1-1-2012

Our Homeland and Our Security: A Look Into America's Critical Infrastructures

Rebecca Sidhu
Pace University

Follow this and additional works at: http://digitalcommons.pace.edu/homelandsecurity

Part of the Criminology and Criminal Justice Commons, and the Defense and Security Studies Commons

Recommended Citation
http://digitalcommons.pace.edu/homelandsecurity/11

This Thesis is brought to you for free and open access by the Dyson College of Arts & Sciences at DigitalCommons@Pace. It has been accepted for inclusion in Master in Management for Public Safety and Homeland Security Professionals Master's Projects by an authorized administrator of DigitalCommons@Pace. For more information, please contact rracelis@pace.edu.
OUR HOMELAND AND OUR SECURITY:
A LOOK INTO AMERICA’S CRITICAL INFRASTRUCTURES

BY

REBECCA SIDHU

SUBMITTED IN PARTIAL FULFILLMENT OF
REQUIREMENTS FOR THE DEGREE OF MASTER OF
ARTS IN MANAGEMENT FOR PUBLIC SAFETY
AND HOMELAND SECURITY

DYSON COLLEGE OF ARTS AND SCIENCES
PACE UNIVERSITY

MAY 2012

APPROVED BY:
Abstract

Since 9/11 this country has been faced with a problem unforeseen prior to the tragic events in 2001: terrorist threats and attacks against the United States. Just a decade later, we are facing complex issues regarding the protection of this nation’s most critical assets. Ordinary Americans depend on banking, public transportation, highways, and other infrastructures to maintain a healthy living. The protection of these assets is conducive to how we sustain freedom and prosperity in America. Addressed in this project are several topics analyzing the safety and security of critical infrastructures including banking and finance, maritime areas, rail way systems, and the critical infrastructures for the U.S. Department of Defense are used as primary examples. In addition to these topics, the issue of human rights, the USA Patriot Act, and military tribunals are included, as well as intelligence assessments against the New York City subway system.

Chapter I contains a report to the Secretary of the U.S. Department of Homeland Security, Janet Napolitano, laying out the need to increase and enhance security measures for the nation’s infrastructures, in this case, seaport security. This gives a broader view on how government agencies of all levels must sustain healthy relationships with private stakeholders and international organizations. As the world becomes smaller with technology, we have to become mindful of how one act of terrorism could be detrimental to not only America but to the global economy.
Acknowledgements

This portfolio is dedicated to those who have supported me all the way through this rigorous process, especially dedicated to my loving family: My mother and father Rubina and Sid, and my siblings Monica, Jessica, and Arjun. Next, I would like to thank my friends and colleagues at the United States Department of Labor Employee Benefits Security Administration who motivated me day in and out regardless of how stressful I became. I would like to give special thanks to a friend at the FBI who guided me through a particular part of this assignment when I needed it the most. And finally, to each of my professors that were accommodating and especially helpful during my times of confusion. Professors for this cohort were professional, experienced, and humble. I am grateful for having learned under a group of instructors that understood the difficulties that came with mastering a graduate degree.

You have all given me so much support the last two years and I will forever be grateful for that.

I am honored to have earned a Master’s degree in Management for Public Service & Homeland Security Professionals.
# America’s Critical Infrastructures

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>2</td>
</tr>
<tr>
<td>Abstract</td>
<td>3</td>
</tr>
<tr>
<td>Chapter I A Strategy to Enhance Safer Ports Through The IURP Program</td>
<td>5</td>
</tr>
<tr>
<td>Chapter II The IURP From A Managerial Standpoint</td>
<td>20</td>
</tr>
<tr>
<td>Chapter III Infrastructures and Cyberterrorism</td>
<td>37</td>
</tr>
<tr>
<td>Chapter IV Military Tribunals and the Constitution</td>
<td>54</td>
</tr>
<tr>
<td>Chapter V The USA PATRIOT Act &amp; Human Rights</td>
<td>66</td>
</tr>
<tr>
<td>Chapter V Technology &amp; Threats Against Maritime Areas</td>
<td>79</td>
</tr>
<tr>
<td>Chapter VII Megacommunities &amp; Maritime Issues</td>
<td>98</td>
</tr>
<tr>
<td>Chapter VIII Protection of Personnel</td>
<td>109</td>
</tr>
<tr>
<td>Chapter IX New York’s Subway System &amp; NYPD JTTF</td>
<td>124</td>
</tr>
<tr>
<td>Chapter X Evaluating the Critical Infrastructure Program</td>
<td>135</td>
</tr>
<tr>
<td>Chapter XI Bioterrorism and Maritime Areas</td>
<td>147</td>
</tr>
<tr>
<td>Conclusion</td>
<td>162</td>
</tr>
</tbody>
</table>
CHAPTER I

The United States Department of Homeland Security:

A Strategy to Enhance Safer Ports Through

The International United Reliance Program

TO: Secretary of Homeland Security Janet Napolitano

FROM: Rebecca Sidhu

SUBJECT: Recommendation to Improve Seaport Security

Strategic Recommendation on Seaport Security

The nation’s current seaport security is woefully inadequate for the 21st century. This memorandum is a strategy to improve the nation’s homeland security and particularly its seaport security. It encourages increased and coordinated efforts abroad to ensure greater seaport cargo security at home.

For nations most susceptible to these dangers, the U.S. Department of Homeland Security (DHS) should consider implementing a new program which I call the International United Reliance Program (IURP). The IURP will be a newly developed area in which the U.S. will have face to face interactions with foreign government officials and their front line security forces. Through diplomatic and peacekeeping efforts via the Department of Defense (DOD) security forces, the U.S. will be doing more than just requesting help; the DHS will have established relationships with countries essential to securing their own seaports, and in essence, preventing weapons of mass destruction
(WMD) and other chemical, biological, radiological, and nuclear weaponry (CBRN) from being sent to the U.S.

Charles Goslin, Vice President of Duo Industries, reported that in November 2002, Abd al-Rahim al-Nashiri, Al Qaida’s operations chief in the Persian Gulf developed a strategy to attack Western shipping targets:

1. Ramming vulnerable vessels at sea;
2. Blowing up medium-sized vessels at ports;
3. Attacking vulnerable, large cargo ships such as super tankers from the air by using explosive-laden small aircraft.

This intelligence is supported by the 2007 National Intelligence Estimate and the 2010 Annual Threat Assessment to the Senate. In addition, Al Qaida operatives have obtained international seamen’s licenses, nonimmigrant visas, and other documentation that enable international port access. The implications of the aforementioned open-source intelligence (OSINT) include enhanced international port security.

Vulnerabilities

High risk countries including Yemen, Israel, Saudi Arabia, Afghanistan, Iraq, Pakistan, and India are prone to extremism; the same types of threats and ideals of extremism now threaten our country. International shipping is an object of threat that is greater in certain countries. The aforementioned countries are more susceptible to these threats because of the greater presence of terrorist cells which operate these areas. With vast amounts of imported goods entering the ports, it makes it difficult for the U.S. to search every package entering our ports.
Christopher Bellavita’s *Homeland Security Affairs: What Is Preventing Homeland Security?* addresses an interesting point, “At the national level, there have been no especially imaginative innovations in policy, strategy or how we are organized to prevent terrorism.” If the theory that we are “secure” at a national level by simply placing new goals and strategies, then we will start to see issues come about as terrorism gets more technically advanced and communication starts to deteriorate amongst U.S. agencies. The idea that if we write down goals and objectives and assume they will be applied correctly across the board with all DHS agencies is a misconception which is a recipe for disaster.

The DHS must analyze what the U.S. is encountering and the resources seaports lack. If we narrow down our efforts to a local level, we will be able to get a better idea of how operations affect the nation on an international level. For example, the main purpose for the coordinated effort between The Port Authority of New York and New Jersey (PA) and the DHS is to increase security by scanning shipments which arrive by ships. While the PA and other DHS personnel are trained to deal with possible scenarios, the DHS has not implemented supply-chain accountability that might identify and trace all transported goods from port of origin to the receiving port.

The PA and DHS do not have a balanced cargo to security personnel ratio. C. Goslin (2007) explains: “Globally, there are very few uniform standards for point-to-point control of security on containers, cargoes, vessels or crews - a port’s security in one nation remains very much at the mercy of a port’s security, or lack thereof, in another nation. Organized crime is entrenched in many ports, and a large majority of seaports still
do not require background checks on dock workers, crane operators or warehouse employees. Most ports lease large portions of their facility to private terminal operating companies, who are responsible for their own security.”

RAND indicates that a container arriving at a U.S. port is subjected to several checks. “The 24-hour advanced manifest rule requires carriers to submit manifest information 24 hours before cargo is loaded onto a U.S. bound vessel. In this time, CBP performs a background screen on the manifest, carrier and shipper to determine if the shipment poses a risk to the United States. In some cases, the container is denied permission to be loaded on the vessel.” Stephen Flynn, a fellow at the Council on Foreign Relations and retired U.S. Coast Guard commander stated “It takes one of their customers saying, ‘Hey I’ve got one of your boxes if you want it back.' Those boxes are a potentially potent weapon for terrorists – whether for use smuggling weapons, explosive materials or terrorists themselves, or as a huge chemical, biological or ‘dirty’ bomb spreading radioactive waste. At present, though, many ports are ill-prepared to deal with that threat.” (Shoen, 2004) “And while advanced technology scanners have helped speed those inspections, just tracking the 200 million containers that move among the world’s top seaports each year is a major undertaking.”(Schoen, 2004) Companies do not know where 40 percent of these shipments are at any given time.

Current DHS Strategic Goals as They Relate to Seaport Security

The DHS has implemented five strategic goals and four objectives in the National Strategy for Homeland Security. One of these goals is to “Protect Our Nation from
The mission is: “We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. We will secure our national borders while welcoming lawful immigrants, visitors, and trade.” This is according to the DHS five year strategic plan titled “One Team, One Mission, Securing Our Homeland.” We have to increase seaport security of the United States and other countries by increasing the effectiveness of how we communicate with security forces abroad. Brian Jackson and David Frelinger’s *Emerging Threats and Security Planning* (2009) frame a middle ground approach to addressing possible threats. Meeting halfway in a proposal rather than burdening a country with its own security forces is essential. “Ideally, the national approach to addressing possible future threats should strive to get as many of the advantages of both ends of the spectrum—responding prudently to threats…but not allowing doing so to threaten the effectiveness and sustainability of existing security efforts by forcing planners to spend disproportionate time focusing on unlikely terrorist scenarios. Analysts could use techniques such as risk analysis or cost/benefit analysis to assess different threats and use their results as a common denominator to determine how much we should worry about different possible attacks and the advisability of different possible responses to them” (B. Jackson & D. Frelinger, 2009).

The DHS’ National Strategy provides four objectives.

1. To prevent and detect radiological/nuclear attacks. To reduce the risk of nuclear and radiological attacks the DHS intends to “develop and implement measures aimed at preventing successful introduction of
nuclear and radiological weapons into the United States, whether by air, land, or sea."

2. To prevent, detect, and protect against biological attacks. The DHS will lead efforts to establish an integrated National Bio-defense Architecture. “We will systematically prioritize and focus efforts, including risk-based threat assessments, biological detectors, bio-surveillance, forensics, and emergency planning systems that can quickly detect, characterize, and respond to biological attack. We will prepare individuals, families, communities, and the nation to respond effectively to biological attacks in the United States and minimize consequences.”

3. To prevent and detect chemical and explosive attacks. We will reduce the risk of and guard against chemical and explosive attacks in the United States. The DHS goes on to say that they will “reduce the risks to our citizens and infrastructure from hazardous chemical and explosive attacks and incidents.”

4. To prevent the introduction of illicit contraband while facilitating trade. The DHS “will guard against unlawful goods and activities entering the United States with minimal impact to legitimate trade.”

The Homeland Security Presidential Directives (HSPD) addresses twenty four directives to combat terrorism. Six directives state how to increase security at a national level
rather than an international level. HSPD 1 created the Homeland Security Council (HSC) and specifies its organization. After President Obama was elected, he combined the HSC into the National Security Council.

1. Directive 3 dated March 11, 2002 states the HSPD for the Homeland Security Advisory System: “to inform all levels of government and local authority, as well as the public, to the current risk of terrorist attacks.” This is related to seaport security in that we have established joint efforts with local, federal and private entities to ensure seaport security.

2. Directive 4 dated September 17, 2002, states the HSPD for National Strategy to Combat Weapons of Mass Destruction: “Set forth a comprehensive strategy to counter the WMD threat in all of its dimensions.” We have to relate this to every element of homeland security including seaport security. WMD are a concern requiring further security checks via better relationship with foreign security forces.

3. Directive 6 dated September 16, 2003, states the HSPD for the Integration and Use of Screening Information: “the policy is to develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct related to terrorism. The directive will be implemented in a manner consistent with the provisions of the Constitution and applicable laws, including those protecting the rights of all Americans.” This seaport security strategy is to foil an attack before it makes its way through our seaports.
4. Directive 7 dated December 17, 2003, states the HSPD for the Critical Infrastructure Identification, Prioritization, and Protection: “establishes a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks, and to work with state and local governments and the private sector to accomplish this objective.” Infrastructure is a crucial part of seaport security. We will have to implement the strategy to provide for better communication efforts.

5. Directive 10 dated April 28, 2004, states the HSPD for Biodefense for the 21st century: “The pillars of this national biodefense program are Threat Awareness, Prevention and Protection, Surveillance and Detection, and Response and Recovery. A classified version of this directive contains specific direction to departments and agencies.” The strategy will be built upon this directive. It is important to put into practice a method to better develop seaport intelligence.

6. Directive 19 dated February 12, 2007, states the HSPD for Combating Terrorism Use of Explosives in the United States: “establishes a national policy, and calls for the development of a national strategy and implementation plan, on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States.” The subject of explosives needs to be heavily scrutinized. Although not all measures are a 100% preventative measure we can certainly tighten the strategies already in place and place further security efforts via this strategy.
These objectives are to be implemented or increased by at least 80% by 2013. These objectives are realistic but not easily applied when lacking the appropriate resources. The recommendation below will improve seaport, homeland, and national security.

Recommendation One:

DHS should widen the scope of detection and inspection of cargo shipments entering the United States.

- DHS should leverage current diplomatic and peacekeeping policies to affirm that the IURP could provide for the safety and security of the host country and the international shipping community.

- DHS should facilitate port-specific information and intelligence sharing initiatives with International Maritime Organization signatory nations.

DHS should prioritize seaport-MOU protocols with state and local governments and private sector entities to facilitate point-to-point tracking capabilities.

