy a MCM vessel to the river way, which conducted several days of intensive minesweeping.

The Patriotic Diver MCM operation cost several hundred thousand dollars in fuel/ship time, as well as merchant marine lay days (idle vessels; mariners; and, cargo). Though the threat was deemed a hoax, this example exhibits the impact that even a faked terrorist M/UWIED attack could have (USN, 2009, p. 11).

From July to September 1984 and in the Gulf of Suez portion of the Red Sea, 23 vessels that were transiting the waterway suffered damage from underwater explosions. This occurrence spurred a massive multinational MCM effort that included USN assets. Though only one naval mine was recovered, it became evident that the Libyan navy had used a civilian ferry to covertly lay a minefield (USN, 2009, p. 11). This incident is an example of the ease by which M/UWIEDs could be as instruments of maritime terror, and that seemingly innocuous vessels can be used to perpetrate a campaign of terror (Truver, 2008, p. 111).

In April of 2004, upon the waters of Lake Ponchartrain, Louisiana, a tugboat operator spotted a suspicious floating object. The USCG was notified. The agency then

contacted the Jefferson Parish Bomb Squad. Upon investigation, the object was found to be an M/UWIED comprising a series of timed pipe bombs that were surrounded by an air filled bag that made the device float just below the surface (USN, 2009, p. 11). This incident exhibits the ease by which M/UWIEDs can be laid in highly trafficked domestic waters. Besides such floating M/UWIEDs, there have been several instances of use by terrorists of limpet weapon types:

Since WWII, there have been several instances where limpet mines have been used by terrorists and/or foreign national irregular forces: In 1973, M/V *Sanya* was sunk in Beirut Harbor, Lebanon, and, in 1985, M/V *Rainbow Warrior* went to the bottom of Auckland Harbour, New Zealand.

A Greek chartered cruise ship, M/V *Sanya* carried 250 U.S. tourists bound for Haifa, Israel. An explosive was attached to hull of the ship just below the waterline and detonated. The Black September Organization—also known as the Abu Nidal Organization—claimed responsibility for the attack as retaliation against Israel. Furthermore, Black September likely perpetrated a previous failed effort to mine vessels moored in the Port of Haifa (Clark et al., 2007, p. 111).

M/V *Rainbow Warrior* was the flagship of the environmental organization Greenpeace, and had arrived in New Zealand to lead a flotilla of boats in protest of French nuclear tests at Mururoa Atoll ("On this day," 2008). Agents of France's Direction Générale de la Sécurité Extérieure were tasked with preventing *Rainbow Warrior* from protesting and, after infiltrating the group and collecting intelligence on the vessel, divers had attached two limpet mines to the hull. They detonated 10 minutes apart

and sank the Greenpeace vessel ("Nuclear-free New Zealand, Page 5–Sinking the Rainbow Warrior," 2013).

In May of 2008, Tamil Sea Tigers sank the Sri Lankan logistics ship M/V *Invincible* with limpet mines. This is an example of the vulnerability of military vessels to frogman attacks while docked in port and/or moored in waterways (DHS, 2008b).

Furthermore, in 2002, Dutch counterterrorism agents investigated a diving school located southeast of Amsterdam as, enrolled in the school, was an Iraqi suspected of being an al-Qaeda recruiter. There were also several Islamic extremists that, under a Tunisian instructor, had become certified SCUBA divers. A Moroccan court later convicted one of the students for planning attacks on U.S. ships in the Strait of Gibraltar (Richardson, 2004, pp. 21-22).

Potential terrorist M/UWIED tactics. During Operation Iraqi Freedom, an Iraqi tugboat was intercepted. It carried numerous naval mines set to detonate by contact. The tugboat was disguised to look like it was carrying regular oil barrels and was configured to lay weapons with a deck mounted conveyor belt (Rios, 2005, p. 20). Other such camouflaged minelayers could also be deployed, using the cover of commercial, fishing, or pleasure vessels. Furthermore, fixed wing aircraft, helicopters, and submersibles could also be used (Truver, 2008, p. 108), and, with a high volume of genuine business and civilian traffic in ports, terrorists could mask their movements prior to an attack, complicating defenses (Watts, 2005, p. 5).

Part of the vessel threat, U.S. intelligence officials had identified by 2002 over 15 cargo vessels that are in al-Qaeda's possession or under the organization's control,

terming these ships part of *al-Qaeda's Navy* (Richardson, 2004, p. 14). Such vessels could easily blend in with, as of 2011, over 79,000 merchant vessels sailing the seas (Equasis Statistics, 2011, p. 6). Many of these merchant vessels are have hidden their ownership under layers of incorporation, and are manned by tens of thousands of seamen that often use false names and fake documentation (Richardson, 2004, p. 14). According to Linnington of the British National Union of Marine Aviation and Shipping Transport Officers, international shipping is:

> …A murky world of corruption, bribes, lawlessness, and flags of convenience. It is an industry ripe for penetration by hardened terrorist cells bent on finding new ways of wreaking havoc. Central to the problem are the states that shipping firms use as flags of convenience. A lot of the industry itself is based on quite a lot of corruption and deceit that fosters anonymity and allows unscrupulous operators. (Harris & Bright, 2001, para. 7)

Commercial vessels can easily be converted to terrorist minelayers. During the First World War (WWI), the United States converted eight civilian steamships for such purposes, with 24 more converted as mine-carrying freighters (Vere, 2014, p. 44). Fishing vessels would also be effective terrorist minelayers, especially since deck equipment such as cranes and winches are standard, and unlikely to arouse suspicion. According to the National Transportation Safety Board's 2010 count, there are 82,047 documented commercial fishing vessels in the United States.

Recreational maritime traffic within or near U.S. maritime ports are prolific, and could be used to perpetrate a terrorist M/UWIED laying operation. The most recent

USCG statistics report a total of 12,101,936 numbered (registered) recreational boats that are in operation upon U.S. waters (USCG, 2013a, p. 65). Pleasure boats can be readily converted to serve as minelayers.

During WWII, the USN drafted and converted cabin cruisers, sailing boats, and yachts into patrol boats. In one case, one yacht was stripped of its pipe organ, three marble fireplaces, and a seaplane before antisubmarine equipment was installed that included depth charges and MIL racks ("The Navy returns pleasure craft," 1944). It does not take a stretch of the imagination to understand that pleasure boats could easily be converted to nefarious purposes, including a platform for laying terrorist M/UWIEDs.

Aircraft—both helicopters and fixed wing types—have a long history of MIL, and civilian types can be converted to lay M/UWIEDs. Combat aerial MIL began on November 20, 1939 when nine German floatplanes laid a field in England's Thames Estuary (Chilstrom, 1992, p. 15). During WWII, U.S. aerial MIL was the primary means of creating large fields—mainly to harm Imperial Japanese shipping and warships (Chilstrom, 1992, p. 18)—and would again be used with effect in the Vietnam War.

In 2006 there was a Defense Agency Threat Reduction (DATR) study conducted by the U.S. Merchant Marine Academy. This DATR study included an attack on the Port of New York-New Jersey that used Italian built naval mines (Evans & Stutin, 2006, p. 19). The Port of New York and New Jersey spans land and water that belongs to two American states and, in 2010, handled 5.3 million loaded and unloaded containers. There are also cruise ship and ferry terminals within the boundaries of this megaport (Port Authority of New York & New Jersey, 2013).

This study stipulated that its naval mines were shipped to multiple post office boxes located throughout the United States, and then forwarded on to post office boxes in New Jersey. Weapon parts were then transported to, assembled, and stored in a Brooklyn, New York basement (Evans & Stutin, 2006, p. 19). It was decided that the laying of these live (as well as dummy) mines would occur before the months of September, October, and November, as these months represented peak volume for cargo at the target port (Evans & Stutin, 2006, p. 20).

The selected target for laying operations were *The Narrows*, a tidal strait that separates Brooklyn and Staten Island; the Red Hook cruise ship terminal opposite Governors Island; various anchorages; and, the port's main shipping channel (Evans & Stutin, 2006, p. 21). The DATR's study hypothetical operation used the cover of harbor dinner cruises, and chose a private yacht as the means to deliver and lay its weapons in the waters of the targeted areas. Along with dinner-specific and general vessel provisions, the M/UWIEDs were loaded and placed in the yacht's master cabin—a location that could be isolated from dinner guests—and a vessel compartment that had been outfitted with a moon pool, an opening in the hull that allows access to the water from inside the cabin. In the study, M/UWIEDs were deployed from the yacht, their locations plotted on a master chart using Global Positioning System (GPS) coordinates, and were set to activate 2 months after likely completion of the laying operation (Evans & Stutin, 2006, p. 21). In consultation with the USN, the DATR study estimated it could lay 162-324 dummy and live mines over 54 nighttime dinner cruises (Evans & Stutin, 2006, p. 23).

I believe the DATR study failed to account for several factors: First, the span of time used to complete the minefield increased the likelihood of detection; second, the study neglected to account for U.S. Postal Service detection techniques for hazardous/illicit components; third, the study neglected to account for U.S. intelligence capabilities, and therefore exaggerated the number of naval mines that could be laid. Though the DATR study exhibited one of many potential covers that terrorists could use to disguise laying operations, these limitations did not negate the conclusion that concentration of U.S. MCM assets in a single continental port imposed a lack of strategic flexibility and reaction time required to combat M/UWIEDs in such a way as to minimize port closure and economic impacts (Evans & Stutin, 2006, p. 31). Such strategic limitations would compound the impact of an event and the subsequent ability to reopen a targeted port and its channels to shipping (Dowd, 2004, p. 3).

Current U.S. MCM. The USN operates dedicated MCM forces that comprise ships, helicopters, and Explosive Ordinance Disposal (EOD) divers, as well as Marine Mammal Systems, Navy Special Warfare Sea-Air-Land teams—commonly known as SEALS—, and Marine Force Recon divers (DOD, 2012, p. 11).

Ships. The United States has 14 *Avenger* class MCM ships (USN, 2009, p. 15). These ships are near the limits of their anticipated and designed service lives, and are due to retire in 2024 (USN, 2009, p. 16). Of the USN's 14 *Avenger*s, four are forward deployed to the Persian Gulf, two in Japan, and the last eight are homeported in San Diego, California (USN, 2009, p. 15).

The Avengers have aboard several MCM systems that include: the SQQ-32 variable depth mine detection and classification sonar that is housed in a stable variable depth body and uses separate search and classification transducers that concurrently show search and classification data. The SQQ-32 can find and classify several naval mine types, including: moored, tethered, and bottom mines standing proud; the SLQ-37 Magnetic/Acoustic Influence Minesweeping System that consists of a straight tail magnetic sweep combined with an acoustic sweeping device that counters acoustic and magnetic influence mines; the SLQ-38 Mechanical Sweep that cuts the tether of buoyant mines that float at or near the surface; and, the SLQ-48(V) Mine Neutralization System that is an UUV for neutralization of bottom and moored mines. When an *Avenger* class detects a target with its primary, hull mounted sonar, the UUV—guided by its own high definition sonar—reacquires the target, and then uses a low light level television camera to inspect, categorize, and ascertain the contact. If the contact is a bottom mine, the UUV places a charge beside it. Once the UUV is retrieved, the charge is detonated, and the mine: destroyed. If the contact is a moored type, the submersible attaches a charge, or, alternatively, can cut the cable. (USN, 2009, p. 16). Despite these impressive sounding capabilities, according to Chief of Naval Operations Admiral Greenert, the *Avenger*s are some of the USN's worst kept ships (Ewing, 2012, p. 4) and are certainly dated.

Helicopters. The USN has a total of 28 MH-53E Sea Dragon helicopters organized in two squadrons. These helicopters can locate, classify, and disable or destroy mines, and can be deployed by strategic airlifter to any point on the globe within 72 hours of an order.

Sea Dragons sport the following MCM equipment: The AQS-24 multiple beam side looking minehunting sonar locates and categorizes bottom, moored, and tethered mines, and can use laser line scan equipment to classify an object as *mine-like*, to positively identify it as a mine or, instead, as not a mine or a mine-like bottom object; the A Mark 2 Acoustic Sweep consists of towed parallel bars that produce medium- to high frequency sound that trigger acoustic-influence mines; the Mark 103 Mechanical Sweep system tows a stout wire and other equipment to handle moored mines in shallow water; the Mark 104 Acoustic Sweep has a venturi tube that encloses a self-rotating cavitating disk driven by water flow as the sweep is towed by the helicopter. This device counters acoustic-influence mines; the Mark 105 Magnetic Sweep uses a sled mounted gas turbine generator to produce electrical power. This power creates a magnetic field that replicates the signatures of surface ships as it is towed behind the helicopter, and counters magnetic-influence bottom mines; and, the Mark 106 Combination Sweep is a grouping of the Mk 104 and Mk 105 sweeps. The Mark 106 can sweep acoustic and magnetic influence mines (USN, 2009, p. 17).

EOD. These sailors are highly trained and highly skilled technical personnel that disable conventional and unconventional ordnance, including CBRNE weapons. In the case of MCM, EOD personnel support minehunting and minesweeping operations, and have training focused in MCM hardware and tactics, methods, and measures to find, classify, deactivate or terminate naval mines, torpedoes, and other underwater weapons, including M/UWIEDs. Key EOD MCM systems include: Nonmagnetic and silent diving

gear; handheld sonars; and, specialized deactivation and recovery equipment (USN, 2009, pp. 17-18).

Marine mammal systems. These are USN dolphins and sea lions that are trained in naval mine detection and neutralization, protection of an area from enemy combat frogmen, and to recover mines, torpedoes, and other submerged objects. Marine mammals are generally more efficient than people or machines at these tasks, and are the only MCM system able to detect bottom mines buried in the mud or sand. These mammals can be quickly airlifted throughout the world or deployed from ships already in operating in a forward area.

Marine Mammal Systems include: Mark 4 Mod (modification) 0 dolphins for detection and neutralization of tethered mines floating near the bottom; Mark 5 Mod 1 sea lions for attachment of retrieval flags to test objects, as well as targets in depths exceeding 152 meters; Mark 6 Mod 1 dolphins for protection against combat frogmen in anchorages, harbors, and in protection of individual ships (a competency first exploited at Cam Rahn Bay, Vietnam in 1971); Mark 7 dolphins used in a post attack environment to detect, locate, and mark or neutralize bottom M/UWIEDs that stand proud or are buried; and, Mark 8 dolphins used in a pre attack environments to detect, locate, and mark or neutralize bottom weapons that stand proud or are buried (USN, 2009, pp. 18-19).

Despite these seemingly formidable sounding systems, it is well known that USN MCM has atrophied and been neglected, especially when compared with past capabilities, or current ones held by the nation's allies and potential enemies. A July 1993 paper by the CNA stated as much, and described a recurring cycle: "Mines cause a

problem in war. MCM becomes a hot topic; Post war budgets decline. MCM must compete with sexier programs; Interest wanes as memories fade; little, if anything, really changes" (Lyons et al., 1993, p. 2). U.S. MCM capabilities are currently in the "Interest wanes as memories fade" stage of this mine warfare cycle, and were described as *brittle* by several USN mine warfare specialists in the spring of 2011 (Truver, 2012, p. 47).

Historically, MCM has represented under 1% of the USN's annual budget for programs and operations. Current specialized MCM systems—surface ships, helicopters, and EOD teams—are aging rapidly or are underfunded, and the United States is transitioning its MCM strategy. Bureaucratic changes—largely driven by strained budgets, though with operations at their core—are impacting U.S. MCM capabilities as well.

The USN, sorely reminded of its MCM limitations during Operation Desert Storm, established a single Flag Officer to oversee mine warfare: Commander Mine Warfare Command. Also, the service established on the staff of the Chief of Naval Operations an Expeditionary Warfare Directorate to supervise budgetary issues and the needs of mine warfare. Acquisition programs, and research and development were placed under the Program Executive Office for Littoral and Mine Warfare, providing an organizational link between the Assistant Secretary of the Navy for Research, Development, and Acquisition, and the Naval Sea Systems Command.

During the post Desert Storm period, and, building upon these reparative organizational moves, key mine warfare positions continued their evolution, with regional Combatant Commanders able to task the Naval Mine and Antisubmarine

Warfare Command with operational planning (USN, 2009, p. 26). Furthermore, the USN's Mine Warfare Command had been merged with the Fleet Antisubmarine Warfare Command in San Diego, California. This merger, when proposed, generated a high level of concern throughout the U.S. mine warfare community. Mine Warfare Command did not concur with the realignment and merger, and stated that the plan could result in dissolution of America's mine warfare capabilities, and would be a decision that would not be easy or inexpensive to reverse (O'Donnell & Truver, 2006).

Exercises. MCM exercises are conducted with regularity. One such exercise is the International Mine Countermeasures Exercise. Such an exercise occurred in 2013 in Bahrain where 41 nations joined the USN in practicing MCM. This large exercise was run over a month—the largest of its kind in the region—and used an assortment of defensive operations intended to safeguard global commerce.

The International Mine Countermeasures Exercise included MCM, maritime security operations, and maritime infrastructure protection. Participating nations operated 35 ships and 18 UUVs, and used over 100 EOD divers. The International Mine Countermeasures Exercise included a 3 day maritime infrastructure protection conference, actual MCM operations, and a discussion of lessons learned (Kelly, 2013). Such exercises are integral to maintaining skills that can be applied to a terrorist M/UWIED event.

Under the federally sponsored Asymmetric Warfare Initiative Port security, USCG, and USN, the Federal Bureau of Investigation [FBI], local law enforcement, and other agencies have conducted joint exercises. Carried out annually since 2003, the

Asymmetric Warfare Initiative exercises have been reported to have included terrorist attacks scenarios such as: An attack on a port chlorine storage tank using explosives; the taking of hostages and/or executions aboard a ship in port; an water-borne attack upon a USN warship in port; limpet mines attached to several vessels anchored, docked, or moored in port; an vessel entering a port with a nuclear weapon aboard; and, an biological disease agent released within a port (Chawkins, 2003). Besides limpet mines attached directly to a target's hull, other M/UWIED weapon types have not featured as part of Asymmetric Warfare Initiative exercises.

Future U.S. MCM. The USN has outlined an MCM vision that is meant to plug gaps in capabilities, and impart a shift from dedicated to organic capabilities. Organic capabilities means that MCM assets should travel with/be a part of amphibious and carrier strike groups, and would include: Improved detection capability; decreased sensor false alarm rates; automatic target recognition; improved neutralization time; improved network communications; and, achievement of fluid detect-to-engage capabilities (USN, 2009, p. 1).

Part of this shift to organic capabilities is the replacement of specialized MCM ships that are slow—unable to keep up with the fastest ships of the USN fleet, the nuclear aircraft carriers—and, if not forward deployed, must be transported by commercial sealift ships (Donaldson, 2013, p. 33). This replacement would be "fast, light, agile, adaptable, precise, and modular" (USN, 2009, p. 19). At the center of this paradigm shift is the littoral combat ship (LCS).

LCS. These corvette sized vessels (114-127 meters) currently comprise two classes: *Freedom* and *Independence*. Both classes of LCS are shallow draft and capable of operating within the confined area and maneuvering space of ports. Though the LCS's are not dedicated mine-hunters or -sweepers, they offer a modular mission system that allows for the fitting of newly developed MCM packages that comprise the latest in automated minehunting and minesweeping technologies. (USN, 2013a).

The LCS MCM mission package systems include: WLD-1 Remote Minehunting System; Coastal Battlefield Reconnaissance & Analysis system; and, the Surface Mine Countermeasures Unmanned Underwater Vehicle. The Coastal Battlefield Reconnaissance & Analysis System uses cross spectrum imaging to detect mines and obstacles in the surf zone, as well as exits from beach landing areas (USN, 2009, pp. 19-21).

LCS hosts the MH-60S multi mission helicopter. This aircraft can employ multiple minehunting and minesweeping hardware that includes: the unmanned and semi-autonomous Remote Multi Mission Vehicle which tows the AQS-20A variable depth Minehunting Sonar System that is able to automatically maintain a preset depth beneath the surface or a specific elevation from the bottom and uses a sensor that can locate and identify bottom and moored M/UWIEDs; the AES-1 Airborne Laser Mine Detection System that uses light to find, categorize, and pinpoint floating and moored M/UWIEDs that are near the surface; the AQS-235 Airborne Mine Neutralization System, a mine-neutralization device that is remotely operated and expendable, relocating previously identified targets and then neutralizes them. Part of the AQS-235 is the Archerfish

Common Mine Neutralizer for use against bottom and other naval mine types; the ALQ-220 Organic Airborne and Surface Influence Sweep that uses electrodes to generate a magnetic signature, as well as a generator that is driven by water flow to create propeller sounds that mimic a target ship's acoustic signature, thusly neutralizes M/UWIED threats in locales where minehunting is restricted due to weapons being buried or because of bottom clutter or debris; the AWS-2 Rapid Airborne Mine Clearance System that reacquires and neutralizes near-surface moored and surface/floating M/UWIEDs by using light detection and ranging to target a Mark 44 Bushmaster II gun that fires a 30 millimeter supercavitating tungsten projectile for weapon neutralization (USN, 2009, pp. 20-21).

New technologies are being developed to supplement the planned LCS MCM mission package. These include: The underwater imaging system that uses commercially available components and adapts high frequency sonar to create high resolution images of channel and port bottoms. This underwater imaging system will aid in detection of bottom changes that might signify a security threat. McCready (2010), chief of the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance research branch at the Development Center, said: "This aids in our ability to cover larger distances quicker, inspect a larger port accurately, and see more objects of interest" (as cited in Marcario, 2010, p. 36). This high frequency sonar allows images to be seen in up to 15 meters of dark, murky water. A new Advanced Sensor Management System uses command and control technologies, linking sensors with

information management systems to expand integration and to present a coherent picture of a port (Marcario, 2010, pp. 36-37).

In addition to Advanced Sensor Management, Automated Scene Understanding uses an advanced algorithm to identify anomalistic behavior by vessels in dense port environments (Marcario, 2010, p. 37). This program would help in the identification of vessels operating outside of established norms, such as movements that might indicate covert MIL activities. However, until LCS is available in planned numbers, and in anticipation of the availability of new technologies, USN is upgrading systems aboard *Avenger* class MCM ships.

Such *Avenger* upgrades include: Modification of the SQQ-32 mine detection sonar with a high frequency wideband capability; providing a more capable Expendable Mine Neutralization System to replace the SLQ-48 Mine Neutralization System; upgrades to the mechanical and acoustic/magnetic influence sweep systems; and, improvements to the ship's bow thruster, communication suite, frequency converters, navigation systems, and voltage regulators (USN, 2009, p. 16).

Port Security

Prior to 9/11, domestic port security was focused on the traditional circumstance of wars, or potential wars between nation states, as well as managing and controlling trade, and preventing piracy and smuggling. The U.S. Government response to such threats was the creation the Revenue Cutter Service in 1790 whose charter stipulated that it enforce regulations regarding the movement of goods by sea, the interdiction of pirates and smugglers, and preventing known enemies from reaching shores of the United States

(SEAPOWER Sea Services Almanac 2006, p. 122). Since these early beginnings, however, U.S. maritime ports, the threats they must contend with, and government policies that seek to mitigate them have all evolved.

In the next section of Chapter 2 I discuss port facilities, as well as legislation, and organizations related to securing them.

Port facilities. There are 361 commercial lake, river, and sea ports in the U.S. MTS. Both publicly and privately owned, these facilities are along the Continental U.S.'s Atlantic and Pacific seaboards, Great Lakes and Gulf of Mexico coastlines, and in Alaska, Guam, Hawai'i, Puerto Rico, and the U.S. Virgin Islands.

These maritime ports construct and sustain facilities for the transfer of intermodal cargo, moving them from ships to barges, trains, and trucks, and also construct and maintain cruise terminals for the passenger industry. Many industrial zones are located at or near ports to exploit incoming raw materials for manufacturing and the ability to move complete products to both the domestic and export markets. Many Foreign Trade Zones—areas of a port property where goods are not subject to inspection or taxation until they are moved out of the zone and through CBP (n.d.) jurisdiction —provide incentives to both commerce and industry (AAPA, 2013a).

Maritime ports in the United States comprise megaports like Houston, Texas; Long Beach, California; and, Miami, Florida; as well as smaller ones such as Erie, Pennsylvania; Fajardo, Puerto Rico; and, Hopewell, Virginia. The largest U.S. port by cargo tonnage is the Port of South Louisiana, Louisiana, and the smallest: Charlotte

Amalie, St. Thomas, U.S. Virgin Islands (NOAA, 2013a). Table 1 lists the top ten ports in the United States.

Over two billion metric tons of cargo is handled by U.S. maritime ports annually (AAPA, 2013a). Some ports cater to specific products, such as the Port of Redwood City, California that handles cement (aggregate, gypsum, and sand) and scrap metal (Port of Redwood City, 2014), while other facilities handle a wide spectrum of exported and imported goods.

Table 1

Top 10 U.S. Maritime Ports by Tonnage (2012)

Port	Rank	Metric tons (millions)
South Louisiana, LA	1	228.7
Houston, TX	2	216.1
New York, NY and NJ	3	199.7
New Orleans, LA	4	71.9
Beaumont, TX	5	71.2
Long Beach, CA	6	70.2
Corpus Christi, TX	7	62.6
Los Angeles, CA	8	56.1
Baton Rouge, LA	9	54.4
Plaquemines, LA	10	52.9

Note. From *National transportation statistics*, by U.S. Department of Transportation, 2012, retrieved from http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_01_57.html. In the public domain.

Such goods include apples, automobiles, coal, corn, iron ore, lumber, machinery, modular homes, phosphate, plastics, potatoes, steel, scrap steel, and wastepaper. Some two-thirds of domestic wheat production, one-third of domestic rice and soybean production, and nearly two-fifths of domestic cotton transit U.S. ports. Also, the

passenger cruise industry is dependent on port facilities. In 2005, ports handled approximately 4.1 million passenger vehicles for the domestic and international markets, and over 9.7 million passengers joined 17 of the largest cruise lines for 4,463 individual cruises (AAPA, 2013a).

