Maritime Port Security:

Preventing Terrorist Attacks in America

Shaina Pearl

California State University Maritime Academy

Abstract

The premise behind this project is to analyze U.S. maritime security after the terrorist attacks of 9/11 by analyzing key legislative acts, the United States Coast Guard, the Customs and Borders Protection agency, and key maritime security initiatives deployed by them. The National Strategy for Maritime Security primarily sets the foundation for a collaborative effort towards the overall protection of U.S. ports, the maritime domain, and the international supply chain. Focusing on the International Ship and Port Security Code (ISPS), Maritime Transportation Security Act of 2002 (MTSA), Security and Accountability for Every Port Act (SAFE Port Act), and the agencies mandated by them, this paper will introduce the legislation and how they were written to support the greater vision of the National Strategy for Maritime Security. While the U.S. maritime sector is safer today than it was prior to 9/11, there are still needed improvements on existing legislation and agency execution. Finally, the project will aim to point out existing deficiencies and propose new ways to strengthen the maritime domain and prevent a future terrorist attack in the United States.

Keywords: Terrorism Prevention, National Strategy for Maritime Security, ISPS, MTSA, SAFE Port Act

U.S. Maritime Security

Maritime Security after the events of 9/11 has become a principle protective element of homeland security and international commerce. U.S. ports and the expansive nature of the maritime industry leaves the government with the difficult task of identifying and preventing future terrorist plots. Policies and procedures have been most commonly created to deal with the criminal element of cargo container exploitation. A shift in focus and tactics are leaving policy makers and maritime officials struggling to adapt to the even more daunting threat of terrorism. Ports operating in the U.S. are not governed under a central authority, but rather a complex web of public and private port ownership and authorities. The varying degree of port management within the U.S. maritime system makes the already difficult task of creating an effective security protocol even more complicated.

There are 361 major ports in the U.S. with nearly 62,000 vessels making 51,000 port calls annually (Chambers & Liu, 2012). With each of these vessels and the two billion tons of freight they carry, there are limitless possibilities for terrorist cells or lone wolves to smuggle weapons of mass destruction across our borders (Targets for Terrorism, 2006). Cruise ship terminals, ferry landings, and tankers amongst others are also all vulnerable to potential attacks, which begs the question: how will the government and its subservient entities prevent terrorism in U.S ports? Coordinated strategies among different law-enforcement agencies through redundant mechanisms and the cooperation with foreign allies help to proactively monitor high risk threats and detect terrorist plots further away from U.S. shores.

Despite the various avenues into which maritime security can branch, for the purpose of this paper, the primary focus will be on the development of a national strategy, legislative action for the deterrence of possible future terrorist attacks in U.S. ports, and the federal law

enforcement agencies in charge of securing U.S. maritime ports. Through research and analysis of the International Ship and Port Security Code (ISPS), Maritime Transportation Security Act of 2002 (MTSA), Security and Accountability for Every Port Act of 2006 (SAFE Port Act), and the agencies that carry out those policies, weaknesses can be identified and solutions suggested.

Literature Review

Maritime security in the United States has gone through rapid change to respond to growing concerns of U.S. port vulnerabilities to a terrorist attack. Many maritime industry leaders and federal agencies lend a hand in gathering the methods and practices that allow for an effective strategy to be created. The purpose of this review is to understand and examine the methods used to create maritime security strategies, the legislation that gives those strategies legal mandate, the agencies that carry out the mandate, and the weaknesses that have been identified for correction. The intent of establishing greater maritime security primarily is for prevention, and therefore will be the focus of this review.

The Need for a National Strategy

A Congressional Research Service prepared a report for the members and committees of Congress in 2007 that characterized the highest priority threat scenarios, the likelihood of a U.S. maritime terrorist attack, and how these wide-ranging scenarios may create policy issues for Congress (Parfomak & Frittelli, 2007). The report uses past terrorist attacks to help establish credible maritime attack scenarios and the implications various terrorist attacks may have on homeland security policy. The bombings of the U.S.S. Cole in 2000 by Al Qaeda and of the French oil tanker Limburg in 2002 show how the infrastructure and systems that make up the maritime domain are vulnerable to attack (Parfomak & Frittelli, 2007). There can almost be an

unlimited number of scenarios depending on the terrorist objectives for an attack, the location, tactics used, or intended target(s) as is demonstrated in the following table.

Table 1. Example Maritime Attack Characteristics

Dimensions	**Example Characteristics**
Perpetrators	• Al Qaeda and affiliates • Disgruntled employees • Islamist unaffiliated • Others • Foreign nationalists
Objectives	• Mass casualties • Trade disruption• Port disruption • Environmental damage
Locations	• 360+ U.S. ports • 9 key shipping bottlenecks • 165 foreign trade partners
Targets	• Military vessels • Cargo vessels • Fuel tankers • Ferries / cruise ships • Port area populations • Ship channels • Port industrial plants • Offshore platforms
Tactics	• Explosives in suicide boats • Explosives in light aircraft • Ramming with vessels • Ship-launched missiles • Harbor mines • Underwater swimmers • Unmanned submarine bombs • Exploding fuel tankers • Explosives in cargo ships • WMDs in cargo ships

Source: (Parfomak & Frittelli, 2007).

Prioritizing maritime security efforts that can best be applied to the largest range of possible scenarios can only be done through extensive evaluation of current and future maritime security strategies (Parfomak & Frittelli, 2007).

A study conducted by The Police Executive Research Forum analyzed 17 different U.S. ports to determine the effectiveness or ineffectiveness of their port security schemes. After analyzing all the security initiatives with industry round tables, government agencies, and local law enforcement, specific practices were deemed more effective than others (Pate, Taylor, & Kubu, 2007). With the hopes of "pushing our borders out" and establishing a methodology for the prioritization of practices and relevance, the Police Executive Research Forum divided up best practices into five general categories. The areas do not necessarily need to be followed in any particular order but can be tailored based on relevance. The five areas include:

1. Threat Awareness
2. Prevention
3. Preparedness
4. Response
5. Recovery (Pate et al., 2007).

The awareness of threats requires the understanding that there are greater potential attack scenarios than there are likely ones (Parfomak & Frittelli, 2007). Understanding the likelihood of certain scenarios is important, but it is also important to note that focusing too much on the Congressional Report's suggestion of scenario prioritization can be constraining based on the quality of available intelligence and the accuracy of the conducted risk assessment. Scenarios

that may be low on the list do not necessarily negate them from being used over the "more likely" situations.

Considering scenario prioritization accuracy is dependent on intelligence and risk assessments; methodologies need to be developed using a consistent framework across public and private entities so that key threat indicators can be identified (Maritime Security Policy Coordinating Committee, 2005). Intelligence sharing and domain awareness is the best leverage over terrorism and creates stronger mechanisms for supporting the implementation phase of maritime security.

By first defining the different groups that are the most likely threats, policies and agencies can determine how best to combat them (U.S. Department of State, 2005). The application of a national strategy helps to better collaborate with the international community and widen intelligence circles. The collection and dissemination of threats will allow for earlier response times further away from U.S. shores (U.S. Department of State, 2005).

The National Strategy for Maritime Security

The primary objectives for a National Strategy for Maritime Security are to prevent terrorist attacks, protect marine-related centers and critical infrastructures, minimize damage, expedite recovery, and safeguard the ocean and its resources (U.S. Department of State, 2005). To best accomplish these objectives, there are five strategic actions included in the strategy. Enhancing international cooperation is the first objective which allows for greater transparency in a multi-flagged merchant marine, and is essential in coordinated efforts for preventing suspicious cargo or people from arriving at their destination (U.S. Department of State, 2005). The second objective, for maximization of domain awareness, does not act as a stand-alone process, but is a necessary facilitator for all other strategic actions. Enhancing awareness and

sharing maritime intelligence for greater situational awareness can be applied to prevention, interdiction, and defense.