The IURP contains outreach programs which identify not only the safety concerns for the U.S. but for other countries also. Conversely, the United States must acknowledge that foreign governmental agencies may not be quick to disseminate information pursuant to a treaty. We should not assume countries will handle treaties the same way. Some countries may not decide to be cooperative, while others may simply feel that the situation is not grave enough to involve the United States. Among the vast amount of
information sharing that goes on between the U.S. and other countries, DHS will have to stand out this issue.

Recommendation Two: Enforce extant IMO Regulations

The U.S. might have to pressure some countries to comply with this strategy. We need to know how to urge them into cooperating. A simple example is that of a door-to-door salesman. No one wants to answer the door because they know someone wants to sell a product. They see this person going around from house to house asking residents if they are interested in investing their time, energy, and money in a product. Rather than marketing an item they are asking a person to buy something by intruding into their space. However, if the salesman took a marketing approach, it would be more compelling. He or she would invite potential investors to his or her place of business and give a sense of welcoming to the investor, making the investor feel comfortable and offering incentives. To market an idea to a country rather than selling an idea are two different approaches. Clearly one works better than the other; the DHS needs to take the approach as a marketer. In a marketing aspect there is a give and take, there must be an advantage to the investing country. While the U.S. is interested in foreign port security, the port of origin also has a vested interest. If the U.S. simply refused to accept goods from ports that do not comply with U.S. and International Organization treaties, we may see cooperation and a willingness to participate in our agenda.

The IMO’s strategic plan dated January 18, 2010 addresses the concerns for seaport security and the challenges they face. “The challenge for IMO is to promote the effective
implementation of the security measures, and to instill a security consciousness in ship and port facility operations, at the same time ensuring that the right balance is struck in trade facilitation and that the flow of seaborne trade continues to be smooth and efficient.” Furthermore, Section 2.9 of the Strategic Plan states, “The Integrated Technical Co-operation Programme (ITCP) is crucial for assisting developing countries to implement IMO instruments for safer and more secure shipping, enhanced environmental protection and facilitation of international maritime traffic. In addition, the ITCP makes a contribution to assisting developing countries to achieve relevant Millennium Development Goals (MDGs). The importance of the ITCP increases further with amendments to existing instruments and developing new ones. in which the particular needs of, and impact on, small states and least developed countries should be taken into account. There are concerns about IMO’s capacity to meet the historical and growing needs of developing countries for technical assistance and, in particular, about the long-term financial sustainability of the ITCP.” The challenge that faces the IMO is funding for these countries and the joint effort the U.S. trying to implement with these foreign entities.

This burden will have to fall on the U.S., particularly the agencies within DHS. There will have to be a determination of the cost/benefit analysis, and a determination of the source of dangerous shipments. At a minimum, it would cost any country millions of dollars to implement such a strategy. To operate additional personnel and security measures, funding will be the main concern. There are two ways in which the IURP can be implemented without placing 100% of the burden on a country. The first is to supply
the funding for these countries to hire the personnel and to purchase necessary equipment necessary to carry out the IURP. The second is to provide the military support and contractors to add to personnel.

The model for more secure ports lies with the help of vulnerable countries from which dangerous goods may be shipped; it is best to keep in mind that given the vast amount of shipments that come from all around the world, the DHS will be able to focus on shipments on a broader scale, giving attention to those shipments which have been deemed to be hazardous.

Recommendation Three: The DHS coordinates with other federal agencies involved with international security.

The DHS should build upon its relationship with DOD to increase foreign port security. The DOD seeks to prevent warfare by approaching a strategy with the idea that “The best way to achieve security is to prevent war when possible and to encourage peaceful change within the international system.” (National Defense Strategy, Department of Defense). DOD’s strategy is to build upon a broad base along with partners to establish long-term security. An example is that of the Afghanistan troop force working alongside Americans so they are better trained and equipped to defend a nation. The DOD also emphasizes the importance of strengthening the “resiliency of the international system to deal with conflict when it occurs. We must be prepared to deal with sudden disruptions, to help prevent them from escalating or endangering international security, and to find ways to bring them swiftly to a conclusion.” The IURP has the same ideals, to establish long term alliances in order to protect dangerous good from entering U.S. soil.
Conclusion

Michael Sheehan, former New York City Deputy Commissioner for Counterterrorism, suggested that whatever is going on in our seaports, “echoes the well-known problem in our airports. Just as commercial aviation is tightly managed while commercial contract air is full of holes, so too are our ports, containerized shipping [is] carefully scrutinized (most of the time) while the rest of our maritime traffic is given an all access pass.”

Immigration and Customs Enforcement, the Coast Guard, and Customs Border Patrol should designate roles to separate divisions who are solely responsible for running the operations of the IURP, thus creating fewer burdens on the Department as a whole. There must be movement to ensure the safety of our ports by logistically implementing the IURP on both security levels on as a business relationship level. Sheehan stated that he was shocked to learn while at the NYPD “how little of that was being done, and how business around our ports relevant to intelligence hadn’t significantly changed since 9/11.”

The IURP is an attempt to increase port security abroad in order to increase security at home, not only for the benefit for the U.S. but also for other countries as well. We cannot simply set goals and objectives and expect them to be followed by other nations. The IURP is a proactive approach to consistent security measures. The U.S. must take measures to ensure that more than just two percent of cargo is being inspected.
References


CHAPTER II

The United States Department of Homeland Security:

The International United Reliance Program from A Managerial Standpoint

Nature of the United States Department of Homeland Security

Eleven days after the September 11 attacks, President George W. Bush implemented the Office of Homeland Security. What once used to be 40 separate agencies in separate departments were combined by the Office of Homeland Security into the 22 agencies of the Department of Homeland Security.

In “A Brief Documentary History of the Department of Homeland Security,” President Bush addressed the nation and proposed the creation of a permanent Cabinet-level Department of Homeland Security to unite essential agencies charged with protecting the homeland. Outlined are four missions corresponding to four proposed divisions in the department. (See Figure 2.2)

2.2: Missions Corresponding to Four Proposed Divisions (Borja, 2008)

<table>
<thead>
<tr>
<th>Border and Transportation Security</th>
<th>Control the borders and prevent terrorists and explosives from entering the country.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Preparedness and Response</td>
<td>Work with state and local authorities to respond quickly and effectively to emergencies.</td>
</tr>
<tr>
<td>Chemical, Biological, Radiological, and Nuclear Countermeasures</td>
<td>Bring together the country’s best scientists to develop technologies that detect biological, chemical, and nuclear weapons to best protect citizens.</td>
</tr>
<tr>
<td>Information Analysis and Infrastructure</td>
<td>Review intelligence and law enforcement information from all agencies of government, and produce a single daily picture of threats against the homeland.</td>
</tr>
</tbody>
</table>
The nature of the DHS is extremely complex which requires the coordination, intelligence, and communications of twenty two agencies. The integration of the International United Reliance Program (IURP) in the DHS is one which must be done by all agencies. This strategy is designed to increase global security throughout international air and cargo ports in an attempt to prevent WMD and dangerous chemicals from entering U.S. ports; these often are unchecked, leaving our country vulnerable. Thus the IURP is not unique to one agency or organization. This strategy is one that the DHS will be able to use in conjunction with the PA, our military forces, and international security forces.

A Homeland Security Strategy and Key Management Principles

The International United Reliance Program (IURP) is a strategy that focuses on the implementation of broader global security through international ports. In recent years we have seen studies linked to terrorism and the lack of screening of U.S. ports. Particularly, the Port Authority of New York and New Jersey Strategic Plan has estimated a forecasted increase in demand for Port Authority Transportation from 2005 to 2020 of 100% for port cargo, and 70% for air cargo. The Port Authority (PA) has set priorities for measuring success in establishing proper accommodations for the increase. “Regional cost benefit analysis, along with other decision-making tools such as risk assessment, life-cycle asset management, and financial tests will allow the agency to pursue projects that meet six
primary organization goals.” They are: economic value, financial capacity, value to customers, stewardship, leadership, and organizational excellence (See Figure 2.1).

2.1: PA’s six primary goals (The Port Authority of New York & New Jersey Strategic Plan)

<table>
<thead>
<tr>
<th>primary goal</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>economic value</td>
<td>To maximize the region’s economic opportunities, productivity, and quality of life through investments in transportation</td>
</tr>
<tr>
<td>financial capacity</td>
<td>To create and maintain the financial capacity necessary to undertake the projects that will significantly benefit the economy of the region</td>
</tr>
<tr>
<td>value to customers</td>
<td>To significantly improve the customer’s daily experience with the region’s transportation network</td>
</tr>
<tr>
<td>stewardship</td>
<td>To protect and sustain our facilities for generations</td>
</tr>
<tr>
<td>leadership</td>
<td>To develop and implement the vision of this plan through partnerships with public and private entities</td>
</tr>
<tr>
<td>organizational excellence</td>
<td>To create an organization that excels in its objective of making optimal policy and investment decisions and implementing them effectively</td>
</tr>
</tbody>
</table>

All of the PA goals are related to security measures that DHS intends will keep weapons of mass destruction (WMD) and other dangerous chemicals from entering the U.S. without hindering international business relations. Global security without impacting international commerce presents a myriad of management difficulties the DHS may
encounter in implementing safer ports through the IURP. The IURP is a proposed strategy by which the U.S. will have face to face interactions with not only foreign government officials but also with their front line security forces. The U.S. will be doing more than just requesting help; the DHS will have established personal contact with those who are important in securing their own ports and preventing WMD and chemical being shipped to the U.S. They will use a wide spectrum of management models.

Where Issues Lie Prior to Implementing the IURP and How We Address Them

Currently, treaties between the United States and other countries rely on how well we develop the relationships to these countries in order to ensure that treaties are continually followed. The same can be said for the IURP. In order to ensure safer ports at home we have to ensure shipments from abroad are scanned and/or checked prior to their departure. Jeff Conklin, in Dialog Mapping, discusses “forces of fragmentation.” Forces of fragmentation “suggests a condition in which the people involved see themselves as more separate than united, and in which information and knowledge are chaotic and scattered.” He writes that the solution to this problem is to have a shared understanding with the same commitments. There are two types of fragmentations which may contribute to communication errors internationally. The first is wicked problems. Extremely common, these problems are usually inevitable in any work setting; they persist due to applying inappropriate methods and tools to solving these problems. If we do not understand problems that persist we cannot simply apply any method in attempt to solve these issues; the key is to first identify the problem and find the appropriate method which can be applied. The second is social complexity. Depending the number of parties, individuals and agencies involved, the more socially complex it is to
communicate with one another. For instance, if we are dealing with a security forces and foreign government agencies in the Middle East there is first a language barrier and second culture barrier (Conklin, 2005).

Dealing with complexities on an international level, the DHS will be to be prepared for seeing this fragmentation. In terms of implementing a strategy or method we also have to take into consideration another fragmentation, and that is technical complexity. Specifically, it “raises the risk of project failure, it is also the most well recognized fragmenting force. . . . Dialogue Mapping is [used] to provide an approach and set of tools for dealing with the nontechnical side of fragmentation” (Conklin, 2005). Dialogue Mapping is extremely important when dealing with the nontechnical complexities because it addresses the problem but allows a diverse group of people (in this case countries) to apply coherence around these problems. Coherence is defined as “shared meaning for key terms and concepts, that participants are clear about their role in the effort, that together they have shared understanding of the background for the project and what the issues are, and that they have a shared commitment to how the project will reach its objectives and achieve success” (Conklin, 2005).

Risk Management and Improving Strategic Managerial Thinking

The United States Government Accountability Office (GAO) testifies before the Subcommittee on Transportation Security and Infrastructure Protection, Homeland Security Committee, and House of Representatives. It addresses several issues regarding management and the assessment of implementing current and new strategies. We must
recognize that there is a risk assessment involved and the GAO is an example of how we need to implement strategies to secure United States ports.

We must implement certain managerial techniques which encourage partnerships across the board not only with agencies within the DHS but with foreign government agencies in countries which are vulnerable to terrorist activity. We have to address issues such as the importance of securing the ports on an international level to maintain a higher degree of security. Furthermore we must assess fiscal issues that come along with international relations.

Norman Rabkin, the Managing Director who testified before the subcommittee, addressed the integration of risk management principles into public sector operations. In this integration, Rabkin describes how “the Port Authority of New York and New Jersey developed and implemented a risk assessment program that guided the agency’s management in setting priorities for a 5-year, $500 million security capital investment program. This methodology has since been applied to over 30 transportation and port agencies across the country, and the Port Authority has moved from conducting individual risk assessments to implementing an ongoing program of risk management.” This is an example of fiscally managing risk with ports in the northeast and across the country. However the challenge still remains on how to integrate this strategy on an international level. Improving communication and partnerships abroad is a still a difficult task as it involved language and cultural barriers. With resources not readily available, this presents key challenges to implementing safety measures. “Technical issues such as the difficult but necessary task of analyzing threat, vulnerability, and the
consequences of a terrorist attack in order to assess and measure risk reduction; and partnership and coordination challenge” still remains a challenge for the DHS (Rabkin, 2008).

Key risk assessment and management can be learned from examples from the private sectors. Partnerships are important more than ever with the increase of terrorist activity. Naming representatives from agencies across the board as a committee can help in developing better coordination and partnership relations.

Rabkin addressed how participants surveyed on risk management felt that it was “fragmented within and across the federal government. . . government wide guidance should be developed.” A government policy which addresses all federal agencies is a sufficient way to reduce overlapping of management and conflicting views from individual agencies.

What Management Must Focus on Daily

There are several managerial principles for the IURP. First, management is dealing with an agency within the DHS, the PA, and private security forces. The question here is how do all these sectors of management work together to ensure employees are operating to their fullest potential without jeopardizing the effectiveness and security of our ports. One of the main issues the PA deals with is congestion. “Critical needs that affect the efficiency of maintaining and operating the system as well as the quality of service [are] efficiency, sound stewardship, and prudent fiscal management, but replacement requires a more intensive capital outlay in the immediate years and thus has been deferred” (The
Port Authority of New York & New Jersey Strategic Plan). They also address congestion and the hazards it may cause on international trade. Management must ensure that congestion does not hinder the IURP’s focus. Instead, we must use different managerial strategies to ensure that there no unnecessary setbacks during this coordination.

Daily managerial strategies which can be used throughout the DHS, the PA, and private sector security personnel can be compared to those listed in Strategy Under Uncertainty by Hugh Courtney, Jane Kirkland, and Patrick Viguerie. In this strategy the writers show how businesses are able to accurately predict future events by capturing a cash-flow analysis. Under this analysis there are four levels of uncertainty: 1) A clear enough future where managers use market research, competitor costs, value chain analysis to determine predictions, 2) Alternative futures which does not clearly make a prediction; however, it can establish probabilities in which outcomes may change based on a development of scenarios, 3) A range of futures where one scenario may lead to an outcome or another scenario, 4) True ambiguity for which managers record what they know in a scenario and what may be known about that scenario and thus arrive at different outcomes. However, when dealing with international countries, scenarios are not always predictable; we must always be ready for possible alternative outcomes and sudden disasters. However, implementing such strategies may increase the creativity levels allowing management to find factors to mitigate this disaster (Courtney, Kirkland, Viguerie, 1997).