Beside handling this wide spectrum of products and services, each port is unique in its bathymetry; bottom sediment; channel layout; climate; current; depth; geography; and, infrastructure that includes: cables; moorings; navigation markers; piers; pipelines; and, wharves. Another challenge is that much underwater port infrastructure is uncharted or its locations forgotten (USN, 2009, p. 24). Such facility nuances makes preparation for and mitigation of a terrorist M/UWIED attack challenging.

Legislation. MTSA and the SAFE Port Act were both created in the aftermath of the 9/11 attacks. Both pieces of legislation were designed to enhance port security, and focus on the threat of CBRNEs delivered by vessels and/or vessel-borne containers. Both these acts failed to recognize the threat and/or potential impact of a terrorist M/UWIED attack or campaign (GAO, 2012).

MTSA was crafted in the immediate aftermath of 9/11, and was designed to further protect U.S. ports and waterways from attack by terrorists by establishing and implementing a spectrum of security enhancements (Caldwell, 2007, pp. 3-4). MTSA's main provisions included: Automatic Identification Systems; Biometric security cards; Facility, national, regional, and vessel security plans; Foreign Port Assessment program; Maritime Safety and Security Teams; Maritime Security Grant program; the creation of Regional Maritime Security Advisory Committees; and, Susceptibility calculations of

infrastructure and ships (Bennett, 2008, p. 173). MTSA also established control measures for noncompliant facilities, such as: Correction of management or operational procedures; Limitations on access; Limitations on operations; Temporary shutdown of operations; up to complete withdrawal of approval of the facilities security plan (Bennett, 2008, p. 175). MTSA is the general framework upon which other programs have been built, one of which is the SAFE Port Act.

The SAFE Port Act was introduced to supplement MTSA. The legislation allocated $400 million for a port security grant program; established that all employees with secure access to ports be checked against a watch list; created joint operations centers; and, expanded placement of radiation detection equipment (*The Safe Port Act: Hearing before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity*, 2006, p. 2). The SAFE Port Act also established CSI; the C-TPAT; Domestic Nuclear Detection Office; TWIC; and, mandated data collection and radiation scanning of all inbound containers (Bennett, 2008, p. 173).

Introduced in 2002, the CSI aimed to facilitate container movement and traffic at sea while increasing security by focusing on use of containers by terrorists (CBP, 2006, p. 2). CBP stated containers could transport terrorists and their equipment, and described an event in October 2001 in which a container was identified that housed a terrorist and support equipment, including a computer, telephones—mobile and satellite—, as well as lawful airport security identification cards (CBP, 2006, p. 11). The CSI seeks to pivot interdiction to beyond U.S. borders by bilaterally cooperating with contracted countries (CBP, 2006, p. 6); by focusing on high-risk containers through evaluation of all

containers destined for U.S.'s ports; to build a container security program that is resistant to terrorist attacks; and, to avoid hindrance of/facilitate legitimate trade. CSI also provided benefits and incentives grants to partner governments and organizations (CBP, 2006, pp. 4-5).

The C-TPAT was introduced by CBP and was fast tracked for implementation—occurring in November of 2001—and was designed to reduce recognized terrorist threats. C-TPAT sought to provide security against terrorist attack by preventing the crossing of the nation's border by CBRNEs (CBP, 2004a, pp. 2-7), and did so by securing the entire supply chain with trustworthy nodes and partners, and thereby provided a forward defense; reducing reliance on defense of points of entry to the United States (CBP, 2004a, p. 10, 2007). C-TPAT is an alliance of carriers, maritime terminals, and shippers that partner up, sharing intelligence, and, thereby, increasing their capacity to respond to an emergency. According to Schaller, Deputy Executive Director of the Georgia Ports Authority:

> The objective is to sanitize the supply chain and to make sure the personnel packing the box are authorized, that security practices are in place, and all access to the cargo is properly controlled all the way from point of origin to arrival at a U.S. port. (Quinn, 2003, p. S64)

C-TPAT also included the Automated Manifest System.

Beginning in May 2003, the 24 Hour Advance Vessel Manifest Rule—known as the *24 Hour Rule*—required that maritime cargo carriers make a declaration to CBP regarding the composition of their cargo. This must be done 24 hours prior to loading a

vessel in the departure port if a port of call is to be within the United States, and be transmitted via the Automated Manifest System. This data is then scrutinized by the Automated Targeting System, resulting in the respective shipment being deemed *dangerous* or *nondangerous*. Cargo that is considered *dangerous* by Automated Targeting System is subjected to rigorous inspection (CBP, 2004b). Supplementing CSI and C-TPAT was the Importer Security Filing and Additional Carrier Requirement of January 2009.

Also called the *10+2 rule*; the Importer Security Filing and Additional Carrier Requirement buttressed the 24 Hour Rule, and improved pre identification of suspicious shipments (CBP, 2009b, p. 1; DHS, 2008). The 10+2 Rule required two more sets of data: a Vessel Stow Plan that detailed each container by: a Hazmat code, where applicable; International Maritime Organization Number; position aboard the vessel where it is stowed; origin port; and, destination port (CBP, 2008, pp. 2-3). Container Status Messages, whereby specified events must be provided to U.S. authorities if they occur no more than 24 hours after the carrier logs them (DHS, 2008a). Furthermore, the vessel operator must now provide information on cargo, including: Buyer; Commodity Harmonized Tariff Schedule of the United States number; Consignee number(s); Container stowing location and consolidator; Country of origin; Seller; Manufacturer or supplier; Record number of importer; and, the Ship to party (DHS, 2008a).

By the end of 2016, the Automated Commercial Environment will be the primary system for the trade community to report imports and exports, and the means by which the government determines admissibility (CBP, 2009a). Operation Safe Commerce

(OSC) is an initiative created by the DHS for the development of gear and procedures to keep the global supply chain secure. The program's primary goal is to reinforce maritime sector security and facilitate trade. The private sector is a partner in OSC (DHS, 2004). Tested equipment includes: E-Seal container intrusion detection; sensors for detection of CBRNE materials; as well as scanners for nonintrusive inspection of containers with gamma- and X-rays, as well as infrared scanners (DOT, 2010).

In 2009, the Coast Guard introduced Maritime Security (MARSEC) levels, a tiered system that communicated predetermined responses to credible dangers. When the Secretary of Homeland Security issues an alert under the National Terrorism Alert System, the USCG commandant determines if said alert is relevant to the MTS and, accordingly, adjusts the MARSEC Level (USCG, 2014e). MARSEC Levels reflect threats to facilities, ports, vessels, and other infrastructure located on or adjacent to U.S. waters. MARSEC Levels apply to Coast Guard regulated assets and facilities within the United States, as well as United States flagged vessels, and foreign flagged vessels operating within U.S. waters (USCG, 2014e). Please see Appendix A for descriptions of MARSEC levels.

Organizations. Throughout U.S. history, many agencies have been charged with port security management. These include: the United States Customs Service; USCG—formerly the Revenue Cutter Service—Immigration & Border Protection; Army/Navy; the Marshall's Service; and the FBI.

After 9/11, several of these agencies became part of the newly created DHS (Clark et al., 2007, p. 30). Currently, the DHS is made up of seven organizations: CBP;

Citizenship & Immigration Services; FEMA; Immigration & Customs Enforcement; the Secret Service; Transportation Security Administration (TSA); and, USCG (DHS, 2014a). Of these DHS agencies, CBP, TSA, and the USCG are responsible for port security management, along with the external partner of the U.S. Maritime Administration (MARAD).

Subordinate to DOT, MARAD is a civilian agency established to support the U.S. commercial maritime industry. Maritime Security Reports and a port security national planning guide are published regularly by MARAD (Frittelli, 2004, p. 11). MTSA requires MARAD to publish a revised version of its national planning guide on port security (MTSA of 2002, Title I § 113). However, CBP and USCG are the two federal agencies with the strongest presence at seaports (Frittelli, 2004, p. 11).

The USCG is the lead maritime law enforcement authority and component of homeland security as related to port security. In order to counter terrorist threats to U.S. maritime ports and USN ships in port, the USCG evaluates, boards, and inspects commercial ships as they approach U.S. territorial waters. A Captain of the Port acts as the main federal official for facility and vessel security in respective port areas (Frittelli, 2004, p. 11). Under the MTSA, the USCG is responsible for the protection of ports, and the facilities and vessels therein, from subversive acts (MTSA, 2002, Title I § 102).

CBP is the lead agency for inspection of cargoes, including cargo containers, as well as vetting of vessel crews and passengers that are to arrive in U.S. maritime ports from one abroad, while TSA has ultimate responsibility for the security of all transport modes moving both goods and people (Frittelli, 2004, p. 11).

If an act of terror were to occur in a U.S. maritime port, including a terrorist M/UWIED incident, the FBI would become the lead investigative agency. The FBI actively seeks to detect and interdict terrorists by participating in Joint Terrorism Task Forces (FBI, 2014). United in their mission to secure and protect U.S. maritime ports, all these government agencies are bureaucracies.

Weber (1864-1920) defined bureaucracy as "a model of organization design based on a legitimate and formal system of authority" (1922/1978, p. 7) and constitutes the most efficient and rational way to organize human activity (1922/1978, p. 7). Weber's model imparts efficiency through accountability, consistency, control, and responsibility, though has disadvantages such as inflexibility and rigidity (Griffin, 2003, pp. 165-166). Furthermore, bureaucracies tend to defend their own entrenched interests rather than act to benefit the whole, and resist changes to established routines, even when such changes are logical and geared towards betterment (Merton, 1957, p. 12). Bureaucracies also struggle for more power and greater rewards, and pursue narrow interests to consolidate and improve their own power positions (Mouzelis, 1967, p. 158). Bureaucracies also seek autonomy.

Autonomy is: "A condition of independence sufficient to permit a group to work out and maintain a distinctive identity" (Wilson, 1989, p. 182). The external aspect of autonomy is domain or jurisdiction, whereas the internal aspect is identity or mission. Agencies with high autonomy have a monopoly jurisdiction, whereby there are few or no bureaucratic rivals and minimal political constraints. Though the government agencies related to port security cooperate, they also strive for autonomy which has led to

duplication in jurisdiction and resources. The MARAD Port and Maritime Security Working Group found that: "…much in the way of organizational *stove piping* and cultural impediments remain that impedes effective, efficient and sustainable development and deployment of optimum homeland and port security" (Clark et al., 2007, p. 30).

Summary and Conclusions

I presented major themes in the reviewed literature in Chapter 2 which included that terrorists continue to seek ways to harm the United States, and that mine warfare is an integral part of naval warfare and the weapons (M/UWIEDs) have been used before in asymmetric warfare by weaker nation states and terrorists alike, and, likely, will be used again to further the nefarious general goals of terrorists.

With the plethora of threats presented by terrorists to U.S. maritime ports, it is perhaps understandable that tedious mine warfare was relegated to a backwater of the nation's maritime security consciousness. After all, an M/UWIED does not disperse chemicals or biological agents, irradiate an embarcadero, blast a city to smithereens, ram a bridge piling or a ferry full of commuters, or sail up to a docked USN warship or a tanker loaded with crude oil or liquid natural gas, and detonate it. Instead, terrorist M/UWIEDs are weapons that wait, and allow those that lay them to escape unnoticed, eluding detection until the weapons detonate and damage or sink a vessel, thereby fouling a port's channel, and sending fear through every captain or crew trying to get their cargo to the U.S. market.

The naval mine and the improvised terrorist equivalent have been underestimated in the global war on terror. These weapons can inflict physical damage to infrastructure, cause numerous casualties, plug up one or more ports, impede maritime transport with resultant economic impacts; thwart the U.S.'s open system of commerce, and psychologically impact the general populace.

In this study I addressed this neglected area of maritime security, filled the gap in understanding regarding the M/UWIED threat, and contributed to the buttressing of homeland maritime security. In Chapter 3, I describe the research design and rationale, role of the researcher, and the methodology I used to accomplish this.

Chapter 3: Research Method

Introduction

The terrorist attacks of 9/11 showed that those seeking to harm the United States could and would use the nation's vast, open, and vulnerable transportation networks. Though the attacks exploited the aviation system, the entire transportation sector is aware of the threat of terrorism (Plant & Young, 2007).

In this qualitative case study, my research purpose was to examine modern naval mine warfare and terrorism as related to the CIKR of maritime ports, increase understanding of the terrorist M/UWIED threat to U.S. maritime ports, explore current relevant security management, and develop recommendations for improving said management.

Sections of Chapter 3 include the research design and rationale, role of the researcher, and the methodology.

Research Design and Rationale

I asked three research questions in my study. Each is sequentially based upon the findings of the previous one:

1. Since 9/11, what port security management improvements have been implemented that mitigate the M/UWIED threat?
2. How could terrorists use M/UWIEDs to attack U.S. maritime ports?
3. What additional port security management improvements should be implemented to further mitigate the M/UWIED threat?

Terrorism was the central phenomenon this study addressed, and I focused on maritime terrorism and the subordinate threat vector of M/UWIEDs. Terrorism is the "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents" (22 USC § 2656 f (d) (2)). Maritime terrorism is terrorism perpetrated within the maritime domain (Chalk, 2008, p. 3).

In this qualitative study, I used von Bertalanffy's (1969) GST as the theoretical framework, which, as discussed in Chapter 1, imparted a methodology that involved analyzing a system, finding problems with a system, formulating alternatives, and then evaluating these alternatives. This process was used to evaluate documents and legislation, and I sought out policies focused on protecting U.S. maritime ports from terrorist M/UWIEDs. Furthermore, an embedded case study of two of California's maritime ports was used to discover problems by examining security and exposing vulnerabilities to M/UWIEDs as well as to formulate alternative policies and evaluate these alternatives.

Case study research seeks a broad point of view and then focuses this until themes converge and intersect at the core of a case (Yin, 2003, p. 14). This occurs when the data collection becomes saturated. Case studies are particularly useful in analyzing concepts where both descriptive and evaluative dimensions exist (Thatcher, 2006, p. 1,632) and, as in this study, are used holistically. The holistic method is a form of qualitative data analysis that heightens the substance of the totality and the interdependence of its parts (Yin, 2003); it is fundamental to a systems approach (Patton, 2002, p. 120) by allowing the researcher to examine the cooperation, competition, and interdependence of the

multiple private and public entities responsible for port security management, as well as the complex methods and technologies used to combat terrorism.

In this embedded case study, I collected data from observations and analyzed this data with description and interpretation before using the narrative form to describe behavior (Creswell, 1998, p. 65) by inductively developing ideas from particulars to abstractions (Creswell, 1998, p. 248). In case studies, researchers focus on analysis of one or more cases and collect data from numerous sources such as documents, observations, physical artifacts, and records, analyzing this data to extract assertions, descriptions, and themes (Creswell, 1998, p. 65). Case studies are widely used for analysis of homeland and national security issues.

For the Project on National Security Reform, Weitz (2013) used the case study to analyze the United States' national security processes, finding them to be inconsistent. However, in some instances, cases illustrated a generally clear and integrated development of strategy, a unified implementation of policy, and tactical planning that was coherent, coordinated, and properly executed. Weitz also found cases whereby strategy and policy were contradictory, divided, and flawed, and others still where it was completely nonexistent. The case studies also involved examining resource allocation, finding that the U.S. security system was capable of doing this efficiently, though, on the other hand, it could do so inadequately and, often, tardily. Weitz (2013) discovered flawed responses in diverse areas such as biodefense, diplomacy, and military operations. These flaws were found to span multiple presidential administrations and stretched from the days of the Cold War to today (Weitz, 2013).

The DOT (2000) has used case studies to assist with determination and implementation of risk and threat management, as well as mitigation. The DOT tested such frameworks by studying several existing programs, which included the nonaccidental release program administered by the Association of American Railroads; regulated medical waste exemptions; and risk management approaches used by selected members of the trucking industry. Through these case studies, the DOT sought to identify adaptability of risk management, as well as identify areas for policy improvement or modification. The DOT case study revealed needed improvements for the respective government and industry programs.

Role of the Researcher

For this study, my role was as ideal observer. An ideal observer is impartial and objective, is free of interests relevant to that which is being studied, and offers the same conclusions to the respective agencies being studied (Drier, 1993, p. 30). Furthermore, "researchers have developed special skills and techniques for observing, describing, and understanding everyday life" (Yin, 2003, p. 73).

In this spirit, I was central to this study, applying academic expertise in mine/naval warfare imparted by an internship at the Royal United Services Institute and lifelong work as a freelance defense journalist and technical writer for the U.S. Naval Institute (including award-winning articles on naval mine warfare), as well as other defense publications.

I have no personal or professional relationship within government agencies or security management personnel and, by use of a GST framework, impartially observed

and reviewed any agencies, documents, entities, legislation, or policy relevant to this study.

Methodology

I collected data for the study holistically. This holistic collection incorporated a document content analysis of open source/nonclassified crime reports; facility/infrastructure information; government threat assessments, legislation; policy papers; maps, satellite imagery, and navigational charts; peer-reviewed academic works and journals. Data collection also included direct observations and inspection of physical artifacts at two U.S. California ports.

Population

The research population included two ports of the MTS. There are 361 such facilities located in the United States (AAPA, 2013a).

Sampling

Ritchie, Lewis, and Elam (2003) stated that the sample size in qualitative studies is lesser than those used in quantitative studies. In a qualitative sample, there is a point where returns diminish, as additional data may not result in additional evidence, and an incidence of datum ensures it is included in the framework of the analysis (Ritchie et al., 2003, p. 102).

The sampling procedure used for this study was nonrandom and convenient. When researchers use nonprobability sampling, cases are not selected in random order as they are nonrandomly chosen (Singleton & Straits, 2005, p. 118). Because of the nature

of maritime infrastructure/ports, the integrity of this sample type did not affect the outcome.

This study's sample size consisted of two ports that are representative of less than 1% of the population. These sample ports were selected for geographic proximity to my home, and their place at both ends of the port size/type spectrum. The sample comprised the Port of Oakland and the Port of Stockton. Both these maritime ports are located in the State of California

The Port of Oakland—a bayside container-borne cargo facility—is considered a megaport, hosts a passenger ferry terminal, is located in Alameda County, California on the eastern shore of San Francisco Bay, and is ranked among the top 50 busiest in the United States. The port has 31 kilometers of waterfront (Port of Oakland, 2014b) and comprises 489 hectares allocated to maritime activities (Caltrans, 2013, p. 2), with 778 (64%) of this area is devoted to container terminals (World Port Source, 2014b). The Port of Oakland is designated by the DOD as one of 16 National Strategic Ports (Caltrans, 2013, p. 2). Strategic ports support major force and materiel deployments for multiple national defense contingency plans. Such ports are designated as strategic on the basis of proximity to military units, transport links to those units, and various port assets, including bathymetry, facilities, and security ("National port readiness network," 2014). The Port of Oakland is served by multiple transport mode links.

These include the highway access routes of I-80, 1-580, I-238, I-980, and I-880, as well as rail links such as BNSF and Union Pacific (UP) railroads that provide double-stack intermodal trailer-on-flatcar service, and access the port via the jointly owned

Oakland Terminal Railway short line (Caltrans, 2013, p. 2). Law enforcement at the Port of Oakland is by the Oakland Police Department (OPD).

OPD has jurisdiction over five areas encompassing the City of Oakland. These five areas are then subdivided into beats, six of which comprise the landward side of the Port of Oakland, its perimeter, and immediate outlying areas: 01X; 02X; 02Y; 05X; 05Y; and, 19X (City of Oakland, 2014). The mission of the OPD is: "To provide the people of Oakland an environment where they can live, work, play, and thrive free from crime and the fear of crime" (OPD, 2014a). The Port of Oakland is connected to the other sample port—the Port of Stockton—by Marine Highway 580 (M-580: Marine Highway [M-580], 2014).

The Port of Stockton—a riverside bulk cargo facility—is considered small, offers no passenger services, and, in 2012, its largest outbound commodity was iron ore and its largest inbound one was liquid fertilizer. The Port of Stockton is located in San Joaquin County, California and upon the San Joaquin River, some 139 kilometers from the entrance to San Francisco Bay. The port comprises approximately 1,699 hectares making it California's largest inland port by area, and the second busiest west coast inland port after Portland, Oregon (Caltrans, 2012, p. 1). The port can berth 17 vessels and contains 102,000 square meters of dockside transit sheds and 715,000 square meters of warehouses (World Port Source, 2014a). Law enforcement at the Port of Stockton is by the Port of Stockton Police Department (POSPD).

POSPD has jurisdiction over the area that comprises the Port of Stockton. The mission of POSPD is: "To provide service, security and protection for the port, its

tenants, employees and surrounding community" (Port of Stockton, 2014c). POSPD enforces local, state, and federal laws, as well as DHS and USCG regulations. POSPD also operates a marine unit (Port of Stockton, 2014c). The Port of Stockton is served by multiple transport mode links.

These include the highway access routes of I-5, SR-4, and SR-99 (Caltrans, 2012, p. 2), as well as rail links such as the Lathrop Union Pacific and Mariposa Burlington Northern Santa Fe rail ramps (M-580: Marine Highway, 2014), and several short line railroads including the California Northern Railroad, Modesto and Empire Traction Company, and the Stockton Terminal and Eastern Railroad. The Port of Stockton is designated as a Foreign Trade Zone, allowing imports and exports to be transshipped without payment of duties (Caltrans, 2012, p. 2), and operations are 24 hours a day and 7 days a week (Caltrans, 2012, p. 1).

Table 2 lists relevant demographics of the studied ports, and, Figures 2 and 3 illustrate their physicalities.

Table 2

Demographics of Study Ports

	Type	Vessels	Cargo	Value of goods
Oakland	Large container	2,121	2,342,504 containers	$41 billion
Stockton	Small bulk	418	2,405,993 metric tons	$1 billion

Note. Oakland data from 2008; Stockton data from 2012. From *U.S. Public Port Facts*, by AAPA, 2013, retrieved from http://www.aapa-ports.org/Industry /content.cfm?ItemNumber=1032. In the public domain.

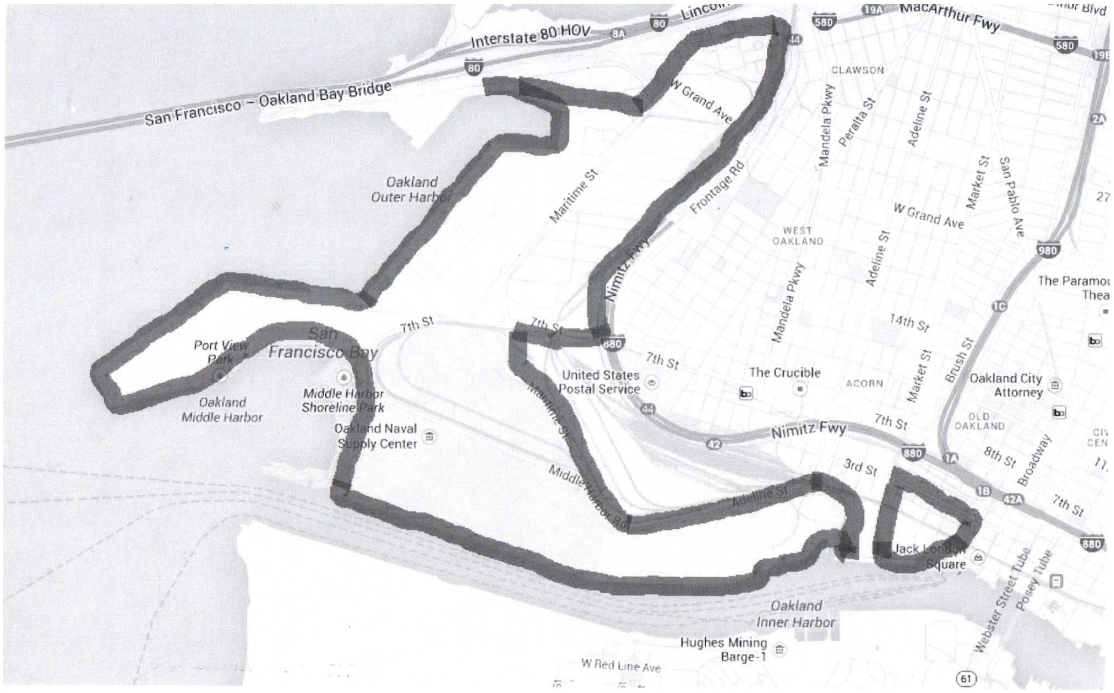

Figure 2. Boundary of maritime division, Port of Oakland. From Google Maps, 2014. Enhancements by author.

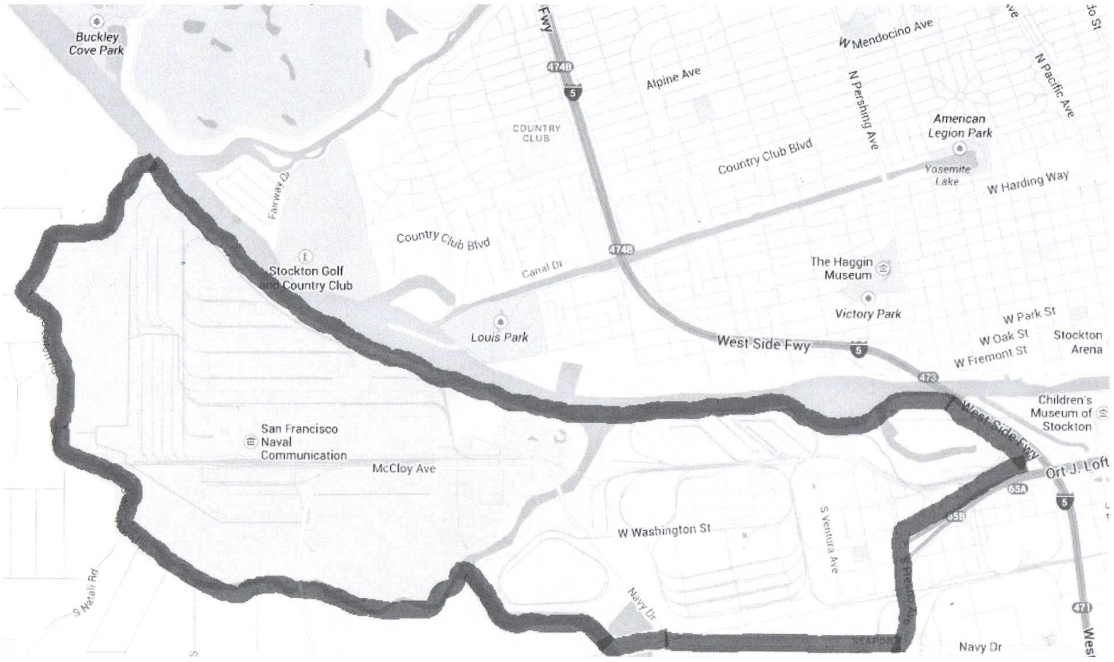

Figure 3. Boundary of maritime division, Port of Stockton. From Google Maps, 2014. Enhancements by author.