The strategy places an important emphasis on public-private sector cohesiveness and the ability to establish a baseline for security criteria along with the necessary measures designated by the Department of Homeland Security (U.S. Department of State, 2005). The third objective is for embedding security into commercial practices, which eliminates systemic vulnerabilities and prevents the possibility of security breaches. The creation of a coordinated network of stakeholders who are actively engaged in coordinated interagency efforts can help minimize "single-point" organizational failures that may result in a breakdown of security processes (Maritime Security Policy Coordinating Committee, 2005, pg. 7). Keeping in mind that there is no central port authority, the strategy made a point to focus on the blending of both private port security practices as well as public policies, and in doing so, helps to achieve the fourth strategic objective of implementing layered security. Layered security enables several different agencies, systems, and protocols to better detect and prevent terrorist attacks through redundancy mechanisms (U.S. Department of State, 2005). Starting far from the homeland, the initial layer of security involves overseas action to identify high risk ports or cargo that will be departing for the United States. With each layer that approaches closer to U.S. shores, there are more physical inspections and interdictions integrated through coordinated agency and private security practices.

The fifth objective ultimately aims to continue the unimpeded flow of commerce. International trade is strongly dependent on a safe maritime transportation sector, and through the achievement of the fifth objective, will continue unhindered while taking the proper precautions to prevent attacks, protect infrastructure, and safeguard U.S. citizens. The ability to

adapt to terrorism as it evolves is an important factor in an applicable strategy towards such a dynamic threat. The National Strategy for Maritime Security, in the end, is just rhetoric that needs to effectively be put into action in order for the five strategic objectives to be met and to secure the maritime transportation system. The legislative action and agencies that carry out those policies follow the vision and principles set forth by the National Strategy.

International and Federal Legislative action

The United States is not the only country to reevaluate maritime security in the wake of 9/11. An International Maritime Organization (IMO) assembly convened in November 2001 to adopt a resolution for the review of measures and procedures to prevent acts of terrorism in the maritime transportation system (IMO, 2008, pg. 16). The IMO in result, adopted several amendments to the already existing Safety of Life at Sea (SOLAS) convention and created an entirely new International Ship and Port Facility Security Code (ISPS). The ISPS Code standardizes a framework for evaluating security risks and allows for member-states to streamline security efforts and combat terrorist acts that may be detrimental to international shipping lanes.

On July 1, 2004, the ISPS Code became a compulsory standard. One hundred and fifty-eight member states uphold and enforce the ISPS Code, which accounts for nearly 99% of the world's merchant fleet's gross tonnage (IMO, 2008, pg. 17). Setting a mandatory maritime security standard on a global scale was a significant spark that prompted the U.S. to build upon the requirements set forth by the IMO and create the Maritime Transportation Security Act of 2002 (107th Congress, 2002).

The MTSA broadly addresses all security aspects of port and intermodal transportation and acknowledges the importance of U.S. ports to the national economy. Creating an entirely

new security framework and requiring security plans for ports, facilities, and vessels, the MTSA laid the groundwork for protecting the nations' ports and waterways. In conjunction with principles made by the National Maritime Strategy, the MTSA provides policy for the entire evolution of a terrorist attack, but only the prevention policies of the act will be addressed. Incorporating the ISPS code into the more stringent and comprehensive policies of the MTSA, the act places greater accountability on U.S. trading partners to maintain antiterrorism measures. In many ways, the U.S. has become the steward for the ISPS code.

The MTSA provides the Coast Guard with a mandate to conduct foreign port assessments to ensure the ISPS code standards are in place. Foreign port assessments aim to prevent the ability for potential threats headed to the U.S. to enter into international waters (107th Congress, 2002). Additionally, the act has developed a Transportation Worker Identification Credential (TWIC), to help better control U.S. port access to only authorized personnel (Caldwell, 2007). Credentialing is an important element of a deployed layer in securing the maritime domain (Parfomak & Frittelli, 2007).

Implementation of the TWIC program did not materialize into a pilot program until the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) was added into the port security framework and amended provisions in the MTSA (109th Congress, 2006). The SAFE Port Act codified the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) (Caldwell, 2007). The CSI program addresses the potential for maritime containers to be used for terrorist activity and was initially only implemented in United States ports shipping the highest volume of containers in January 2002. The SAFE Port Act required additional data be made available to the Customs and Border Protection (CBP) so that officials could better carry out the ability to detect high risk containers and systematized the

CBP's capacity to secure container shipments (109th Congress, 2006). In 2002, CBP first selected CSI ports based on the volume of U.S.-bound shipments. Twenty-three foreign ports were picked initially, but as the CSI program was made into law in 2006 with the SAFE Port Act, the program began to expand to include more ports.

Customs and Border Protection

To better understand CSI, Wendy Keefer (2007) breaks down the layered defense strategy used primarily for container port security. CBP policy makers needed to take a broader look at container security and differentiate the existing policies against "traditional" criminal activity and terrorist activity. Termed as the modern-day Trojan horse, containers arrive into the U.S. with little oversight. There is a relative amount of anonymity involved with the contents of a shipping container which requires a series of different people having access to them during the transport process. International container shipments are expected to double between 2001 and 2020 which dictates the need for more cost-effective methods for container screenings. Security needs to begin outside of the United States (Keefer, 2007). Prescreening containers prior to the departure from the port of origin can significantly prevent a terrorist attack from occurring in U.S. ports (Keefer, 2007).

In effort to meet new requirements set forth by the SAFE Port Act, there has been enhanced management and the placement of U.S. customs officials in foreign ports to better identify and surveil high risk cargo (Caldwell, 2007). Fifty-eight ports worldwide now operate CSI and over 80% of all maritime cargo shipped into the U.S can be prescreened (U.S. Customs and Border Protection, 2011). Only 5% of all containers entering the U.S through the maritime port system however, are physically examined by CBP officials (Keefer, 2007). The low number of containers physically examined brings up an important point. Only those containers deemed

high risk are prescreened. Core elements of the CSI involves automated advance targeting information to focus resources on the cargo that intelligence dictates to be a potential risk to maritime security.

In 2009, the strategic trade corridor prioritization model was approved by the Secretary of Homeland Security to help bolster the CSI program to have greater resources for targeting information (U.S. Customs and Border Protection, 2011). In order to accommodate the increase of containers in ports, a set of criteria for assessing risk was produced (109th Congress, 2006, pg. 18). High risk shipment data collected from the CBP's Automated Target System (ATS) and information provided by The Department of Energy (DOE) provides CBP with country threat information and shipping lane information in order to prioritize risky foreign ports (109th Congress, 2006, pg. 20).

Another CBP program that is independent from the CSI program but works as an additional tier of security is the Customs Trade Partnership Against Terrorism (CTPAT). Codified alongside CSI in the SAFE Port Act, the program is an important strategic action in the National Strategy (Caldwell, 2007). CTPAT is a public-private partnership run on a voluntary basis to strengthen the international supply chain. With more than 11,400 partners accepted into the program that comprehensively covers all facets of the supply chain community, the CTPAT program is a valuable tool for information gathering, and establishing a coordinated security plan (CTPAT, n.d.). Businesses involved in the international supply chain and principle stakeholders agree to cooperate with CBP and the anti-terrorism effort.

Applicants help to identify possibly security gaps and carry out best practices within their portion of the supply chain (CTPAT, n.d.). In order to incentivize the program and encourage a steady growth of participants, CBP has provided a number of benefits to the CTPAT Partners.

Partners are considered low risk and are given certain lenience when entering the country. By providing security profiles and implementing anti-terrorist security measures, companies receive front line inspections, reduced number of CBP examinations, and can receive similar treatment by other foreign Customs entities that have signed Mutual Recognition with the U.S. (CTPAT, n.d.).

United States Coast Guard

While the CBP is invaluable in container security, the USCG focuses on port security and anti-terrorism measures. An article appearing in the Coast Guard Outlook written by (Ret.) Capt. Lundquist (2011) breaks down the Coast Guard's program for meeting the requirements set forth by legislation on maritime security. The ISPS code sets the minimum port security standards internationally, and the MTSA is the legislation that mandates the USCG to assess foreign ports for anti-terrorism measures. Once the Coast Guard received the mandate, they in turn created the International Port Security (IPS) Program. Foreign port security assessments began in 2004 and were an added element into the USCG's layered security methodology of keeping terror threats "far-from-the-homeland" (Lundquist, 2011). Using the ISPS as a guideline, the Coast Guard has been able to conduct security assessments in more than 150 countries that trade with the U.S. in the maritime sector (Lundquist, 2011).