The third strategy is most pertinent to the IURP. First, DHS managers among the involved agencies will have to involve employees to “identify the nature and extent of
residual certainties,” specifically, collecting intelligence, potential timelines for worst case scenario possibilities, and which country may be vulnerable to sending unchecked shipments to the U.S. Second, they must “choose a strategic posture” which would involve allowing security forces abroad and U.S. law enforcement officers to conduct security checks and verifications without hindering international commerce. Third, managers must “build a portfolio of actions.” If for any reason scenarios and outcomes of these scenarios are likely, then we must ensure that the right supplies and communication plans are in place so we are able to prevent or mitigate such scenarios. Finally, managers much “actively manage the strategy” by monitoring overseas communication and oversight of shipments departing for the U.S.; daily briefs to upper management are necessary in order to continually keep communication flowing, and employees must review daily memos to ensure they are aware of alerts (Courtney, Kirkland, Viguerie, 1997).

To communicate effectively under extreme circumstances it is important consider daily precautions to ensure measures are taken to address possible terrorist strikes. The dissemination of information among the DHS, the PA, private security enforcement, and through the IURP with other countries is an attempt to increase security and intelligence gathering.

In the event of a catastrophic event, management will have to mitigate the chaos using the information gathered from aforementioned strategies. For example, in the midst of a terrorist attack the DHS and other law enforcement agencies will be involved with first responders to keep ground zero in as much control as possible. However, this not the
only important factor; we also have to discover where these attacks were planned, how they were able to gather the material necessary to carry out an attack, and which individuals or extremist groups are involved. There will have to be step by step actions by the DHS to ensure that both air cargo and shipping ports are secure. The first step is to be in contact with the PA to ensure that all ports are on heightened security. The second is to ensure consistent communication with other countries abroad so that frequent and up to date information is disseminated. The third is to provide for security at these ports by sending Coast Guards and other law enforcement personnel to ports to secure the parameters and conduct immediate investigations into any suspicious activities.

William Pelfrey in the *Journal of Homeland Security and Emergency Management* wrote on The Cycle of Preparedness: Establishing a Framework for Terrorist Threats (2005). He identifies one of the major difficulties in preparing for a disaster is the analysis and assessments of an event that has not occurred yet or may never occur. In figure 2.3 Pelfrey models a strategic diagram in which the major elements of preparedness occurs as a cycle. This cycle is the process by which “agencies, organizations, jurisdictions, and the nation, can become central” (Pelfrey, 2005). This considers preparedness techniques for dealing with WMD’s and terrorist activities.

Figure 2.3: Major elements of the Cycle of Preparedness (Pelfrey, 2005)
Group Dynamics and Individualities of Personnel: Addressing Strengths and Weaknesses

In today’s fast paced society, the world has seen an increase of technology, communication, and population. The world has become much smaller due to technology and with that comes competing industries. Because employees are aware that they may be easily replaced, it is not unusual to find some feeling they are not contributing. Although bonuses are a motivating factor, aside from monetary rewards, there are other ways to motivate employees.

Stephen Robbins and Dave DeCenzo, authors of *Fundamentals of Management* (2008) discuss the concept behind employee recognition. Applying such concepts to government employees is important; managers must know in what area every employee is able to contribute, specifically, how to recognize these achievements and how to reward them. Robbins and DeCenzo developed the Big Five Model of Personality: extroversion, agreeableness, conscientiousness, emotional stability and openness to experience.

We must recognize that not everyone performs at the same caliber. How one may go about bringing results or a solution to a problem may not be the same way another person
may handle the situation. The way we perceive and go about handling a situation are
different depending on the situation and the person involved in solving the problem.
Robbins and DeCenzo write, “By recognizing that people approach problem solving,
decision making, and job interactions differently, a manager can better understand why,
for instance, an employee is uncomfortable with making quick decisions or why an
employee insists on gathering as much information as possible before addressing a
problem.” If we simply take the time to analyze one’s work performance, we will be able
to find a unique trait in each individual that can contribute to the success of an agency.

Disagreements or different perceptions of an individual could present issues in
management, turning it into a blame game. A manager would need to avoid that and
focus on the situation as a whole. Especially when dealing with government agencies
(specifically the DHS), we have to make fast decisions; problems will happen but will
have to be resolved quickly without hindering an investigation. Robbin’s fundamental
attribution error is that judgments can be easily made and may be seen as poor work
progress.

Recognition need not be monetary, but perhaps a quick office wide email on success on a
case or report. Management can encourage employees to work together on projects
which may have been successful in the past. It is best not to judge, but rather give
constructive criticism so an employee’s performance is better next time. A good way to
recognize one’s work is through governmental appraisals. Tracking an employee’s
record for the fiscal year is an effective way to acknowledge how each employee
contributed to specific duties and responsibilities.
Group problem solving versus individual problem solving is what some would consider a debate among agencies. From a management point of view, groups may be the dominant route. Dealing with the DHS, one can only imagine what type of tug of wars agencies encounter when dealing with a problem.

William Huitt, author of the article “Problem solving and decision making: Consideration of individual differences using the Myers-Briggs Type Indicator,” (1992) discusses the research on personality and cognitive styles that is particular to each individual’s problem solving approach. He writes “Most models of problem solving and decision making include at least four phases, 1) an Input phase in which a problem is perceived and an attempt is made to understand the situation or problem; 2) a Processing phase in which alternatives are generated and evaluated and a solution is selected; 3) an Output phase which includes planning for and implementing the solution; and 4) a Review phase in which the solution is evaluated and modifications are made, if necessary. Most researchers describe the problem-solving/decision-making process as beginning with the perception of a gap and ending with the implementation and evaluation of a solution to fill that gap.”

Huitt goes on to address how individual differences may have implications on group solving decisions. It is important to address these issues before allowing situations to get out of hand as a manager. Each employee must recognize the situation and act accordingly. “Individual differences in problem-solving and decision making must be considered to adequately understand the dynamics in problem solving and decision making. . . . Attention must be paid to both the problem-solving process and the specific
techniques associated with important personal characteristics” (Huitt, 1992). All this is very true, but when dealing with more than one agency, it would be hard to pay attention to each individual’s way of solving problems.

In times of disaster how do managers get employees to react under pressing situations? A manager in the DHS must know individual personality traits for managing and solving problems. If we have someone that’s an extrovert and someone who is perceptive and another who is intuitive, this can lead to better results. Each group working with different personalities can work together while bringing their individualities to the table.

It is up to management to understand personality clashes and dismantle any hostility during chaos. Just as in the private sector, project managers can be extremely beneficial in dividing up group solving issues to each individual. It is not fair for one to be perceived as having a better solution than the other as it may create some kind of undermining judgment towards the others, especially if managers keep picking those same individuals to solve a problem.

Every problem has a different solution. Every solution, however, should include a group effort. While one might outshine the other, it may be simply because that person’s way of coming up with a solution reflects their own personality trait. It’s different in every aspect, and a manager would not want to undermine anyone’s ability to reach a solution by making them work individually. A group effort may show what each individual can
bring to the table. Robbins lists five personality dimensions which influence a person’s ability to cope in a disastrous situation:

- Self-awareness: being aware of what you’re feeling.
- Self-management: the ability to manage your own emotions and impulses.
- Self—motivation: the ability to persist in the face of setbacks and failures.
- Empathy: the ability to sense how others are feeling.
- Social skills: the ability to handle the emotions of others.

These dimensions are defined as emotional intelligence which Robbins defines as “an assortment of noncognitive skills, capabilities, and competencies that influences a person’s ability to cope with environmental demands and pressures.” Recognizing these dimensions is to know how first responders and other employees react and cope with sudden chaos.

Insubordination and the Repercussions

Insubordination is a problem among all companies and agencies worldwide. Particularly within the DHS it is important to note that many agencies under one department may lead to several instances where insubordination may develop, a major one being employees of a particular agency not recognizing the managerial style of another. There is an ego factor which needs to be overcome and controlled. Individuals who display insubordination must face sanctions such as suspension and possibly termination. In a department such as the DHS, agencies cannot waste all managerial resources on insubordination while terrorism is at its peak since the U.S. was attacked in 2001. Strictness and zero tolerance for any employees who display such behavior is not
acceptable with DHS agencies and tough sanctions are to be implemented to deter employees from acting out against management and their colleagues.

Overall Managerial Aspects in Securing U.S. Ports

How do we guard our ports without jeopardizing international commerce? The answer is to develop international relations with foreign government agencies and implement the IURP to ensure what may not was scanned at the ports in the United States that they were in some way scanned before departing a foreign city. Verification of some sort whether it be a stamp, a barcode, or a computer generated recording system, could be a way to further secure our borders from retrieving WMD and other hazardous material.

To implement the IURP, the managerial integrations of international relations begins within the DHS. We must focus on working on the employees of the agencies and ensuring everyone is following the same agenda without concern. There must be an overall agreement among higher levels of authority throughout these agencies; to do this close monitoring of group efforts and communication between personnel and countries abroad will have to be scrutinized. There is no one checklist to figure out what will work the best, that is why we must focus on as many different aspects of risk assessment as possible to ensure utmost security and success for the IURP.
References


The Port Authority Strategic Plan: Transportation for Regional Prosperity. 2006.
CHAPTER III

The United States Department of Homeland Security:

A Strategic Plan to Protect Elements of the Infrastructure from Cyber Terrorism

Executive Summary:

One of the nation’s top priorities is the safety and stability of the United States’ infrastructure both at home and abroad. As technology advanced throughout the years, different components became more closely linked. Prior to technological advances, systems of our infrastructure were independent of one another with very little linkage. However, today’s operations, through advances in technology, have become interlinked through computer systems.

Critical infrastructures such as oil, telecommunication, gas, electricity, banking, nuclear plants, law enforcement and emergency services are at a high risk should there be a cyber-attack. The Cyberterrorism Defense Analysis Center (CDAC) states that “the threat of cyberterrorism to our technical infrastructure is real and immediate. Computers and servers in the United States are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency, and sophistication each year. As our nation’s critical infrastructure grows more reliant on information technologies, it also becomes more exposed to attackers, both foreign and domestic. These attacks can threaten our nation’s economy, public works, communication systems, and computer networks” (FEMA).

This report will analyze an element of the nation’s infrastructure vulnerable to the infiltration by terrorists via cyberspace and furthermore address the process in which we
can strategically minimize threats in industries threatened by cyber terrorism. The main focus for this report will be on a critical infrastructure of the banking and finance divisions. The oversight of such areas would typically fall under the watchful eye of the U.S. Department of Treasury. It is extremely crucial for this country and for others alike in securing and maintaining the economy around the world. Recently, we have seen white collar crimes alter the lives of thousands through attempts to defraud the American people and the government. For example, Bernie Madoff defrauded thousands across the world through the Ponzi scheme: he embezzled $65 billion over the course of 30 years.

The banking industry, the SEC, the FBI, and other government agencies were unable to discover this until a whistleblower testified before Congress. How can we deal with situations like this? Simply put, the government has developed regulations regarding the transparency of hedge funds and investment advisors. The same can be said for individuals attempting to infiltrate banking and government computer systems in an effort to fund terrorist activities.

Purpose:

This plan has been developed to counter the threats of terrorist groups to destroy elements of the infrastructure via the banking systems. One way in which terrorists attempt to infiltrate such areas is by money laundering, an action which is difficult to trace if not caught early. According to a February 2011 report by the Director of National Intelligence, “We continue to monitor the chemical, biological, radiological, and nuclear (CBRN) threat closely. Some terror groups remain interested in acquiring CBRN materials and threaten to use them. Poorly secured stocks of CBRN provide potential
source material for terror attacks” (Clapper, 2011). We will have to strengthen relationships with outside stakeholders both on a domestic and international level. Private sector entities responsible for protecting the areas of cyberspace and contracts with the United States Government will have to be improved.

Scope:

The scope of this coverage will be narrowed down to the United States banking infrastructure as it relates to countries which share the same financial firms and deal with everyday trades and commerce transaction. The United States, Europe and Asia play a crucial role in maintaining the global economy infrastructure. Should anything happen within the systems which are responsible for trades, shipments, and energy production, the world could be severely paralyzed. A slight oversight on a potential terrorist lead may result in terrorist funding which can lead to obtaining weapons that are detrimental to countries considered to be enemies. Most entities, both private and public sector, conduct business via computer technology. This plan is specifically produced to address the importance of saving our banking and finance infrastructure from cyberterrorism. We cannot afford to lose systems critical to maintaining the workings of the nation’s economy. An example of how we already protect our infrastructure abroad is through the Department of Defense (DOD), an entity which operates internationally. There is quite a bit of dependence on international military forces to help protect infrastructures abroad. “The resilience and reliability of supporting infrastructures throughout areas of military operations and DOD activities are crucial. Military commanders and defense sectors place a value on the growing interdependency of national, international, and
multinational infrastructures. Facilitating international cooperation and information are necessary to assure global critical infrastructures are available to DOD when required” (Department of Defense, OUSDP). By narrowing down the areas in which most transactions occur we will be able to apply mandates that will require stricter policies so that terrorists are unable to infiltrate one of the most important areas of sustaining our livelihood.

Mandates:

Several factors alter how the Department of Treasury operates. For example, “Several industry sectors considered to be critical infrastructures use industrial control systems in their daily activities. These industries could be significantly affected by a cyber-attack targeting industrial control systems such as supervisory control and data acquisition (SCADA) systems, distributed control systems, and others” (Shea, 2002).

Figure 1.1: Current organizational structure Department of Treasury: Office of Terrorism And Financial Intelligence (Treasury)
From reviewing the structure above and the restrictions that may be mandated through certain divisions, it appears as though SCADA systems are at risk because enforcement efforts solely by the United States may not be enough to foil an attempt to launder money to a terrorist organization. The Office of Intelligence is a critical element in enforcing secure banking measures. The Office of Intelligence and Analysis (OIA) “is a component of the U.S. Department of the Treasury’s Office of Terrorism and Financial Intelligence (TFI). TFI marshals the Department’s intelligence and enforcement functions with the twin aims of safeguarding the financial system against illicit use and combating rogue nations, terrorist facilitators, weapons of mass destruction (WMD) proliferators, money launderers, drug kingpins, and other national security threats” (Office of Intelligence and Analysis).