Instrumentation

This study's instrumentation included document content analysis, direct observation, and inspection of physical artifacts.

Document content analysis. With document content analysis I sought to protect authenticity of the respective research, and offer a precise reading of a specific document set. This systematic process is referred to as *credibility* in the qualitative tradition. My objective was to offer a truthful account of the information found in respective documents, and to provide a scientific interpretation of the meanings found therein (Wesley, 2010, p. 5).

External validity is a concern for analysis of documents. Inquiries must offer insight that extends beyond the specific cases under study, and qualitative document analysis relies upon researchers to assess the broader applicability lessons drawn from findings. The results deemed from document analysis can be confirmed in that inferences can be traced back to the primary documents, corroborating findings (Wesley, 2010, p. 5). This analytic approach relies on cause and effect relationships to reach conclusions, and I assume linearity that allowed me to adjust for differences across settings (Garcia & Wantchekon, 2010, p. 136). In the case of this study, such settings included the spectrum of U.S. maritime ports.

Researchers must meticulously report results of analyses, to form the basis upon which their interpretations are based. This is known as *thick description*, a process by which findings are grounded. In order for a document content analysis to be trustworthy and systematic, an empirical process is necessary (Wesley, 2010, p. 9):

During the first step of this process, I took a broad overview to find general themes. This step involved recording noticeable patterns as memos or marginalia. The second step was axial coding whereby I reviewed entire documents, manually tagged specific passages that fit the theme-categories identified in the first step. The final step entailed selective coding whereby I examined the documents to find miscoded passages and discrepant evidence. By finding discrepant evidence that may undermine researcher interpretations, an audit trail was created (Wesley, 2010, p. 9).

The document content analysis—outlined in Appendix B—examined open source (nonclassified) legislation, literature, policy, and threat assessments from various U.S. agencies and organizations, including: the DHS; DOD; GAO; MARAD; Merchant Marine Academy; Naval Institute; and, Naval War College. In this study's content analysis I sought assertions, descriptions, interpretations, policies, procedures, tactics, and themes that were directed towards general interdiction of mine attacks and/or MCM. For each of the two sample ports, I analyzed open source (nonclassified) documents for content that included: charts; crime reports; port facilities and infrastructure; maps; satellite imagery; and, security management.

Direct observation. The direct observation of the Port of Oakland and the Port of Stockton was conducted from adjacent public rights of way that allowed me to observe port infrastructure without intruding. These observations were conducted twice per port during varying conditions, were several hours in duration each, and were based on the Direct Observation of Ports – Checklist (Appendix C), recorded using the Direct Observation of Ports – Record Sheet (Appendix D), and copied into the software Excel

and Word—hereafter referred to as *the database*—for analysis and storage. The recorded direct observation data comprised the relevant checklist number, the port being observed, the location name and GPS coordinates of the point of observation, the date, times (start and end), weather conditions, and observations.

Inspection of physical artifacts. Inspection of physical artifacts at the Port of Oakland and the Port of Stockton was conducted by document content analysis, including: maps, satellite imagery, and navigational charts, as well as during the aforementioned direct observations.

The document content analysis, direct observation, and inspection of physical artifacts were applied to the research questions as follows:

In Research Question 1 I asked: Since 9/11, what port security management improvements have been implemented that mitigate the terrorist M/UWIED threat? To effectively answer this question, I performed a content analysis of legislation, literature, policy, and threat assessments from September 11, 2001 to September 11, 2014.

In Research Question 2 I asked: How could terrorists use M/UWIEDs to attack U.S. maritime ports? To effectively answer this question, I analyzed documents for content, performed direct observation of two ports, inspected their physical artifacts, and acted as a *Red Team*. A Red Team is a military term for personnel who assess the defenses of friendly forces using enemy tactics (Delgaudio, 2010). Red Teaming views problems from the perspective of an adversary or competitor. A Red Team's goal is enhancement of decision making by using prevalent adversarial tactics and strategies (Mateski, 2014), and to provide alternative analysis of a problem. Alternative analysis

challenges assumptions to identify alternative outcomes, capturing the implicit or explicit results in a written product for relevant policy makers (Fishbein & Treverton, 2004). Red Teams are employed by various government agencies to provide data on the effectiveness of essential security measures (Delgaudio, 2010). In this study, the Red Team action was to design a hypothetical M/UWIED attack utilizing standard weapon types and laying techniques.

In Research Question 3 I asked: What port security management improvements should be implemented to further mitigate the terrorist M/UWIED threat? To effectively answer this question, I used results of Research Question 1 and 2 to perform an MAA aimed at countering the terrorist M/UWIED threat vector.

Data Collection

Data collection was accomplished by triangulation of evidence from document content analysis, direct observation, and inspection of physical artifacts. Political scientists corroborate findings by utilizing other types and evidentiary sources (Boyatzis, 1998, p. XIII), strengthening the validity of a case study (Yin, 2003, p. 36), and buttressing subjective, qualitative interpretations with objective, analyses of content (Hesse-Beber & Leavey, 2006, pp. 326-330). This study's data included both primary and secondary sources.

Primary data collection uses direct observation, and can be accomplished actively or passively (Singleton & Straits, 2005, p. 367). This study's primary data collection was passive in nature, whereby I oversaw specific features without questioning individuals (Davis, 2000, p. 65). Secondary data were collected by both manual and online means.

Based on primary sources, the use of secondary data saves time and assists with discovery of solutions to research problems (Davis, 2000, p. 57).

Data Analysis

This study used the theoretical framework of GST developed by von Bertalanffy (1969) to develop a research framework. GST was chosen since multiple stakeholders—private and public—are involved in, and responsible for, security management at U.S. maritime ports. Senge (1990) found GST beneficial for determination of influences that lie beneath events and facets of a decentralized system (p. 73), such as that of U.S. port security management.

I analyzed the primary and secondary data with explanation building and associated by a causal link. According to Yin (2003, p. 120), by using this type of data analysis, a researcher develops explanations concerning the research problem before causally linking them. Data were organized by research questions. This organization began by sorting data collected from document analysis, direct observations, and inspection of physical artifacts, and explanations were articulated to make certain of causal links and a connection of findings.

MAA is used to develop a strategy-to-task map of activities related to U.S. port security; to identify shortfalls related to the particular task (Steen, 2003) of countering the terrorist M/UWIED threat; and, analyzing and defining solutions relevant to the identified shortfalls (Hoon, 2013, p. 522).

Issues of Trustworthiness

Issues of trustworthiness in any study are credibility, transferability, dependability, and confirmability. To be credible, this study incorporated multiple sources, including: document content analysis, direct observations, and inspection of physical artifacts. Only peer-reviewed journals, and/or vetted government sources were used. This study is externally valid/transferable due to the sampling model, and conclusions are directly relevant and transferable across the MTS. This study is dependable because of evidentiary triangulation. Such triangulation strengthens the dependability of case studies (Yin, 2003, p. 36). This study is confirmable due to reflexivity, whereby explanations were built and associated by causal link (Yin, 2003, p. 120).

Ethical Procedures

There were no human participants in this study. Primary observation was by me and involved only port facilities and their physical artifacts. All secondary sources were open source/nonclassified. A review of my methodology was conducted by the Institutional Review Board (IRB) of Walden University which granted approval under authorization number 07-29-14-00131691 (Appendix E). Furthermore, I completed the National Institute of Health (NIH) Office of Extramural Research's "Protecting Human Research Participants" training, and was granted NIH certification number 1471116 (Appendix F).

Summary

Terrorism was the central phenomenon I addressed in this qualitative study, with a focus on maritime terrorism and the subordinate threat vector of M/UWIEDs as related to U.S. maritime ports. The research population was the 361 ports the MTS's ports, and the nonrandom sample consists of the Port of Oakland and the Port of Stockton ($n = 2$).

For this study's holistic case study, my role was as observer, and data collection was accomplished by a triangulation of evidence that included document content analysis, direct observation, and inspection of physical artifacts. Data analysis was by explanation building. I present the findings of my study in Chapter 4.

Chapter 4: Results

Introduction

The purpose of this case study was to examine the areas of modern naval mine warfare and terrorism as related to the CIKR of U.S. maritime ports. My intent was to discover implemented port security management improvements relevant to the threat of terrorist M/UWIEDs; to examine this threat from an adversarial position; and to explore means of mitigating this threat by developing recommendations for bureaucratic and policy reform. This qualitative study focused on two ports in California—Oakland and Stockton—used a holistic method of data collection, and was based on theoretical framework of GST as developed by von Bertalanffy (1969).

In this study I asked three research questions:

1. Since 9/11, what port security management improvements have been implemented that mitigate the M/UWIED threat?
2. How could terrorists use M/UWIEDs to attack U.S. maritime ports?
3. What additional port security management improvements should be implemented to further mitigate the M/UWIED threat?

To answer the research questions, I collected open source/nonclassified documents, including crime reports; facility/infrastructure information; government threat assessments, legislation, and policy; maps, satellite imagery, and navigational charts; and peer-reviewed academic works and journals. I also directly observed and inspected physical artifacts at two ports. These data were then analyzed for results. Chapter 4 is organized by documents, direct observation, and inspection of physical artifacts, and it is

broken down by data collection, analysis, and results, with the results presented according to research question.

Data Collection

Data collection included documents, direct observation, and inspection of physical artifacts.

Document Content Analysis

Multiple databases were used to collect open source/nonclassified documents, which included the following: EBSCO; Google Scholar (only using peer-reviewed scholarly works retrieved from this search engine); Homeland Security Digital Library; International Security & Counterterrorism Reference Center; LexisNexis Academic; Military and Government Collection; ProQuest Central and Dissertations; Political Science Complete; Political Science: A SAGE Full-text Collection; U.S. Naval Institute Archives; and Walden University's Academic Complete, and Thoreau.

Furthermore, crime reports for 2013 were requested from the OPD and POSPD under the California Public Records Act (Government Code §§ 6250-6276.48/California Constitution Article I, Section 3). Both law enforcement organizations provided data deemed releasable under the security provisions of the California Public Records Act. The OPD provided two Excel spreadsheets with summary reports for activity within beats that included the landward portion of the Port of Oakland and comprised 32,329 calls for service and 6,468 reported crimes. POSPD provided over 700 pages of detailed incident reports that comprised 176 calls for service and reported crimes. Document content was collected to address Research Questions 1 and 2.

Document collection for Research Question 1 sought directives, hearings, laws, and policies regarding general interdiction of mine attacks and/or MCM in U.S. maritime ports from September 11, 2001 to September 11, 2014; this was accomplished by examination of documents from various U.S. agencies and organizations, including Congress; DHS; DOD; DOT; GAO; and the White House. These secondary data were collected by both manual and online means, and I coded it by phrases, subjects, topics, and words associated with mine warfare, MCM, and port security, including *GAO assessment; hardware; MCM; MCM hardware; MTSA implementation; port security; Port Security Grant Program (PSGP); port security legislation; port security legislation implementation; port security legislation recommendations; SAFE Port Act implementation; SAFE Port Act reauthorization; USCG strategy;* and *USN mine warfare*.

During the document collection phase for Research Question 2, I sought assertions, descriptions, interpretations, policies, procedures, tactics, and themes regarding mine warfare and the current state of port security, and I accomplished this by examining crime reports, directives, legislation, literature, policy, and threat assessments from various California and U.S. agencies and organizations, including DHS; DOD; GAO; MARAD; Merchant Marine Academy; Naval Institute; Naval War College; NOAA; OPD; POSPD; USCG; and the White House. These secondary data were collected by manual and online means, and I coded it by phrases, subjects, topics, and words associated with mine warfare, MCM, and port security, including crimes of relevance to this research; GAO assessment; general crimes; hardware; MCM; MCM hardware; mine warfare campaigns; MIL future; MIL/MCM future; MIL/MCM weapons;

MTSA implementation; port security; Port Security Grant Program (PSGP); port security legislation; port security legislation implementation; port security legislation recommendations; SAFE Port Act implementation; SAFE Port Act reauthorization; terrorism limpet mines; USCG strategy; USN mine warfare; and UUVs.

Direct Observation

Research Question 2 required collection of data by direct observation.

Direct observations were conducted at both the Port of Oakland and the Port of Stockton from adjacent public rights of way to view port infrastructure without intruding. Said observations were passive in nature, whereby I oversaw specific features without questioning individuals (Davis, 2000, p. 65). These observations were based on the Direct Observation of Ports – Checklist (Appendix C), and I recorded them using the Direct Observation of Ports – Record Sheet (Appendix D). The recorded direct observation data comprised the relevant checklist number, the port being observed, the location name and GPS coordinates of the point of observation, the date, times (start and end), weather conditions, and observations. Data were copied into the database for organization, coding, analysis, and storage.

Two observations per port were conducted, were several hours in duration each, and transpired during varying conditions. Direct observation of the ports occurred from both fixed/land-based points as well as mobile/water-borne platforms.

Port of Oakland. Direct observation of the port occurred from the Alameda Main Street Ferry Terminal (GPS coordinates: 37.790655, -122.294197) and Middle Harbor Shoreline Park (GPS coordinates: 37.805491, -122.324731). The Alameda Main Street

Ferry Terminal observation was completed on September 18, 2014, and lasted from 0530-0930. The Middle Harbor Shoreline Park observation was completed on September 18, 2014, and lasted from 1205-1530.

Alameda Main Street Ferry Terminal is operated by the San Francisco Bay Area Water Emergency Transportation Authority, a regional public transit agency that provides ferry service on the San Francisco Bay, and is tasked with coordinating a water transit response to regional emergencies, such as a major earthquake that damages transbay bridges/and or rail tunnels (San Francisco Bay Area Water Emergency Transportation Authority, n.d.). Under the San Francisco Bay Ferry brand, Water Emergency Transportation Authority utilizes a fleet of 12 high-speed passenger ferries to carry over 1.8 million passengers annually between the cities of Alameda, Oakland, San Francisco, South San Francisco, and Vallejo. The Alameda Main Street Ferry Terminal offers year-round service between Alameda and San Francisco's Ferry Building/Pier 41 terminals (San Francisco Bay Area Water Emergency Transportation Authority, n.d.). This location offered observational access to the waterfront, as well as views of the Port of Oakland's Matson Terminal (Berths 60 to 63), and the harbor channel and middle harbor (Port of Oakland, 2014a).

Middle Harbor Shoreline Park is a 15-hectare shoreline park administered and operated by the Port of Oakland (Port of Oakland, 2014a). The park offers access to the shoreline and provides views of San Francisco Bay, the Port of Oakland's Ben E. Nutter Terminal (Berths 35 to 38) and Oakland International Container Terminal (Berths 55 to

59), as well as the harbor channel and middle harbor, and all subsequent maritime activity (Port of Oakland, 2014a).

The Figures 4 and 5 show the locations from where each direct observation of the Port of Oakland was conducted:

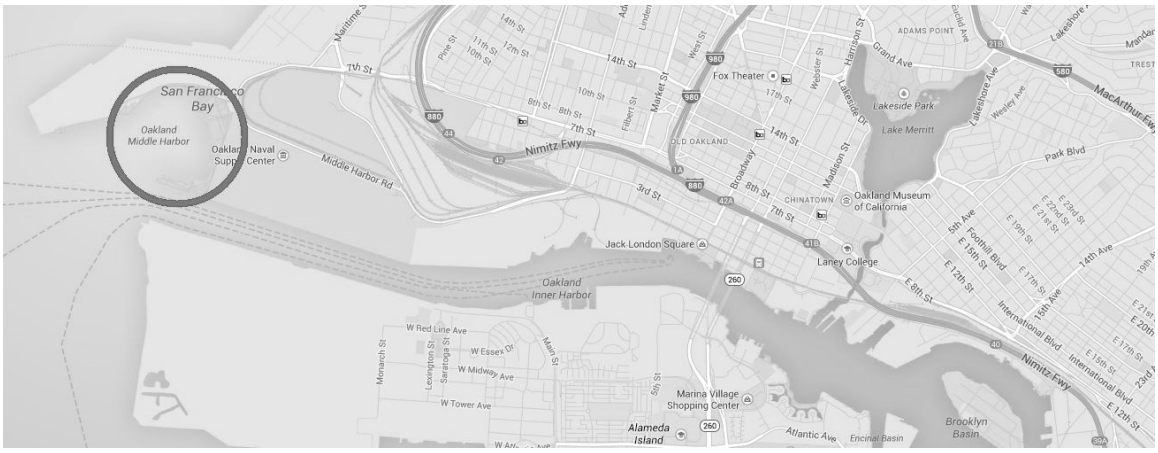

Figure 4. Direct observation of Port of Oakland at Middle Harbor Shoreline Park. From Google Maps, 2014. Enhancements by author.

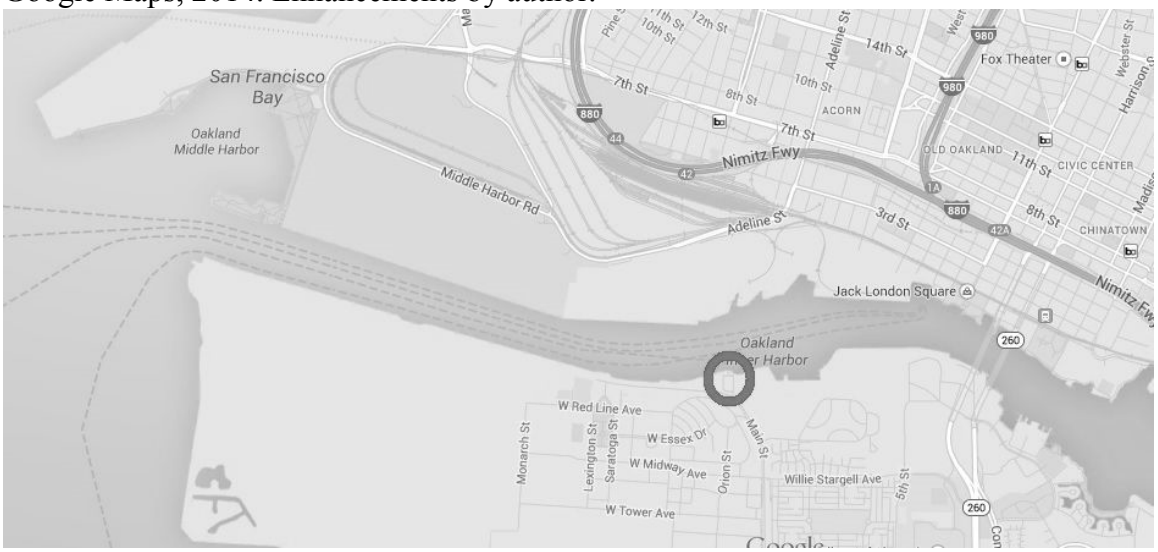

Figure 5. Direct observation of Port of Oakland at Alameda Main Street Ferry Terminal. From Google Maps, 2014. Enhancements by author.

Port of Stockton. Direct observation of the port occurred from Louis Park-Pixie Woods (GPS coordinates: 37.956436, -121.345094) and from aboard M/V *California Sunset*. The M/V *California Sunset* sailed an out-and-back route, with departure from Tuleburg levee/Weber Avenue Wharf, McLeod Lake (GPS coordinates: 37.952709, -121.297252), and came about for a return voyage at Burns Cutoff, where the Calaveras River meets the San Joaquin River (GPS coordinates: 37.967272, -121.369983). The Louis Park-Pixie Woods observation was completed on August 29, 2014, and lasted from 1245-1600. The M/V *California Sunset* observation was completed on September 11, 2014—the thirteenth anniversary of the 9/11 attacks—and lasted from 1245-1515

Louis Park-Pixie Woods is a community park located on the San Joaquin River across from the Port of Stockton. Besides entertainment, recreation and sports facilities, the park offers a boat ramp and access to the waterfront along a levee and several small beaches (City of Stockton, 2012). Furthermore, this vantage point provided a view of the Port of Stockton's primary channel as well as the port's West Complex berths, specifically berths 14 through 20 (Port of Stockton, 2014a).

M/V *California Sunset* is operated by Opportunity Cruises, and is a passenger motor vessel certified by the USCG to carry up to 80 persons. Opportunity Cruises generally provides cruises along the San Joaquin River and the California Delta, and was contracted by the Port of Stockton to operate free educational cruises that emphasized the economic contribution, facilities, and history of the port while providing close up views of Port of Stockton operations (Opportunity Cruises, 2012). This vessel and its out-and-

back voyage allowed me to view the entirety of the Port of Stockton's infrastructure, as well as relevant activity within the property during the period of observation.

The Figures 6 and 7 show the locations from where each direct observation of the Port of Stockton was conducted:

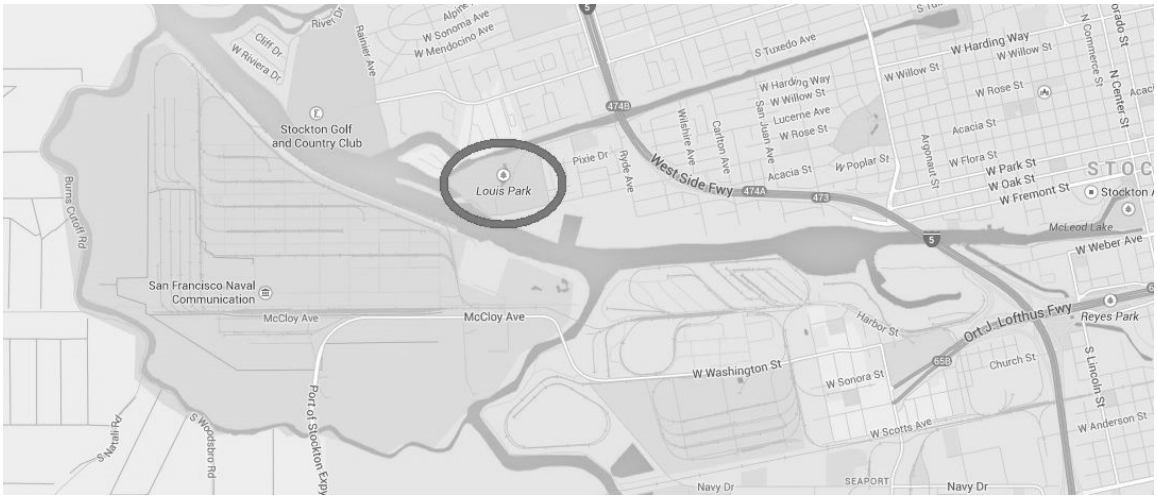

Figure 6. Direct observation of Port of Stockton at Louis Park-Pixie Woods. From Google Maps, 2014. Enhancements by author.

Figure 7. Direct observation of Port of Stockton from M/V *California Sunset*. From Google Maps, 2014. Enhancements by author.

Inspection of Physical Artifacts

Research Question 2 also required an inspection of physical artifacts by collection of open source/nonclassified documents and collection of relevant data during the direct observation phase, as outlined in both Appendices A and B.

Through the document collection I sought to identify: bathymetry; boat ramps; bridges; cables; channels; hazards; levees; markers; moorings; navigational aids; piers; pipelines; public spaces; restricted zones; and, wharves, and this was accomplished by examination of facility/infrastructure information; maps; navigational charts; and, satellite imagery from various U.S. agencies and organizations, including: DOT; MARAD; NOAA; and, USCG. I collected primary data by direct observation and secondary data by both manual and online means. Data were copied into the database for organization, analysis, and storage.

All data collection was consistent with the plan outlined in Chapter 3 and Walden University Institutional Review Board approval number 07-29-14-00131691. There were 784 online and hard-copy documents and two Excel spreadsheets collected. Data were electronically and manually copied into the database for organization, coding, analysis, and storage. An internal audit was then conducted to verify accuracy and to locate miscoded passages.

Data Analysis

Analysis for Research Question 1 included a document content analysis. For Research Question 2, analysis included a document content analysis, as well as

categorization of data collected during direct observations/inspection of physical artifacts. Analysis for Research Question 3 used GST and MAA.

Data analysis for Research Question 1 occurred in three steps: General themes, axial coding, and selective coding. Data were first analyzed for assertions, descriptions, interpretations, policies, procedures, tactics, and general themes that were directed towards interdiction of mine attacks and/or MCM. The units of analysis were phrases, subjects, topics, and words associated with mine warfare, MCM, and port security. These included: GAO Assessment; hardware; MCM; MCM hardware; Mine warfare campaigns; MIL future; MIL/MCM future; MIL/MCM weapons; MTSA implementation; Port security; Port Security Grant Program (PSGP); Port security legislation; Port security legislation implementation; Port security legislation recommendations; SAFE Port Act implementation; SAFE Port Act reauthorization; Terrorism limpet mines; USCG strategy; USN mine warfare; and, UUVs. An annotated bibliography of each document's specific passages that fit theme-categories identified in the first step were then axially coded by disaggregation and tagging.

The final step of the data analysis was completed once core concepts and categories emerged during the previous step. These concepts and categories were, after further definition, development, and refinement, selectively aggregated to tell the larger story (Price, 2010, pp. 158-159). During this final step, documents were re-examined to discover discrepant evidence. None were discovered. Results were recorded in the database.