(Ret.) Capt. Lundquist (2011) notes, that while the ISPS code is compulsory, the U.S.'s adaptation of the ISPS code through the International Port Security (IPS) Program has no international authority. In order to create a mutually beneficial IPS Program and increase other countries' cooperation, the USCG actively works with trading nations to develop and train stronger terror prevention measures (Lundquist, 2011).

A GAO report on the efforts made by the Coast Guard's program to secure the global supply chain and prevent a terrorist attack addresses the risk-informed model created to help the IPS Program make better informed operational decisions (Caldwell, 2014). The IPS program's risk assessment model is solely used for assessing port security, whereas CBP uses their own processes for container security in CSI. The risk model is made up of four components to help the Coast Guard determine where IPS program resources should be focused. Country threat, foreign port assessment, country responsiveness, and country wealth are the four measures used to make up the risk model (Caldwell, 2014). Depending on the result of the risk model, the Coast Guard can determine how best to implement the IPS program on an individual country basis. The risk model is updated annually and gauges the number of visits needed, the number of officials needed, and if the country requires more assistance or training (Caldwell, 2014).

The Coast Guard has additionally established a public-private partnership with regional Area Maritime Security Committees (AMSCs). Mandated under MTSA, the committee is a collective group of government and industry professionals working to improve security within the maritime sector (USCG, 2017). Ultimately, the Coast Guard alongside the AMSCs can harmonize security protocol and efforts to carry out national preventive goals. In 2016, there have been 45 training exercises nationally, 671 meetings, 332 Joint Agency training meetings, and 189 Maritime Security training events (USCG, 2017). The collaborative relationships created through AMSCs have improved information sharing and simplifies the dynamic nature of the maritime industry by allowing the regional committees to reflect the needs in their port area and increase domain awareness (Caldwell, 2007, pg.8).

Interagency Collaboration

Initially established by the SAFE Port Act in 2006, the DHS delegated the authority of implementing the Interagency Operations Centers (IOC) in 2009 to the Coast Guard (USCG, 2012). IOCs operate in 35 of the nation's ports deemed most critical. The WatchKeeper system operated in the IOCs was made to enable greater interagency cooperation and shared mission tasking, but is currently deployed only in 19 of the 35 sectors (USCG, 2012). With WatchKeeper, IOCs primarily function for Integrated Vessel Targeting (IVT), Interagency Operations Planning (IOP), and Operations Monitoring (OM) (Wilbur, 2013, pg. 2-3). Coast Guard, CBP, and applicable IOC members make up an Integrated Vessel Targeting Team (IVTT) to carry out IVT findings.

Through an iterative process occurring at intervals of 96, 72, 48, and 24 hours prior to a vessel arriving, the IVTT vets and determines if an individual vessel is cleared of threats. (Wilbur, 2013, pg. 3). Information is integrated from other systems like ATS operated by CBP, the Coast Guards Ship Arrival Notification System (SANS), and Automatic Identification System (AIS) into WatchKeeper to evaluate vessel and cargo risk levels. Superimposing the various layers of information provided by different data collecting systems creates a clearer and more definitive risk profile for prevention operations to be carried out (Wilbur, 2013, pg.4-5).

Weaknesses Identified in Current Security Practices

Ten years after the enactment of the MTSA, the GAO assessed the progress of the act and the implementation process of all maritime security programs. Determination of effective execution of programs currently in practice can broadly be broken down into management, the ability to utilize systems and resources, and public-private collaboration (Caldwell, 2012, pg. 16). In 2006, Stephen Flynn gave testimony to the United States House of Representatives Coast Guard and Maritime Transportation Subcommittee. The testimony pointed out continued

weakness in the maritime transportation system even with the many initiatives and policies set into motion by U.S. governing agencies.

Lack of Management

Flynn (2006) regarded the MTSA to be "more of a sketch than a security blueprint". Quick response needed by DHS after 9/11 resulted in an "implement and amend" mindset, which significantly flawed the ability for the MTSA or CSI programs to have long-term success (Caldwell, 2012, pg. 16). The MTSA requires ports and vessels to organize and maintain new physical, passenger/cargo, and personnel security, but fails to explain what that security is. Port authorities primarily fall into the role of determining and funding many of the new security protocols enforced by the MTSA mandate (Flynn, 2006). Lack of management and oversight of newly required MTSA legislation creates weaknesses in security practices as each port interprets and administrates new protocol. Flynn's overall interpretation of the seemingly large strides made by U.S. government initiatives are more symbolic than realistically effective. Funding aside, the overall approach for maritime security has been piecemeal lawmaking. Individual agencies promote trademark programs that fail to take into account other programs also in place (Flynn, 2006).

The SAFE Port Act was enacted in 2006 to strengthen and add to the security framework initially created by the MTSA, but has still left needed improvements to be made. Lack of management and the ability to create a realistic roll out plan for TWIC cards under the MTSA resulted in the requirement under the SAFE Port Act to establish the implementation phases for the program. The deadline set forth by the SAFE Port Act for July of 2007 was not met and did not have the software needed to maintain TWIC enrollment (Caldwell, 2007).

Lack of System and Resource Utilization

Stephen Caldwell (2014) identifies many weaknesses that could be improved by the Coast Guard utilization of resources. Maritime domain awareness and information sharing has been consistently named as a necessary first step for stopping threats before they can be materialized. A common Coast Guard map-based information system called Common Operating Picture (COP) is displayed through Enterprise Geographic Information System (EGIS) software, which according to this report, is not successfully operational and therefore cannot assist in information sharing or prevention (Caldwell, 2014, pg. 7).

The MTSA also requires Automatic Identification Systems (AIS), a tracking system that automatically uploads ship data via satellite, to be equipped in ships operating in or approaching U.S. waters, but do not have the systems in place to detect vessels outside of a 20 NM radius (Flynn, 2006). Even with the Coast Guard's requirement for 96-hour advance notification of arrival with crew and cargo manifests, the accuracy of vessel reporting cannot be confirmed. Vital information functions such as the EGIS is one system in a string of systems that are relied on for identifying terrorist threats prior to arriving on U.S. shores to improve maritime domain awareness. Severe lack of funding and personnel significantly affect the ability for the programs to perform up to needed standards. Coast Guard officials told GAO assessors that 21 of its 35 sectors, nearly 60%, struggled to maintain strategic, operational, and tactical efforts due to inadequate staffing (Caldwell, 2012, pg. 22).

Plans made by the Coast Guard to build a Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) system meant to improve the monitoring of the maritime domain never materialized (Caldwell, 2014, pg. 8). The system would have allowed for the USCG to better execute missions with a more accurate system to detect and classify high risk targets. Several issues along the way left the units unable to

communicate with each other and the inability to meet the needed $2.5 billion price tag means wasted time and resources that could otherwise have been allocated to more effective programs (Caldwell, 2014).

Limitations in successful deployment of needed technological systems are not isolated to just the Coast Guard. DHS developed a computerized system called the Automated Targeting System (ATS) that uses information on in-bound cargo to assign a risk score. The ATS system, discussed in the CBP portion of this paper, is the primary process used for risk assessments. According to the 2014 GAO report, the ATS system is not yet fully operational. Continued assessments are needed to demonstrate the ability to internalize the rules that accurately identify risks (Caldwell, 2014).

Issues brought forth by a GAO report from 2007 indicate that despite the prioritization of foreign ports based on results from their risk assessment model, many of the highest risk ports do not have a CSI presence (Caldwell, 2007). Expansion of the CSI program has its challenges. The SAFE Port Act requires 100% container scanning, but implementation of this requirement has continuously been pushed back. Budgetary constraints make the risk prioritization tool a greater indicator in resource allocation. Certain ports that are on the lower threat risk scale may need to be closed according to the report (Caldwell, 2007, pg. 23).