Current mandates from financial firms require reporting and disclosure pursuant to certain acts put in place after September 11th. One such act is the Financial Anti-Terrorism Act of 2001 which adheres to punishments and mandates through federal jurisdictions in at least four main components (House of Representatives, 2001):

1. Allow for Federal subpoenas for funds in bank accounts;
2. Jurisdictional rights over foreign money-laundering attempts through any type of foreign bank;
3. Anti-money laundering language entered upon retention agreements between a financial institution and a prospective client or investor;
4. If an individual or group is found to have engaged in illegal financial acts they are punished pursuant to the Act.

Mandates like the foregoing are beneficial for governments who are attempting to locate possible terrorists trying to fund their criminal acts through wire transfers and infiltration via financial firms and investments.

Stakeholder Analysis

Certain stakeholders in the banking area are numerous; however, we have to realize that because of mandates in the Act, they are required to have oversight with anti-money laundering rules. Stakeholders in the public sector include the following:

1. United States government;
2. Foreign governments who have entered into treaties with the United States regarding anti-money laundering rules and regulations.

Stakeholders in the private sector include the following:

All financial institutions including but not limited to: banking firms, hedge funds, investment advisors, and investment managers. In accordance with investment rules with off shore and on shore entities, they all add language to prospectus memoranda regarding the anti-money laundering rules; These stakeholders are critical in operating with the strategic goals and operations set forth in this report.
Vision Statement

Currently the Department of Treasury’s vision statement is as follows:

“The Department strives to achieve prosperity and stability in the U.S. and global economy currently and in the future. This fervent desire serves as the inspiration for the people of the Treasury Department, sets the direction for the organization, and provides the foundation for strategic planning” (Strategic Plan, 2010).

The new strategic plan being proposed in this report will continue the vision of the Department of Treasury’s current statement. However, in addition to the foregoing we will have to add how we intend to consistently apply efforts through newly negotiated agreements with countries and private stakeholders. Specifically the vision statement should include the following: “To increase efforts of the Financial Anti-Terrorism Act of 2001, we will sustain a foundation for maintaining most current agreements which adhere to newly implemented strategic goals.”

Mission Statement

The Department of Treasury’s mission statement is as follows:

“Maintain a strong economy and create economic and job opportunities by promoting conditions that enable economic growth and stability at home and abroad, strengthen national security by combating threats and protecting the integrity of the financial system, and manage the U.S. Government’s finances and resources effectively” (Strategic Plan, 2010). In order to create a strong economy and promote conditions to enable economic growth we must follow orders of the new strategic plan so that potential terrorist
infiltrations within our banking and commerce infrastructures do not subject the world’s economy to a complete downfall.

Internal and External Situational Analysis

The chart below indicates all the controls which may have an impact on how we implement our strategic planning process:

| INTERNAL STRENGTHS | • Excellent task force measures created  
|                    | • Internal management staff seems to be aware of the goals and new strategic assessments implemented since 2001  
|                    | • Department of Treasury is premiere force in securing the banking industry from elements of cyber terrorism |

| INTERNAL WEAKNESSES | • After review previous strategic plans, the Department of Treasury needs better relations seem to lack with agencies that may be of assistance when dealing with international relations (ie. State Department)  
|                    | • Lack of transparency from banking industries  
|                    | • Certain rules exempt banks and other financial institutions from reporting to the government possible red flags |

| EXTERNAL STRENGTHS | • Good relationships with other private sector stakeholders  
|                    | • Good relationships with other nations that are also interested in protecting their own banking infrastructure |

| EXTERNAL WEAKNESSES | • Different rules and regulations prevent certain measures to be
Identify the Strategic Issues

Strategically, an issue that arises from a situation analysis is that of inner managerial controls. In order to place strategic goals on an international basis, we ensure that all internal controls within the Department are rid of the internal weaknesses. There is little transparency amongst governments, and obtaining cooperation from reluctant countries can make it difficult for the United States to enforce its efforts to screening banking industries and protecting the infrastructure. Another strategic issue is that of the timeline. Previous strategic plans have not gone beyond five years, and given the advancement in technology we must prepare these plans so that we can apply them over a ten year plan. As administrations change we have to maintain the strategic plan or we may risk another change in a strategic plan; we need to be on the same page for at least a decade before we can start seeing results in the long term.
Performance Goals

To determine whether or not a performance goal has been successful will be measured by the outcomes. Below are four strategic performance goals and the anticipated outcome for each goal:

Figure 1.2 Performance Goals and Expected Outcomes

<table>
<thead>
<tr>
<th>STRATEGIC GOAL</th>
<th>EXPECTED OUTCOME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Annual auditing procedures specifically set for the oversight of governmental cyber security in charge of financial transactions between the United States and other countries (ie. Countries such in Europe &amp; Asia)</td>
<td>As a result of the oversight we will expect to see an increase of transparency of transactions that are conducted between countries that are prone to terrorist activity.</td>
</tr>
<tr>
<td>2) Combat national cyber threats by assigning private sector network security firms to monitor international financial firms</td>
<td>Without burdening the government in its entirety the outcome here is to leverage some of the assistance of network security to industries who have sophisticated resources to monitor financial transactions on an international basis.</td>
</tr>
<tr>
<td>3) Accountability for management and those in charge of implementing protective procedures</td>
<td>With this goal we will be able to filter out areas which are not obtaining additional security measures and thus save money on areas which have not been successful in assessing accountability among government bodies.</td>
</tr>
<tr>
<td>4) Ensure that international stakeholders are also taking precautions to ensure the safety of their own areas of network security which are vital to the</td>
<td>Annual training and meetings with private sector network security companies must be aware of international security measures and</td>
</tr>
</tbody>
</table>
Performance Indicator

Performance indicators utilized to measure the outcomes of the plan are audits and assessments by the Office of Inspector General and statistics compiled by stakeholders responsible for securing lines of financial transactions. Studies retrieved from countries in Europe and Asia will be used to compare risk assessments from previous years. Continual communication ties by the Treasury Department and financial sector firms both at home and abroad are the performance indicators through which we will be able to establish whether or not the strategic planning process is succeeding.

Strategy for Implementation

The strategy will be implemented by the United States Department of Treasury in conjunction with financial sector stakeholders both at home and abroad. For example, Goldman Sachs has an interest in foreign investments throughout the world. If we can encourage transparency through transactions which occur between countries that are most susceptible to terrorism, we can decrease the threat of extremists infiltrating these banking system and destroying some of the most important aspects of commerce. Also responsible for implementing such strategic operations are foreign governmental bodies. They must be held responsible for understanding how the banking and finance industry is critical to the infrastructure within the banking and finance industry. As reported in the
Fiscal Year 2010 Performance and Accountability Report, “Treasury served a leading role in establishing the Afghanistan Threat Finance Cell (ATFC) a Kabul-based task force charged with collection, analysis, and dissemination of intelligence to disrupt funding and support for the Taliban and other terrorist and insurgent networks in Afghanistan. It provides threat finance expertise to U.S. civilian and military leaders and assists Afghan authorities in investigations of insurgent finance, narcotics trafficking, and government corruption. Through this assistance, the ATFC has helped build the capacity of Afghan authorities to operate independently, a key U.S. policy goal in Afghanistan” (Performance and Accountability Report, 2010). The ultimate goal here is to eliminate cyber threats within the infrastructure of our banking and finance industry. There are several strategic factors implemented by the Department of Treasury to diminish such threats; however, these goals are not 100% preventative measures so we must keep an ongoing effort to deter criminal acts. Instead of a three to five year plan, this new strategic plan will aim to achieve results within a five to ten year time period. This will be implemented by OIA and private network security companies. All private stakeholders and foreign governmental agencies responsible for governing financial transactions will have to secure their connections for any funds going to and from the United States through foreign avenues.

Budget and Resources

The Department of Treasury has designed a strategy to promote better objectives. For FY 2012, Treasury’s new budget reflects a new plan coordinated by the government to seek better developed objectives. Specifically, “The Presidential Policy Directive on Global Development – the culmination of months of interagency research and debate –
concludes that we should ‘redouble our efforts to support, reform, and modernize multilateral development organizations most critical to our interests,’ and to that end, ‘renew our leadership in the multilateral development banks.’"

Figure 1.3 reflects the budget requests and appropriations by the Department:

<table>
<thead>
<tr>
<th></th>
<th>FY 2010 Approp.</th>
<th>FY 2011 CR Level</th>
<th>FY 2012 Request</th>
<th>FY 2012 Request Full Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Poverty Reduction and Economic Growth (MDBs)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>International Development Association (IDA)</td>
<td></td>
<td>1,262.5</td>
<td>1,358.5</td>
<td>1,358,500,000</td>
</tr>
<tr>
<td>Int’l Bank for Reconstruction and Development (IBRD)</td>
<td></td>
<td>117.4</td>
<td></td>
<td>117,364,344</td>
</tr>
<tr>
<td>Inter-American Development Bank (IDB and FSO)</td>
<td></td>
<td>102.0</td>
<td></td>
<td>102,018,035</td>
</tr>
<tr>
<td>Multilateral Investment Fund (MIF)</td>
<td></td>
<td>25.0</td>
<td>25.0</td>
<td>25,000,000</td>
</tr>
<tr>
<td>Inter-American Investment Corporation (IIC)</td>
<td></td>
<td>4.7</td>
<td>20.4</td>
<td>20,428,519</td>
</tr>
<tr>
<td>Asian Development Bank (AsDB)</td>
<td>0.0</td>
<td></td>
<td>106.6</td>
<td>106,585,848</td>
</tr>
<tr>
<td>Asian Development Fund (AsDF)</td>
<td>105.0</td>
<td>105.0</td>
<td>115.3</td>
<td>115,250,000</td>
</tr>
<tr>
<td>African Development Bank (AfDB)</td>
<td></td>
<td>32.4</td>
<td></td>
<td>32,417,720</td>
</tr>
</tbody>
</table>
Over $2 billion is necessary to implement the plan in developing countries as well as industrialized countries. Over the course of five years the strategic performance goals require a long term effort in hopes of increasing international oversight while risks are minimized.

Over a five to ten year plan, funds between $10 billion to $20 billion will be required. This number is based on estimated totals for 2010. An estimated $2 billion a year needed to apply to the development of other banks is easily doubled, with stricter security measures which require more personnel and contractor. Not only are we sustaining the security of other banking divisions countries but we have to ensure that commerce and other legitimate trades done through our banking systems do not negatively affect the nation’s economy.

Conclusion

As we entered the 21st century the entire world was rattled by the events of September 11th. The impact on the economy rippled beyond ground zero. Over the past nine and a half years terrorists have become more sophisticated and are now changing the way they attack countries they consider to be enemies. We must rely on these strategic efforts put in place to deter such activity. If we stop them in their tracks from every possible angle,
including the infiltration through our banking and commerce infrastructure, then we possibly may have foiled an attack that may have ended in utter destruction. If we want to prevent another September 11th then we must start from the very beginning; we must localize and attack the sources. Just as ground forces are eliminating terrorist cells in the Middle East, we must also continue to help eliminate them in cyberspace.
References

Clapper, J. Office of The Director of National Intelligence, (2011). Statement for the
record on the Worldwide Threat Assessment. Retrieved from
http://www.dni.gov

Department of Defense, The Office of The Under Secretary of Defense for Policy. (n.d.).

FEMA, Cyberterrorism Defense Analysis Center. (n.d.) Retrieved from
http://www.gpo.gov

Geightner, T. The Department of the Treasury, International Programs Justification of


The Department of The Treasury, (2010). Performance and accountability report


CHAPTER IV

The United States Department of Homeland Security:
Constitutional Issues Relating to Military Tribunals

Introduction:

Constitutional issues relating to the management and strategic planning of the International United Reliance Program (IURP) is difficult to analyze simply because it is an international development. Simply put the IURP deals with two main components, foreign security forces and the United States Coast Guard (USCG). The USCG is a branch of the U.S. Armed Forces and as result is governed by the Uniform Code of Military Justice (UCMJ).

Currently, treaties between the United States and other countries rely on how well we develop the relationships in order to ensure that treaties are continually followed. The same can be said for the IURP. In order to ensure safer ports at home we have to ensure shipments from abroad are scanned and/or checked prior to their departure. Jeff Conklin who wrote a chapter on Wicked Problems & Social Complexity discusses “forces of fragmentation.” Forces of fragmentation “suggests a condition in which the people involved see themselves as more separate than united, and in which information and knowledge are chaotic and scattered.” He writes that the solution to this problem is to have a shared understanding with the same commitments. There are elements which may contribute to communication errors internationally. Extremely common, these problems are usually inevitable in any work setting; they usually persist due to applying inappropriate methods and tools to solve these problems. If we do not understand
problems, we cannot simply apply any method in attempt to solve them; the key is to first identify the problem and find the appropriate method which can be applied. Depending on the individuals and agencies involved, it becomes much more socially complex to communicate. For instance, if we are dealing with a security forces and foreign government agencies in the Middle East there is a language barrier and a culture barrier (Conklin, 2005).

The Department of Homeland Security (DHS) will have to be prepared to deal with such elements. Implementing a strategy means that we have to also take into consideration the technical complexities, specifically, they “raise the risk of project failure; [they are] also the most well recognized fragmenting force. Dialogue Mapping provides an approach and set of tools for dealing with the nontechnical side of fragmentation” (Conklin, 2005). Dialogue Mapping is extremely important when dealing with the nontechnical complexities. It not only addresses the problems involved, but it also allows diverse countries to apply “coherency” to such complexities. Coherence is defined as “shared meaning for key terms and concepts, that [all] are clear about their roles in the effort, that together they have shared understanding of the background for the project and what the issues are, and that they have a shared commitment to how the project will reach its objectives and achieve success” (Conklin, 2005).

As we can see from the foregoing, we are able to analyze safety measures based on management and strategic methods and also analyze the military aspect when we detain criminals who are involved with terrorism and conspiracy. This legal analysis from a
military standpoint will provide for the issues surrounding the UCMJ and military tribunals. With the analysis of the UCMJ, we will also show how broad military authority contributes to issues involving military tribunals and the uses of interrogations.

The Uniform Code of Military Justice:

The UCMJ is a body of law which governs aspects of the military. Certain laws and procedures are put in place for military personnel. Due to unique circumstances the UCMJ exists because of the operations of the military and the international entities that these forces are dealing with; it covers not only at a domestic level but also aspects of detention of non-U.S. citizens. The purpose of this military code is to show how we operate with laws governing our military efforts abroad. Specifically, “Military law includes jurisdiction exercised by courts-martial and the jurisdiction exercised by commanders with respect to nonjudicial punishment. The purpose of military law is to promote justice, to assist in maintaining good order and discipline in the armed forces, to promote efficiency and effectiveness in the military establishment, and thereby to strengthen the national security of the United States” (Manual For Courts-Martial). The UCMJ’s purpose is to protect the rights of those detainees held during times of war and how procedures are implemented. The UCMJ also provides rules and regulations for military personnel. This includes cadets, reservists, active duty soldiers, and active duty retirees.