Data analysis for Research Question 2 occurred by the method of collection, and then employed a Red Team perspective:

Document content analysis occurred in three steps: General themes, axial coding, and selective coding. Data were first analyzed for assertions, crimes, descriptions, interpretations, policies, procedures, tactics, and general themes that were directed towards interdiction of mine attacks and/or MCM, port facilities/infrastructure, and, port security. The units of analysis were phrases, subjects, topics, and words associated with mine warfare. Specific passages that fit theme-categories identified in the first step were then axially coded by disaggregation and tagging. The final step of the data analysis was completed once core concepts and categories emerged during the previous step.

These concepts and categories were, after further definition, development, and refinement, selectively aggregated to tell the larger story (Price, 2010, pp. 158-159). During this final step, documents were re-examined to discover discrepant evidence. Regarding crime reports provided by the OPD and POSPD, all calls for service and reported crimes were sorted into general crimes and those of relevance to this research. Collected data were then recorded in the database.

Data collected during the direct observation and inspection of physical artifacts phase and recorded in the database were organized by Checklist item number and the observations assessed against the research question. Explanations were then framed to verify that a causal link existed.

Finally, I analyzed security from the perspective of an adversary, and employed a Red Team perspective to design a hypothetical M/UWIED attack against the sample ports by utilizing standard weapon types and laying techniques.

Data analysis for Research Question 3 was applied to analysis of data from Research Questions 1 and 2. The methodology conforms to MAA and utilizes GST, a theory that espouses analysis of an existing system by asking: What are the limitations of the present system?; What alternative systems are possible?; and, What are the costs of continuing the present system and changing to alternative systems (Skyttner, 2006, pp. 470-471)? The primary drive of this systems analysis is to assist commercial and industrial decision makers as well as public policymakers in the resolution of problems (Hordijk, 2014).

In applying the GST data analyses framework to this research question, I articulated what the system should do; second, registered what the system had done; third, worked out the difference between the first and second steps; fourth, explained the causes of these differences; and, fifth, controlled the system to minimize the difference (Skyttner, 2006, p. 459). MAA was then applied to the analysis.

MAA identified and related functions that were grouped together to increase the dependability, trustworthiness, and wholeness of the information. These item groups comprised areas of desired improvement/reform, including: mine warfare; organizations; and physical security. Next, the functions were broken down into tasks (HSSAI, 2007, p. 6). Mine warfare became adversary pathways and MCM; organizations became roles and

responsibilities, and budgets and procurement; and, physical security: landside and waterside. Such organization is consistent with MAA (HSSAI, 2007, p. 6).

Results

With data collection and analysis complete, I compiled the results and answered the research questions.

Research Question 1

In Research Question 1 I asked: "Since 9/11, what port security management improvements have been implemented that mitigate the terrorist naval mine/underwater improvised explosive device threat?" Results from question's document content analysis revealed that, since 9/11, maritime and port security has been realigned from the post WWII focus on piracy and smuggling and towards the terrorist threat. In order to give context to this 9/11 realignment, I begin by summarizing the security regimes established after WWII.

In 1948, the United Nations set up the International Maritime Organization (IMO), and, in 1974, the International Convention for the Safety of Life at Sea was established. Between 1974 and the terrorist attacks of 9/11, numerous other international regulations were approved by the IMO's Maritime Safety Committee: Circular 443 on Measures to Prevent Unlawful Acts against Passengers and Crews on Board Ships, 1986; Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988; Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, 1988; Circular 754 on Passenger ferry security, 1996 (Eski, 2012, p. 421). An amendment to the International Convention for

the Safety of Life at Sea, the International Ship and Port Facility Security Code exemplifies international post 9/11 legislation that embodied considerable reform to port security management. Article 2 of the code's preamble stated: "Following the tragic events of 11th September 2001, the 22nd session of the Assembly of the IMO unanimously agreed to the development of new measures relating to the security of ships and of port facilities" (IMO, 2002, p. 2).

The International Ship and Port Facility Security Code amended the Safety of Life at Sea Convention regarding minimal security regimes for government agencies, ports, and vessels. This code, instituted in answer to apparent threats maritime infrastructure and vessels, established a wide ranging set of procedures that increased the security. In the United States, the MTSA, National Security Presidential Directive-41/Homeland Security Presidential Directive-13 (NSPD-41/HSPD-13), and the SAFE Port Act were created in the aftermath of the 9/11 attacks and were designed to enhance port security.

MTSA was enacted by the 107th U.S. Congress and signed into law on November 25, 2002 by President Bush (MTSA, 2002). MTSA represented the first major legislation since 9/11 that addressed port security. Though this legislation did not address the specific threat of M/UWIEDs, the act contained provisions meant to deter and prevent transportation security incidents by utilization of a "risk-based system for evaluating the potential for violations of security zones designated by the Secretary on the waters subject to the jurisdiction of the United States" (MTSA § 70103 (H)). The MTSA directed that the "Area Maritime Transportation Security Plan for an area shall, when implemented in conjunction with the National Maritime Transportation Security Plan, be

adequate to deter a transportation security incident in or near the area to the maximum extent practicable" (MTSA § 70103 2(A)). "The whole [maritime] system is built for speed and efficiency. Anytime you introduce security measures, you slow the system down. There's certain resistance to change, and [MTSA requested] huge changes in the way the maritime community operates," said Captain Dale, USCG (Peters, 2014, p. 1).

For the first time, ports would have to perform a balancing act by considering both business and security procedures (Quinn, 2003, p. S60). MTSA was a major step forward for U.S. port security, though just a first one towards preventing terrorists from exploiting security holes in what is generally a wide open system (Peters, 2014, p. 4). Under MTSA's provisions, the USCG required that access to port facilities be regulated, though left it up to each respective authority to decide how best to accomplish this, and was to ensure plans were compliant with the act's requirements (Peters, 2014, p. 2). Since inception, MTSA imposed a bureaucratic burden on the USCG. "We had to build a staff in record speed," said Commander Suzanne Englebert (Peters, 2014, p. 3). Problems with implementing the MTSA is that the USCG is propagating some regulations, and the MARAD, others procedures (Quinn, 2003, p. S64). Furthermore, funding has been an ongoing issue, especially during the last decade, as federal security grants have been slashed or postponed.

"We asked for $36 million and received $1.5 million…in the next round, we asked for $15 million and got $3.2 million…" griped Cunnigham at the Port of Los Angeles (Quinn, 2003, p. S60), and, according to Wong, Media Relations, Long Beach asked for $45 million and got $20 million (Quinn, 2003, p. S60). Besides reduced

funding, those responsible for port security and implementing federal mandates, a lack of coordination and guidance is also an impediment to success (Quinn, 2003, p. S59). Earl, Port Security Consultant, added that, "While some ports have gotten some funding, it certainly hasn't been enough. So, it becomes a question of determining priorities. The key issue is that every port needs its own unique security program" (Quinn, 2003, p. S60).

A provision of MTSA, the PSGP has, since 2003, provided more than $2.9 billion to port authorities, operators, and local and state agencies responsible for providing port security. In 2013, the PSGP allocated over $93 million to 271 recipients within 81 distinct U.S. port areas, and, in 2014, $100 million was awarded ("Evaluating Port Security: Progress Made and Challenges Ahead," 2014 p. 9). PSGP assigned port areas groupings that were founded on rankings of relative risk.

PSGP Group I was for those ports deemed highest risk; and, Group II, which includes ports not identified in Group I, I.e. *all other port areas* (DHS, 2014b, p. 1). In Fiscal Year (FY) 2014, in order to ensure that those ports ranked as under the highest risk received the most available funds, Group I ports were allotted the bulk (DHS, 2014b, p. 2). PSGP does not designate ferry allocation (DHS, 2014b, p. 1). However, certain ferry systems are eligible to apply for PSGP funds instead of the standard Transit Security Grant Program if a system is tasked with coordinating a water transit response to regional emergencies (DHS, 2014, p. 2), such as those operating on San Francisco Bay. In 2013, the Port of Oakland received $2,204,000 in PSGP funding, while the Port of Stockton received $1,573,750 (DHS, 2013).

In 2003, the DHS funded Operation Safe Commerce, a $28 million dollar grant given to over 15 companies that included: Atlantic USA; Boeing; Innolog; L.L. Bean; Parsons Brinkerhoff; Sara Lee Coffee and Tea Foodservice; SPC; Unisys Karachi; and, Unisys Santos. The grant allowed TSA to analyze supply chains and the companies to innovate security solutions. DHS Secretary Ridge said, “Operation Safe Commerce is about building on our capabilities and strengthening each layer of defense. This program provides the resources to find innovative new ways for ports to track and protect cargo entering the U.S. from all over the world” (Rios, 2011, para. 1). The Port Authority of New York and New Jersey, and Bearing Point managed the project (Rios, 2011, para. 1).

On December 21, 2004, President Bush signed NSPD-41/HSPD-13 regarding Maritime Security Policy. NSPD-41/HSPD-13 sought to secure the maritime domain, which was defined as "All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime related activities, infrastructure, people, cargo, and vessels and other conveyances” (NSPD-41/HSPD-13, 2004, p. 2). In order to accomplish this goal, NSPD-41/HSPD-13 established a Maritime Security Policy Coordinating Committee to supervise the development of a National Strategy for Maritime Security and subordinate plans for implementation (NSPD-41/HSPD-13, 2004, p. 2). As part of the National Maritime Transportation Security Plan, the National Strategy for Maritime Security (NSMS) would:

> … [P]resent an over-arching plan to implement this directive and address all of the components of the maritime domain, including domestic, international, public,

> and private components. It shall further incorporate a global, cross discipline approach to the maritime domain centered on a layered, defense-in-depth framework that may be adjusted based on the threat level. (NSPD-41/HSPD-13, 2004, p. 5)

Though focused on threats from environmental damage, nation states, transnational criminals and piracy, and, unlawful sea-borne immigration, the terrorist threat is recognized by the NSMS, and mines are mentioned as a potential vector: "[Naval] mines are an effective weapon because they are low cost, readily available, easily deployed, difficult to counter, and require minimal training" (DOD & DHS, 2005, p. 4). However, NSMS simply directed that criminal, hostile, or terrorist acts in the maritime domain be prevented by detection, deterrence, and interdiction (DOD & DHS, 2005, p. 8).

In order to improve cargo and maritime security through improved and layered defenses, SAFE Port Act was enacted by the 109th U.S. Congress and, on October 13, 2006, was signed into law by President Bush (SAFE Port Act, 2006).

The SAFE Port Act made a number of adjustments to programs, and created additional programs while changing others. The SAFE Port Act established and codified new initiatives and programs, and altered several of the provisions stipulated by MTSA ("Evaluating Port Security: Progress Made and Challenges Ahead," 2014 p. 2).

In assessing MTSA and general U.S. port security, including implementation of NSPD-41/HSPD-13, the GAO found port security policy incomplete and unsatisfactory in several areas, including: the TWIC; Foreign Seafarer Identification; Foreign Port

Assessments (Tenth Anniversary of the Maritime Transportation Security Act, 2012, pp. 5-6); as well as maritime domain awareness and dissemination of information; domestic port security; and, defense of the global supply chain. Though DHS agencies along with other port partners had enhanced visibility over the maritime domain, challenges remained, specifically, USCG's weak management of technology acquisitions had resulted in acquisitions that did not fully achieve intended purposes. Also, TSA and USCG administered a program requiring maritime workers to get a biometric identification card to enter particular port areas. GAO found weaknesses regarding this program's enrollment and background checks. Finally, regarding protection of the global supply chain, GAO found that DHS programs had been implemented with only varying levels of success (Maritime Security: Progress and Challenges with Selected Port Security Program*s*, 2014, p. 2).

In testimony before the U.S. House of Representatives Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, the CBP and USCG cited funding as a primary impediment to the complete and effective execution of both the MTSA's and SAFE Port Act's provisions (The Safe Port Act: Hearing before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, 2006, pp. 42-44), and, in 2010, Secretary of Homeland Security Napolitano—specifically citing the mandate to inspect 100% of all inbound containers, though speaking broadly about many U.S. port security programs—told the U.S. Senate Committee on Commerce, Science, and Transportation that she doubted the challenge could be met. "It will be

expensive. Very expensive," Secretary Napolitano said (SAFE Port Act Reauthorization: Securing Our Nation's Critical Infrastructure, 2010, p. 2).

In summary, since 9/11, overall port security has been improved as federal agencies have established committees to distribute information with relevant stakeholders, and efforts have been made to create interagency operations centers that watch port activities, conduct port patrols and the escort of vessels, to write and test with exercises port level plans for the interdiction and response to terrorist attacks, and security regimes at foreign ports have been assessed ("Maritime Security: The SAFE Port Act and Efforts to Secure Our Nation's Seaports," 2007, p. 2). Though protection of naval vessels and cruise ships from frogmen has been improved, and this helps mitigate the threat presented by terrorist limpet mines, there is, however, little progress in mitigating other weapon types and laying techniques represented by the overall terrorist M/UWIED threat.

Research Question 2

In Research Question 2 I asked: "How could terrorists use M/UWIEDs to attack U.S. maritime ports?" This question's results are organized by method of collection: document content analysis; direct observation of ports/inspection of physical artifacts; and, the Red Team hypothetical terrorist M/UWIED attack, with, where relevant, subgroupings that include: Mine warfare; Port security; and, the study ports.

Documents. A document content analysis was conducted of current mine warfare, the state of port security, as well as the study ports:

Mine warfare. The laying of naval mines, or the threat thereof, in homeland ports would have multiple consequences, including: impacting U.S. maritime services from operating within or deploying from these ports; the impediment or disruption of maritime commerce with resultant economic losses; a ripple effect over the global system of maritime shipping; and, resultant MCM costs (Lundquist, 2014, p. 39).

Despite this weighty threat, mine warfare goals and programs usually compete with each other for resources, begging the questions: Should the United States emphasize MCM at the expense of offensive or defensive mines and MIL?; What is the best way to allocate scarce resources between minehunting and minesweeping?; How can a Navy that likes aircraft carriers and submarines be convinced to sustain a modern mining capability? During Secretary of Defense Cohen's stint as a senior military advisor, he was once asked by a general: "What do we have to do, to keep the Navy's attention focused on mine warfare?" Cohen replied: "Ships got to sink and people have to die, or it will be business as usual" (Truver, 2014, p. 10).

MCM. The United States has been embroiled in land wars, and its strategic and tactical attention has been focused on this domain. Though this fact has taken focus off maritime conflict, especially mine warfare, there are lessons learned by the U.S. Army and Marine Corps in coping with land mines/improvised explosive devices in Afghanistan and Iraq, and several are transferable to the maritime domain and the countering of M/UWIEDs (Reynolds, 2013, p. 55).

These lessons that are transferable from the land to maritime domain include incorporation of UUVs and remotely operated vehicles onto existing ships and aircraft;

augment current MCM squadrons with technical analysis and exploitation specialists; create a database to record and analyze intelligence on naval mines; and, integrate MCM personnel and teams into naval strike groups at planning and operational level (Reynolds, 2013, p. 57). As the United States shifts its military focus to the Pacific theater and a rising Communist Chinese People's Liberation Army Navy with its formidable antiaccess/area denial systems and tactics that include mine warfare, the USN is once again heeding the threat and focusing on its capability to hunt and sweep mines; a capability judged in the spring of 2011 by USN mine warfare specialists as brittle (Rios, 2011).

As part of its Pacific shift, the USN established the Mine Warfare Center of Excellence at the Naval Mine and Antisubmarine Warfare Command, and located mine warfare forces together in order to improve training and readiness. Furthermore, the service has forward deployed MCM EOD detachments, helicopters, ships, and staff to guarantee quick responses to mine crises anywhere in the world (21st Century U.S. Navy mine warfare, 2012, p. 56), and, in an austere budget environment, has repurposed existing hardware towards the mission.

For example, U.S.S. *Ponce*—an aged amphibious transport dock—has been converted into an afloat forward staging base for the mine warfare mission (Ewing, 2012, p. 1). Using its large flight deck, *Ponce* serves as a Lilly pad for MH-53 Sea Dragon and other minehunting helicopters. Also, *Ponce* serves as a mother ship for MCM vessels, and her well deck could hold barges, patrol boats, or transport vessels, while its vehicle stowage areas: spare parts and specialized equipment (Ewing, 2012, p. 3).

The USN has also established a new Mine Countermeasures Vision that is based on making unmanned and modular MCM systems part of aircraft carrier and expeditionary strike groups. The Mine Countermeasures Vision also includes the capability for the Mine Countermeasures Force to be dispersed over large geographical areas with supporting environment and intelligence surveillance systems all networked through a system of nodes. Overarching operational concepts of Mine Countermeasures Vision are the development of unmanned and modular systems that cooperate under a networked command and control system; and to stand up a collaborative system that can form and disseminate a Common Environmental Picture (21st Century U.S. Navy mine warfare, 2012, p. 57).

Hardware. Subordinate to the fleet organic MCM capability, hardware development and investment are in the areas of air-borne MCM, unmanned systems, and automatic target recognition for minehunting sensors (Donaldson, 2013, p. 33). Unmanned systems are perfect for the so-called *3D missions*: "Dull, Dangerous, and Dirty" (Withington, 2010, p. 61), and are a means to reduce the burden on personnel while increasing port overwatch. Furthermore, several unmanned craft can be bought for the price of a single manned Coast Guard vessel (Withington, 2010, p. 62). Other hardware systems are also maturing and coming into the fleet.

New technologies include advanced targeting algorithms and counter-countermeasures (21st Century U.S. Navy mine warfare, 2012, p. 57), and active synthetic aperture sonar is an imaging method that takes several pings propagated along a survey path and associates the returns (Sternlicht, Fernandez, & Marston, 2013, p. 32). The U.S.

Office of Naval Research advanced synthetic aperture sonars to find, pinpoint, and classify mines, and will be used for surveillance of the operational environ; hunting, classification, and mapping operations; and reacquiring and identifying mine-like objects for consequent nullification (Sternlicht et al., 2013, p. 32). Acoustic frequency greater than 100 kilohertz—centimeter scale wavelengths—are used to image the seabed's surface consistency and locate any manmade objects located there. In order to image buried objects that stand proud of the bottom, longer wavelengths are used as they propagate deeper into sediment (Sternlicht et al., 2013, p. 32), such as bottom M/UWIEDs. Applying these advances is the Small Synthetic Aperture Mine-hunter (SSAM).

Developed by the Naval Surface Warfare Center Panama City Division and the Applied Research Laboratory of Penn State University, the SSAM uses multiple wavelength sensors to accurately image the seabed. The SSAM is carried by a Woods Hole Oceanographic Institution Remote Environmental Monitoring Unit S 600 that can be operated to a depth of 600 meters (Sternlicht et al., 2013, p. 32). The second generation SSAM has been in the field since 2010, and was designed to hunt objects in the shallow waters of near shore environments, particularly objects that stand proud of the bottom (Sternlicht et al., 2013, p. 33). Third generation SSAM is being designed to improve detection, localization, and classification capabilities against fully buried objects (Sternlicht et al., 2013, p. 35). With the LCS representing the bulk of the USN's future MCM vessels, Knifefish will be a primary system.

Knifefish Surface Mine Countermeasure UUV is built by General Dynamics Advanced Information Systems, and reliably detects and identifies buried mines in high clutter environments. Though designed for deployment aboard the LCS, Knifefish can be used aboard other vessels too (Lundquist, 2014, p. 39).

Despite this renewed recognition of the threat from mines, the focus remains on expeditionary warfare. Charged with domestic maritime security, the USCG, for the foreseeable future, will have no organic MCM capability of its own, and, since "scenarios recommend themselves as guide rails for the development of requirements, and they should cover a wide spectrum of possible tasks" (Schwarz, 2014, p. 125), this capability shortfall must be addressed if the threat of terrorist M/UWIEDs to homeland ports is to be mitigated.

Port security. According to Mitre, Security Director of the International Longshore and Warehouse Union, enormous security gaps exist at ports, particularly considering the poor identification measures for workers, particularly among truck drivers who enter ports on a regular basis (as cited in Peters, 2014, p. 5).

A 2005 DHS threat evaluation found gaps in MTS security, specifically: Detection of CBRNE weapons on vessels, both cargo and passenger; Detection of underwater terrorist activity; Infiltration of terrorists in cargo containers; Rapid response to a terrorist event on a ship or in a port; Response capability to deal with CBRNE terrorist events on a vessel; and, Small boat attacks (DHS, 2005, p. 17). Note there is no specific mention of the threat from terrorist M/UWIEDs, though the evaluation

recognized the general threat of underwater terrorist activity, interdiction of which would be integral to mitigating the terrorist M/UWIED threat.

Recent labor issues also have port security implications. For example, there has been a supply chain disruption that has been occurring since July 2014. The problem is worst at Los Angeles and Long Beach where, due to organizational problems, new Triple-Es—massive container ships that can transport up to 18,000 containers at once ("Triple-E: The world's largest ship," 2013)—and suspected purposeful worker slowdowns, the ports have been overwhelmed and backed up. The problem has become so bad in Southern California that the railroad Burlington Northern Santa Fe has refused to take additional containers from these facilities, as storage areas are full. At the Ports of Oakland, Seattle, and Tacoma, the Pacific Maritime Association has laid outright blame for the problem on slowdowns by members of the International Longshore and Warehouse Union (Wright, 2015). Such disruptions have a ripple effect that impact CBP inspections of containers.

The study ports. Maritime ports are "intersections of insecurity and security" (Chalk, 2008), and are stereotyped as "centers of moral corruption and decadence, cultural wastelands, and axes of large scale international drug traffic" (Van Hooydonk, 2007, pp. 28–30). The following subsections summarize results from crime data collected from the Port of Oakland and the Port of Stockton:

Port of Oakland. General crimes that occurred within port boundaries for 2013, and that the OPD responded to—sometimes with assistance from the Alameda County Sheriffs, and/or California Highway Patrol, though always as reporting agency with

jurisdiction within the port—ranged from abandoned vehicles, assaults, arson, blue alerts (violence versus law enforcement), cruelty to elders/dependents, disorderly conduct, and carjackings; traffic incidents/moving violations, such as failure to stop at signs, suspended or revoked driver's licenses, and collisions between vehicles—to disorderly conduct, felony bench warrants, fights, grand theft, murder, narcotics, sexual crimes, vandalism, and willful discharge of firearms (OPD, 2014b). However, there were several crimes/incidents of interest to this research's Red Team analysis, as well as in Research Question 3.

These included (number of occurrences in parentheses): Absent without leave (1); Alter/Forge/Falsify driver's license/identification (147); Carrying a concealed firearm in a vehicle (4); Damage to a telephone/power line (1); Grand theft of a truck (8); Security check (1,262); Special enforcement (140); Surveillance (1); Suspicious person/vehicle (598); Theft by forged/invalid identity card (13); Trespassing (270); and, Yellow alert (1) at the port (OPD, 2014b).

Port of Stockton. General crimes that occurred within port boundaries for 2013, and that the POSPD responded to—sometimes with assistance from the California Highway Patrol, San Joaquin County Sheriff Department, and/or Stockton Police Department, though always as reporting agency—ranged from abandoned animals, computer fraud, and, possession of narcotics; traffic incidents/moving violations, such as failure to stop at signs, suspended or revoked driver's licenses, collisions between vehicles, and truck damage to port infrastructure—gate houses; gangways; dock stanchions; power lines; pillars; and, light poles—to petty and grand theft, train

derailments, spilled truck loads, and water leaks that flooded roadways (POSPD, 2014). However, there were several crimes/incidents of relevance to this research's Red Team analysis, as well as in Research Question 3.

These included (number of occurrences in parentheses): An animal welfare check (1), whereby a seal was caught/entangled under a dock; Assisting an outside agency (1), whereby large numbers of POSPD personnel/units were drawn from the port to assist San Joaquin Sheriffs with a "shots fired call;" Breach of port security (17), whereby trucks or other vehicles entered/bypassed the port gatehouse by piggybacking (riding closely to another vehicle in order to deceive gate sensors); Environmental (1), whereby a large sheen/oil slick surrounded a vessel in port; Explosive material (1), whereby 100 kilograms of gunpowder was discovered in a port building; Impersonating law enforcement (1), whereby a person driving a railroad issued vehicle pulled another vehicle over and claimed to be an officer; Intoxicated in public (1), whereby a longshoreman was working under the influence of alcohol; Invalid/Fake ID (10), whereby employees/contractors entering the port presented false identification valid ID at gates; Person in the water (1), whereby a man went overboard from a docking vessel; Possession of an illegal weapon (1), a firearm; Power failure/outage (1), whereby security systems/cameras were affected; Trespassing (3), whereby the port was infiltrated via train by one foreign national, and two homeless citizens; Unescorted crew members (1), whereby a foreign national without an entry visa left port property; and, a Vessel incident (1) when the M/V *Claxton Bay* lost rudder control as she departed the wharf (POSPD, 2014).

Direct observations. I then conducted two direct observations for each of the sample ports:

The Port of Oakland. Both observations were land-based, with the first completed from the Alameda Main Street Ferry Terminal, Alameda, and, the second, from Middle Harbor Shoreline Park, Oakland.

The Alameda Main Street Ferry Terminal observation was completed on September 18, 2014, and lasted from 0530-0930. This time span comprised the darkness of pre-dawn hours and extended through sunrise into early morning light. Alameda Main Street Ferry Terminal is adjacent to the port's Turning Basin, and is directly across the primary navigation channel from Middle Harbor which includes the Roundhouse Property and Matson Terminal (Berths 60-63). During this observation, the weather was rain with rolling/intermittent fog, 16° C with 30% precipitation, wind at 0 km/h, and the sea/water state was calm with the tide flooding (high tide for the day occurred between 0800-1000). The MARSEC during this first observation was Level 1 (Checklist item 1).

The majority of the ship loading wharfs comprised concrete platforms suspended by concrete pilings (Checklist item 3). The M/Vs *Matson A* (Matson, Inc.) and *Singapore Express* (Hapag-Lloyd) were both docked and at berth. The *Matson A* was at berth 59 and being loaded with containers by port cranes XC18 and 19, with *Singapore Express* idle at berths 60-61 occupying the working area of cranes XC446 and 447. Two sailboats were observed making way in the port's primary navigation channel. The first was making way under sail power along the wharf (berths 57-63) and proximate to docked ships; and the

second was under power in the center of the primary navigation channel (Checklist item 6).