Public-Private Collaboration

Running within the same vein as Flynn's concerns, Coast Guard programs were not initially developed with input from other law enforcement agencies or port stakeholders. Lack of partner coordination has hindered information sharing systems with other agencies. IOCs are an important element in identifying and preventing threats from materializing into attacks, in theory. Key industry stakeholders are unable to obtain security clearances and in result cannot receive

SECRET clearance information that may be important for decision making abilities. Lack of data transparency between public and private entities hinders the IOCs ability to effectively deploy information-sharing practices (Caldwell, 2007).

Critical information provided by the private sector side is similarly withheld by port partners of the Coast Guard WatchKeeper system's because data is not updated or maintained. Lack of information sharing on both sides of the public-private relationship cripples the ability for the system to aid in preventing terrorism. More than 80% of port partners who have the system installed claim that it does not help them with mission performance (United States Government Accountability Office, 2012). The failure to consult port authorities in the developing and implementation phase of IOCs makes the ability to fully execute the SAFE Port Act's requirements unlikely.

In seventeen years since 9/11, the United States has evolved through necessity in maritime security protocol. The magnitude and immense scale of the maritime transportation system inevitably leaves programs and legislation introduced under duress to require some revision and adjustment. Through trial and error, processes can be corrected and fortified. With weaknesses identified and corrections are made, future attacks can be prevented and U.S. ports can operate without fear of a terrorist attack.

Creative Portion

National Strategy

With 9/11 acting as the catalyst, maritime security in America was completely overhauled to better address terrorism and the potential threat of another attack. The National Strategy for Maritime Security, as discussed in the literature review portion of this paper, helps to align U.S. strategies for securing waterways and the international supply chain. A legitimate

fear created after planes were used as weapons, and the plausible analogous use of a vessel as a weapon, lends towards the creation of a cohesive national approach to protecting the maritime domain. The strategy was created in 2004 with a Homeland Security Presidential Directive-13 (HSPD-13) and broadly formed methodology for the various agencies that play a role in securing the maritime transportation system in the U.S. (GAO, 2008, pg.1). In order to harmonize the different departments and subsidiary groups into a single streamlined process, the strategy includes eight different implementation plans to further facilitate policy decisions.

National Strategy Implementation Plans

Preventative measures are the first line of defense and start with strengthening maritime domain awareness. Not all eight plans that make up the broader National Strategy apply to the prevention side of fighting terrorism and therefore the Maritime Infrastructure Recovery Plan and Maritime Commerce Security Plan will not be focused on. The first implementation plan is the National Plan to Achieve Maritime Domain Awareness (MDA) that sets the foundation for prevention efforts and works hand in hand with the Global Maritime Intelligence Integration Plan (United States Department of State, 2005). Both of these plans allow for stronger transparency mechanisms to foster strong decision-making abilities and early threat detection. The International Outreach and Coordination Strategy is essential, particularly because the plan works to establish stronger foreign relations that garner greater support and leniency on U.S. initiatives that operate abroad. In order to effectively deploy any security practices or legislation, non-federal maritime entities need to have a seat at the table. The Domestic Outreach Plan aims to provide industry leaders to help develop security policies that will be realistically attainable (Maritime Security Policy Coordinating Committee, 2005). The National Strategy for Maritime Security is not a legally binding document and relies on legislation and initiatives. In order to

best encompass the goals of the strategy, the Maritime Transportation System Security Plan has a committee of both public and private maritime backgrounds to provide recommendations on improving the regulatory framework for maritime security (Maritime Security Policy Coordinating Committee, 2005).

Legislation Created to Improve National Security

International Ship and Port Security Code (ISPS)

International Maritime Organization (IMO) quickly responded to increased needs of security measures for international shipping lanes and the international supply chain with the adoption of many Safety of Life at Sea (SOLAS) amendments, preserved primarily in the newly formed International Ship and Port Security Code (ISPS) (IMO, 2008, pg. 16). Originally created just two months after 9/11, the code eventually became an internationally mandatory regulation. Upholding international law falls upon the shoulders of those member-states that have signed and ratified the ISPS code and accounts for nearly 99% of the global shipping market (IMO, 2008, pg. 17). The ISPS code develops a security framework based on risk assessment and is broadly generalized to be adopted in a global context. With proper risk assessment measures, the ISPS code aims to prevent ships from being used as a weapon, as a tool to transport high risk assets, or for a ship to be the target (IMO, 2008, pg. 17).

Maritime Transportation Security Act of 2002 (MTSA)

As mentioned before, the effective practice of requirements held within the International Maritime Organization resolution is dependent on individual country oversight. The U.S. took the framework set forth by the International Ship and Port Security Code (ISPS) one step further to include more tailored security practices and mandates. In 2002, the Maritime Transportation Security Act (MTSA) was formed with the ISPS code codified within it. The 107th Congress

understood that there was an intense need to protect U.S. ports and waterways, and that any terrorist attack in the maritime transportation sector would devastate the U.S. economy and international trade (107th Congress, 2002). The MTSA was the initial legislative response to the 9/11 attacks, in regards to maritime security, and focuses heavily on port security. Two main requirements discussed in the previous literature review section is the Coast Guard mandate for enforcing anti-terrorism measures domestically and abroad in their International Port Security Program (IPS), and the new development of a Transportation Worker Identification Credential (TWIC).

SAFE Port Act

A few years after the MTSA was set into motion, there were certain improvements needed to address the complicated and dynamic issue of maritime terrorism. In 2006, Congress passes the SAFE Port Act as a way to bolster some MTSA programs and to create new programs for issues the MTSA did not touch. Initially required by the MTSA, the TWIC program did not coalesce until the SAFE Port Act included a roll out plan. The SAFE Port Act took measures to protect container security by codifying the CBP's Container Security Initiative (CSI) program and the Customs-Trade Partnership against Terrorism (C-TPAT). The CSI program was established in 2002 as a way to screen container cargo entering the U.S. through risk assessment methodologies. Once codified through the SAFE Port Act in 2006, resources needed for expansion provided the CBP with the tools to better detect and deter high-risk cargo in foreign ports before departing for the U.S. (109th Congress, 2006). C-TPAT works as a conduit for public-private voluntary partnerships between the CBP and supply-chain businesses by agreeing to incorporate security protocol that can prevent possible terrorist attacks.

Interagency collaboration or Interagency Operations Centers (IOCs), established under the act was founded under the belief that no one agency or program was going to be able to cover all vulnerabilities in the U.S. maritime transportation sector. Coordinated efforts between both the CBP and the USCG create stronger cooperative mechanisms that foster transparency and intelligence sharing. Resources are better utilized and programs such as Coast Guard run WatchKeeper can incorporate different agency systems like CBP's Automated Target System (ATS) and the Coast Guard Ship Arrival Notification System (SANS) to evaluate data and high-risk targets (Wilbur, 2013).

Agencies that are given mandate by legislation

Customs and Border Protection (CBP)

The CBP had to quickly shift focus from using container security measures to detect criminal activity to detecting terrorism. This paradigm shift set in motion a new way of thinking for border protection and resulted in the Container Security Initiative (CSI) program. Later codified by the SAFE Port Act, the CSI program uses information provided by their Automated Target System (ATS) and information given from the Department of Energy (DOE) that is inputted into an algorithm and assigns a risk score (109th Congress, 2006, pg. 20). Depending on the assigned risk score, a container is flagged for physical examination by CBP officers. The CSI program has been expanded with the SAFE Port Act to include foreign ports. The purpose of the expanded program to include foreign ports is to identify a high-risk container prior to its ever leaving into international waters. Prescreening containers in foreign ports with high volumes headed towards America is a proactive way to prevent a terrorist attack in the U.S.. Also codified alongside the CSI program is the C-TPAT. The voluntary partnership established between privately owned companies operating in the international supply chain and CBP aims to identify

and correct weaknesses within the supply chain. By agreeing to participate in the program, partners must use best security practices as deemed by the CBP and create security plans that can be coordinated with CBP in exchange for fewer inspections and expedited examinations (CTPAT, n.d.). C-TPAT helps to embed best practices into commercial companies which falls into the greater National Strategy of the Domestic Outreach Plan.