For example, the USCG is responsible for securing our borders in areas outside of the jurisdiction of customs enforcement. RAND suggests that a container arriving at a U.S.
port is subjected to several checks. “The 24-hour advanced manifest rule requires carriers to submit manifest information 24 hours before cargo is loaded onto a U.S. bound vessel. In this time, Customs Border Patrol performs a background check on the manifest, carrier and shipper to determine if the shipment poses a risk to the United States.” With the UCMJ in place, the USCG will have to implement the regulations set in place to enforce laws that are crucial to securing our borders.

Military Tribunal Overview

After September 11, 2001, President Bush implemented military tribunals for anyone who assisted in terrorist attacks against the United States. “One of the principal methods of legislative control over military trials, including tribunals, are the Articles of War that Congress enacts into law. The Constitution vests in Congress the power to ‘constitute tribunals inferior to the Supreme Court,’ to ‘make rules for the Government and Regulation of the land and naval Forces,’ and to ‘define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations.’ By enacting Articles of War, Congress defined not only the procedures but also the punishments to be applied to the field of military law” (Fisher).

Issues 1: Trials:

David Kellogg, author of “Jus Post Bellum: The Importance of War Crimes Trials” (2002) posts an interesting question regarding detainees: “Those captured al Qaeda fighters were certainly not innocent civilians. But neither were they legitimate soldiers. President Bush’s use of the term ‘unlawful combatants’ comes fairly close to an accurate description, but what does that tell us about how we are to treat them?” This is a fair
question. We need to take an in depth look at how we treat detainees who are not soldiers. Are they to be prosecuted in federal court or in a military tribunal. While the definition of a military tribunal seems clear, we have to note that these tribunals are significantly different from that of courts-martial because we are not trying individuals who are a part of the armed forces. The ability to have a fair trial during a military tribunal for detainees is questionable. First, charges are brought by military personnel and the jury contains members of the armed forces. This may indicate prejudice on the part of the jury. In fact, it can be simple to say that members on a jury may have a bias against an individual due to the nature of the allegations. This is an issue that poses a legitimate concern for how we can try individuals impartially. Since every aspect of a military tribunal is handled by military officials, and this includes the judges, jurors, and lawyers, we must question the impartiality against these detainees. There is a legitimate concern of whether or not they are receiving a fair and balanced trial and if the evidence used to convict a person of a war-crime is sufficient. Jennifer Elsea, legislative attorney, for the American Law Division questions the legitimacy of international law and the constitutionality of military tribunals in that, “tribunals could violate any rights the accused may have under the Constitution as well as their rights under international law, thereby undercutting the legitimacy of any verdicts rendered by the tribunals. The Administration initially responded that the M.O. provided only the minimum requirements for a full and fair trial, and that the Secretary of Defense intended to establish rules prescribing detailed procedural safeguards for tribunals established” (Elsea). This is an aspect of our culture that has evolved since September 11th and we are still evolving and re-analyzing the way we put alleged terrorists on trial.
**Issue 2: Treatment of Detainees Awaiting Trial:**

Prior to detaining individuals they must be deemed “enemy combatant.” The way in which they are ruled as enemy combatant is up to the discretion of the military. Once they are ruled as enemy combatants, they are placed in a detention center created specifically for suspect terrorists. Because of the Geneva Conventions, prisoners of war are to be treated humanely and torture is not permitted. “Measures that seek to eliminate (rather than merely circumscribe) detainees’ ability to bring constitutional challenges regarding the circumstances of their detention would likely be subject to serious legal challenge…it is clear that the procedural and substantive due process protections of the Constitution apply to all persons within the United States, regardless of their citizenship” (Garcia). However, this has not been the case for individuals kept in prisons such as Guantanamo Bay. There are detainees who have been held for several years without any charges. Marked as enemy combatants, these individuals were not brought to trial nor were they read their rights pursuant to the Geneva Conventions or the U.S. Constitution.

**Issue 3: Rights of Detainees**

Pursuant to military tribunals all detainees are allotted the rights of the U.S. Constitution. One serious concern that has been debated since September 11th are rights that detainees are given and whether or not detainees are notified of their rights. “Various constitutional provisions, most notably those arising from the Fifth and Sixth Amendments to the U.S. Constitution, apply to defendants throughout the process of criminal prosecutions” (Garcia). The right to plead the Fifth Amendment and the right to a speedy trial have clearly not been implemented for individuals awaiting trial.
However, an argument which has been brought up regarding enemy combatants subject to military tribunals is, “the application of these constitutional requirements might differ depending upon the forum in which charges are brought. The Fifth Amendment’s requirement that no person be held to answer for a capital or infamous crime unless on a presentment or indictment of a grand jury, and the Sixth Amendment’s requirements concerning trial by jury, have been found to be inapplicable to trials by military commissions or courts-martial.” (Garcia) There is a gap in regards to the Constitutional rights for individuals held in places like Guantanamo. Although clearly applied through legislation that Constitutional rights are allotted for all individuals detained in the United States and outside of the United States, there is a discrepancy on how these rights are applied for those who are considered to be enemy combatants and if whether or not they are subject to a military tribunal. Not only are they subject to longer detentions without being protected by the Sixth Amendment, they are not being charged for crimes alleged against these individuals. Furthermore, there has not been a process in which a determination has been made as to whether or not these individuals will be tried in a military tribunal or in federal court.

*Issue 4: Hearsay Rulings*

Regardless of what type of venue, every court has procedural rules set in place to provide for evidentiary rules. For example, in cases in which hearsay is permissible in court, there are standards that are substantially different from one another when it involves hearsay in trials involving terrorism. “In prosecutions alleging material support to terrorist organizations, evidence of statements by co-conspirators may be introduced against a defendant at trial even if those statements would not have qualified under a
hearsay exception. Before these statements may be admitted, it is necessary to establish that the conspiracy exists” (Garcia). Is this fair for the purposes of convicting a potential terrorist or co-conspirator? Hearsay brought into military tribunals under the under Military Commission Rules of Evidence are much more lenient and permissive in these courts. “While courts have yet to rule as to whether the Confrontation Clause’s protections against hearsay extend to noncitizens brought before military commissions held at Guantanamo, it would certainly appear to restrict the use of hearsay evidence in cases brought against detainees transferred to the United States” (Garcia). There is a lot of confusion involving the rights of individuals being held for terrorist acts inside the United States and outside of the United States (ie, Guantanamo). There are statements which may contradict or show inconsistency and interfere with the verdict for the individual on trial.

Issue 5: Geneva Conventions vs. Military Tribunal workings

The last four issues focused on specific matters concerning the treatment and rights of prisoners held during times of war. Particularly these were the rights of individuals subject to military tribunals. Matters which lead to the charges of individuals and how they are obtained come to question. The first subject which comes to mind is interrogation techniques used against individuals who are being held for allegations related to terrorism. Let us focus on an issue which has been a topic of controversy for many years: waterboarding. Is this seen as a violation of the Geneva Conventions? One assessment is that since no real physical harm is being done to the individual, this is not a form of torture. The same hold true for stress positions; we do not see any signs of physical torture so we believe these individuals are not being tortured; therefore this does
not violate the Geneva Conventions. The Bush Administration argued that Al Qaeda and similar organizations were not subject to the Geneva Conventions. Even in a CRS Report to Congress in 2008, “the Court held that such tribunals did not comply with the Uniform Code of Military Justice or the laws of war, including the Geneva Conventions” (Garcia). However, the aftermath of such a ruling led to many controversies surrounding the CIA’s and Department of Defense’s interrogation methods. This is a direct conflict about how we try these detainees. First, we do not know if the detainees are even subject to a military tribunal; second, when a decision on how they will be tried still remains undecided, they are treated as individuals who are deemed war criminals and therefore treated in a manner that does not comply with the Geneva Conventions. An example of how such techniques were abusive towards these detainees is seen in 2004. “Investigations related to the allegations at Abu Ghraib revealed that some of the techniques discussed for ‘unlawful combatants’ had come into use in Iraq, although none of the prisoners there was deemed to be an unlawful combatant” (Elsea). These types of acts have smeared images of our military forces across the globe. Abuse allegations by the military forces and the proof alike will be a matter of investigation if we fail to determine how we treat our prisoners.

Conclusion

As we transitioned from the workings of the USCG and the governing rules of the USMJ, this analysis showed how an Armed Forces member overseeing the waters of the United States (in addition to other military forces protecting our nation) can lead us into an area which will remain a controversial issue for many years. The United States and the UCMJ are in a difficult position, because we have to balance rules and regulations relating to the
rights of individuals and the crimes that they may have committed. Those held on
terrorism allegations inside the United States and those who are being held outside of the
United States will generate debate amongst all political parties. There are problems with
military tribunals in which the previous administration demonstrated that these are not
applicable under the Geneva Conventions. As a result of such rulings, we have seen
numerous counts of abuse in Abu Ghraib and detainees being held for years without a
single charge or determination of whether or not they will be tried in federal court or a
military tribunal. The U.S. Constitution does not apply to terrorists because of the nature
of the acts they have committed. These are not crimes suitable for civilian courts and
should be tried in a court specific to the crimes committed against our country.
References


CHAPTER V
The USA PATRIOT Act vs. Human Rights

Is the United States Infringing Upon Human Rights?

Since the tragic events of September 11th took place in 2001, we have seen a significant increase in law enforcement activities. Particularly, we saw the creation of The Department of Homeland Security (DHS) which placed twenty two federal agencies under one department to ensure coordination of counterintelligence reports. Along with the creation of the DHS we also saw the creation of the USAPATRIOTACT (Act). Signed into law by then President H.W. Bush on October 26, 2001, the USAPATRIOTACT stands for: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.

John Podesta, author of *USA PATRIOT Act: The Good, the Bad, and the Sunset*, has stated that the Act’s purpose is “to expand surveillance powers to track terrorists; all residents, not just the terrorists, are affected. . . . There are several common sense changes that could be made to the new law that would provide better protections for civil liberties without sacrificing security. Because of the rapidity with which the law was enacted, Congress, wisely included a four-year sunset of many of the provisions of the new Act. That sunset will allow Congress to make some needed adjustments, hopefully in a calmer climate, and strengthen the protections for civil liberties without sacrificing security.” This view is shared among many individuals who have attempted to change this legislation or to have it dropped by any means. The American Civil Liberties Union
(ACLU) is an advocate of human rights and the Act is one that this group feels is an infringement upon not only the civil liberties of U.S. citizens but also threatens how we view human rights laws as whole. President Obama had signed an extension of the PATRIOT Act in February 2010.

Since inception of the Act, this new law has created much controversy over the years with respect to civil rights and whether or not this violates human rights as a whole. In order to understand the controversy we must first have a good understanding of the Act, how it is applied, and finally whether or not we can conclude if this infringes upon human rights of not only the citizens of the U.S. but also those who live abroad.

On October 26, 2001 former President George H.W. Bush remarked after signing the Act, “This bill was carefully drafted and considered. Led by the members of Congress on this stage, and those seated in the audience, it was crafted with skill and care, determination and a spirit of bipartisanship for which the entire nation is grateful. This bill met with an overwhelming agreement in Congress, because it upholds and respects the civil liberties guaranteed by our Constitution” (Reclaiming Patriotism, 2009). This statement is controversial for some believe that the Act in fact does not uphold the civil liberties granted by our Constitution.
Provisions within the Act that make this law controversial have led some to believe that not only does it infringe upon human and civil rights of our country’s citizens, but also that the Act may not have had a major impact on how we counter terrorism. The issue is not whether or not this infringes up on the rights of would be terrorists, but rather of U.S. citizens. The purpose of this analysis is to provide a background and a response as to why the Act does not infringe upon human rights or the civil liberties of our citizens.

Every country defines human rights and civil liberties (used interchangeably and labeled as “civil liberties” hereafter) differently. The way the United States defines civil liberties is drafted within the Constitution. However, since the Constitution is a living document, one can safely assume that that the definition is constantly changing. When the Constitution was drafted, it was during a time when the population was small, religion was one, and politics were new. Forward 224 years later and we find that globalization has created a massive melting pot in America. Because of this we have seen the evolving of the Constitution. The Second Amendment which states that an individual has the right to bear arms was a very lenient stipulation when it was created compared to now when licenses and strict regulations have been enforced. The idea that the American government must do everything possible to protect this country can be agreed upon by many Americans; however some Americans do not want their privacy violated in any way. One could even say that the Act interferes with human rights. The Act lists five factors to pursue in order to counter terrorism: 1) improve sharing of information between law enforcement and foreign intelligence agencies; 2) gather antiterrorism intelligence by taking advantage of the flexible warrants requirement of the Foreign
Intelligence Surveillance Act (FISA); 3) expand wiretap authority over electronic communications; 4) seize funding utilized in terrorist activities; and 5) impose mandatory detention and deportation of non-U.S. citizens who are suspected of having links to terrorist organization (Banks, 2004). An analysis of these five elements will dictate how the Act can provide for the safety and security of human rights rather than have a negative impact on human rights.

Improve Sharing of Information between Law Enforcement and Foreign Intelligence Agencies

Since inception of the DHS twenty two federal agencies have been granted the power to share intelligence information for the sake of protecting the borders and infrastructure of the United States. Section 203 of the Act contains provisions in which intelligence sharing and grand jury material can be shared among agencies in order to better facilitate counterterrorism efforts. Specifically, Section 203 provides for the following:

“Procedures.—The Attorney General shall establish procedures for the disclosure of information pursuant to section 2517(6) and Rule 6(e)(3)(C)(i)(V) of the 19 Federal Rules of Criminal Procedure that identifies a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 22 1801)). Foreign Intelligence information.— (1) in general.—Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any federal law enforcement, intelligence, protective, immigration, national defense, or national security
official in order to assist the official receiving that information in the performance of his official duties. Any federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person’s official duties subject to any limitations on the unauthorized disclosure of such information. (2) Definition.—In this subsection, the term “‘foreign intelligence information’” means— (A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against— (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power.”

Information is vital so that various government agencies are able to protect human rights. We cannot simply deny the fact that this not been vital in foiling potential terrorist attacks. There has been very little concern as to whether these agencies serve little purpose to protecting the life and liberties of an individual. Organizations opposed to the Act fail to recognize that this Act contains provisions that attempt to coordinate efforts so that intelligence is more streamlined and efficient.