At daybreak, an Alameda County Sheriff's marine patrol vessel was observed making way along the port's primary navigation channel and was headed for open bay (Checklist item 7). Two Port of Oakland vehicles were observed moving along the docks. Both had flashing yellow rooftop light bars and patrolled approximately 1 hour apart beginning at dawn (Checklist item 8). Besides commercial jets climbing out over the port as they departed Oakland and San Francisco international airports, one light aircraft (identified as a Cessna) flew at medium altitude as it followed the port's primary navigation channel (Checklist item 9).

Camera towers were observed around the port property supplemented by bright lighting. I was unable to determine if the waterway was covered by said camera towers, though extensive coverage of the berths, container depots, rail yards, and truck marshalling areas appeared to be offered (Checklist item 12).

At dawn (sunrise was 0654), a pod of seals appeared in the primary navigation channel. They surfaced frequently and appeared to be feeding. Though I was unable to determine the species, common visitors to San Francisco Bay include Harbor Seals and Sea Lions (Checklist item 13).

The Middle Harbor Shoreline Park observation was completed on September 18, 2014, and lasted from 1205-1530. This time span comprised the light of midday. Middle Harbor Shoreline Park is adjacent to TraPac Terminal (Berths 30-32), Joint Intermodal Rail Terminal, and Hanjin Terminal (Berths 55-56). Observations were conducted from

within park boundaries at Point Arnold, as well as at the Port Operations Viewing Area and the park's Observation Tower. During this observation, the weather was cloudy with drizzle/light rain, 22° C with 30% precipitation, wind at 13 km/h, and the sea/water state was light chop with the tide ebbing (low tide for the day occurred between 1500-1700). The MARSEC during this first observation was Level 1 (Checklist item 1).

During the observation period, two vessels made way along the primary navigation channel: a recreational vessel at high-speed, and a Port of Oakland pilot vessel at medium speed (Checklist item 6).

During the observation period, a single Park Security vehicle (a Kawasaki Mule small all-terrain vehicle) made a rapid cursory sweep of the parking lot adjacent to the Port Operations Viewing Area. The respective security person was not vigilant as he was engaged in using a cell phone (texting) while operating his vehicle, and was therefore in violation of California Vehicular Code § 23123.5 (California Department of Motor Vehicles, 2011). As I departed the observation area in my own vehicle, a private security vehicle—belonging to Securitas USA—was observed patrolling the perimeter of port property. The operator appeared to be vigilant, scanned his field of vision, and even met eyes with me (Checklist item 8).

As I deployed for the observation, a USCG helicopter was observed overflying the port property. Using prior knowledge, I identified said aircraft as an HH-65C Dolphin. This identification was based on the evident Fenestron ducted fan antitorque device/tail rotor, as well as the aircraft's unique fuselage shape and rotor configuration (Checklist item 9). Prior to entering the direct observation location, I drove around the

port property's perimeter and observed 2.44 m high chain link fencing topped with either concertina wire or barbed wire outriggers, guarded entry points with gate arms at select gates, and a barrier of concrete K-rails along port access roads (Checklist item 10). Furthermore, several camera towers were observed during said circuitous route, with each seeming to sport speakers for a public announcement system and/or sirens (Checklist item 12).

The Port of Stockton. The first observation was land-based and completed from the vantage point of Louis Park-Pixie Woods, Stockton, with the second water-borne and completed aboard the M/V *California Sunset*.

The Louis Park-Pixie Woods observation was completed on August 29, 2014, and lasted from 1245-1600. This time span comprised the light of midday. Louis Park-Pixie Woods is directly across the primary navigation channel from the port's Embarcadero on Rough and Ready Island. During this observation, the weather was partly cloudy, 31° C with 0% precipitation, wind at 16 km/h, and the sea/water state was light chop with the tide ebbing (low tide for the day occurred between 1500-1700). The MARSEC during this first observation was Level 1 (Checklist item 1).

During this observation, multiple recreational watercrafts were observed. Said watercrafts sailed past ships that were at berth, and did so at high-speed. A Dutch flagged bulk carrier—M/V *Star Lima*—was discharging fertilizer at Dock 14 (Checklist item 6).

During the duration of the observation, no marine security patrols were visible (Checklist item 7), nor were foot or vehicle patrols observed sweeping port property

(Checklist item 8). The port was overflown by two civilian aircraft: one fast mover/business jet at medium altitude, and one helicopter at low level (Checklist item 9).

There was no evidence of neglected fencelines or other physical barriers along the primary channel (Checklist item 10), though one instance of graffiti was apparent on levee infrastructure adjacent to the port facility (Checklist item 11).

There was no apparent camera surveillance from the park-side shore (Checklist item 12).

The M/V *California Sunset* observation was completed on September 11, 2014—the thirteenth anniversary of the 9/11 attacks—and lasted from 1245-1515. This time span comprised the light of midday. The M/V *California Sunset* sailed an out-and-back route, departing Tuleburg levee/Weber Avenue Wharf, McLeod Lake, and coming about for a return voyage at Burns Cutoff, where the Calaveras River meets the San Joaquin River. During said observation, the weather was clear, 37° C with 0% precipitation, wind at 3 km/h, and the sea/water state was calm with the tide ebbing (low tide for the day occurred between 14:00-16:00). The MARSEC during this observation was Level 1 (Checklist item 1).

Warning signs for a buried pipeline were observed between channel marker 41 (starboard) and 42 (port) (Checklist item 3), and levees along the primary channel were protected by riprap in the wake zone (Checklist item 4).

During the voyage, multiple observations of relevance to Checklist item 5 were made: There were houseboats, recreational vehicles, and trailers parked or docked along the riverfront and adjacent to port facilities; abandoned boats—some appearing to be

seaworthy/usable—were in the riverfront yard of Stockton Iron Works; multiple abandoned/derelict buildings were observed along the riverfront; boat ramps were located under the I-5 viaduct, as well as parking and an homeless encampment; there was low or nonexistent fencing along the I-5 corridor at the port's perimeter; levee access beside the Perry Newman grain dock was open; an illegal camp/trailer home was present on the levee; multiple chain link fencelines were in disrepair along the levee adjacent to port property, with multiple small beaches, docks, and natural cover available; there are multiple private homes, many with docks, across from or adjacent to port property; and, there was no fence along the levee at West Marine.

Multiple cabin cruisers and other recreational vessels were docked at Stockton Marina and at the Sailing Club; M/V *Golden Arrow I*, a Panamanian flagged bulk carrier was discharging cement at Berths 3 and 4; several small recreational fishing boats were within port waters, including at Burns Cutoff, Mormon Slough, and the Turning Basin, with several sailing at high-speed past docked ships; and, the *Google Barge* and both M-580 barges—*A* and *B*—were at berth (Checklist item 6). The *Google Barge* is one of four floating barges built between 2010 and 2012, and commissioned by Google as interactive spaces for people to experience new technologies (Visit Stockton, 2014). The M-580 barges are tugged between the Port of Stockton and Port of Oakland, and are configured for containers (M-580: Marine Highway, 2014).

No marine security patrols were observed during this direct observation of the port (Checklist item 7).

Though no dedicated land-based patrols—either in vehicles or on foot—were observed, several port employees (dock workers/longshoremen) were present at the wharf's bulk cement facility, and contracted dredging vessels were manned at Wharf 9, as was the tugboat *Arthur Brusco* (Checklist item 8).

There were no overflights of port property by civilian aircraft (Checklist item 9) while M/V *California Sunset* made way along the San Joaquin River.

Though several levee fencelines were observed as being damaged and open near natural cover, fencelines within port property were well maintained and topped with barbed wire. However, an open and unattended gate was observed at the port's property line adjacent to Burns Cutoff (Checklist item 10).

There were multiple instances of graffiti along levees indicating the occurrence of illegal activities near port property and along the riverfront (Checklist item 11).

During the observation, a vertical takeoff and landing/quadcopter was air-borne and under the remote control of several operators at the levee outside the Commander's House. These operators worked from an unmarked pickup truck, and contacted the captain of the M/V *California Sunset*. Said captain informed those aboard that Port of Stockton personnel were operating the remotely operated aerial vehicle, and that it was to perform a flyby of the vessel, taking pictures and video for promotional purposes (Checklist item 12).

Finally, several environmental conditions were observed, including thick, green algae, predominantly so at McLeod Lake, and there were large rafts of water hyacinth (Eichhornia crassipes) all along the primary navigation channel, including at the port's

East Complex. Algae blooms are common in Stockton waters due to agricultural fertilizer runoff. This leads to a condition of low water-borne oxygen which is detrimental to fish populations and violates several environmental mandates. To mitigate this, the City of Stockton has deployed aerator pipes in several locations across the primary channel, including within port waters at Dock 20. These aerators force oxygen into the water and create a line of bubbles (Checklist item 13). Water hyacinth is a floating plant native to the Amazon basin. Varying in size from a few centimeters to over a meter tall, water hyacinth have lavender flowers, and leathery rounded leaves that are attached to flexible stalks that end in dark feathered roots. Water hyacinth is an invasive nuisance in the southeastern United States, as well as in California and Washington State. A hectare of healthy water hyacinth can weigh up to 73 metric tons ("Water hyacinth: Eichhornia crassipes," 2014). The spread of water hyacinth throughout the Sacramento-San Joaquin Delta has become an impediment to navigation and is interfering with commerce and security. "The hyacinth situation…has become a disaster," said Wells, Executive Director of the California Delta Chambers and Visitor's Bureau, adding: "Law enforcement boats cannot travel through the hyacinth and this opens up a possible national security threat as terrorists could attack ships…" ("Out of control hyacinth," 2014, para. 3). The Port of Stockton hired harvesters to scoop the plants from the main channel and the city is engaged in spraying to clear marinas and other waterways. Hyacinth has never been eradicated anywhere in the world, so the issue becomes one of control (Meza, 2014). "It's the worst I've seen and I've worked here for 20 years," said a worker at the Port of Stockton ("Out of control hyacinth," 2014, para. 4).

Inspection of physical artifacts. Each of the sample ports offers unique physical artifacts:

Port of Oakland. Port bathymetry, port infrastructure, and port physical design was inspected, as well as nonsecure access to proximate waterways (Checklist items 2-5):

At high tide, channel capacity is able to accommodate fully loaded Panamax size vessels. The port has 18 deep water berths, five container terminals, and 36 container gantry cranes, 30 of which represent post Panamax types (for ships that exceed Panamax specifications), and rail/truck (intermodal) access which is on-port. Bathymetry includes shipping channels and the majority of berths dredged to 15 meters (at mean lower low water), allowing the port to accommodate up to 13,000 container capacity vessels. There are multiple submerged cables, pipes, and tunnels that that cross the primary channel, or are buried within the primary channel (NOAA, 2013c). Figure 8 shows the navigational chart upon which these bathymetry and infrastructure assessments were based:

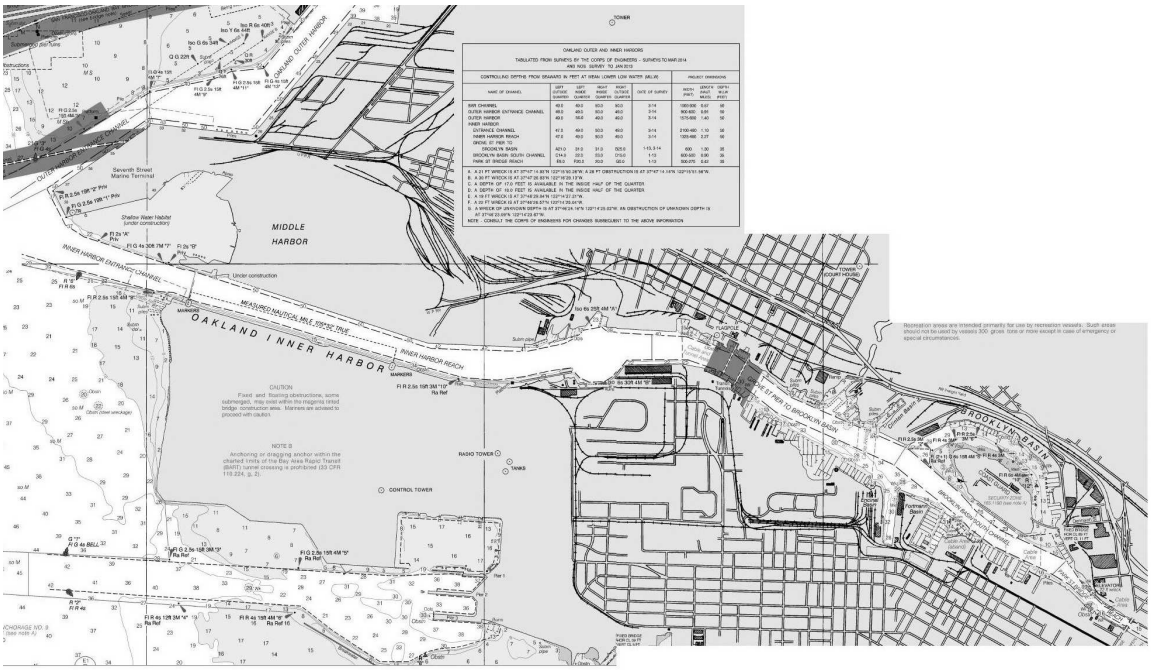

Figure 8. Navigation chart: Port of Oakland. From *Nav Chart Reference—San Francisco Bay Candlestick Point to Angel Island* (Chart 18650), by U.S. Department of Commerce/National Oceanic & Atmospheric Administration, 2013, retrieved from http://www.charts.noaa.gov/OnLineViewer/18650.shtml. In the public domain.

Port of Stockton. Port bathymetry, port infrastructure, and port physical design was inspected, as well as unsecured access to proximate waterways (Checklist items 2-5):

At high tide, the Port of Stockton's channel capacity is able to accommodate partially loaded Panamax size vessels. The port has 15 deepwater berths, two mobile harbor cranes, and rail access which is on-port. Bathymetry includes a dredged 11 meter deep (at mean lower low water) primary channel (Caltrans, 2012, p. 1), and berths range in depth from 10 to 11 meters. There are multiple submerged cables and pipes that cross the channel, and the I-5 highway spans the channel with a viaduct bridge that runs parallel to Mormon Slough (NOAA, 2013b). Nonsecure access to proximate waterways include: Brookside Golf and Country Club; Browns Island/Stockton Golf and Country

Club; Buckley Cove Park and Marina; Louis Park-Pixie Woods (includes two boat ramps); the levees that run along the San Joaquin River/M-580 and parallel to Burns Cutoff Road, as well as a multitude of private residences with docks along Atherton Island Place, Brookside Road, and West Riviera Drive. The port operates several video cameras for security, as well as for bat and owl nesting boxes, and public views of port facilities (Port of Stockton, 2014b). Figure 9 shows the navigational chart upon which these bathymetry and infrastructure assessments were based

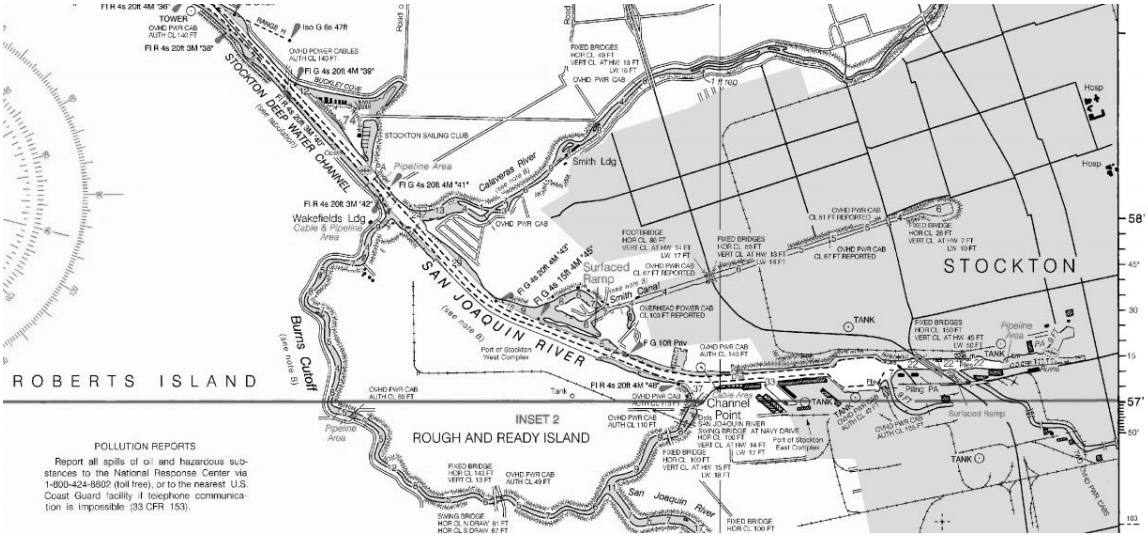

Figure 9. Navigation chart: Port of Stockton. From *Nav Chart Reference—Sacramento and San Joaquin Rivers* (Chart 18661), by U.S. Department of Commerce/National Oceanic & Atmospheric Administration, 2013, retrieved from http://ocsdata.ncd.noaa.gov/BookletChart/18661_BookletChart.pdf. In the public domain.

Red team. Red Teams try to penetrate defenses and thereby find problems and risks that insiders may have missed (McLeod, 2013). Results from this research question's document content analysis, direct observation, and inspection of physical artifacts identified vulnerabilities to terrorist M/UWIEDs. With respective tactics to

exploit said vulnerabilities, Red Team actions can be generalized to other ports of the MTS, as well of those of friends and allies abroad.

M/UWIEDs. Terrorist M/UWIEDs could come in a variety of forms, including: limpet, bottom, moored, and floating. Such weapons could be manufactured by nation states and supplied to or purchased by a terrorist or terrorist group, or constructed from readily available blueprints and materials.

Limpet. Limpet mines are simple in design as they are essentially waterproof timed devices with a means to be attached to submerged infrastructure or a vessel hull, such as by magnets or marine epoxy.

In a limpet M/UWIED attack scenario at a U.S. port, divers/frogmen would attempt to infiltrate a port undetected in order to reach and attack critical or symbolic target vessels such as passenger ships—cruise liners or ferries—which carry large numbers of people; oil tankers, liquid natural gas carriers, or other vessels that transport hazardous cargo. Limpet mines would be particularly effective in rapidly sinking a car ferry as the large internal space allocated to vehicles would flood rapidly and quickly overcome a vessels natural buoyancy or ability to pump out (Bonomo, Bergamo, Freliger, Gordon, & Jackson, 2007, p. 79). Such a scenario is not unrealistic. Al-Qaeda's head of operations in Southeast Asia, Omar al-Faruq, was apprehended in Indonesia in 2002, confessing to investigators there were plans for SCUBA attacks on U.S. warships docked in the Port of Surabaya (Richardson, 2004, pp. 22-23). Use of an Aqua Lung closed circuit breathing system does not send telltale bubbles to the surface (Richardson, 2004, p. 22) and imparts further stealth to such operatives.

Bottom/moored/floating. These three weapon types are essentially similar in design, save for their anchor/tether mechanism, and are generally deployed by aircraft or vessel.

During WWI, the North Sea Mine Barrage was a substantial minefield that was laid from the Orkneys to Norway by the U.S. and British navies (Vere, 2014, pp. 34-35), and was comprised of Mark 6 mines. The Mark 6 was a simple design that was comprised of a steel sphere that contained a buoyancy chamber and explosive material, in this case: TNT. The depth of the mine below the water surface was controlled by a mooring cable that unwound from a reel as the minelayer deployed it to the water. At the cable's end was an anchor with a wood pole that jutted beneath it. With the deployment zone depth known to the layers, the pole's length was equal to the depth desired for the mine to float beneath the water's surface. When the pole struck bottom, it locked the cable reel, and the anchor pulled the buoyant sphere to said desired depth. A float extended a copper antenna above the mine sphere that, when it touched the steel hull of a ship, would form a battery with salt water acting as an electrolyte to complete the circuit, therefore triggering detonation. A crude safety switch—protecting the minelayer and giving it time to depart the area—was a salt pellet that held open the detonating circuit, and took approximately 20 minutes to dissolve, rendering the mine safe for that period of time (Vere, 2014, p. 44). A design such as that of the Mk 6 could be improvised and, by altering or removing the anchor/tether mechanism, converted from moored to bottom or floating types.

Attack. A Red team attack was formulated for each of the sample ports. Given the sensitivity of homeland security issues, the details of the analysis will not be included. Rather, summaries of the relevant findings captured in this analysis are presented, though details of the Red Team's hypothetical attacks are available to appropriate authorities.

The Port of Oakland presented several vulnerabilities for exploitation by a Red Team, including: marine life; access from/security upon Alameda Island; small vessel traffic; and, weather. Marine life—specifically the Harbor Seals/Sea Lions that are prevalent in the waters of the port—are a presence that could act as a means of deception/camouflage for divers traversing/operating within the primary navigation channel, for as written by Sun Tzu (544 BC-496 BC)—an often quoted Chinese military general, strategist, and philosopher: "All warfare is deception" (Sun, 1972/2009). Alameda Island, due to its geographic proximity to the port, access to the Nimitz Freeway/Interstate 880, and its offer of multiple sally points for terrorist operations against the port, was therefore singled out as a Port of Oakland vulnerability. Small vessels are widespread in the shared commercial/recreational primary navigation channel of Oakland's Inner Harbor. As discussed in the Literature Review section (Chapter 2) of this research, small commercial and/or recreational vessels can be converted into effective minelayers. Weather is also a factor in offering cover for terrorist M/UWIED operations against the port, especially dense morning fog banks. The port tends to be blanketed by such banks just as ship traffic and imports increase for the holidays (Thanksgiving through Christmas). Fog offers natural cover for terrorist M/UWIED laying operations, specifically when combined with the aforementioned vulnerabilities.

The Port of Stockton presented several vulnerabilities for exploitation by a Red Team, including: geography; plant life; and small vessels. Unique among the study ports, this facility's waterway access terminates near its location. Unlike the through-type facility represented by the Port of Oakland, the Port of Stockton is located at a waterway terminus. Such geography could be exploited by terrorists to isolate the port or circumvent the port's security measures by attacking vessels along the lengths of the San Joaquin River/Marine Highway 580, an area that is, by its geographic vastness, not securable. Vulnerability to use of small vessels to attack this facility is similar to that of the Port of Oakland and most, if not all, of the MTS, as such vessels are exempt from the security provisions of the MTSA (Peters, 2014, p. 2), and could be used as M/UWIED layers within the facility's boundaries. Specific to the Port of Stockton is the proliferation of water-borne plant life, specifically water hyacinth. Water hyacinth propagation peaks in September, and could be used as a means of disguising terrorist M/UWIEDs. Furthermore, the use by the Port of Stockton of aerators to mitigate its water oxygenation/algae problem could be exploited by enemy frogmen to camouflage telltale SCUBA bubbles.

Besides exploitation of these vulnerabilities, standard diversionary/force dividing terrorist tactics should be expected to coincide with a terrorist M/UWIED attack upon one or more U.S. maritime ports, including: Cyberattack upon the facilities; one or more truck bombs detonating at security checkpoints and/or within the landward area of a port, likely targeting communications, power, or other vital infrastructure; infiltration by suicide foot teams with small arms and explosives; small aircraft loaded with explosives

and flown into port infrastructure (such as the port's command center), or into a docked vessel; and, small boats loaded with explosives and rammed into port infrastructure and/or vessels.

In summary, vulnerabilities exist within U.S. MCM and port security which could be exploited by terrorists seeking to unleash an M/UWIED attack or campaign. U.S. MCM capabilities are focused on expeditionary warfare, and new tactics and technologies are centered on providing an organic capability to amphibious and carrier strike groups operating globally. The USCG—the lead agency for port security—has no MCM capability, and USN mine sweepers are afield in support of, primarily, Persian Gulf operations to counter the threat to freedom of navigation presented by rogue states like the Islamic Republic of Iran, and as a balance against antiaccess/area denial capabilities presented by rising naval powers, specifically the People's Republic of China. Furthermore, though port security has been improved since 9/11, measures continue to be focused on the threat from CBRNE weapons, and have yet to come to terms with the threat from terrorist M/UWIEDs.

Research Question 3

In Research Question 3 I asked: "What port security management improvements should be implemented to further mitigate the M/UWIED threat?" The results for this question were organized by functional groups: Mine warfare; Organizations; and, Physical security; and then by subordinate tasks. For mine warfare, these tasks were adversary pathways and MCM; for organizations: roles and responsibilities, and budgets

and procurement; and, for physical security: landside and waterside. The limitations, alternatives, and evaluations of each of these tasks were then presented.

Mine warfare. Understanding enemy tactics and countering them is essential to mitigating the terrorist M/UWIED threat. Therefore, the tasks related to the function of mine warfare are: adversary pathways—how an enemy could lay mines—and MCM—countering them once laid.

Limitations. Analysis of adversary pathways models the security system, breaks the adversary's pathway into component steps from offsite to the CIKR that is being protected. The component steps relate to the adversary defeating a security element—either a detection or delay element—and analogous probability of detection or delay (Nuclear Security Science and Policy Institute, 2014). M/UWIEDs can be assembled off-site, and transported to and laid within a port area by civilian pleasure and/or commercial fishing boats. Both of these vessel types are exempt from the port security provisions enshrined in MTSA (Peters, 2014, p. 2). Detection would be accomplished by random or violation based investigation, whereby a land vehicle transporting M/UWIED components would be pulled over by police for an equipment or moving violation, or by a marine patrol—either police or USCG—conducting a random vessel safety inspection. Detection may also occur by visual means, whereby port security recognizes by camera or eye that suspicious activity—up to and including observing an M/UWIED laying operation—is occurring, and alerts law enforcement. An operational delay might occur due to natural conditions such as currents or weather, or by the presence of law enforcement assets within the operational area. It is likely, however, that any terrorists

would have contingency plans to deal with such occurrences, and be operationally flexible enough to circumvent such luck based detection or delays.