Coast Guard

The Coast Guard and the CBP have somewhat of a dichotomy when it comes to homeland security. The CBP focuses on container security whereas the Coast Guard focuses on port security. Both areas of security are essential in preventing U.S. terrorist attacks in the maritime domain. The Coast Guard created a layered security methodology, as displayed in Figure 1, that breaks down all levels of the international supply chain within the maritime domain.

The prevention side of maritime security lies within the outer most layers of operational arenas. Because the layered security method uses a "far from the homeland approach", the Coast Guard programs that provide foreign port inspections are essential in identifying high risk ports. The next layer uses surveillance and tracking technologies as well as deployed Coast Guard Cutters to interdict and board any suspicious vessels while operating in international waters. Once in the U.S. Economic Exclusive Zone, which starts 200 nautical miles out for the U.S. coast, Coast Guard and Interagency Operation Centers use vessel arrival information to determine if further action is required for risky vessels. The inner most layers of security include private partnerships, vessel escorts, and actions to protect critical port infrastructure.

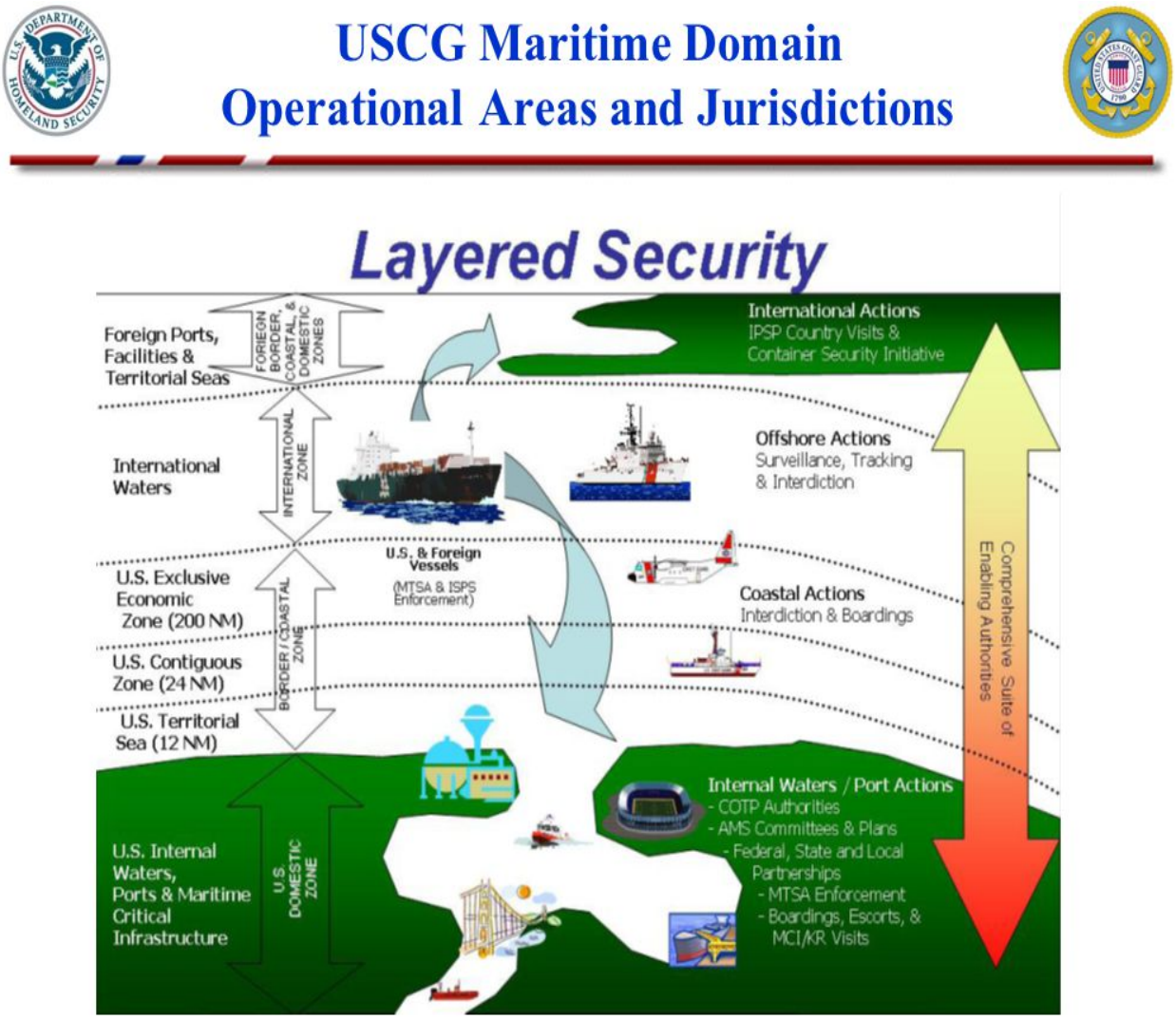

Figure 1- Source: Provided by USCG LT. CMDR Celina Ladyga

For this project, the outer layer will be focused on. Once the MTSA provided a mandate, the Coast Guard created the International Port Security (IPS) Program, which focuses on the earliest stages of the layered security approach.

The foreign port assessments are based on the already required ISPS code guidelines and are used as the framework for Coast Guard inspections. Often times working in tandem with host country port law enforcement, stronger anti-terrorism measures can be initiated and port vulnerabilities fixed. The Coast Guard uses four different weighted rules in their risk assessment

methodology to establish port risk. The four rules involve initial foreign port assessment, country wealth, threat, and responsiveness. The results of the risk model help the Coast Guard to identify how many inspections and officers are needed a year for each port (Caldwell, 2014).

Risk models can also help Coast Guard officials determine if training is required for foreign port authorities in order for ISPS designated measures to be met and maintained. There is an old Chinese adage, "If you give a poor man a fish, then you feed him for a day. If you teach a poor man to fish, then you feed him for a lifetime (Lao, n.d.)." This proverb lends itself perfectly to the Coast Guard's desire to train foreign port officials to achieve stronger autonomy in deploying anti-terrorism protocols. Stronger foreign ports do not just protect the host country, but will also protect and strengthen U.S. port security. Coast Guard run Area Maritime Security Committees (AMSCs), similar to the CBP's CTPAT program, works with the cooperation of the private maritime industry. AMSCs, however, also run training events and exercises with participating industry professionals to strengthen and synthesize security protocol on a regional basis (Caldwell, 2007).

Weaknesses Identified for Correction

International Ship and Port Security Code

The ISPS code, while the first of its kind to improve international maritime security standards, is not legally binding. The United Nations (UN), is made up of different member-nations that legitimize resolutions and legislation by agreeing to uphold them. This principle also applies to the ISPS standards were made compulsory in 2004 (IMO, 2008). Nations need to ensure that ports operating within their borders are abiding by ISPS regulations. U.S. Coast Guard officials through the IPS program work to assess foreign ports to ensure ISPS is upheld,

but sovereignty plays an important role in the Coast Guard's ability to carry out inspections. Only countries that are willing to cooperate with U.S. officials will agree to the IPS program.

The code also isn't as far reaching as it should be. As it stands, the ISPS applies to passenger ships that transit internationally, cargo vessels that are more than or equal to 500 gross tons with international ports of call, off-shore drilling facilities, and port facilities (IMO, 2008, pg. 17). Vessels that do not fit into the applicable criteria are left unmonitored and open ports and/or vessels to the risk of a terrorist attack.

Maritime Transportation Security Act

Many requirements set forth by the MTSA and the SAFE Port Act have not been implemented in full which jeopardizes the integrity of security processes and policies. The MTSA established the TWIC program, but did not incorporate a roll out plan or a means to implement the program nationally. Systems that were needed to accommodate applicant data or background checks were not considered and resulted in the TWIC program to be more a concept then a palpable result. The MTSA required the satellite vessel tracking system, Automatic Identification Systems (AIS), to be equipped in all U.S. operating vessels. MTSA, however, did not require the Coast Guard, who is in charge of protecting U.S. waterways, to adopt newer systems that can detect vessels beyond 20 Nautical Miles (Flynn, 2006). Referencing Figure 1 of the Coast Guard's layered security jurisdictions, 20 Nautical Miles is within the U.S. Contiguous zone, and does not fit into the "far from the homeland" attitude.