Gather Antiterrorism Intelligence by Taking Advantage of the Flexible Warrants Requirement of the Foreign Intelligence Surveillance Act (FISA)

In Title II of the Act, there are several sections which provide for exceptions on how this country can allow for the facilitation of information gathering via wiretaps and other communication surveillance. FISA was enacted in 1978 which gave government oversight of foreign activities. Opponents of the Act consider this a vital piece of the Act
which violates human rights and the civil liberties of those who wish to keep their privacy. However, FISA is an act which does not affect the human rights of U.S. citizens. Although FISA has extremely lenient exceptions for obtaining a warrant, this is one part of the Act in which we do not see a violation of human rights.

FISA is crucial in obtaining certain information on individuals who may be involved with terrorist activities, espionage, and foreign governmental activities leading up to a potentially detrimental situation. While most believe that their phones may be tapped, the fact is, unless the government has reason to believe that an individual has ties to potential terror threats, the chances of being wiretapped by the government is not as significant as it may seem. Foreign intelligence gathering is a crucial part of the Act through which we can operate under a wide discretion of authority. Section 214 of Title II of the Act does pertain to outside foreign terror suspects based on certain elements of reasonable doubt. In order to investigate organizations or persons that are foreign nationals, the U.S. Government must specify certain elements that warrant such investigations under FISA and must certify that “the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” Furthermore such investigations must specify the identity, if known, of the person who is the subject of the investigation and the identity, if known, of the person to whom is
leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.

Other sections in Title II of the Act describe warrants placed under FISA. Still others such as 223 involve civil action suits against the United States which may be filed by a victim when there have been unauthorized disclosures. Specifically, the Act provides for the implementation of Title 18 of the USC 2520: “Administrative discipline.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.”

One can assert here that wide discretion is not limitless for the government. The U.S. must observe certain boundaries in order to proceed with investigations into foreign intelligence interests, because that may also have an impact on a national level. Civil rights in this case are not fully dismissed. Individuals are allotted the right to sue the
United States if in fact they discover the investigation into them was unjust. Civil liberties remain at bay as described in Title II of the Act.

Expand Wiretap Authority over Electronic Communications

The use of electronic wiretaps by the government has been one of the main criticisms of the Act. Americans today are concerned with having their liberties stripped away by the fact that the government is allowed to tap into their conversations or emails or internet searches. Under Title II Section 225 of the Act, FISA has placed immunity for compliance with FISA wiretap. As such, Section 225 specifically states: “No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act.” By that definition, it can be easily inferred that there is immunity for anyone who gives any information pertaining to certain interests in individuals the government may have. Although true, some do not recognize that Title 18 still applies in this situation. Because of Title 18, we acknowledge the fact that probable cause still remains in effect and authorities, though given wider discretion, must be able to provide ample information to higher court officials that the investigations into certain individuals warrant possible terrorist ties. Again, the FISA we enacted in 1978 and thereafter empowers government officials who have been applying the FISA these past three decades. Having considered what has been conducted in the past prior to the Act, it can be argues there was a discreet PATRIOT Act already in place.
Seize Funding Utilized in Terrorist Activities

This is one of the lesser constraints of the Act that does not infringe upon human rights.

We recognize that major terrorist organizations are operating because of the funding they receive from various “legal” organizations. Title III of the Act has almost fifty sections which explain the implications for anti-money laundering laws and other acts such as Bank Secrecy Act. Title III involves not only government law enforcement agencies, but also private sector banking industries who are required to report certain suspicious activities. For example, if an individual deposits over $10,000 in his or her bank account, the bank will automatically file a suspicious activity report which is reported to the government. Should this person’s name appear on one of these reports, the government can go in and investigate whether or not these funds are for legal purposes and track where this money may lead. What may be a concern to individuals who feel that their rights are being violated is that every single banking activity they are involved with is being monitored by the government. However, there are sections of Title III of the Act which outline suspicious activities which will then lead to the interest of the government (not the other way around).

To randomly suspect individuals that could be involved with illegal activities would be very inefficient, so Title III lays out certain provisions under law that both public and private sector entities must adhere to; Sections 311, 312, 313, 314, 315, 316, 217, 318, 319, 320, 321, 322, 323, 324, 325, 327, 330, and Subtitle B under the Bank Secrecy Act entail amendments pursuant to the Act which detail and outline who may be investigated, how private sector entities are to be involved, what recommendations for criminal
penalties shall be, and most importantly, to what extent the government has jurisdiction. Individuals who fear that their banking records are being tracked by the government must recognize that they will not be targeted persons of interest unless, again, the government receives information based upon certain activity reports or if for any reason the person’s name is related to a terrorist organization. Civil rights are not a factor here since government oversight on money laundering schemes is also investigated with persons that are involved in organized crime or other criminal elements. Simply put, just because these clauses are inserted into the Act does not mean that they are designed specifically for “spying” on individuals. These sections have been in place for many years and have been included with the Act as a means to cover the grounds of terrorist activities. There is no reason to believe a person is being monitored by the government unless that person is involved with illegal activities.

Impose Mandatory Detention and Deportation of Non-U. S. Citizens Who Are Suspected of Having Links to Terrorist Organizations

Protecting our borders from individuals who are deemed dangerous to the safety and security of the United States is vital. However, how do we deal with individuals that are a threat to this country that are already living within the borders of the United States? Organizations such as the ACLU could argue that targeting individuals with names related to those that are deemed persons of interest could be infringing upon their civil rights. An article entitled, “Reclaiming Patriotism: A Call to Reconsider the Patriot Act,” drafted by the ACLU, addresses the implications for certain individuals who are suspected of providing material support to terrorist organizations.
Specifically, the ACLU suggests that “Such unjust and counter-productive consequences are a direct result of the overbroad and unconstitutionally vague definition of material support in the statute. The First Amendment protects an individual’s right to join or support political organizations and to associate with others in order to pursue common goals. The framers understood that protecting speech and assembly were essential to the creation and functioning of a vibrant democracy. As a result, the government cannot punish mere membership in or political association with disfavored groups – even those that engage in both lawful and unlawful activity – without the strictest safeguards” (Reclaiming patriotism, 2009) The argument here suggests that the U.S. will impose criminal charges on anyone that is merely “suspected” of providing material support to terrorist organizations. However, the Department of Justice cannot simply deport a non-U.S. citizen based merely on suspicion. The ACLU also claims that the individuals who support a political organization are fully within their rights to do so and are protected by the First Amendment. However, it seems that the ACLU’s argument is vague itself. The government should not allow individuals who are suspected of supporting terrorist organizations to continue to do so; the First Amendment does not protect those who express their freedoms in a manner which advocates violence.

Section 405 of the Act provides for the following: “The Attorney General, in consultation with the appropriate heads of other federal agencies, including the Secretary of State, Secretary of the Treasury, and the Secretary of Transportation, shall report to Congress on the feasibility of enhancing the Integrated Automated Fingerprint Identification System (IAFIS) of the Federal Bureau of Investigation and other identification systems in
order to better identify a person who holds a foreign passport or a visa and may be wanted in connection with a criminal investigation in the United States or abroad, before the issuance of a visa to that person or the entry or exit from the United States by that person."

In furtherance of this provision Subtitle B of Section 405 discusses the enhancements to immigration provisions. For example, Section 212 (a)(3) of the Immigration and Nationality Act amended a clause regarding a representative of a foreign terrorist organization. Section 405 of the Act states that “This clause specifically identifies individuals of interest who are attempting to cause harm against individuals of the United States.” Many rights are supported by the First Amendment; however, funding a terrorist organization should not be tolerated. Terrorist organizations attempt to strip away the rights that individuals are entitled to; we cannot simply argue the fact that denying an individual the right to support a terrorist organization either directly or indirectly is in violation of their civil liberties. The deportation of non-U.S. citizens is a vital position that the Department of Justice takes in order to protect the civil liberties of this nation.

Human rights and the civil liberties we are all entitled to should never be stripped away. The rights afforded to individuals in this country and around the world need to be protected, and the development of the PATRIOT Act helps in furthering that protection.
References


CHAPTER VI

The Shipping Ports of New York and New Jersey: Analyzing Strategies to Secure Maritime Assets and the United States

Technology, Cyber-threats and Maritime Critical Infrastructure

Executive Summary

The critical infrastructure of maritime security has changed over the years. Cyber-security has advanced in both the private and public sectors across the world. The purpose of this paper is to analyze maritime security and the cyber-threats facing today’s network of shipping ports and vessels. An analysis including critical nodes, budget restraints, cyber terrorist attacks, human error, and natural disasters is necessary in order to implement better maritime security that could have an impact on our critical infrastructures as well as global infrastructures.

Introduction

With the advancement of technology, the critical infrastructure within the United States has had to develop new strategies to accommodate threats that were not considered a security risk a decade earlier. However, the United States must also consider technological threats to infrastructure at sea. Maritime activity and ports on land are vulnerable to cyber-threats on a global scale. Terrorist attacks, natural disasters, and cyber-threats are just some of the main concerns that need to be considered when developing safeguards to technological components.
September 11th is an example of how the maritime infrastructure gravely impacts the economy, the airlines, and the buildings which were hit by the planes. The amount of physical damage caused by this tragic terrorist attack is nothing compared to the thousands of lives lost on that day; in addition, we have lost thousands more battling on the front lines in the Middle East to gain control of our security against terrorist threats for over a decade.

The European Network and Information Security Agency (ENISA) has done a similar analysis of security aspects of their maritime operations. In November 2011, a report drafted by ENISA concluded in an analysis that “a key characteristic identified is that a general insufficient focus on cyber security within the maritime sector exists. As a direct consequence, the overall sectorial capabilities to consistently assess and deal with cyber security challenges, are inherently reduced. One root cause of this situation is linked to insufficient awareness of the key stakeholders involved (e.g. governments, port authorities, shipping companies, telecommunication providers etc.) on the security challenges, vulnerabilities and threats specific to this sector” (ENISA, 2011). These threats correlate similarly with threats that are present within the United States. ENISA’s report on maritime security is an excellent referencing tool for the United States government to battle against cyber-threats from terrorists within the maritime infrastructure.

In this report, there will be an analysis and then a final recommendation as to how maritime security should be advanced so we can maintain proper security measures
towards our maritime critical infrastructure. The analysis of the following components is key to understanding the maritime infrastructure:

- Critical nodes and the links to maritime security identified through a network analysis
- Identifying both direct and indirect dependencies among the Department of Homeland Security (DHS) and U.S. Coast Guard, and characterizing how damage can spread across multiple infrastructures and threats specific to maritime security
- Defining and applying the method of analysis which combines the following: fault tree, event analysis, and the Model Base Vulnerability Analysis (MBVA)
- Recommendation as to which risk allocation strategy would be best suited for maritime security and the Port Security Grand Program investment strategy
- Analyzing Supervisory Control and Data Acquisition (SCADA) and identifying the threats and vulnerabilities
- Analyzing the impact of the internet on maritime security, and how safeguards become vulnerable to threats
- Assessment of the maritime security and a prediction for 2012 and beyond

As briefly noted, maritime security is responsible for carrying out certain strategies to help lessen the risk of cyber-attacks as well as terrorist attacks against shipping vessels. The surge of Somali pirates is an example of how vital it is to strategically control and
change our assessments based on current existing threats towards not only international
government organizations but also those being taken hostage.

Section One: Critical Nodes and the Links To Maritime Security Identified Through a
Network Analysis

There are several factors that become pertinent to maritime security: critical nodes;
physical or technological items that are important parts of how an entire operation
conducts business. There are several nodes, one of which is seaports. Seaports are
critical to the global supply chain. They are important in supporting a global economic
structure which allows for resources to be insourced or outsourced to other countries.

An attack on these seaports would not only be detrimental to the economy of the United
States but also to those who trade with the United States. Other critical nodes include:
 petroleum storage facilities, railroad lines, U.S. cities, and neighborhoods which lie just a
short distance from these seaports. Should a U.S. seaport succumb to an attack, it would
likely impact all the other critical nodes in its surrounding areas and possibly inflict a
high number of casualties within those areas.

According to a review, Managing Critical Infrastructure Risks, seaports, “make a huge
contribution to the U.S. economy by facilitating trade and tourism, providing jobs, and
supplementing energy needs. U.S. seaports handle 95% of overseas trade by weight and
75% by value” (Linkov, 2007). Furthermore, they estimate that the “economic impact[s]
of a major terrorist attack at a U.S. seaport vary. Earlier studies predicted that port
closing could cost the economy as much as $1 trillion.” So considering the vital areas around these seaports, any damage inflicted upon the maritime critical nodes could be debilitating to our nation’s economy and human life.

Section Two: Identifying Both Direct and Indirect Dependencies Among the Department of Homeland Security (DHS) and U.S. Coast Guard, and the Spread of Damage Across Multiple Critical Infrastructures

As previously mentioned, closing a single port due to a disaster could cost the nation up to $1 trillion in damages. Such a hit could make this economy head towards a deep recession, if not a depression. The Port of New York and New Jersey is an example of how it can be extremely detrimental to not only the safety and security of our homeland but as well as to the global economy. Direct dependencies include the reliance on other countries to maintain their security roles, ensuring that each container does not have weapons of mass destruction, drugs, or biological weapons. Pre-screening thousands of cargo shipments a day is extremely difficult for the DHS to oversee. As a result, the U.S. Coast Guard, Customs Border Patrol, and local law enforcement agencies also have a direct impact in securing our nation’s critical nodes.

Indirect dependencies include the use of technology from business to interact with the DHS and its agencies and are willing to disclose what is contained within these cargo shipments. Cooperation from outside resources, particularly the private sector, can help maintain inventory as to what is expected from outside cargo. Bills of lading are vital tools in completing this task. In order to prevent the spread of damage across multiple critical infrastructures, we have to maintain a strong support system among multiple
agencies. From the Drug Enforcement Agency, to the Customs Border Patrol, the U.S. Coast Guard, and international organizations, all have a vital role in protecting each of their jurisdictions so that we do not cause harm to the global economy. The Marine Transportation System (MTS) guides interdependent roles and defines how Critical Infrastructure and Key Roles (CI/KR) are critical to these interdependencies.

Particularly, “The CI/KR within the maritime sector constitutes a vital part of the complex systems necessary for public well-being, as well as economic and national security. They are essential for the free movement of passengers and goods throughout the world. Some physical and cyber assets, as well as associated infrastructure, also function as defense critical infrastructure; their availability must be constantly assured for national security operations worldwide. Just-in-time methods, utilized within industries, must be considered for their implications on risk and vulnerability. Beyond the immediate casualties, the consequences of an incident on one node of maritime critical infrastructure may include disruption of entire systems, cause congestion and limit capacity for product delivery, cause significant damage to the economy, or create an inability to project military force. Protecting maritime infrastructure networks must address individual elements, as well as intermodal aspects and their interdependencies positioned both within a regulatory environment, and a system of systems” (Transportation Sector-Specific, Sec. 5).