The USCG has no MCM capabilities organic to its fleet of aircraft, boats, and cutters. After the U.S.S. *Guardian*—one of the USN's 14 *Avenger* class minesweepers—ran aground on the Tubataha Reef while transiting in the Sulu Sea (a body of water in the southwestern area of the Philippines) and had to be scrapped (Martinez, 2013), the service now has just 13 dedicated minesweepers in its fleets. At any one time, 11 are forward deployed at Manama, Bahrain and Sasebo, Japan, leaving just two in San Diego, California (USN, 2013b) that would be available for homeland operations. Furthermore, should a terrorist M/UWIED attack occur on the eastern seaboard, the *Avenger*'s 14 knot speed would preclude a timely response, and, should simultaneous attacks occur, especially dispersed throughout the homeland, response time would be excessive, especially if attacks occurred at inland ports, such as upon the Great Lakes. There are also problems with development of the LCS mine warfare mission module. Notwithstanding over 6 years of development, some of the systems that comprise the new ships mine warfare mission module have been outright failures or did so poorly in tests, that the USN was forced to field older minesweeping systems and create ad hoc ones to challenge a grim mine threat around the Strait of Hormuz ("It's all in the package," 2014).

Alternatives. In order to mitigate such potential adversary pathways, there is a need for increased maritime domain awareness, patrols, and surveillance.

Small motorboats and fishing vessels—currently exempted by MTSA (Peters, 2014, p. 2)—that transit navigation channels shared with a commercial port, or that are adjacent to port infrastructure, should report to port control via radio. This is similar to how small private aircraft must contact air traffic control prior to transiting an airport's airspace or approach/departure lanes. Furthermore, during increased MARSEC levels, exclusion zones should be established around a port, whereby small craft would be banned from entrance and/or be subjected to inspection. In general, random safety inspections of small motorboats and fishing vessels should be increased. Finally, detecting and interdicting components required to assemble M/UWIEDs is essential. However, such intelligence based programs are beyond the scope of this study.

MCM assets should be included among USCG's inventory of aircraft, boats, and cutters. This could be limited to minehunting or extend into minesweeping, and could be accomplished by modifying current hardware or purchasing new ones. Aircraft, such as the MH-65 Dolphin and MH-60J/T Jayhawk helicopters could be adapted to mount the AES-1 Air-borne Laser Mine Detection System for minehunting. The Air-borne Laser Mine Detection System pod attaches to the aircraft with a standard mount and connects electrically to the operator console by umbilical cable. (Northrop Grumman Corporation, 2014a). For minesweeping, the AWS-2 Rapid Air-borne Mine Clearance System (Northrop Grumman Corporation, 2014b) uses a universal door mount already installed on USCG Jayhawks. Minehunting sonar sets could be installed on current boats and cutters operating in area and district commands. Rudimentary capabilities could comprise standard fish/depth finders for smaller boats, the GEC-Marconi Type 2093M variable

depth minehunting sonar for midsize cutters, and the AN/SQQ-32(V)4 minehunting sonar set (Program Executive Office: Littoral Combat Ship, 2014) for larger ones. Since the AN/SQQ-32(V)4 is a large hardware package that has through-hull requirements, its installation would be limited to larger vessels, such as the 82 meter Medium Endurance Cutter (USCG, 2014b). Furthermore, most USCG vessels have Electro Optical/Infrared cameras on board, and personnel should be trained to spot mines with them. According to Jeff Nicholas, Maritime Business Development Manager for FLIR Systems:

> Cameras can be used against a floating or moored mine where part of the mine is exposed above the water or at least very near the surface. The key is to have the cameras mounted high enough, so that the angle of the line-of-sight is not shallow, and part of the mine must be exposed with some temperature difference between the mine and the background. Usually, there will be a difference from the surrounding seawater, but more so in areas where there is a pronounced difference between air and sea temperatures. (Lundquist, 2014, p. 40)

Ultimately, though—the alternative I wished to emphasize—is procurement by the USCG of an MCM capable vessel. One of the two variants of the LCS (*Freedom*- and *Independence*-class) would be ideal, as they are shallow draft and capable of operating within the confined area and maneuvering space of ports (USN, 2013a). In addition, the MCM mission package is interchangeable with the surface warfare mission package (that includes: Mk. 46 MOD (X) Gun Weapon System; surface-to-surface missiles that are able to engage the threat from fast moving small boats; an MH-60R helicopter; and, two 11 meter Rigid Hull Inflatable Boats with cradles and parts (USN, 2014c), allowing

USCG stations to rapidly change the vessel's capabilities for the spectrum of the service's missions. For example, a USCG LCS could conduct standard patrols with the surface warfare mission package under its missions of: ports, waterways, and coastal security (PWCS); drug interdiction; defense readiness; migrant interdiction; marine environmental protection; and, other law enforcement (USCG, 2014c); and then swap its mission package to the MCM type for specialized minehunting and sweeping operations. In addition to domestic port security, USCG LCS's could contribute to foreign port security during expeditionary warfare assignments, supplementing USN assets.

An alternative to LCS would be procurement of allied/foreign designs. For example, the *Katanpää* class Mine Hunter, Coastal vessels are in service with Finnish Navy and constructed by Italy's Intermarine S.p.A. The *Katanpää* class ships are multipurpose in that they have, besides MCM capabilities, hydrographic survey capability, UUV deployment and control, and explosive ordnance disposal. The *Katanpää* class operates along the coasts and archipelagos of Finland's Baltic waters, though is also designed to be effective in open waters and for interoperability with NATO forces (Donaldson, 2013, p. 33).

Evaluation. The cost of continuing the present security system, one that is solely focused on CBRNE weapons is risky, as, demoting irregular and unconventional threats to a secondary priority, the 9/11 attacks showed, is a devastating strategic error (Adams, 2014, p. 19). The terrorist M/UWIED threat vector warrants budgetary consideration/funding.

The costs of implementing a USCG MCM capability would range from minor (adding minehunting hardware to existing aircraft, boats, and cutters) to substantial (procuring the LCS and its mine warfare mission package). However, such budgetary impacts would be relatively minor compared to the economic impacts of a successful terrorist M/UWIED attack upon the MTS.

Organizations. The efficient management of port security is essential to countering the terrorist M/UWIED threat. Therefore, the tasks related to the function of organizations are: roles and responsibilities, and budgets and procurement.

Limitations. The U.S. maritime services—the USCG and USN—have mission statements that encompass responsibility for freedom of navigation and security upon the territorial waters of the United States (USCG, 2013b; USN, 2013c), and are of obvious relevance to securing U.S. ports from the threat of terrorist M/UWIEDs, with the USCG responsible for preventing such an attack, and the USN for MCM should such an attack be successful.

The USCG has a diverse portfolio of missions that, by law, include: PWCS; drug interdiction; aids to navigation; search and rescue; living marine resources; marine safety; defense readiness; migrant interdiction; marine environmental protection; ice operations; and, other law enforcement (USCG, 2014c). These eleven missions were divided between homeland security and nonhomeland security by the Homeland Security Act of 2002, making PWCS the first homeland security mission, with the Commandant of the Coast Guard designating PWCS as the service's primary focus alongside search and rescue (USCG, 2014d).

The USN's mission is: "To maintain, train and equip combat ready naval forces capable of winning wars, deterring aggression and maintaining freedom of the seas" (USN, 2013c). This mission requires the navy to operate in the subsurface, surface, air, space, and cyber domains.

However, the stated purposes of an organization, such as those iterated by mission/objective statements, can be misleading, and can conceal, distort, idealize, omit, and rationalize essential aspects of the organization's function (Katz & Kahn, 1966, p. 206).

The U.S. maritime services are monocratic bureaucracies, organized, as Weber (1952) stated, "in a clearly defined hierarchy of offices," adding that, these organizations are "…capable of attaining the highest degree of efficiency and is…the most rational known means of carrying out imperative control over human beings" (p. 21). Marcson (1961) described this authority pattern as "a system of controls in which a superior in a hierarchical organization exercises ultimate control over subordinates" (p. 73). Weber would not consider the U.S. maritime services as ideal in that the owners—citizens/taxpayers—exercise control through their representatives in the three branches of the government, not through direct, executive control, nor do they coordinate the activities of the people and tools necessary to achieve the goals of the organizations. Monocratic nonideal bureaucracy is characteristic of most military establishments in that a clear chain of command is needed with absolute authority over subordinates, and that, even in a democracy—direct or representative—direct control by the owners would likely impede goal achievement through lack of relevant knowledge and divided decision

making (Becker & Gordon, 1966, p. 325). Such organizational limitations limit the ability of U.S. maritime services to recognize and react efficiently and effectively to new threats. Furthermore, the budgetary environment—which includes sequestration, as well as procurement—and outdated hardware, compound the challenges faced by U.S. maritime services as related to the terrorist M/UWIED threat.

In FY 2013, the USCG's PWCS mission was allocated $1,800,274; in FY 2014: $1,777,419; and made a FY 2015 request of $1,750,770 (USCG, 2014a). Furthermore, exemplifying the lack of focus on MCM capabilities by the U.S. maritime services, of the $148 billion procured for the USN's FY 2015 base budget, less than 1% has been allocated to MCM (USN, 2014b).

As the USCG operates vessels dating from the 1950s and 1960s, recapitalizing the fleet is a high and urgent priority, especially considering the service's increased homeland security responsibilities. Deepwater, an integrated, multiyear $25 billion project was meant to address these procurements. However, the program has had difficulties since its inception, with negative reviews from the defense industry and the GAO. According to former Commandant, Admiral Allen:

> Our people are demoralized by it, they don't deserve it, and it really impedes our ability to execute our mission… You will see changes shortly in the Coast Guard in our acquisition organization… It will be significantly different than we have done in the past. ("USCG's Deepwater effort," 2011, para. 9)

Alternatives. Bureaucratic reform would enable the USCG and USN to overcome systemic budgetary waste and procurement inefficiencies. Reforms initiated in the 1980s

and 1990s were to enable government to serve the public interest through efficiency and honesty. Honesty meant a government free of particularism—a political theory that each political group has a right to promote its own interests, independent to the interests of larger groups—; free of featherbedding—hiring more workers than needed to complete a given job, or adopting complex and time consuming procedures to employ additional workers—; and, outright theft of public funds (Barzelay, 1992, p. 533). This new paradigm shifted bureaucratic goals away from administration, control, the justification of costs, and the following of rules and procedures, and over to citizen value, product, delivering of value, and adherence to norms (Barzelay, 1992, p. 538). The move towards the post bureaucratic paradigm in the United States culminated with the 1993 National Performance Review; the so-called Gore Report. The goal of this report was to increase the efficiency of federal bureaucracy, to decrease the expenditures required by its operation, and to shift the bureaucratic culture away from prerogative and self-regard toward dynamism and delegation of power (Shafritz, Russell, & Borick, 2007, p. 112).

After this era of reinvention, privatization became the next tack taken toward increased bureaucratic efficiency. Privatization was a method widely seen as a threat to public administration (Shafritz et al., 2007, p. 116). Like other government agencies, the USCG and USN, too, had adopted this method. Privatization received extensive criticism, including that such a strategy led to corruption, made it difficult to monitor performance and outcomes, reduced control over services, and limited competition. The U.S. armed forces exist, simply, to fight. Even this, however, has been privatized/outsourced at some levels, as with the controversial use of private security in the Iraq War (Shafritz et al.,

2007, p. 119). A major criticism of the current structure of the U.S. armed forces is that they are officer heavy, with too many admirals and generals overseeing too many special offices. Organizationally, this means that vertical differentiation is extensive, to the detriment of horizontal differentiation, thus making the U.S. armed forces tall organizational structures whereby they are laden with extensive and various levels of management (Nickels, McHugh, & McHugh, 2008, p. 213). This makes them highly bureaucratic, and high levels of bureaucracy translate to waste and inefficient procurement.

In 2010, Admiral Papp, Commandant of the Coast Guard, offered a broad modernization of the Blueprint for Continuous Improvement that detailed the objectives and structure the USCG wanted for its Acquisition Directorate. Since the recapitalization of USCG assets is critical to future readiness, the blueprint has to steady acquisition activities for this recapitalization to be successful (USCG, 2010, p. 2). The blueprint instituted reforms that are still in force, and included means to avoid duplicate efforts by creating strong partnerships; checks and balances; commitment to transparency; departmental oversight; independent validation; organic certifications; robust strategic planning; and, standard references for acquisition management (USCG, 2010, pp. 19-20). According to Vice Admiral Currier, Chief of Staff, “Our piece is to be aggressive in our management of the acquisition process so that we control costs, manage risks and bring these systems on board at the lowest dollar figure we can” (USCG, 2010, p. 20).

The greatest challenge to the USN’s budget is the growth of personnel costs. Chief of Naval Operations, Admiral Greenert, said, "We cannot sustain our current

personnel cost trajectory. We need to address this problem sooner rather than later" (USN, 2014a, para. 2). Due to a reduction of fleet size by some 25 ships with corresponding reductions in manpower, personnel costs have risen. This has affected USN's ability to balance investments (USN, 2014a).

Evaluations. Recognizing that the growth of personnel costs is unsustainable, DOD proposed compensation reforms that are estimated to save the USN $123 million in FY 2015 and $3.1 billion over the 5 year Future Years Defense Plan (USN, 2014a).

The Coast Guard and Maritime Transportation Act of 2014 (CGMT) reduced the number of commissioned USCG officers eligible for promotion from 7,200 to 6,700 (CGMT, § 201) and required the Commandant, every 4 years after FY 2019, to give Congress a unified major acquisition statement that identifies existing and potential future gaps in USCG capabilities by using mission hour targets (CGMT, § 209). CGMT also authorized $17.5 billion for continuing USCG operations FY 2015-2016 (CGMT). According to Representative Hunter (California), the bill's sponsor, the legislation will:

> Improve the effectiveness of Coast Guard missions by reducing inefficient operations and enhancing oversight, places the Coast Guard's major systems acquisition program on a sustainable track, and encourages job growth in the U.S. maritime industry by cutting regulatory burdens on job creation. (House of Representatives, Transportation and Infrastructure Committee, 2014, para. 4)

Such personnel cost reforms, the CGMT's 9% reduction in potentially promotable officers, and alignment procurement with mission needs are needed first steps to remedy the aforementioned task limitations of budgets and procurement.

Physical security. Securing a port and adjacent waterways is essential to countering the terrorist M/UWIED threat. Therefore, the tasks related to the function of physical security are: landside and waterside.

Limitations. Port landside security as related to terrorist M/UWIEDs includes infiltration of weapons and/or their components for use as part of a mining campaign. Such infiltration can be facilitated by fenceline exploitation, as well as train or truck/vehicle entry. Both the document content analysis and direct observations conducted by this study exposed the potential for these types of perimeter infiltration, including: neglected or open fencelines, and train and vehicle-borne security breaches at facilities. Potential infiltration of terrorists and/or M/UWIEDs or their components by train is likely as, railroad spurs penetrate port perimeters at multiple points and often are not subject to the same security procedures as trucks/vehicles. Also, trespassing upon railroad property, including at mainlines and yards, and *train jumping* is relatively easy due to lack of physical security and the sheer size of rail networks (Plant & Young, 2007).

Operation Neptune Shield is the Coast Guard's plan for protecting ports at waterside. As part of Neptune Shield's regulations and security systems are three Maritime Safety and Security Teams (MSST). Each MSST is composed of approximately 40 active duty Coast Guard personnel that are equipped with armed boats for patrol, detect and countering of threats. MSSTs were deployed to replace Coast Guard Port Security Units that had been created to protect U.S. maritime ports in the immediate aftermath of the 9/11 attacks. There are plans and budget requests to expand the number

of MSSTs ("Operation Neptune Shield Aims to Protect," 2002). A limitation of port waterside security is lack of jurisdictional control, whereby waterways are monitored/secured by a mix of local, county, state, and federal agencies.

Alternatives. By adopting improved physical security, ports can reduce the risk of terrorist M/UWIED and/or other threat vectors.

Fences are a simple yet effective means of securing a port's perimeter. However, fences must be maintained and their gates secured. Furthermore, fences should be treated as sensors, not just impediments, and when supplemented by appropriate systems, can locate a cut or climb attempt to a single fence panel (PureTech Systems, n.d.).

Beyond fences, landside perimeter security must rely on video intrusion, loitering, and object detection. Such video systems need to offer complete coverage of access points and port area, and should incorporate thermal imaging for night/inclement weather and offer target tracking. On top of such capabilities, optical character recognition—face matching tied to national databases—is essential considering the number of people that access port facilities each day, doing so primarily by trains and trucks/vehicles.

Though general railroad security is beyond the scope of this research, inspection of trains entering port facilities is needed. Truck-specific alternatives include a designated CB radio channel that truckers can use to contact port security, and that closed circuit TV cameras at port gates should include the capability to surveil trucks from overhead and underneath. According to Ralph Earl, port security consultant: "Trucks are the main problem…there should be a secure, quarantined area where verification and clearance can be accomplished before access is gained to the port itself…" (Quinn, 2003, p. S62). Such

alternative landside physical security recommendations should be implemented across the spectrum of MTS facilities.

Waterside security must include periodic surveillance of port bathymetry. By updating bottom topography, new objects can be recognized and investigated, offering the basis for speedy MCM due to detailed knowledge of the environment (Schwarz, 2014, p. 126) and the creation of "Q routes"—narrow channels that have been swept and cleared of mines (Reynolds, 2013, p. 55)—during a terrorist M/UWIED incident.

Maritime security is focused on large commercial vessels, and their cargoes and crew. Since terrorists could exploit small vessels for their purposes, the security regime, including MTSA, has to move beyond traditional safety and basic law enforcement concerns, and recognize the threat such vessels can pose, up to and including being used to transport and lay terrorist M/UWIEDs. CBP's Pleasure Boat Reporting System relies on boaters self-reporting, and, it is estimated that only a small fraction of arrivals do so, allowing foreign boater traffic to operate unimpeded in U.S. maritime ports and waters (DHS, 2008c, p. i).

Finally, the educational outreach under America's Waterway Watch—a program that emboldens backers to report dubious activities to the Coast Guard—should be expanded to include the terrorist M/UWIED threat and how to recognize activity that could be part of such a threat (USCG, 2012). Such education should be extended to longshoremen as well, as, according to Rooney of the Port Authority of New York and New Jersey: "Our longshoremen are the port's first line of defense. If anybody can make a judgment…it's these guys" (Quinn, 2003, p. S62).

Evaluations. Converting a port perimeter fenceline to include a cut/climb sensor, as well as installing video detection with target track and respective management software is approximately $550,000 per facility. Such cost includes intrusion alarms and signal systems; facility management systems; perimeter security/detection systems, fences, and sensors, as well as ancillary services (General Services Administration Federal Supply Center, 2010).

The cost associated with educational outreaches through America's Waterway Watch and annual longshoreman safety and security training would be negligible, and could be procured from Homeland Security grants and/or union dues. Expansion of the Pleasure Boat Reporting System would incur costs that could be absorbed by a fee collected from foreign vessel owners entering U.S. waters.

With lower risk of attack, port authorities could enjoy reduced insurance rates and subsequent cost of operations. Such reduced costs translate to lower port access fees for shippers and, therefore, increase vessel visitation to the facility.

In summary, results of Research Question 3 highlighted limitations related to the port security functions of mine warfare; organizations; and, physical security, and offered and evaluated alternatives to increase port security as related to the threat of terrorist M/UWIEDs.

Evidence of Trustworthiness

In this study I implemented credibility, transferability, dependability, and confirmability strategies stated in Chapter 3 with no adjustments.

Credibility was accomplished by incorporation of multiple sources, including: document content analysis, direct observations, and inspection of physical artifacts. Such evidentiary triangulation strengthens the credibility of case studies (Yin, 2003, p. 36). Furthermore, all documents were from peer-reviewed journals, and/or vetted government sources.

Transferability was accomplished by selection of the sampling model. The sampling model was two ports that reside at opposite ends of the type spectrum, with varying size, tonnage handled, cargo handled, number of vessels calling on the port, value of cargo handled, as well as physicality such as location—open water versus river—and variety of surrounding infrastructure. Because of this sampling model, and the blanket effect of U.S. port security management policy across the 361 ports of the MTS, conclusions are directly relevant and transferable across this system, as well as those of friends and allies abroad that employ similar systems, and tend to emulate U.S. policy.

Dependability, reliability, and validity were accomplished by triangulation. By incorporating document content analysis, direct observations, and inspection of physical artifacts, and triangulating collection and analysis, results are strengthened and inherently dependable.

Confirmability was accomplished through reflexivity. As data were analyzed, explanations were built and associated by causal link (Yin, 2003, p. 120). By using the cause and effect type of data analysis, I developed explanations before causally linking them. When effects became evident, per reflexivity, I bent back on the cause to analyze the circular relationship.

Summary

In Chapter 4 I presented the research questions of this study by data collection, coding, analysis, and results. In Research Question 1, I performed a document content analysis of U.S. port security directives, hearings, laws, and policies from September 11, 2001 to September 11, 2014, and found that overall port security has been improved since 9/11, steps have been taken to establish interagency operations centers, and security at foreign origination ports have been assessed and buttressed. However, the threat vector of terrorist M/UWIEDs has not been included in said improvements, and the focus of security regimes is on CBRNE weapons.

In Research Question 2, I performed a document content analysis of crime reports directives, legislation, literature, policy, and threat assessments regarding mine warfare and the current state of port security, performed direct observation of two ports, and inspected their physical artifacts. The document content analysis revealed several findings, including that: though port security has improved since 9/11, gaps exists that could be exploited by terrorists, mine warfare has been neglected by the United States, and what capability that exists is focused on expeditionary warfare and forward basing far from homeland ports; and, during 2013, both study ports experienced security breaches or other crimes indicative of potential avenues for facilitation of a terrorist M/UWIED attack. The direct observation and inspection of physical artifacts at the Port of Oakland and Port of Stockton revealed different strengths and weaknesses. However, by the very nature of port operations, a terrorist or terrorist group could use an

M/UWIED attack to disrupt one or more ports, and/or cause damage to vessels, port infrastructure, and general commerce.

In Research Question 3, I collected and organized results from Research Question 1 and 2 by performing an MAA by port security functions of mine warfare, organizations, and physical security, and, utilizing GST, presented limitations, alternatives, and evaluations, finding that interdiction of adversary pathways are incomplete, that the MCM capabilities of U.S. maritime services are limited in their ability to respond rapidly and effectively to a terrorist M/UWIED attack at one or more homeland ports, that U.S. maritime services are hampered as organizations by budgetary and procurement issues, and that ports are vulnerable to infiltration at both the landside and waterside. In Chapter 5 of this study I interpret the findings of the study as addressed in Chapter 4, as well as discuss limitations, recommendations, and implications.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

Since 9/11, there has been much focus on securing the United States' CIKR from terrorist attack, with the federal government spending billions of dollars to this end, including over $7 billion on port security alone (The Safe Port Act: Hearing before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, 2006, p. 2). Much of this expenditure has been aimed at securing ports from the infiltration of CBRNEs. However, these efforts have neglected to recognize the threat presented by a centuries-old weapon type: the M/UWIED.

The purpose of this qualitative study was to examine the threat to U.S. maritime ports presented by terrorist M/UWIEDs, and I sought to do so from an adversarial perspective with the intent of discovering security improvements that could help mitigate this threat by recommending bureaucratic and policy reform.

This study was qualitative in nature, used the theoretical framework of GST (von Bertalanffy, 1969) to examine existing documents and legislation enacted since 9/11, and employed a sample of two California ports—Oakland and Stockton—that represented opposite ends of the sample size/type spectrum.

Key findings of this study were as follows: Since 9/11, overall port security has been improved. However, there has been little progress in countering the threat presented by terrorist M/UWIEDs; vulnerabilities exist within U.S. MCM and port security that could be exploited by terrorists seeking to unleash an M/UWIED attack or campaign; and there are limitations in U.S. mine warfare, maritime service organizations, and physical

port security that could be exploited by those that seek to do harm to the MTS by utilizing the inherent advantages offered by M/UWIEDs.

Interpretation of the Findings

The 9/11 terrorist attacks showed U.S. security agencies to expect the unexpected. However, the expected threat to U.S. maritime ports and the urban areas they often occupy (CBRNE weapons) have been the focus of security management—a worst-case physical damage scenario—while the potential for mass destruction of the economic and psychological sort represented by weapons like M/UWIEDs has been, essentially, ignored.

By recognizing and examining the threat presented by terrorist M/UWIEDs to U.S. maritime ports, as well as the vast system of commerce that these facilities support, this study's findings extend knowledge in the discipline of homeland security by exploring logical questions related to this threat. Furthermore, this study's results extended discipline knowledge found in the peer-reviewed literature described in Chapter 2, specifically in the thematic areas contained therein: terrorism, mine warfare, and port security.

Government stakeholders know that "terrorists seek to exploit the complexity of the maritime domain and the vulnerabilities of the global supply system" (USCG, 2007, p. 5). Terrorists choose maritime targets that are economic, environmental, hazardous/volatile, symbolic, or passenger laden (Murphy, 2008, pp. 200-212), and one of the tactics available to terrorists is to attack ships in port (Rodeman, 2003, p. 7). My

study's results extend knowledge of the general terrorist threat as well as the specific one related to the MTS by recognizing and examining the vector of M/UWIEDs.

As stated by Truver (2008), small commercial, fishing, or pleasure vessels, which are exempt from the provisions of the MTSA, could be used as camouflaged minelayers by terrorists (p. 108). Watts (2005) stated that the high volume of genuine small vessel traffic in ports could mask terrorist movements and operations prior to an attack, thus making nominal defense difficult (p. 5). During the direct observation portion of this study, I was able to confirm these findings regarding the vulnerability of ports to these vessel types, as they are prevalent, and operate freely within waterways.