Systems required under the MTSA that were delegated to the Coast Guard include the Common Operating Picture (COP), which aimed to improve maritime domain awareness through an Enterprise Geographic Information System (EGIS) software. The EGIS was never produced for full agency adoption or made operational (Caldwell, 2014, pg. 7). It is also important to note

that the MTSA was created nearly three years prior to the National Strategy for Maritime Security. The MTSA was seemingly a knee-jerk reaction to the 9/11 attacks. Concepts and programs created under the MTSA used the ISPS as a model, but failed to fully address all the vulnerabilities U.S. ports are susceptible to. In order to attempt to acknowledge some of the issues not addressed in the MTSA, the SAFE Port Act was introduced.

SAFE Port Act

In 2006 when the SAFE Port Act was introduced to amend certain features in the MTSA that did not materialize, the CSI program and CTPAT were codified. Unfortunately, there are similar weaknesses in the SAFE Port Act that affect full effective capability. The CSI program uses the ATS system as a vital component in container risk assessment, but is not fully up and running at all U.S. ports (Caldwell, 2014). Some of the information filtered through the ATS algorithm is provided by DOE, but other information is provided by cargo manifests and crew lists sent ahead of arrival. Dependence on the accuracy of information provided can leave the system susceptible to inaccurate risk scores. Considering there is a possibility for unreliable risk assessments, the need for 100% container inspection required under the SAFE Port Act seems like a safety net for high risk cargo that may pass through the cracks. This requirement, however, has continuously been delayed by Congressional vote. There is not enough support to provide the necessary funding for technologies that can accomplish 100% inspection without hindering trade, leaving the metaphorical can to be kicked down the road in two year increments (Caldwell, 2014).

Interagency Operation Centers (IOCs) founded under this act utilize the system WatchKeeper to share information and intelligence across agency and private company lines. The collaborative system that integrates CBP and Coast Guard information structures is not as

effectual as it should be. The system needs port input to create a consistent baseline of security, but ports do not currently use the system (United States Government Accountability Office, 2012). The failure to bring in port authorities and private industry professionals at the commencement of the systems development makes WatchKeeper inoperative. Interagency collaboration is absolutely essential for preventive security efforts, but the poor execution of the IOC system has tainted the center's ability to be fully effective.

CBP

In 2005, plans were in the works for the expansion of the CSI program to reach into more foreign ports and conduct 100% scanning. A risk assessment model was created in anticipation of the programs growth called the Strategic Trade Corridor Prioritization Model (Caldwell, 2007, pg. 21). Country threat, shipping lane information, and data provided by ATS make up components that influence the risk model prioritization (Caldwell, 2007, pg. 21). Through the new model created by CBP, 356 ports were suggested for CSI expansion, but that was later narrowed down to 187 ports. Even with cutting down the number from 356 to 187, CBP reduced the amount of ports for the expansion down to 22 (Caldwell, 2007). The 22 ports left had the highest risk scores and the highest volume of containers shipped to the United States.

CSI was never expanded into these high-risk ports and rather than reallocating resources from low risk ports that have a CSI presence to the 22 high risk ports, CBP has abandoned the Strategic Trade Corridor Prioritization Model altogether. CBP has not reassessed the model or the risk scores assigned since 2005 (Caldwell, 2007). Failure to re-evaluate risk assessment models on an annual basis diminishes the accuracy of port risk values and is a stark contrast from the Coast Guard's annual reassessment policy. Using current and up-to-date information to determine risk and keeping consistent policies with the Coast Guard risk model can create a

clearer picture for resource allocation. Legal constraints of a host nation can hamper the ability for CBP officers to scan containers in ports in which the CSI is present. Electronically scanned cargo images may only be viewed by CSI officials if host government custom officials agree to allow the CBP officers to observe (Caldwell, 2007). Cooperation with foreign custom agencies can vary depending on a ports' risk score, and leaves unmonitored gaps in cargo screening.

CTPAT has been a successful private-public partnership, but has not taken advantage of mutual recognition arrangements with other foreign customs agencies. Mutual Recognition Agreements (MRA) of Customs controls are created with customs practices and cargo inspections of two countries that are accepted by the other and can also be extended to an authorized economic operator (AEO) program like the CTPAT (United States Government Accountability Office, 2012, pg. 28). Other nations have similar working AEO programs that the CBP could enter MRAs with, but have not pursued those negotiations. Failure to take advantage of MRAs stagnate the CTPAT membership and cuts off communication lines with other AEO programs operating around the world.

Coast Guard

In order to enhance maritime domain awareness, the Coast Guard visualized a system called Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR). Theoretically, the system would enable the Coast Guard's operating capacity to detect, assess, and interdict targets appraised to be high risk, but it was never fully created once funding ran dry (Caldwell, 2014, pg. 8). The long line of ineffectual software and systems shows how far the U.S. is from where it could be or should be if these systems were actually operational.

A program that has seen positive results is the International Port Security (IPS) program run by the Coast Guard. Approximately 150 countries work in coordination with the USCG's IPS program, which is a lofty feat and significantly improves port security. Issues, however, arise when considering how spread thin the ISPS liaison officers (ISPSLO) are. Required to oversee large operating arenas, there are only 13 ISPSLOs to cover all IPS ports in South America, the Middle East, Europe, and Africa. All of the Asian ports have only six ISPSLOs to oversee IPS operations (Flynn, 2006). There is no program in place for ISPSLOs to be formally trained on commercial port common practices, port security, how to manage an inspection team, or differences between host countries prior to receiving the role (Flynn, 2006). As most active duty Coast Guard officers' billets run anywhere from two to four years. Once an ISPSLO has learned the job and established relationships with host countries, a new ISPSLO arrives and the cycle repeats.

Regional Coast Guard sectors and AMSCs are required to participate in a collective exercise to test security plans with no more than 18 months separating exercises (United States Government Accountability Office, 2012, pg. 14). In order to incorporate the Transportation Security Agency (TSA) into AMSC exercises, an extension program called the Port Security Training Exercise Program (PortSTEP) was introduced to encompass the whole port community. Confusion was created between MTSA required AMSC exercises, the added PortSTEP exercises, and the newly added SAFE Port Act Interagency Operation Centers (IOC) port security exercises (Government Accountability Office, 2012, pg. 15). AMSCs have not been able to distinguish the difference in exercise requirements set forth by different legislation or programs. Lack of scope and clear understanding for requirements makes fulfilling needed action difficult.

Proposed Solution to Improve Preventative Security Measures and Correct Weaknesses

Ways to make the National Strategy more effective

Depending on the specificity of each plan and each agency's interpretation of those plans, effective implementation may or may not happen. With no centralized authority to maintain sole oversight over processes and implementation plans of the National Strategy for Maritime Security, there is a heavy reliance on guidelines set forth by individual plans. There is a breakdown in cohesiveness between the different plans that convolute how best to apply solutions. For instance, wide ranging scope and differing definitions makes it difficult to overlap different implementation methodologies. The National Strategy states that the objective and scope is to harmonize the different departments to allow for effective implementation of security strategies, whereas the Maritime Transportation Security System plan states its scope is to protect the different components that make up transportation security (Maritime Security Policy Coordinating Committee, 2005). By first defining what the threat is, and creating a risk assessment based on the defined threat, there are can be a more cohesive and consistent process for establishing a solution.

With each plan having varying levels of detail, scope, and no specific solutions suggested, there is a relatively high degree of difficulty in ensuring any solution created will actually be effective. Each plan also addresses different components that make up maritime security that overlap one another. By breaking down each plan into tasks and cross-referencing which tasks overlap, needs can be better prioritized and tackled on an interagency level (GAO, 2008, pg. 23). With different agencies left to develop individual plans, resources are not utilized as efficiently as they could be. Intelligence falls into different silos based on agency and plan, which inherently works against the purpose of a National Strategy for Maritime Security. More

tangible efforts made to meet the objectives of the National Strategy can be seen in the legislative acts created by the IMO and Congress. Many of the National Strategy implementation plans are overlapped by supporting acts such as ISPS code, the MTSA, and the SAFE Port Act.