The Transportation Sector-Specific Plan for the Maritime Model Implementation Plan indicates that communication with outside stakeholders is important to sustaining other critical infrastructures such as the economy, travel, banking and finance industries.
“Maritime model stakeholders are formalizing new coordination processes using the Sector Partnership Model espoused in the National Infrastructure Protection Plan (NIPP). The Maritime Model Government Coordinating Council (MMGCC) has [been] formed.” (Transportation Sector-Specific, Sec. 5). The development of these councils and securing partnerships is a vital example of how we can control certain interdependencies by using advisor councils to speak on these agencies’ behalf. It is useful to have multiple areas that control one sector of a critical infrastructure. In this case, councils are utilized to correspond with interdependent entities while the agencies themselves are responsible for implementing the security measures.

Section Three: Defining and Applying the Method of Analysis which Combines the Following: Fault Tree, Event Analysis, and the Model Based Vulnerability Analysis (MBVA)

Before we begin to combine these analyses let us briefly differentiate each analysis:

*Fault Tree Analysis (FTA):* This is a top-down model in which the system is used to analyze the probability of function failure of a security measure that is in place.

*Event Analysis (EA):* This is a statistical analysis which determines whether the combination of two or more departments will be a successful merge or a failed merge.

*MBVA:* This is a “comprehensive method of analysis that combines network, fault, event, and risk analysis into a single methodology for quantitatively analyzing a sector component such as a hub. In MBVA, hubs are identified, hub vulnerabilities are organized and quantified using a fault tree, all possible events are organized as an event tree, and then an optimal investment strategy is computed that minimizes risk. MBVA
gives the policy analyst a top-to-bottom tool for achieving critical infrastructure protection under budgetary constraints” (Lewis, 2006).

In a metropolis like New York, ports require many strategic plans because of the unique placement and the populations which surround these ports. The most popular methodology that relates to the shipping ports and maritime security is through the FTA. With maritime security, there are many identifiable hazards that can be represented by the FTA. For example, a mathematical model can compare the past accident data so we can identify which factors have influenced these incidents the most. We can then use the FTA to predict future incidents.

In cyber terrorism attacks we have to predict the probability of attacks. In order to do that we will use the FTA, the best fitted model, in order to determine that risk. For instance, if we see that cyber-attacks have increased in the last five years and that of five hundred incident reports only forty were successful we can use logic to determine how technology has advanced and if the maritime infrastructure has been updating their security software programs. If programs have not been updated since the last attack, then it can be safe to assume that future attacks will happen. However, if it is found that cyber security has been increased, then we can use the probability that if attacks have been occurring at the same rate with the same mechanisms, then the stronger security programs could lessen the chances of a threat to the maritime security programs. The FTA is the model that best fits for this critical infrastructure.
Section Four: Recommendation as to which Risk Allocation Strategy Would Be Best Suited for Maritime Security and the Port Security Grand Program (PSGP)

A report titled “Maritime and Terrorism: Risk and Liability” was produced by the RAND Center for Terrorism Risk Management Policy. RAND researchers discuss the likelihood of terrorists striking maritime activities. There is potential impact on life, economy, and leaves much room for civil liability against the United States government. RAND’s risk assessment primarily involves risks associated with attacks on passenger and container shipping and originated “from a broad assessment of related threats and vulnerabilities, based on a combination of historical data regarding previous attacks, and on a series of interviews with counterterrorism experts. [They] then investigated the likely consequences that would follow from different modes of attack, drawing on historical data and publicly available analyses, and by framing those consequences in terms of human effects (e.g., casualties), economic effects (e.g., property damage and business disruption), and intangible effects (e.g., political and governmental responses). Finally, [they] combined the information on threat, vulnerability, and consequences to generate estimates of relative risk, in connection with attack scenarios involving ferries, cruise ships, and container shipping. [The] qualitative method for generating these risk estimates involved the use of defined ordinal scales to assess terrorists’ intents and capabilities, target vulnerabilities, and attack consequences” (RAND, 2006).

 Particularly with shipping ports, risks are not easily recognizable due to the fact they can vary from explosives, to natural disasters, to human errors. In this case, a policy maker
determines allocation of budget to threat countermeasures. As strategy to use for the shipping port example (NY/NJ), the apportion risk reduction method would be ideal for the following reasons:

- Easy to implement
- Incorporates political issues
- Corporate/organizational structure
- Time line - schedule constraints
- How efficiently budgets can be utilized

The DHS U.S. Coast Guard Congressional Justification for FY 2011 identifies savings associated with targeted management and technology efficiencies and consolidation initiatives. Specifically, “The Coast Guard will continue to leverage available efficiencies to maximize service delivery and provide the nation with the highest possible return on investment. Proposed efficiency highlights include small boat logistics management improvements, contract insourcing, headquarters management efficiencies, and the consolidation of intelligence fusion centers under a single operational command.”

The budget includes reallocation of “Maritime Safety and Security Teams (MSSTs), and realignment of existing rotary wing (i.e., helicopter) capacity to the Great Lakes region. For example, the Coast Guard will decommission four HECs and four HU-25 Falcons in FY 2011. Additionally, the Coast Guard will implement a regionalized MSST operational construct” (Department of Homeland Security: US Coast Guard, 2011). The MSSTs will be decreased from twelve to seven teams in which resources will be apportioned to higher commanding officials in order to address ports that are at the highest risks.
The risk reduction method could be readily used for the NY/NJ shipping ports simply because of dense population and the amount of critical infrastructure that surrounds these ports. We have to recognize the developments of other CI/KR in order to assess whether budgetary constraints will either help maritime security or whether will deter agencies and stakeholders from continuing and advancing security measures. In this case, it allows for the reallocation of assets to other agencies so they can utilize those funds to assist in securing ports.

Along with these risk assessments come investment strategies. One particular investment strategy comes from the DHS Federal Emergency Management Agency (FEMA). It is known as the Port Security Grand Program (PSGP) and it provides funding for transportation infrastructure security which includes maritime port authorities. This investment strategy supports wide risk management, creates better training programs, expands recovery capabilities, and assists in deterring attacks involving explosives and cyber-attacks. “The PSGP implements objectives addressed in a series of post-9/11 laws, strategy documents, plans, Executive Orders (EOs) and Homeland Security Presidential Directives (HSPDs). Of particular significance are the National Preparedness Guidelines and its associated work products, including the National Infrastructure Protection Plan (NIPP) and its sector-specific plans. The National Preparedness Guidelines provide an all-hazards vision regarding the nation’s four core preparedness objectives: prevent, protect, respond to, and recover from terrorist attacks and catastrophic natural disasters. In addition, Presidential Policy Directive/PPD-8 is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose
the greatest risk to the security of the nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters. At the regional port level, Area Maritime Security Plans (AMSPs), Port-Wide Risk Mitigation Plans (PRMPs), Facility Security Plans (FSPs), and analytical products such as the Maritime Security Risk Analysis Model (MSRAM) are used in support of the NIPP by identifying critical security needs specific to a port area. Area Maritime Security Committees, which are comprised of port stakeholders representing all levels of government and the port industry, use these various plans and tools to prioritize funding needs and rank port security project proposals” (FEMA, 2011).

The chart below shows the available funding for FY 2011 (FEMA, 2011).

Table 1: FY 2011 PSGP Funding

<table>
<thead>
<tr>
<th>Available Funding Group</th>
<th>FY 2011 PSGP Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group I</td>
<td>$141,017,400</td>
</tr>
<tr>
<td>Group II</td>
<td>$70,508,700</td>
</tr>
<tr>
<td>Group III</td>
<td>$11,751,450</td>
</tr>
<tr>
<td>All Other Port Areas</td>
<td>$11,751,450</td>
</tr>
<tr>
<td>TOTAL</td>
<td>$235,029,000</td>
</tr>
</tbody>
</table>

This investment strategy is specific and addresses components necessary to advance the operation and security measures for maritime shipping ports. Guidelines set forth by FEMA indicate that we have already begun to recognize the important of budgets and investing in personnel and technology.
Section Five: Analyzing the Impact of Safeguards on the Internet of Maritime Security

Cyber-attacks against the United States have become more recent with the advancement and accessibility of computers. We have seen hackers infiltrate some of the most restricted locations of the government including the Defense Department and the CIA. We cannot afford to jeopardize one of the most vulnerable critical infrastructures which maintain free trade and the global economy. Hackers such as “Anonymous” have proclaimed themselves undefeatable, able to access any sensitive information, and infringe upon classified information. As one of the marquee countries able to combat terrorism, we will have to analyze the safeguards that are set in place to counter such threats. In order to combat these threats the United States must look to coordinate with other port security agencies worldwide. Communication, the streamlining of documents and sensitive information, and the use of operating machinery via an online connection are deemed security risks to maritime port security. The Customs-Trade Partnership Against Terrorism (C-TPAT) is a program that has been utilized to help increase security for maritime shipping cargo to the United States and around the world. There are now online reporting hotlines, which are streamlined connections for any information regarding threats against shipping vessels or the ports. This is known as the Automated Commercial Environment (ACE). ACE does the following:

- Allows trade participants access to and management of their trade information via reports
- Expedites legitimate trade by providing CBP with tools to efficiently process imports(exports) and move goods quickly across the border
- Improves communication, collaboration and compliance efforts between CBP and
the trade community

- Facilitates efficient collection, processing and analysis of commercial import and export data
- Provides an information-sharing platform for trade data throughout government agencies.

In a February 8, 2012 report by the CBP, it is said that ACE “is the United States commercial trade processing system designed to automate border processing, to enhance border security and foster our nation’s economic security through lawful international trade and travel. ACE will eventually replace the current import processing system for U.S. Customs and Border Protection (CBP), the Automated Commercial System (ACS). ACE is part of a multi-year CBP modernization effort that is being deployed in phases” (ACE, 2012). These and similar designs create information that is streamlined and more secure because of the steps of approval it must go through to have cargo enter the United States.

Section Six: Analyzing Supervisory Control and Data Acquisition SCADA and Identifying the Threats and Vulnerabilities

The Supervisory Control and Data Acquisitions (SCADA) has been faulty because of its failure to keep up with current threats. Maritime security has been known to withstand and deter threats; however, with SCADA systems information is usually within confined units. With the use of cameras, metal detectors, radiation detectors, and security CCTV personnel there is a primary concern with how to advance in technology while catering to
the prevention of cyber-threats. SCADA systems have been placed on ships and collect
data and send it via an electronic communication line.

Threats remain at a high rate with these SCADA systems because agencies have been
unable to keep up with the advancement of technological threats. A hearing before the
Committee on Commerce, Science, and Transportation, and the United States Senate in
February 2010 discussed how SCADA protocols “used in control systems were not
designed to be attack resistant; they were originally used in electromechanical systems,
where you had to physically access the control, turn the knob, and so on.” It is now
believed to have control systems with unique identification numbers that connect with
one another via the internet. Threats to SCADA systems are significant and the United
States can no longer rely solely upon these systems to keep mechanisms secure or use
them as deterrents from cyber-attacks. In the same report it was suggested that there are
advancements the government can make with SCADA:

1. We should insist on some standards, through existing standards bodies, of Smart
   Grid components. NIST, for example, has led a cyber-security working group that
   recently released a second draft of Smart Grid Cyber security Strategy and
   Requirements document.

2. We need better transparency on how Smart Grid components are built and of what
   they are built. There are some mechanisms that can help establish transparency
   such as the Common Criteria, which is ISO-standard, and the Department of
   Homeland Security materials on improving software assurance and acquisition
With respect to maritime and the shipping ports, DHS and the U.S. Coast Guard must be able to access information on the status of shipping vessels from a remote location. In order to do that, SCADA would have to be upgraded to current GPS tracking signals. SCADA’s risk and threat to being hacked will have to be monitored by a technology group responsible for making sure secure measures are in place to monitor vessels. As cargos approach shipping ports, it is important to inventory freights so that the government has information on the cargo and reports are readily available. In recent years, SCADA has become more advanced; however, it is still stagnant compared to other state of the art technologies. CCTV Monitors, GPS trackers, technology groups solely responsible for monitoring shipping vessels via upgraded SCADA systems could great increase the security levels of maritime security.

Section Seven: Conclusion and the Assessment for 2012 and Beyond

Though we cannot prevent every terrorist or cyber-attack, security has been put into place since September 11th and has been reanalyzed on numerous occasions. All agencies and private sector entities have one common goal related to threats: deterrence. Security measures that are implemented online, in the waters, and on land all have to do with better safeguarding our homeland, our citizens, and our critical infrastructures. Maritime port security is one that has been addressed less frequently than that of other critical infrastructures. However, safeguarding the ports is a matter of safeguarding the global
economy and free trade. All critical infrastructures are related and all share common threats. We have been able to address the problems associated with maritime security and we are now developing more strategies to counter threats as they advance.

As for what will happen beyond 2012, it is up to our management policies and strategic analyzers who continually gather information and compare the current threats against past data. Advisory councils, local government assistance, streamlined online cargo control, and better training exercises all add to the advancement of securing our borders.
References


http://books.google.com


Retrieved from : 


www.fema.gov/government/grant/psgp.
CHAPTER VII

United States Shipping Ports and Megacommunity

Multi-Disciplinary Approaches

Executive Summary

The purpose of analyzing megacommunities and the U.S. Maritime entities is to offer insight as to how maritime security is sustained through the following entities: stakeholders, government agencies, Non-Governmental Organizations (NGO’s) and citizens. Terrorist threats and natural disasters which threaten the U.S. coasts, including shipping ports, are unpredictable and with a thorough analysis we can systematically implement strategies which involve a tri-factor leadership response that can disseminate information and communicate efficiently. The strategy to improving the megacommunity involves much of the public because they are an integral part of sustaining the safety and security of the nation’s maritime assets.