Evans and Stutin (2006) found that the concentration of U.S. MCM assets in a single continental port lacked the strategic flexibility and reaction time required to combat M/UWIEDs in such a way as to minimize port closure and economic impacts (p. 31). Dowd (2004) stated that the damage from an M/UWIED event would be strictly linked to the speed of a response effort and the subsequent ability to open a targeted port(s) and its channels to shipping (p. 3). In the course of my study, I found that the United States has little employable MCM capability located in or near the homeland and continues to concentrate these limited capabilities in one west coast port (San Diego). This limited capability and its geographic concentration precludes a rapid response to a terrorist M/UWIED attack, especially if such an attack was part of a campaign that included multiple ports on across the geographic expanse of the MTS. In addition, this limited capability could easily be diluted and divided by false terrorist claims regarding

mining of a port, such as with the case of the Patriotic Diver incident in the Sacramento River (USN, 2009, p. 11).

GST allowed me to investigate the interaction of multiple organizations (Senge, 1990, p. 73) responsible for U.S. port security and, as expressed by Patton (2002), allowed a view of things "as whole entities embedded in context and still larger wholes" (p. 120). This holisticism allowed an examination and interpretation of the complex systems inherent to port security and, overlaid with the DHS's standard MAA, permitted me to focus on the goal, missions, objectives, and functions (HSSAI, 2007) related to protecting U.S. maritime ports from terrorist M/UWIEDs.

The MARAD Port and Maritime Security Working Group (as cited in Clark et al., 2007) stated "much in the way of organizational stove piping and cultural impediments remain that impedes effective, efficient and sustainable development and deployment of optimum homeland and port security" (p. 30). My study confirmed that such organizational problems continue to plague the agencies responsible for U.S. port security and that budget constraints and inefficient procurement is compounding potential vulnerabilities to terrorism, specifically the terrorist M/UWIED threat.

Limitations of the Study

This study could only exploit data available to the public, and I was unable to use that which was of a classified nature. This limitation precluded examination of classified DHS documents related to terrorist M/UWIED campaigns or intelligence, or documents related to criminal activity/security at the Ports of Oakland and Stockton that were

deemed not releasable under the security provisions of the California Public Records Act and/or general national security concerns.

Despite this limitation, the results from my study and related interpretations should be used to inspire and guide future studies that examine this potent threat. By using my study's framework and method of observing and examining U.S. maritime port facilities with the mindset of an adversary, knowledge in the discipline will be advanced. By guiding those with access to classified data, this study acts a foundation upon which to base further research and threat assessments to steer U.S. CIKR policy in an appropriate and relevant direction, thereby advancing homeland security.

Recommendations

Academia plays an important role in CIKR protection. Through research and analysis, academics provide innovative thinking and perspective on threats (DHS, 2009, p. 28). Based on the strengths and limitations of this study, the following recommendations are presented for further study:

First, the potential for terrorist to utilize M/UWIEDs against nonport components of the MTS should be investigated. These nonport components include 40,234 kilometers of navigable channels; 238 locks at 192 locations; the Great Lakes and St. Lawrence Seaway; over 3,700 marine terminals; and, numerous recreational marinas and water transportation (ferry) facilities (DOT, n.d.).

Second, research into funding strategies for expansion of port security regimes related to the M/UWIED threat should be conducted. Such research could include examination of potential federal sources and/or a user service tax/shipper's surcharge.

Third, an investigation of the potential use by terrorists of cyberattacks against port facilities is needed as, like other computerized systems, port security management software can be infiltrated and manipulated to facilitate a terrorist M/UWIED attack or campaign.

Fourth, this study should be replicated, though without the limitation of using only nonclassified data. This would necessitate a threat assessment by a government agency or by academia with security clearance. Furthermore, Red Team attacks on U.S. ports should be conducted in cooperation with port security agents and the maritime services.

Implications

The findings from this case study contribute to positive social change by providing data to key stakeholders responsible for making policy regarding counterterrorism, mine warfare, and port security, thereby contributing to overall U.S. homeland security.

Due to societal reliance upon maritime trade for economic wellbeing and maintenance of the standard of living, port security is a major issue in the United States. Because maritime transport is the foundation upon which our modern globalized society rests, it is essential that the entire spectrum of threats to the MTS be recognized, that security of the system be enhanced and maintained, and that security measures not become burdensome by impeding commerce and, therefore, increasing costs of goods.

Maritime port security is an integral part of protecting U.S. CIKR from terrorist attack. Current port security is focused on the mass destruction component of the

spectrum—specifically, the threat of CBRNEs infiltration via containers—and has neglected to focus on lower intensity threats, such as that presented by terrorist M/UWIEDs. Further research and government threat assessments

Though improvements to port security have been made since 9/11, these improvements must continue and U.S. port security management should recognize the entire spectrum of threat vectors to the facilities—specifically terrorist M/UWIEDs—and apply appropriate resources towards mitigating them. Therefore, the results of my study have brought to light the following specific recommendations:

- Small motorboats and fishing vessels that transit navigation channels shared with a commercial port, or that are adjacent to port infrastructure, should report to port control via radio.
- During increased MARSEC levels, exclusion zones should be established around a port, whereby small craft would be banned from entrance and/or be subjected to inspection.
- MCM assets should be included among USCG's inventory of aircraft, boats, and cutters.
- Reduce systemic budgetary waste and procurement inefficiencies in the U.S. maritime services through bureaucratic reform.
- Port security fences must be maintained and their gates secured. Furthermore, fences should be treated as sensors, not just impediments, and include cut or climb sensors.
- Ports should install video intrusion, loitering, and object detection.

- Trains entering port facilities should be inspected at the property boundary.
- Ports should have a designated CB radio channel for truckers to contact port security in an uncertain situation.
- Closed circuit TV cameras at port gates should include truck undercarriage and overhead surveillance.
- Port bathymetry should be periodically surveyed and compared to baseline surveys for recognition of new/suspicious objects.
- The educational outreach under America's Waterway Watch should be expanded to include tactics and hardware that terrorist might employ as part of an M/UWIED attack or campaign.
- Establish a *culture of security* among port personnel and longshoremen and establish whistleblower protections to all such workers.

Though beyond the scope of this study, I also recommend that intelligence-based programs that detect and interdict components relevant to the design and/or assembly of M/UWIEDs be established or expanded. I also recommend that general railroad security be improved, as railroads are a key component of intermodal transportation of which the MTS is a component. Due to decentralized openness of the railroad system, it is ripe for attack or exploitation by terrorists (Plant & Young, 2007; Sullivant, 2007), including as a means to infiltrate ports with weapons or operatives.

It is my hope that, with implementation of these recommendations, that security management at U.S. maritime ports will be improved, thereby improving overall homeland security, and that my work will therefore contribute to positive social change.

Conclusion

The majority of U.S. exports and imports move through maritime ports (USN, 2009, p. 11), CIKR that are essential to the nation's economy, public health and safety, security, and way of life. Such facilities are representative of the type of high value target that are coveted by terrorists seeking to further their strategic goals.

M/UWIEDs are the quintessential asymmetric naval weapon (Truver, 2008, p. 107). They have been used by domestic terrorists in the Sacramento River and Lake Ponchartrain; and, by foreign terrorists and irregular forces against the vessels *Bridgeton*, *Invincible*, and *Rainbow Warrior*, as well as in multiple North African and Middle Eastern theaters where commercial and military vessels have been crippled or sunk. If 9/11 taught those charged with U.S. security anything, it is to expect the unexpected, and it is only prudent to expect that terrorists will employ such cheap and easily made weapons in homeland waters.

In hopes of contributing to positive social change by improving security management at United States maritime ports, I examined the terrorist M/UWIED threat and made recommendations for mitigation. It is imperative that these recommendations be implemented by stakeholders, public and private. Finally, additional research outlined in Chapter 5 should be conducted to further improve security at U.S. maritime ports.

References

Adams, D. A. (2014). Repeating three strategic mistakes. *U.S. Naval Institute Proceedings*, *140*(9), 18-23.

American Association of Port Authorities. (2013a). U.S. port industry. Retrieved from http://web.archive.org/web/20070104213136/http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1022&navItemNumber=901

American Association of Port Authorities. (2013b). U.S. public port facts. Retrieved from http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032

Bajoria, J., & Bruno, G. (2012). Al-Qaeda backgrounder. Retrieved from http://www.cfr.org/terrorist-organizations-and-networks/al-qaeda-k-al-qaida-al-qaida/p9126

Barzelay, M. (1992). Breaking through bureaucracy. In J.M. Shafritz, A.C. Hyde, & S.J. Parkes (Eds.), *Classics of public administration* (p. 533). Boston, MA: Thomson-Wadsworth.

Becker, S. W., & Gordon, G. (1966). An entrepreneurial theory of formal organizations Part I: Patterns of formal organizations. *Administrative Science Quarterly*, *11*(3), 315-334.

Bennett, J. (2008). *Maritime security*. Burlington, MA: Butterworth-Heinemann.

Bonomo, J., Bergamo, G., Freliger, D. R., Gordon, J., IV, & Jackson, B. A. (2007). *Stealing the sword: Limiting terrorist use of advanced conventional weapons*. Santa Monica, CA: Rand Corporation.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and*

code development. Thousand Oaks, CA: Sage Publications.

Caldwell, S. L. (2007). *Maritime Security: Observations on selected aspects of the SAFE Port Act* (GAO-07-754T). Washington, DC: Government Accountability Office.

California Department of Motor Vehicles. (2011). Electronic wireless communications device: Prohibited use. Retrieved from https://www.dmv.ca.gov/pubs/vctop/d11/vc23123_5.htm

Caltrans. (2012,). *Freight planning fact sheet: Port of Stockton*. Retrieved from http://www.dot.ca.gov/hq/tpp/offices/ogm/ships/Fact_Sheets/Port_of_Stockton_Fact_Sheet_073012.pdf

Caltrans. (2013). *Freight planning fact sheet: Port of Oakland*. Retrieved from http://dot.ca.gov/hq/tpp/offices/ogm/ships/Fact_Sheets/Port_of_Oakland_Fact_Sheet_073012.pdf

Canal de Panamá. (2014). *FAQ: What are the lock dimensions?* Retrieved from http://micanaldepanama.com/expansion/faq/

Chalk, P. (2008). *The maritime dimension of international security: Terrorism, piracy, and challenges for the United States*. Santa Monica, CA: RAND Corporation.

Chawkins, S. (2003, November 6). Agencies get a taste of terrorism in action. *Los Angeles Times*, p. 5.

Chilstrom, J. S. (1992). *Mines away! The significance of U.S. Army Air Force's minelaying in World War II*. Montgomery, AL: Air University Press Maxwell AFB.

City of Oakland. (2014). City of Oakland police areas. Retrieved from

http://www2.oaklandnet.com/oakca1/groups/police/documents/image/oak047364.pdf

City of Stockton. (2012, August). Parks and community centers. Retrieved from http://www.stocktongov.com/files/LegalParks.pdf

Clark, B., Nincic, D., & Fidler, N. (2007). *Protecting America's ports: Are we there yet?* Vallejo, CA: California Maritime Academy

Coast Guard and Maritime Transportation Act of 2014, H.R.4005, 113th Cong. (2014).

Corbin, J., & Strauss, A. (2008). *Basics of qualitative research* (3rd ed.). Los Angeles, CA: Sage Publications, Inc.

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among the five traditions*. Thousand Oaks, CA: Sage Publications, Inc.

Davis, D. (2000). *Business research for decision making* (5th ed.). Pacific Grove, CA: Duxbury Thomson Learning.

Delgaudio, R. (Director). (2010). *Please remove your shoes* [Documentary]. United States: Black Pearl Productions.

Delta Boating.com. (2014). Tide tables for the California Delta. Hourly tides for Stockton. Retrieved from http://deltaboating.com/tides/stockton.php

Donaldson, P. (2013). Mine Warfare. *Naval Forces*, *34*(1), 33-38.

Dowd, F. J. (2004). *Terrorist mines in the United States maritime domain: A credible threat?* Newport, RI: Joint Military Operations Department, Naval War College.

Drier, J. (1993). Structures of normative theories. *The Monist*, *76*, 22-40. Retrieved from http://www.brown.edu/Departments/Philosophy/onlinepapers/dreier/Structures_of

_Normative_Theories.pdf

Edwards, J. J., & Gallagher, C. M. (2014). Mine and undersea warfare for the future. *U.S. Naval Institute Proceedings*, *140*(8), 70-75.

English, B. (2003). *Al-Qaeda targeting ocean liners*. Fox News Channel, Retrieved from http:// http://www.foxnews.com/story/2003/12/30/report-al-qaeda-targeting-ocean-liners/

Equasis Statistics. (2011). *The world merchant fleet in 2011*. Retrieved from www.emsa.europa.eu/news-a-press-centre/download/1933/1554/23.html

Eski, Y. (2012). Port of call: Towards a criminology of port security. *Criminology and Criminal Justice*, *11*(415).

Evaluating port security: Progress made and challenges ahead, Hearing before the U.S. Senate Committee on Homeland Security and Governmental Affairs. 113th Cong. (2014).

Evans, M., & Stutin, T. (2006). *Anticipating the waiting weapon: U.S. ports and terrorist sea mining*. Kings Point, NY: Department of Marine Transportation, United States Merchant Marine Academy.

Ewing, P. (2012, June 17). A new way for mine warfare. USNI News. Retrieved from http://news.usni.org/2012/06/17/new-way-mine-warfare

Federal Emergency Management Agency. (2013). *FY 2013 Port Security Grant Program*. Retrieved from http://www.fema.gov/fy-2013-port-security-grant-program-psgp-0

Fishbein, W., & Treverton, G. (2004, October). Rethinking "alternative analysis" to

address transnational threats. The Sherman Kent Center for Intelligence Analysis. *Occasional Papers*, *3*(2). Retrieved from https://www.cia.gov/library/kent-center-occasional-papers/vol3no2.htm

Flynn, S. (2004). *America the vulnerable: How our government is failing to protect us from terrorism*. New York, NY: HarperCollins.

Frittelli, J. F. (2004). *Port and maritime security: Background and issues for Congress*. Congressional Research Service. Washington, DC: Library of Congress.

Garcia, F. M., & Wantchekon, L. (2010). *Theory, external validity, and experimental inference: Some conjectures*. The ANNALS of the American Academy of Political and Social Science. Retrieved from http://www.africanastudies.as.nyu.edu/docs/IO/2807/Newconvertedvalidity2.pdf

General Accounting Office. (2002). *Combatting terrorism: Actions needed to improve force protection for DOD deployments through domestic seaports* (Report to the Chairman, Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government reform, House of Representatives). Washington, DC.

General Accounting Office. (2012). *Security and Accountability For Every Port Act of 2006*. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-109publ347/html/PLAW-109publ347.htm

General Services Administration Federal Supply Center. (2010). *Federal Supply Schedule 084 - Total Solutions for Law Enforcement, Security, Facility Management Systems, Fire Rescue, Special Purpose clothing, Marine Craft and*

Emergency/Disaster Response: FSC Group 63 - Alarm and Signal Systems/Facility Management Systems, Professional Security/Facility Management Services and Guard Services. Retrieved from https://www.gsaadvantage.gov/ref_text/GS07F9169S/0DKV75.1MVIDR_GS-07F-9169S_GS07F9169SPURETECH.PDF

The geography of transport systems. (2015). Retrieved from https://people.hofstra.edu/geotrans/eng/ch3en/conc3en/containerships.html

Goforth, C. (2015, March 9). The siren song of deep water: Ports race to accommodate post Panamax ships. *Al Jazeera America*. Retrieved from http://america.aljazeera.com/articles/2015/3/9/ports-race-to-accommodate-post-panamax-ships.html

Griffin, R. W. (2003). *Fundamentals of management: Core concepts and applications*. New York, NY: Houghton Mifflin Co.

Griset, P. L., & Mahan, S. (2003). *Terrorism in perspective*. Thousand Oaks, CA: Sage Publications, Inc.

Harris, P., & Bright, M. (2001, December 23). How the armada of terror menaces Britain. *The Observer*. Retrieved from http://www.theguardian.com/world/2001/dec/23/september11.terrorism2

Hartmann, G. K. (1991). *Weapons that wait – Mine warfare in the U.S. Navy*. Annapolis, MD: Naval Institute Press.

Hesse-Biber, S. N., & Leavy, P. (2006). *The practice of qualitative research*. Thousand Oaks, CA: Sage Publications.

Homeland Security Studies and Analysis Institute. (2007). *Homeland security strategic analysis: Mission area analysis*. (RP 05-05-03). Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA493506

Hoon, C. (2013). Meta-synthesis of qualitative case studies: An approach to theory building. *Organizational Research Methods, 16*, 522-556

Hordijk, L. (2014). *What is systems analysis?* International Institute for Applied Systems Analysis. Retrieved from http://www.iiasa.ac.at/web/home/about/whatisiiasa/whatissystemsanalysis/what_is_systems_analysis.html

House of Representatives, Transportation and Infrastructure Committee. (2014, February 6). Committee Leaders Introduce Coast Guard & Maritime Transportation Bill [Press release]. Retrieved from https://transportation.house.gov/news/documentsingle.aspx?DocumentID=369179

Ilachinski, A. (1996). *Land warfare and complexity, Part II: An assessment of the applicability of nonlinear dynamics and complex systems theory to the study of land warfare*. Center for Naval Analyses. Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?view&did=466649

International Maritime Organization. (2002). ISPS Code Conference of Contracting Governments to the International Convention for the SOLAS 1974: SOLAS/ CONF.5/34, 17 December. London: International Maritime Organization.

International Maritime Organization. (2014). ISPS Code. Retrieved from

http://www.imo.org/OurWork/Security/Instruments/Pages/ISPSCode.aspx

International Society for the Systems Sciences. (2014). Origin and purpose of the ISSS. Retrieved from http://isss.org/world/

It's all in the package: The littoral combat ship's mission modules. (2014, September 22). *Defense Industry Daily*. Retrieved from http://www.defenseindustrydaily.com/its-all-in-the-package-the-littoral-combat-ships-mission-modules-016450/

Jackson, G. M. (2000). *Warden's five-ring system theory: Legitimate wartime military targeting or an increased potential to violate the law and norms of expected behavior?* Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?view&did=2517

Jordan, G., & Reed, J. H. (2007, September). Using systems theory and logic models to define integrated outcomes and performance measures in multi program settings. *Research Evaluation*, *16*(3), 169-181. doi:10.3152/095820207X243909

Katz, D., & Kahn, R. L. (1966). The social psychology of organizations. In Editor J. M. Shafritz, A. C. Hyde, & S. J. Parkes (Eds.), *Classics of public administration*, (pg. 206). Boston, MA: Thomson-Wadsworth.

Kelly, J. (2013, May 7). *International mine countermeasures exercise 2013 begins*. Navy live: The official blog of the U.S. Navy. Retrieved from http://navylive.dodlive.mil/2013/05/08/mine-warfare-and-the-global-mine-threat/

Larsen, G., Haugh, B., & Lichtblau, D. (2006). *Analyzing adversaries as complex adaptive systems*. Institute for Defense Analyses. Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?view&did=27614

Lekic, S. (2011, April 29). Gaddafi forces mining Misrata Port: NATO. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2011/04/29/gaddafi-misrata-port_n_855574.html

Levine, M., Gordon-Meek, J., Thomas, & Ferran, L. (2014, September 23). What is the Khorasan Group, Targeted By U.S. in Syria? Retrieved from http://abcnews.go.com/International/khorasan-group-targeted-us-syria/story?id=25700467

Libyan government threatens aid ships heading for besieged port city. (2011, April 29). Retrieved from http://www.cnn.com/2011/WORLD/africa/04/29/libya.war/

Lundquist, E. (2014). Countermine warfare. *Military Technology*, *38*(3), 39-41.

Lyons, Jr., D., Baker, E., Edlow, S., & Perrin, D. (1993). *The mine threat: Show stoppers or speed bumps*. Alexandria, VA: Center for Naval Analyses.

M-580: Marine Highway. (2014). *The M-580 California green trade corridor: Your Central Valley connection to the world!* Retrieved from http://m-580.com

Marcario, J. C. (2010). Port technology R&D. *Sea Power*, *53*(5), 34-40.

Marcson, S. (1961). Organization and authority in industrial research. *Social Forces*, (40), 71-76.

Maritime Connector. (2014). *Ship sizes: Panamax and New Panamax*. Retrieved from http://maritime-connector.com/wiki/panamax/

Maritime Security: Progress and Challenges with Selected Port Security Programs, Statement of Stephen L. Caldwell, Director, Homeland Security and Justice, Testimony before the Senate Committee on Homeland Security and Governmental

Affairs, U.S. Senate (2014).

Maritime Security: The SAFE Port Act and Efforts to Secure Our Nation's Seaports, Statement of Stephen L. Caldwell, Director Homeland Security and Justice Issues, Testimony before the Committee on Commerce, Science, and Transportation U.S. Senate (2007).

Maritime Transportation Security Act of 2002. Public Law 107–295.

Martinez, L. (2013, January 16). U.S. Navy minesweeper runs aground on reef in the Philippines. *ABC News*. Retrieved from http://abcnews.go.com/blogs/politics/2013/01/us-navy-minesweeper-runs-aground-on-reef-in-the-philippines/

Mateski, M. (Editor). (2014). Red teaming and alternative analysis. *Red Team Journal*. Retrieved from http://redteamjournal.com/about/red-teaming-and-alternative-analysis/

McLeod, L. E. (2013, September 23). *3 Situations that call for a red team*. Retrieved from http://www.huffingtonpost.com/lisa-earle-mcleod/three-situations-that-cal_b_3974886.html

Merton, R. K. (1957). *Social theory and social structure*. New York, NY: Free Press.

Meza, M. (2014, October 23). Port of Stockton hires harvesters for hyacinth issue: Weeds cause problems for businesses, boaters. *KCRA News*. Retrieved from http://www.kcra.com/news/port-of-stockton-contracts-harvesters-for-hyacinth-issue/29310616

Modernization of the Panama Canal. (2015). *Evolution of container ships*. Retrieved from

http://www.washingtonpost.com/wp-srv/special/world/modernization-of-panama-canal/

Mouzelis, N. P. (1967). *Organization and bureaucracy*. Chicago, IL: Aldine Publishing Co.

Murphy, M. N. (2008). *Small boats, weak states, dirty money: Piracy and maritime terrorism in the modern world*. New York, NY: Columbia University Press.

National port readiness network. (2014). Retrieved from http://www.globalsecurity.org/military/agency/dot/nprn.htm

National Security Presidential Directive-41/Homeland Security Presidential Directive-13 (2004 comp.)

National Transportation Safety Board. (2010). *Commercial fishing vessel count by state/jurisdiction and federally-documented by the U.S. Coast Guard*. Retrieved from http://www.ntsb.gov/news/events/2010/fishing_vessel/background/USCG%202008%20CFVs%20Count%20vt%20State%20and%20Documentation%20Type.pdf

The Navy returns pleasure craft. (1944, December 14). Miami News. Retrieved from http://news.google.com/newspapers?nid=2206&dat=19441217&id=SxUyAAAAIBAJ&sjid=EucFAAAAIBAJ&pg=5300,202721

Neffenger, P. V. (2013). Safeguarding our hemisphere. *U.S. Naval Institute Proceedings, 139*(10)*, 18-23.*

Nelson, E. (2012). Maritime terrorism and piracy: Existing and potential threats. *Global Security Studies*, *3*(1), 15-28.

Nickels, W. G., McHugh, J. M., & McHugh, S. M. (2008). *Understanding business* (8th ed.). New York, NY: McGraw-Hill/Irwin.

Northrop Grumman Corporation. (2014a). *Airborne laser mine detection system*. Retrieved by, http://www.northropgrumman.com/Capabilities/AirborneLaserMineDetectionSystem/Pages/default.aspx

Northrop Grumman Corporation. (2014b). Rapid airborne mine clearance system. Retrieved by, http://www.northropgrumman.com/Capabilities/RAMICS/Pages/default.aspx

Nuclear-free New Zealand, Page 5–Sinking the Rainbow Warrior (2013, October 30). Retrieved from http://www.nzhistory.net.nz/politics/nuclear-free-new-zealand/rainbow-warrior

Nuclear Security Science and Policy Institute. (2014). Pathways analysis. *Texas A&M University Nuclear Engineering*. Retrieved by, http://nsspi.tamu.edu/nsep/courses/physical-protection-systems/single-path-analysis/pathways-analysis

Oakland Police Department. (2014a). Our mission, vision, and values. Retrieved from http://www2.oaklandnet.com/Government/o/OPD/a/mission/index.htm

Oakland Police Department. (2014b). Public records request: Calls for service and incidents – 2013.

O'Donnell, R., & Truver, S. C. (2006). Mine warfare confronts an uncertain future. *U.S. Naval Institute Proceedings*, *132*(7), 42-45.

On this day, 1950-2005: July 10. (2008). Retrieved from http://news.bbc.co.uk/onthisday/hi/dates/stories/july/10/newsid_2499000/2499283.stm

Operation Neptune Shield aims to protect U.S. Ports. (2002, April 5). Retrieved from, http://www.marinelink.com/news/article/operation-neptune-shield-aims-to-protect-u-s/321232.aspx

Opportunity Cruises. (2012). *Cruise the delta with us!* Retrieved from http://opportunitycruises.com/

Out of control hyacinth turning California Delta into a weed patch. (2014, October 22). *Central Valley Business Times*. Retrieved from http://www.centralvalleybusinesstimes.com/stories/001/?ID=26993

Parfomak, P. W., & Frittelli, J. F. (2007). Maritime security: Potential terrorist attacks and protection priorities. Retrieved from http://www.fas.org/sgp/crs/homesec/RL33787.pdf

Patton, M. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Paulsen, V. (2003, March 25). Minelaying boats towed to safety. *CNN*. Retrieved from http://www.cnn.com/2003/WORLD/meast/03/25/sprj.irq.mines/

Peters, K. (2004). Covering the waterfront. *Government Executive*, *36*(15), 40-47.