Interagency Cooperation

In order to successfully deploy protective measures embodied in initiatives like CSI or ISP, there needs to be better processes in place to overlap resources and intelligence. Many ports inspected by Coast Guard officials are also checked by CBP officers, but not at the same time. These two agencies work toward a common goal, but do not cooperate with one another to pool resources. Each agency focuses on their key programs without working to combine methodologies that will tackle the bigger picture of preventing terrorism. Both CBP and CG officers should make interagency inspection groups that can go into high risk ports to check port and cargo security protocol. Certain ports that may not have the CSI program present, but allow the ISP program, may be made more accessible through a joint team. A joint team used for foreign port inspections can use the Coast Guard's current risk assessment methodology to include container risk protocol so that high risk ports and cargo can be flagged and prioritized accordingly.

Stronger International Relations

The United States should place greater emphasis on international cooperation especially with regional pacts like the European Union (EU) and the Association of Southeast Asian Nations (ASEAN) (Flynn, 2006). Growing and strengthening relationships with the international community will improve the ability for programs that depend on host country cooperation to carry out security protocols for port and container security. Nations with vetted and approved security practices and protocol can make up a United Nations multinational audit group that can

ensure the ISPS code is maintained. Because the ISPS has been made into a compulsory standard, the United States should not be the only nation holding other ISPS signatories to the required standard. An internationally assembled audit group would free up Coast Guard funding and personnel under the ISP program that can either be diverted to the CBP for their CSI program or towards improving systems the Coast Guard need in order to secure the maritime domain and prevent future terrorist attacks.

Creating more Mutual Recognition Agreements (MRAs) with other nations or with Authorized Economic Operators (AEO) programs like the CTPAT would mean more links in the international supply chain would go through a vetted program. The more private sector industry leaders that agree to use strong preventative practices the higher chance of being able to close security gaps and strengthen the international supply chain against terrorism. Companies will receive more benefits the larger CTPAT becomes and will therefore more likely encourage other international supply chain businesses to join.

Technologies Need to Be invested In

Software technologies are a necessary cost to improve the odds of combing through the maritime domain for terrorist threats. Systems like the Customs and Borders Protection's Automated Tracking System, the Interagency Operations System's WatchKeeper, and the Coast Guard's Common Operating Picture map-based information system are tools that should be made nationally accessible for all ports or agencies that require them. Every possible resource should be made available to DHS if there is genuine concern for protecting U.S. ports from terrorism. The Coast Guard requires 96, 72, and 24-hour vessel notifications prior to arrival in the U.S., but currently do not have the systems in place that can detect vessels beyond a 20 Nautical Mile range. Taking advantage of already existing programs, the Coast Guard can use

the IMO's required Long Range Identification and Tracking system (LRIT), which currently only transmits to one Navigation Center (NAVCEN) in Alexandria, VA (United States Coast Guard, 2015). Coast Guard sectors that have access to ship data from LRIT can confirm information provided to them by vessel prior notifications and identify inconsistencies or concerns.

CBP also needs a way to confirm information that is provided to them by vessels on their way to the U.S.. Cargo manifests can be prone to mistakes, and can't be confirmed for accuracy (Flynn, 2006). Information, whether correct or not, is entered into the ATS system to help determine risk scores. The CBP should work with foreign customs agencies to cross-reference vessel data to identify irregularities or inconsistencies. Taking advantage of the LRIT system, CBP officers can have real-time updates to establish a timeline for needed interdiction prior to entering U.S. waters.

Technologies and equipment that allow for fast and effective cargo scanning, if invested in, will allow for 100% container inspections to be conducted. Congress has continuously voted to extend the requirement for 100% scanning because it was believed that the technology did not exist to handle the volume of containers without impeding trade, but that notion is false. Pilot technologies such as Nex-Gen Scanners can scan every truck with a container that passes through the terminal gate in 30-40 seconds (Kulisch, 2016). In the ports of LA/LB, CBP has ten non-intrusive imaging pieces of equipment in what is still a very manual process and limited in its ability to inspect the needed number of containers (Kulisch, 2016). The Nex-Gen Scanner can detect fissionable radioactive material in containers, even if it's shielded, and automatically upload the imaging into their The Passport machine. The Passport can create a 3-D image and breakdown the material into elemental components to determine if a fission detection has been

weaponized (Kulisch, 2016). High risk containers will be flagged to notify CBP inspectors that further action is needed.

The Nex-Gen Scanners may still not be able to inspect 100%, but through proper prioritization, resources and inspection systems can be optimized. Following Maritime Security (MARSEC) levels designated by the Coast Guard Commandant, CBP can correlate the number of containers scanned and images examined. MARSEC levels go from the minimum level at 1 to the strictest level at 3, with each level requiring more or less security measures to be applied (Flynn, 2006). Incorporating the amounts of scans conducted by the Nex-Gen Scanners into a correlating MARSEC level is a logical way to prioritize based on risk level. Technologies backed by the government will subsequently also help with the continued staffing shortages of CBP officers. Fewer people will be able to manage more container flow with the aid of systems that can pick out only legitimate threats.

Funding

Technologies and required systems will only be introduced if there is adequate funding provided to develop and install them into American ports. Beyond systems upgrades, the government needs to provide funding for necessary port infrastructure improvements. An estimated combined amount of $66 billion investment is needed to improve security infrastructure (MAREX, 2017). Although just an estimation and a very unlikely sum to acquire, current political climate appears to be moving in the opposite direction with budget cuts. The Trump administration shows a 23% decrease in Harbor Maintenance Trust Funds from 2017 to 2018, and the Department of Homeland Security's Port Security Grant Program (PSGP) was cut by 52% (MAREX. 2017). The PSGP plays a vital role in helping ports maintain infrastructure

against terrorism and the larger Maritime Infrastructure Recovery Plan under the National Strategy for Maritime Terrorism.

The Coast Guard has several different programs under their jurisdiction, one of which is the Interagency Operations Center (IOC). In order to further develop IOC effectiveness, an estimated $260 million would be needed to upgrade information systems and facilities in 24 sectors that oversee the highest priority ports in the country (Caldwell, 2007, pg.10). Improving IOC abilities will meet the National Strategies for achieving domain awareness, domestic outreach, as well as improving global maritime intelligence. The ISP program, besides inspecting foreign ports, also train and assist to improve countries that have port facilities needing basic security measures. Many times, that assistance is financial so that facilities can implement fencing, lighting, and communication devices (Caldwell, 2007, pg. 17). Budget constraints and no sign of added funding will limit the Coast Guard's ability to provide financial assistance to ports that require improved anti-terrorism measures.

CBP has had to reassess how resources are used because of budget cuts and continue to deal with maintaining optimal staff numbers in CSI ports. The MTSA and the SAFE Port Act has created very lofty requirements of the Coast Guard and CBP, but continue to cut funding essential for these agencies to be able to meet what is expected of them. Cutting programs and constantly having to reassess resources available hurts the agencies' proficiency. If the government wants to secure the nations ports and achieve the National Strategy for Maritime Security, funding needs to be increased.

Summary

The efforts made by the U.S. government in the wake of 9/11 to protect the homeland resulted in a barrage of legislative action that forced the entire maritime industry to rethink

security protocol. The National Strategy for Maritime Security was created to form a new foundation for agency cooperation in order to produce a safer maritime transportation sector. The legislative acts that were created to help carry out the National Strategy formed a complex system of programs and initiatives meant to cover all elements of maritime security. The International Ship and Port Security Code (ISPS), Maritime Transportation Security Act of 2002 (MTSA), Security and Accountability for Every Port Act of 2006 (SAFE Port Act), and the agencies that helped to enforced them, collectively worked to prevent a terrorist attack from occurring in a U.S. port.