Plant, J., & Young, R. (2007). *Securing and protecting America's railroad system: U.S. railroad and opportunities for terrorist threats*. Harrisburg, PA: Pennsylvania State University School of Public Affairs.

Port Authority of NY & NJ. (2013). About the port. Retrieved from http://www.panynj.gov/port/about-port.html

Port of Oakland. (2014a). Maritime: Facts & figures. Retrieved from http://www.portofoakland.com/maritime/factsfigures.aspx?utm_source=redirect&utm_medium=old_site_request

Port of Oakland. (2014b).Your port, your partner. Retrieved from http://www.portofoakland.com/pdf/about/YPYP.pdf

Port of Redwood City. (2014). 1st quarter tonnage & vessel report, FY 2014. Retrieved from http://www.redwoodcityport.com/p7iq/Assets/1st_Quarter_Tonnage_&_Vessel_Report_July_1_thru_Sep_30.2013.pdf

Port of Stockton. (2014a). Berthing facilities. Retrieved from http://www.portofstockton.com/berthing-facilities

Port of Stockton. (2014b). Shipcam. Retrieved from http://www.portofstockton.com/shipcam

Port of Stockton. (2014c). Port of Stockton Police Department. Retrieved from http://www.portofstockton.com/pos-police

Port of Stockton Police Department. (2014). Public records request: Crimes and incidents – 2013.

Price, J. (2010). Coding: Selective coding. In A. Mills, G. Durepos, & E. Wiebe (Eds.), *Encyclopedia of case study research*. (pp. 158-159). Thousand Oaks, CA: SAGE Publications, Inc.

Priest, D., & Farah, D. (2003, October 14). Iranian force's long ties to Al Qaeda. *Washington Post*. Retrieved from http://www.democraticunderground.com/discuss/duboard.php?az=view_all&address=103x16429

Program Executive Office: Littoral Combat Ship. (2014). *AN/SQQ-32(V)4 Minehunting sonar set high frequency wide band upgrade*. Retrieved by, http://www.powerstarinc.com/sqq32.pdf

Project on Defense Alternatives. (2002, 25 June). *Dislocating Alcyoneus: How to combat al-Qaeda and the new terrorism* (Briefing Memo no. 23). Washington, DC: Conetta, C.

PureTech Systems. (n.d.). *Case study: Port security. Integrating fence detection and video analytics*. Retrieved from http://www.puretechsystems.com/docs/charlestoncasestudy.pdf

Quinn, J. P. (2003). Covering the waterfront: Port security since 9.11. Logistics Management (2002), *42*(10), S59-S64. Retrieved from http://search.proquest.com/docview/197203894?accountid=14872

Reflagged tanker crippled by mine; retaliation not planned. (1987, July 25). Retrieved from http://alb.merlinone.net/mweb/wmsql.wm.request?oneimage&imageid=5427116

Renuart, Jr., V. E., & Egli, D. S. (Spring 2008). Closing the capability gap: Developing new solutions to counter maritime threats. *Naval War College Review*, *61*(2).

Reynolds, T. S. (2013). Learning from IEDs. *U.S. Naval Institute's Proceedings*, *139*(8),

54-59.

Richardson, M. (2004). *A time bomb for global trade: Maritime related terrorist in an age of weapons of mass destruction*. Singapore: ISEAS Publications.

Richey, W. (1987, August 12). Mine warfare in gulf suits Iran's political and military aims. *The Christian Science Monitor*. Retrieved from http://search.proquest.com/docview/1034957932?accountid=14872

Rios, J. J. (2005, June). *Naval mines in the 21st century: Can NATO navies meet the challenge?* (Master's Thesis). Monterey, CA: Naval Postgraduate School.

Rios, J. J. (2011). *Mine Warfare Branch program briefing, Panama City, FL., 11 May*. Mine Warfare Association conference. Risk Watch (2014). Operation Safe Commerce: Operation Safe Commerce Analysis Arrives in Port. Retrieved from http://riskwatch.com/operation-safe-commerce/

Ritchie, J., Lewis, J., & Elam, G. (2003). *Designing and selecting samples*. Jane Ritchie, & Jane Lewis (Eds.), Qualitative research practice. A guide for social science students and researchers (pp. 77-108) Thousand Oaks, CA: Sage Publications, Inc.

Rodeman, C. (2003). *In search of an operational doctrine for maritime counterterrorism*. (Master's Thesis). Newport, RI: Naval War College.

The Safe Port Act: Hearing before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the Committee on Homeland Security, House of Representatives, 109th Cong. (2006).

SAFE Port Act Reauthorization: Securing Our Nation's Critical Infrastructure: Hearing

before the U.S. Senate Committee on Commerce, Science, and Transportation, 111th Cong. (2010).

San Francisco Bay Area Water Emergency Transportation Authority. (n.d.). San Francisco Bay Ferry: Alameda. Retrieved from http://sanfranciscobayferry.com/route/pier41/alameda

Savitz, S. (2006, April). Psychology and the mined: Over-coming psychological barriers to the use of statistics in mine warfare. Alexandria, VA: Center for Naval Analyses.

Security and Accountability for Every Port Act of 2006. Public Law 109-347.

Schwan, M. (2012). *Border cracks: Approaching border security from a complexity theory and systems perspective*. Newport, RI: Naval Postgraduate School. Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?view&did=732181

Schwarz, M. (2014). Future mine countermeasures. *Naval War College Review*, *67*(3), 123-141.

SEAPOWER Sea Services Almanac 2006, January 2006, United States Navy League.

The secret world of cargo ships. (2013, November 15). *The Week*. p. 40.

Senge, P. (1990). *The fifth discipline: The art and practice of learning organization*. New York, NY: Doubleday.

Shafritz, J. M., Russell, E. W., & Borick, C. P. (2007). *Introducing public administration* (5th ed.). New York, NY: Pearson-Longman.

Singleton, R. A., & Straits, B. C. (2005). *Approaches to social research* (4th ed.). New York, NY: Oxford University.

Skyttner, L. (2006). *General systems theory: Problems, perspectives, practice* (2nd ed.). River Edge, NJ: World Scientific.

Sparks, M. E. (2005). *A critical vulnerability, a valid threat. U.S. ports and terrorist mining*. Norfolk, VA: Joint Forces Staff College Joint Advanced Warfighting School.

Steen, P. (2003, July). *Qualitative data analysis in homeland security evaluation. Journal of Homeland Security*. Homeland Security Studies and Analysis Institute. Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?view&did=442213

Sternlicht, D. D., Fernandez, J. E., & Marston, T. M. (2013). Advances in synthetic aperture sonar transform mine countermeasures and undersea warfare. *CHIPS*, (2). 32-36.

Sullivant, J. (2007). *Strategies for protecting national critical infrastructure assets: A focus on problem solving*. Hoboken, NJ: John Wiley & Sons.

Sun, T. (2009). *The art of war*. (L. Giles, Trans.) Retrieved from http://classics.mit.edu/Tzu/artwar.html (Original work published in 1972).

Tenth Anniversary of the Maritime Transportation Security Act: Are We Safer? Hearing Before the Subcommittee on Coast Guard and Maritime Transportation of the Committee on Transportation and Infrastructure, House of Representatives, 112th Cong. (2012). Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?view&did=729255

Thatcher, D. (2006). The normative case study. *American Journal of Sociology*, *111*(6), 1631-1676.

Triple-E: The world's largest ship. (2013). Retrieved from http://www.worldslargestship.com/about/faq/

The Security and Accountability For Every Port Act of 2006. Public Law 109–347.

Truver, S. C. (2008). Mines and underwater IEDs in U.S. ports and waterways: Context, threats, challenges, and solutions. *Naval War College Review*, *61*(1).

Truver, S. C. (2012). Taking mines seriously. *Naval War College Review*, *65*(2), 30-66.

Truver, S. C. (2014, August). Position open: USN mine warfare champion. *Mine Lines*. Springfield, VA: Mine Warfare Association. 9-14.

21st century U.S. Navy mine warfare. (2012). *Military Technology*, *12*, 56-57.

U.S. Coast Guard. (2007). *The U.S. Coast Guard strategy for maritime safety, security, and stewardship*. Retrieved from https://www.hsdl.org/?view&did=470382

U.S. Coast Guard. (2010). *Strategic plan: A blueprint for acquisition improvement*. Retrieved from https://www.uscg.mil/acquisition/aboutus/pdf/Blueprint.pdf

U.S. Coast Guard. (2012). *America's waterway watch*. Retrieved from http://americaswaterwaywatch.uscg.mil/home.html

U.S. Coast Guard. (2013a). *Boating statistics* (COMDTPUB P16754.26). Retrieved from http://www.uscgboating.org/assets/1/News/2012ReportR2.pdf

U.S. Coast Guard. (2013b). *Mission statement*. Retrieved from http://www.uscg.mil/hq/cg5/cg551/Mission.asp

U.S. Coast Guard. (2014a). *2013 performance highlights & 2015 budget in brief*. Retrieved from http://www.uscg.mil/budget/docs/2015_Budget_in_Brief.pdf

U.S. Coast Guard. (2014b). *Aircraft, Boats, and Cutters*. Retrieved by,

https://www.uscg.mil/datasheet/

U.S. Coast Guard. (2014c). *Missions: Ready today…preparing for tomorrow*. Retrieved from http://www.uscg.mil/top/missions/

U.S. Coast Guard. (2014d). *Office of Counterterrorism & Defense Operations Policy: Ports, Waterways & Coastal Security*. Retrieved from http://www.uscg.mil/hq/cg5/cg532/pwcs.asp

U.S. Coast Guard. (2014e). *U.S. Coast Guard Maritime Security (MARSEC) Levels*. Retrieved from http://www.uscg.mil/safetylevels/whatismarsec.asp

U.S. Customs & Border Protection. (n.d.). *About foreign-trade zones and contact info: An introduction to foreign-trade zones*. Retrieved from http://www.cbp.gov/border-security/ports-entry/cargo-security/cargo-control/foreign-trade-zones/about

U.S. Customs & Border Protection. (2004a). *Securing the global supply chain*. Retrieved from http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_strate gicplan.ctt/ctpat_strategicplan.pdf

U.S. Customs & Border Protection. (2004b). *24-Hour-advance-vessel-manifest-rule FAQ*. Retrieved from http://www.customs.gov/ImageCache/cgov/content/import/carriers/24hour_5frule/24hour_5ffa q_2edoc/v1/24hour_5ffaq.doc

U.S. Customs & Border Protection. (2006). *Container Security Initiative - Strategic Plan*. Retrieved from http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/csi/csi_strategic_plan.

ctt/csi_strategic_plan.pdf

U.S. Customs & Border Protection. (2007). *C-TPAT overview*. Retrieved from http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml

U.S. Customs & Border Protection. (2008). *FAQ - New cargo security requirements for maritime carriers and importers*. Retrieved from http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/carriers/security_filing/import_faq.ctt/import_faq.pdf

U.S. Customs & Border Protection. (2009a). *ACE and automated systems*. Retrieved from http://www.cbp.gov/trade/automated

U.S. Customs & Border Protection. (2009b). *Importer security filing and additional requirements*. Retrieved from http://www.cbp.gov/linkhandler/cgov/newsroom/publications/trade/import_sf_carry.ctt/import_sf_carry.pdf

U.S. Department of Commerce/National Oceanic & Atmospheric Administration. (2013a). *Major U.S. port cities and satellite ports FY 1999/2000 Ranked by total cargo tonnage*. Retrieved from http://www.ngs.noaa.gov/RSD/coastal/projects/coastal/ports_list.html

U.S. Department of Commerce/National Oceanic & Atmospheric Administration. (2013b). *Nav chart reference –Sacramento and San Joaquin Rivers*. Chart 18661. Retrieved from http://ocsdata.ncd.noaa.gov/BookletChart/18661_BookletChart.pdf

U.S. Department of Commerce/National Oceanic & Atmospheric Administration. (2013c). *Nav chart reference –San Francisco Bay Candlestick Point to Angel Island.* Chart 18650. Retrieved from http://www.charts.noaa.gov/OnLineViewer/18650.shtml

U.S. Department of Commerce/National Oceanic & Atmospheric Administration. (2014a). *Ocean facts*. Retrieved from http://oceanservice.noaa.gov/facts/bathymetry.html

U.S. Department of Commerce/National Oceanic & Atmospheric Administration. (2014b). *What is sonar?* Retrieved from http://oceanservice.noaa.gov/facts/sonar.html

U.S. Department of Defense & U.S. Department of Homeland Security. (2005). *The National Strategy for Maritime Security*. Retrieved from http://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html

U.S. Department of Homeland Security. (2005, October). *Maritime Transportation System Security Recommendations for the National Strategy for Maritime Security*. Retrieved from http://www.dhs.gov/xlibrary/assets/HSPD_MTSSPlan.pdf

U.S. Department of Homeland Security. (2007). *National Strategy for Homeland Security*. Retrieved from http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

U.S. Department of Homeland Security. (2008a). *Fact sheet: New cargo security requirements for maritime carriers and importers*. Retrieved from

http://www.dhs.gov/xnews/releases/pr_1227548591399.shtm

U.S. Department of Homeland Security. (2008b). National Maritime Terrorism Threat Assessment, CG- HSEC-006-08. USCG Intelligence Coordination Center, Washington, DC

U.S. Department of Homeland Security. (2008c). *Small vessel security strategy*. Retrieved from http://www.dhs.gov/xlibrary/assets/small-vessel-security-strategy.pdf

U.S. Department of Homeland Security. (2010). *Organizational chart*. Retrieved from http://www.dhs.gov/xlibrary/assets/dhs-orgchart.pdf

U.S. Department of Homeland Security. (2013). FY 2013 Port Security Grant Program (PSGP). Retrieved from http://www.fema.gov/media-library-data/8d0439562c89644a68954505a49cbc77/FY_2013_Port_Security_Grant_Program_Fact_Sheet+-+Final.pdf

U.S. Department of Homeland Security. (2014a). *National Infrastructure Protection Plan*. Retrieved from http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

U.S. Department of Homeland Security. (2014b). FY 2014 Port Security Grant Program. Retrieved from http://www.fema.gov/media-library-data/1395152051671-37cb2991cd7fb4c1429970c5d3a31ead/FY_2014_PSGP_Fact+Sheet_Final.pdf

U.S. Department of State. (2006). *Country reports on terrorism*. Retrieved from http://www.state.gov/j/ct/rls/crt/2006/82738.htm

U.S. Department of Transportation. (n.d.). Marine transportation system. Retrieved from http://www.marad.dot.gov/ports_landing_page/marine_transportation_system/MT

S.htm

U.S. Department of Transportation. (2000). *Three case studies for the risk management framework for hazardous materials transportation. Research and Special Programs Administration*. Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?view&did=233026

U.S. Department of Transportation. (2010). *The freight technology story*. Retrieved from http://www.ops.fhwa.dot.gov/freight/intermodal/freight_tech_story/appa.htm

U.S. Department of Transportation. (2012). *National transportation statistics*. Retrieved from http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_01_57.html

U.S. Federal Bureau of Investigation. (2014). *Protecting America from terrorist attack: Our joint terrorism task forces*. Retrieved from http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs

U.S. Navy. (1996). *Mine Warfare*. (MCWP 3-3.1.2). Retrieved from http://archive.org/stream/milmanual-mcwp-3-3.1.2-mine-warfare/mcwp_3-3.1.2_mine_warfare_djvu.txt

U.S. Navy. (2009). *21st Century U.S. Navy mine warfare: Ensuring global access and commerce*. Program Executive Office Littoral and Mine Warfare/Expeditionary Warfare Directorate. Washington, DC: United States Department of Defense.

U.S. Navy. (2013a). *Fact file: Littoral combat ship*. Retrieved from http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=1650&ct=4

U.S. Navy. (2013b). *Fact file: Mine countermeasures ships*. Retrieved from http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=1900&ct=4

U.S. Navy. (2013c). *Mission statement*. Retrieved from http://www.navy.mil/navydata/organization/org-top.asp

U.S. Navy. (2014a). *CNO explains Navy's compensation reform at congressional hearing*. Retrieved from http://www.navy.mil/submit/display.asp?story_id=80834

U.S. Navy. (2014b). *Department of the Navy FY 2015 president's budget*. Retrieved from http://www.finance.hq.navy.mil/FMB/15pres/DON_PB15_Press_Brief.pdf

U.S. Navy. (2014c). *Littoral combat ships-Surface warfare (SUW) mission package*. Retrieved from http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=437&ct=2

U.S. Coast Guard's Deepwater effort sinks. (2011, December 14). *Defense Industry Daily*. Retrieved from http://www.defenseindustrydaily.com/us-coast-guards-deepwater-effort-hits-more-rough-sailing-02863/

Van Hooydonk, E. (2007) Soft values of seaports: A strategy for the restoration of public support for seaports. Apeldoorn: Garant Publishers.

Vere, H. (2014, October). 100 years back, wire rope was pivotal in combat operations on the seas. *Wire Rope News & Sling Technology*, *36*(1), 34-58.

Visit Stockton. (2014). *Google barge in Stockton*. Retrieved from http://www.visitstockton.org/google-barge-stockton

von Bertalanffy, L. (1969). *General systems theory: Foundations, development, applications*. New York: George Braziller.

Water hyacinth: Eichhornia crassipes (2014). *UF/IFAS Center for Aquatic and Invasive Plants*. Retrieved from http://plants.ifas.ufl.edu/node/141

Watts, R. (2005) Maritime critical infrastructure protection: Multi agency command and control in an asymmetric environment. *Homeland Security Affairs*, *I*(2).

Weber, M. (1952). Merton, R. K., Gray, A., Hockey, B., & Selvin, H. (Eds.). *The essentials of bureaucratic organization: An ideal-type construction*. Glencoe, IL: Free Press.

Weber, M. (1978). *Economy and society*. Los Angeles, CA: University of California Press. (Original work published 1922).

Weitz, R. (2013). *Project on national security reform: Case studies working group report, Vol. II*. Army War College - Strategic Studies Institute. Retrieved from https://www-hsdl-org.ezp.waldenulibrary.org/?view&did=704596

Wesley, J. (2010, April). *Qualitative document analysis in political science*. T2PP Workshop, Vrije Universiteit: Amsterdam, The Netherlands. Retrieved from http://www.poltext.org/sites/poltext.org/files/p2wesley._09102010_131253.pdf

White House National Security Council. (2006). *National strategy for combating terrorism*. Washington, DC

Wilson, J. Q. (1989). *Bureaucracy: What government agencies do and why they do it*. New York, NY: Basic Books.

Withers, P. (n.d.) Information security threat vectors. Information Systems Audit and Control Association. Retrieved from https://www.isaca.org/chapters5/Virginia/Events/Documents/Past%20Pres%2020

11-03%20Threat%20Vectors.pdf

Withington, T. (2010). Unmanned surface vehicles (USV) - Add-ons or organic assets of surface forces? *Naval Forces*, *31*(6), 61-68.

World Port Source. (2014a). Port of Stockton: Port commerce. Retrieved from http://www.worldportsource.com/ports/commerce/USA_CA_Port_of_Stockton_232.php

World Port Source. (2014b). Port of Oakland: Port commerce. Retrieved from http://www.worldportsource.com/ports/commerce/USA_CA_Port_of_Oakland_231.php

Wright, R. (2015, January 10/11) Material transport. Mediator poised to tackle U.S. container ports dispute. *Financial Times*. pg. 22.

Yin, R. (2003). *Case study research design and methods* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Zalman, A. (2014). *Jihadi*. Retrieved from http://terrorism.about.com/od/politicalislamterrorism/g/Jihadi.htm

Appendix A: USCG MARSEC Levels

MARSEC Level 1 is the level whereby minimum appropriate security measures are maintained.

MARSEC Level 2 is the level whereby appropriate additional protective security measures are maintained for a period of time resultant from heightened risk of a transportation security incident.

MARSEC Level 3 is the level whereby further specific protective security measures are 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.

MARSEC Level 1 generally applies in the absence of a National Terrorism Alert System or when the Commandant determines that the Alert is not applicable to the MTS. If a National Terrorism Alert System Alert is applicable, the Commandant will consider a MARSEC Level change for the maritime industry, Coast Guard, or both.

Source: USCG (2014). *U.S. Coast Guard Maritime Security (MARSEC) Levels*. Retrieved from http://www.uscg.mil/safetylevels/whatismarsec.asp

Appendix B: Document Content Analysis

Part 1 – Legislation, Literature, and Threat Assessments (General Port Security)

Step 1: General Themes

- Assertions, descriptions, interpretations, policies, procedures, and tactics of relevance to port security, naval mines/underwater improvised explosive devices, and MCM.
- Unit of analysis are phrases, subjects, topics, and words. Such will include language associated with mine warfare and MCM.

Step 2: Axial Coding

- Tag specific passages that fit theme-categories identified in step 1.

Step 3: Selective Coding

- Examination of documents to discover discrepant evidence.

Part 2 – Case Study (Port of Oakland & Port of Stockton)

1: Charts

- Bathymetry, channels, hazards, markers, navigational aids, restricted zones.

2: Crime Reports

- Property damage, trespassing, and vandalism.

3: Facilities and Infrastructure

- Cables, moorings, piers and wharves, navigation markers, and pipelines.

4: Maps/Satellite Imagery

- Boat ramps, bridges, levees, and public spaces.

5: Security Management

- Marine- and land-based patrols, perimeter and property protection, and cooperative efforts with surrounding law enforcement. To be obtained from open source (nonclassified) documents.

Appendix C: Direct Observation of Ports—Checklist

____ 1. Identify port Maritime Security level.

____ 2. Identify port bathymetry.

____ 3. Identify port infrastructure.

____ 4. Identify port's physical design.

____ 5. Identify nonsecure access to proximate waterways including bridges, farmland, levees, marinas, nature reserves, and parks.

____ 6. Identify commercial and recreational vessel traffic within port channels and waterways.

____ 7. Observe marine patrols around vessels.

____ 8. Observe foot or vehicle patrols of port perimeter.

____ 9. Observe overflight of port property and waterways by civilian aircraft.

____ 10. Evaluate port perimeter's physical barriers (fence lines, etc.) and ease of access by trespassers.

____ 11. Identify signs of criminal behavior on port infrastructure/property.

____ 12. Observe remote video surveillance.

____ 13. Search out other evidence of relevance to this study and not specified within this checklist.

Appendix D: Direct Observation of Ports—Record Sheet

Checklist Item No.	Port OAK STK	Location & GPS Coordinate	Date, Times & Weather	Observation / Notes

Appendix E: IRB Approval

Your IRB approval number is 07-29-14-00131691.

The Institutional Review Board confirms that your doctoral capstone entitled, "A Case Study in Port Security: The Threat from Terrorist Naval Mines/Underwater Improvised Explosive Devices" meets Walden University's ethical standards. Since this project will serve as a Walden doctoral capstone, the Walden IRB will oversee your capstone data analysis and results reporting. You are approved by Walden University to conduct the project.

Sincerely,
Libby Munson
Research Ethics Support Specialist
Office of Research Ethics and Compliance
Email: irb@waldenu.edu
Fax: 626-605-0472
Phone: 612-312-1341
Office address for Walden University:
100 Washington Avenue South
Suite 900
Minneapolis, MN 55401

Appendix F: NIH Certificate

Certificate·of·Completion¶

The·National·Institutes·of·Health·(NIH)·Office·of·Extramural·Research·certifies·that·**Peter·von·Bleichert**·successfully·completed·the·NIH·Web-based·training·course·"Protecting·Human·Research·Participants".¶

Date·of·completion:·05/20/2014·¶

Certification·Number:·1471116·¤

Appendix G: List of Abbreviations

9/11 ..... September 11, 2001 terrorist attack on New York and Washington, DC

AAPA ..... American Association of Port Authorities

CBP ..... U.S. Customs and Border Protection

CBRNE ..... Chemical, Biological, Radiological, Nuclear, High yield explosive

CGMT ..... Coast Guard and Maritime Transportation Act of 2014

CIKR ..... Critical Infrastructure and Key Resources

CNA. ..... Center for Naval Analyses

CSI ..... Container Security Initiative

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

DATR ..... Defense Agency Threat Reduction

DOD ..... U.S. Department of Defense

DHS ..... U.S. Department of Homeland Security

DOT ..... U.S. Department of Transportation

FBI ..... Federal Bureau of Investigation

FY ..... Fiscal Year

GAO ..... Government Accountability Office

GPS ..... Global Positioning System

GST ..... General systems theory

HSSAI ..... Homeland Security Studies and Analysis Institute

HSPD-13 ..... Homeland Security Presidential Directive-13

IMO ..... International Maritime Organization

IRB ..... Institutional Review Board

IRG..... Iranian Revolutionary Guard

M-580..... Marine Highway 580

M/UWIED.....Naval Mine/Underwater Improvised Explosive Device

MAA .....Mission Area Analysis

MARAD..... U.S. Maritime Administration

MARSEC ..... Maritime Security

MCM..... Mine Countermeasures

MIL .....Minelaying

MSST .....Maritime Safety and Security Teams

MTS .....Marine Transportation System

MTSA .....Maritime Transportation Security Act of 2002

NATO .....North Atlantic Treaty Organization

NIH .....National Institute of Health

NIPP..... National Infrastructure Protection Plan

NOAA .....National Oceanic & Atmospheric Administration

NSC.....White House National Security Council

NSMS.....National Strategy for Maritime Security

NSPD-41 ..... National Security Presidential Directive-41

OPD..... Oakland Police Department

OSC.....Operation Safe Commerce

POSPD ..... Port of Stockton Police Department

PSGP ..... Port Security Grant Program

PWCS ..... Ports, Waterways, and Coastal Security

SAFE Port Act ..... Security and Accountability for Every Port Act of 2006

SRCC ..... Strikes, Riots and Civil Commotion

SCUBA ..... Self-Contained Underwater Breathing Apparatus

SSAM ..... Small Synthetic Aperture Mine-hunter

TWIC ..... Transportation Worker Identification Credential

USC ..... United States Code

USCG ..... U.S. Coast Guard

USN ..... U.S. Navy

WWI ..... First World War

WWII ..... Second World War