The immediate and urgent need for stronger security mechanisms and preventative measures left the U.S. with the MTSA, a poorly thought out plan that was primarily based on the ISPS, but did not create clear policy to specifically address U.S. ports or the maritime domain. The retroactive nature of the National Strategy for Maritime Security leaves the MTSA of 2002 as a small stepping stone towards the vision created by the National Strategy in 2005. One large benefit of the MTSA was the national adoption of ISPS requirements and the beginnings of a paradigm shift from criminal focus to terrorism in maritime security protocols. Efforts to align the MTSA more with the National Strategy led to the adoption of the SAFE Port Act introduced in 2006. In order to help relieve some issues unanswered by its MTSA predecessor, container security needs and private partnership collaborations were incorporated in the SAFE Port Act through the codification of the Container Security Initiative (CSI) and the Customs-Trade Partnership against Terrorism (C-TPAT).

Variables that may affect the strength of programs proposed or enforced involve interagency collaboration, international cooperation and responsiveness, the introduction of newer technologies, and government funding. Beyond U.S. waters, the Coast Guard and CBP

rely heavily on host nations granting access to port facilities and customs information. The inability to inspect ISPS or CSI compliance in countries exporting shipped goods to the U.S. nullifies the program's possible benefits. Systems required under the MTSA and SAFE Port Act that have yet to be made completely accessible abates government action to address the issue. Proposed security funding is dependent on Presidential administration proposals, Congressional backing, and resource allocation, all of which can vary significantly based on election results or annual fiscal prosperity. These two variables can have rippling effects that may affect every element of preventative security in U.S. maritime ports.

Plan of Action

In order to improve and broaden the role of U.S. agencies abroad, there needs to be greater international relationships that are mutually beneficial. A realistic approach to achieve this would include the Coast Guard and CBP to:

- Work with regional pacts to encourage cooperation such as the European Union (EU) and Association of Southeast Asian Nations (ASEAN)
- Establish a multi-national, United Nations formed audit group to enforce IMO ISPS code requirements
- Form more Mutual Recognition Agreements (MRA) with other nations customs controllers, as well as Authorized Economic Operator (AEO) programs to free up resources
- Utilize more private sector industry leaders to form more realistic systems and processes that can be applied to already existing port security standard operating procedures

- Create overlapping interagency protocols that allow for joint risk assessment methodologies and pooled resources under Interagency Operation Centers (IOC)

Success of the proposed plan of action relies heavily on funds provided by the federal government. Basic infrastructure needs along with system support have been thwarted because of agency budget cuts. The programs that primarily deal with the terrorist threat are not the sole objective for the Coast Guard or CBP, which leaves critical terrorist prevention programs competing against other agency initiatives that may be equally important.

A primary concern for future developments of terror prevention measures in U.S. ports is the ability to apply existing policy and initiatives to such a dynamic threat. As noted in the literature review portion, scenario prioritization and threat awareness were fundamental in creating a national strategy, but should also be applied and re-evaluated on an annual basis. Threat scenarios that were prioritized early in the development of a national strategy may not necessarily remain true over 15 years after the fact. Flexibility and the fluidity of policy are critical pillars for terror prevention. As physical security measures have tightened oversight abilities, terror organizations have evolved to more sophisticated cyber-attacks. Cyber information sharing and the ability to incorporate existing committees like the Interagency Operations Committee (IOC) and Area Maritime Security Committees (AMSCs) into Cyber security protocol may ease the threat. Leveraging partnerships and consistently re-evaluating threat/attack scenarios will work to address the future development of U.S. maritime port terror prevention measures.

References

107th Congress. (2002, November 25). Maritime Transportation Security Act of 2002. Retrieved January 28, 2018, from https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf

109th Congress. (2006, October 13). Security and Accountability for Every Port Act of 2006. Retrieved February 1, 2018, from https://www.congress.gov/109/plaws/publ347/PLAW-109publ347.pdf

Caldwell, S. (2007, October 30). The SAFE Port Act: Status and Implementation One Year Later. Retrieved January 27, 2018, from https://www.gao.gov/new.items/d08126t.pdf

Caldwell, S. (2014, June 4). Progress and Challenges with Selected Port Security Programs. Retrieved February 2, 2018, from https://www.gao.gov/assets/670/663784.pdf

Chambers, M., & Liu, M. (2012). Maritime Trade and Transportation by the Numbers. Retrieved January 26, 2018, from https://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/by_the_numbers/maritime_trade_and_transportation/index.html

CTPAT: Customs Trade Partnership Against Terrorism. (n.d.). Retrieved February 06, 2018, from https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat

Flynn, S. (2006, March 9). The Continued Vulnerability of the Global Maritime Transportation System. Retrieved January 25, 2018, from https://www.cfr.org/report/continued-vulnerability-global-maritime-transportation-system

IMO. (2008). Contribution of the International Maritime Organization to the Secretary-General's Report on Oceans and the Law of the Sea, 2008. Retrieved February 2, 2018, from http://www.un.org/depts/los/consultative_process/mar_sec_submissions/imo.pdf

Keefer, W. (2007, October). Container Port Security: A Layered Defense Strategy to Protect the Homeland and the International Supply Chain. Retrieved January 27, 2018, from https://scholarship.law.campbell.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1462&context=clr

Kulisch, E. (2016, August 18). U.S. lawmakers say with new technology, it's time to inspect all inbound containers. Retrieved March 02, 2018, from http://www.westarusa.com/u-s-lawmakers-say-new-technology-time-inspect-inbound-containers/

Ladyga, C. (2018, February 21). Layered Security [E-mail to the author].

Lundquist, E. (2011, March 17). International Port Security Program. Retrieved February 06, 2018, from https://www.defensemedianetwork.com/stories/international-port-security-program/

MAREX. (2017, May 23). Trump's Budget Request Cuts Port Funding. Retrieved March 02, 2018, from https://www.maritime-executive.com/article/trumps-budget-request-cuts-port-funding#gs.Z_4uJU0

Maritime Security Policy Coordinating Committee. (2005, October). Maritime Transportation System Security Recommendations for The National Strategy for Maritime Security. Retrieved January 30, 2018, from https://www.dhs.gov/sites/default/files/publications/HSPD_MTSSPlan_0.pdf

Parfomak, P., & Frittelli, J. (2007, January 9). Maritime Security: Potential Terrorist Attacks and Protection Priorities. Retrieved January 23, 2018, from https://fas.org/sgp/crs/homesec/RL33787.pdf

Pate, A., Taylor, B., & Kubu, B. (2007, November 20). Protecting America's Ports: Promising Practices. Retrieved January 30, 2018, from https://www.ncjrs.gov/pdffiles1/nij/grants/221075.pdf

U.S. Coast Guard. (2017, November 1). Area Maritime Security Committees 2016 Annual Report. Retrieved February 3, 2018, from http://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/AMSC%20Consolidated%20reports/2016/AMSC%202016%20Annual%20Report%20(signed).pdf?ver=2017-11-08-084656-947

Targets for Terrorism: Ports. (2006, January 1). Retrieved January 18, 2018, from https://www.cfr.org/backgrounder/targets-terrorism-ports

U.S. Customs and Border Protection. (2011, May). Container Security Initiative in Summary. Retrieved February 1, 2018, from https://www.cbp.gov/sites/default/files/documents/csi_brochure_2011_3.pdf

United States Coast Guard. (2012, August). DHS Interagency Operations Centers. Retrieved February 6, 2018, from http://onlinepubs.trb.org/onlinepubs/conferences/2012/HSCAMSC/Presentations/3B-Clark.pdf

United States Department of State. (2005, September 01). The National Strategy for Maritime Security. Retrieved February 06, 2018, from https://www.state.gov/t/pm/rls/othr/misc/255321.htm

United States Government Accountability Office. (2008, June). Maritime Security. Retrieved February 2, 2018, from https://www.gao.gov/new.items/d08672.pdf

United States Government Accountability Office. (2013, September 13). Supply Chain Security. Retrieved January 24, 2018, from https://www.gao.gov/assets/660/657893.pdf

Wilbur, R., Capt. (2013, January 4). Interagency Operations Center (IOC) WatchKeeper. Retrieved February 5, 2018, from https://www.dhs.gov/sites/default/files/publications/privacy_pia_uscg_watchkeeper_20130104_0.pdf