Introduction

The United State Maritime structure consisting of shipping vessels and shipping ports are at risk for terrorist attacks and natural disasters. However, none has occurred yet. The concern a megacommunity has encompasses the public sector stakeholders, private sector stakeholders. Disasters from natural events, human error, or terrorist attacks can result in damage far more widespread than just the disaster site itself. A chemical attack, hurricane, or other terrorist attack could have the potential of impacting an entire nation. The loss of a shipping port could cost the country of up to $1 trillion in damages. The
closure of a shipping port could have detrimental effects on the nation’s economy, global economy, affecting those who are employed in such industries. The megacommunity vital to the security of the nation’s maritime assets involves the following stakeholders:


2. Private: Oil factories, airports, shipping companies, trucking companies, companies operating along rail lines.

It is not only important to consider the megacommunity among the private, public, and NGO’s, it is important to include the public so that we understand the impacts citizens may endure should a disaster strike our maritime assets. In order to obtain a sufficient understanding as to how the megacommunity strategies affects the safety and security of the nation’s maritime assets and its citizens, an analysis of the following is critical:

1. advisory groups and how they can help a megacommunity develop better emergency response times

2. ways to resolve conflicts in a megacommunity when opposing views threaten to weaken relationships amongst sectors and stakeholders

3. involving the public for better communication

Through these three sections we will be able to grasp a better understanding as to how stakeholders and the public can cooperate to provide safer havens for people and the country’s maritime assets.
Section One: Understanding How Advisory Groups Assist Emergency Response Communications

The aftermath of Hurricane Katrina proved to be an example of how communication failures resulted in hundreds of deaths and billions of dollars worth of damages. The Federal Emergency Management Agency (FEMA) was considered a failure with resources and emergency responses arriving too late. Media and public scrutiny left the federal government scrambling for answers. Natural disasters are unpredictable but emergency response groups must be ready to activate necessary actions in order to mitigate a disaster when it occurs. The Community and Regional Resilience Institute (CARRI) Gulfport Advisory Group is an example of how the state of Mississippi joins both the public and private sectors to contribute their resources and ideas. During Katrina, consequences were overlooked. “Emergency plans foresaw cell phone communication as one layer in a redundant communication system. Emergency responders, including police, would oversee public safety with available emergency vehicles, while households would stockpile food and water, and the Red Cross would supply back-up source emergency rations. These plans failed as there was no anticipation of disrupted landlines and emergency communications that prompted an overwhelming demand on the undamaged cell-phone relay towers. With power off, emergency vehicles could not be refueled, and some emergency responders redirected their efforts to evacuating and caring for their own families. The possibility that the Red Cross would not be able to enter the city was not anticipated, nor the desperation and looting that
followed the exhaustion of meager food and water stockpiles while the officials blockaded entry of additional emergency supplies” (Colten, 2008). The diminished communication lines led emergency response workers to act for themselves; other helpless individuals were left fending for themselves without any communication lines or way out of the waters surrounding their residences.

Advisory groups are developed so that communication lines can remain open and sustain operability. There are reasons why an advisory group can be resourceful in providing security to our maritime assets:

   1. it improves communication and collaboration across all sectors
   2. it describes how individuals and families have the ability to prepare for disasters
   3. it increase resources for post-traumatic stress for individuals who have been in disasters
   4. it preserve the way to restore an area to the way it was prior to the disaster

The way we choose to mitigate a natural disaster or an attack against the United States depends upon how a megacommunity reacts. Megacommunities can be successful with an advisory group to take care of underlying factors of potential consequences and the aftermath of such consequences. Just as every president needs a cabinet to sustain operability so does a megacommunity. The maritime plays a crucial part in sustaining a global economy and free trade. Shipping vessels vulnerable to chemical and radiological attacks could affect not only the resources being shipped but as well as the surrounding communities. The ports of New York and New Jersey are excellent examples of how
docks are surrounded by dense populations, oil storage, and one of the world’s biggest financial centers.

With the advancement of technology, the critical infrastructure within the United States has had to develop new strategies to accommodate threats that were not considered a security risk before. However, the United States must also consider technological threats to infrastructure at sea. Shipping and ports on land are vulnerable to threats on a global scale. Terrorist attacks, natural disasters, and cyber-threats are just some of the main concerns that need to be considered when developing safeguards.

The Transportation Sector-Specific Plan for the Maritime Model Implementation Plan indicates that organizations with outside stakeholders are important to sustaining other critical infrastructures such as the economy, travel, banking and finance industries.

“Maritime model stakeholders are formalizing new coordination processes using the Sector Partnership Model espoused in the National Infrastructure Protection Plan (NIPP). The Maritime Model Government Coordinating Council (MMGCC) has been formed” (Transportation Sector-Specific, Sec. 5). The development of these councils and partnerships is a vital example of how we can control certain interdependencies by using advisory councils to speak on these agencies’ behalf. It is useful to have multiple areas that control one sector of a critical infrastructure. In this case, councils are utilized to correspond with interdependent entities while the agencies themselves are responsible for implementing the security measures.
Section Two: Ways to Resolve Conflict in a Megacommunity, especially when Opposing Views Threaten to Weaken the Relationships

To strengthen working relationships amongst private and public stakeholders, we have to develop continuous exercises which require the sectors to work together. One example was the idea of tabletop exercises presented by Richard Andrews, the Senior Director for Homeland Security Projects, National Center for Crisis and Continuity Coordination.

“One step that any organization can take to reach out to other public and private entities in its region is to conduct joint tabletop exercises. In contrast to full-scale training exercises that require physical deployment and response during a simulated crisis environment, the tabletop framework focuses on strategic planning, tactical safety and response drills.” This develops better working relationships amongst sectors but it also involves the public for better awareness. “Tabletop exercises can provide an effective forum for public- and private-sector organizations to discuss a full range of crisis-response issues. The exercises are designed to determine the level of coordination and communication readiness of several organizations in response to a variety of manmade and natural emergency situations, such as an escalation in the Homeland Security Advisory System” (Andrews, 2003).

Section Three: Involving the Public to Sustain Better Communication Efforts

To preserve an area that once held its own culture and history and quality, it is important that we try our best to have these cities retain citizens and continue to grow and prosper. Public forums give communities a sense of involvement with better insight as to how
citizens can sustain their livings with the resources available to them. A megacommunity which involves private security stakeholders as well as industrial stakeholders responsible for the outsourcing materials to other countries via shipping vessels could struggle without the understanding of communities surrounding these ports. Although federal and state stakeholders have provided tools and reports to grasp an understanding of public awareness, it is important to involve the public so that we learn how to sustain these communities.

There are a few ways in which the public could be informed and involved with sustaining the safety and security of maritime assets and surrounding ports:

1. Monthly newsletters with dates and times of meetings
2. Funds available to enhance security
3. Focus on public questions and concerns via surveys and a current questions/comments hotline

The Information Sharing and Analysis Centers (ISACs) have been described as one of the only “community forums for the sharing of information among public and private entities in crisis situations. These organizations primarily focus on communication within a specific industry and are often unable to provide members with the type of timely emergency information that national or state-level organizations would be able to provide” (Andrews, 2003).

Andrews also address the concerns of privacy and liability. They must be addressed to prevent classified information from being shared with the public. “The public-sector
organizations we work with value the benefits of information sharing, [but] some companies are hesitant to collaborate in crisis communications due to the potential legal ramifications of sharing potentially incomplete or inaccurate information. A baseline standard of acceptable good citizen information sharing must be established to prevent the threat of legal action from blocking vital collaboration between the public and private sectors.”

Public forums and involvement give a good idea of how a megacommunity approach will work. For example, in the private sector a store does not know how to handle its customers without feedback. They cannot simply guess how consumers will maneuver themselves around a store without some kind of organization of departments. If they are scattered, then there could be confusion and disruption amongst shoppers. This can cause longer lines, more questions as to where items are located and crowdedness. However, with feedback from the consumers, department heads could revamp their organization’s structure so that customers may shop more efficiently with little disruption. We can apply the same idea of effective preparedness to the government’s critical infrastructure. Without proper evacuation or security procedures intact, agencies cannot expect the public to immediately comply and react the way they may “think” they will; public forums and their involvement is merely a way to ensure that they are well informed on evacuation procedures and are able to take proper safety measure to advert disastrous events such as those of Hurricane Katrina.
Conclusion

RAND researchers discuss the likelihood of a scenario in which terrorists could strike maritime activities. There is potential impact on life and the economy, and leaves room for civil liability against the United States government. RAND’s risk assessment primarily involved risks associated with attacks on passenger and container shipping; it “began from a broad assessment of related threats and vulnerabilities, based on a combination of historical data regarding previous attacks, and on a series of interviews with counterterrorism experts. [They] then investigated the likely consequences that would follow from different modes of attack, drawing on historical data and publicly available analyses, and by framing those consequences in terms of human effects (e.g., casualties), economic effects (e.g., property damage and business disruption), and intangible effects (e.g., political and governmental responses). Finally, [they] combined the information on threat, vulnerability, and consequences to generate estimates of relative risk, in connection with attack scenarios involving ferries, cruise ships, and container shipping. [The] qualitative method for generating these risk estimates involved the use of defined ordinal scales to assess terrorists’ intents and capabilities, target vulnerabilities, and attack consequences” (RAND, 2006).

These vulnerabilities are critical and must be addressed on a regular basis. As time shifts so does technology, and so it is the responsibility of a megacommunity to ensure that the public and our critical infrastructure assets are secured and plans are accurately reflected in reports to Congress. Although are no guarantees of safety, there are certainly steps
that can be put in place to ensure that the public sector, private sector, and the public are well informed and are aware of threats at the same time.
References


CHAPTER VIII

The United States Department of Defense:

Securing Personnel Through Protecting the Infrastructure

Introduction

With the threat of terrorism very much still prevalent today, we have focused our attention on areas outside of the Middle East. Since the September 11th attacks, the United States has increased its counterterrorism (CT) personnel throughout the world. Not only have we allied with other countries to fight terrorism we have set up “shop” in areas that are prone to more terrorist attacks. In addition to extremist Islamic groups, we have also focused on areas where drug trafficking is prevalent such as Columbia, Cuba, Afghanistan, and within the U.S. According to iJET Intelligent Risk Systems, an agency which maintains the security risks for 182 countries, the following ten countries reported in 2003 were at the highest risk of terrorism: (iJET)

Figure 1.1

| Colombia          | FARC declared war on the current president because he vowed to rid the country of terrorism. FARC has been known to conduct kidnappings and shootings which involve casualties of civilians regardless of affiliation. |


<table>
<thead>
<tr>
<th>Country</th>
<th>Recent bombings in this country were due to the Jemaah Islamiyah extremists which operated cells in this country.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indonesia</td>
<td>Terrorist groups, particularly Palestinian terrorist groups were conducting mass suicide bombings in busy areas. Hamas was one of the main culprits in this country; they were able develop sophisticated methods that could hide under the radar and thus succeed in their mission.</td>
</tr>
<tr>
<td>Israel</td>
<td>This country has been an open area for Al Qaeda due to the poor border controls in place. With close proximity to other countries in Africa it has been susceptible to terrorist attacks.</td>
</tr>
<tr>
<td>Kenya</td>
<td>This is an unstable nation; the national population is 50% Muslim. With religious and ethnic tensions the country is susceptible to extremist groups operating and developing terrorist cells.</td>
</tr>
<tr>
<td>Nigeria</td>
<td>There have been several smaller attacks in</td>
</tr>
<tr>
<td>Country</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Russia</td>
<td>Threats have always been prevalent in this country. Militants outraged at the election of Putin have carried out acts in Chechnya. They aim for civilian targets making it one of the most dangerous areas in Russia.</td>
</tr>
<tr>
<td>Spain</td>
<td>The ETA separatist group has been an extreme threat to law enforcement and a particular area of concern to those involved with combating terrorism as they are the targets.</td>
</tr>
<tr>
<td>Thailand</td>
<td>Tourists and foreign companies in this country have been the main targets for terrorists. It has a big effect on the economy. Terrorists are capable of committing large scale suicide attacks in malls, restaurants, and large buildings.</td>
</tr>
<tr>
<td>Yemen</td>
<td>Al-Qaeda has developed massive numbers of terrorist cells in this country. Because...</td>
</tr>
</tbody>
</table>
they are in remote locations it is almost impossible to locate them.

A country of particular interest still relevant today on this list is Spain. We have to consider the impact of both local and foreign law enforcement security personnel and the security measures that must be sustained for them.

The purpose of this report is to determine how we can engage in CT efforts while protecting the security and intelligence personnel assigned to this region. We will take Spain as an example and use the Department of Defense (DOD) and their use of infrastructure to consider whether or not these infrastructures are sufficient enough to defend our personnel.

DOD Task

The task set for DOD is protecting personnel and the operating assets against any number of threats. We will take into consideration the range of threats in the region and the impact it will have on our CT measures as an enterprise.

This depends on how prepared we are and how fast we are able to respond to a warning about what is threatening our security personnel. Management must consider three aspects:

1. Determine how terrorism even at the most minimal security risk impacts the organization;
2. Assess and monitor these threats to see how our infrastructure and personnel are impacted;

3. Direct and engage in an appropriate response.

Desired Results for the DOD

With proper knowledge and reaction we will be able to determine the threats to DOD personnel, infrastructure, and other assets (e.g. employee and military vehicles, employee residences, and documents). We will also be able to communicate with other U.S. agencies and security forces within Spain to set warning systems against other threats that affect our ability to conduct CT strategies. Finally, we will be able to deploy emergency responses in case an attack has been carried out.

Threats to DOD CT Personnel in Spain

The main threats in Spain are militant groups aimed at dismantling the security forces within this country. It does not matter whether they are the local authorities or foreign security forces. The Spain separatist group, Euskadi ta Askatasuna (ETA) is one of the biggest threats to CT forces in this country. Their aim is to disable and dismantle the government’s security and law enforcement personnel and infrastructure. ETA has established great unease in the Spanish government. Although the ETA has also aimed its violence against tourists and other civilians, the majority of their victims involve government officials.
The Council on Foreign Relations states that the “ETA’s secular nationalist agenda has nothing to do with the Islamist fundamentalism of Osama bin Laden’s terrorist network, and experts say there is no credible evidence of any systematic cooperation between ETA and al-Qaeda” (http://www.cfr.org/france). Al-Qaeda, however, is found in parts of Spain but is not considered to be a part of this particular separatist group. Because these two entities are prevalent in Spain we have to keep in mind that they are a threat to both the government and civilians at a very high rate.

The DOD must consider how to secure their personnel, particularly the noncombatant personnel which include administrators, intelligence analysts, and communication posts.

Task 1: Determine How Terrorism Even At The Most Minimal Security Risk Impacts The Organization

We have already established the two main terrorist groups that threatened the DOD personnel and organization as a whole. Even as the ETA disappeared for a while in the mid 2000’s, security strategies for the government still did not change because Spain had to stay on guard at all times. If there was an attack on DOD personnel and its infrastructure, we would suffer severe consequences. Our intelligence would be dismantled, our communication would be destroyed, and security forces would have to increase their communication and intelligence efforts in an attempt to alleviate any problem, making us prone to more attacks.
Figure 1.2 below is an example of how DOD personnel can be updated with alerts and threats so they can prepare for the worst. To avoid these mistakes of miscommunication we have to understand how these types of attacks can impact our infrastructure and of course, the most important assets of the U.S. Government, our personnel.

Figure 1.2

<table>
<thead>
<tr>
<th>Live alerts that are messaged to individuals</th>
<th>These can be delivered to one’s cell phone or email address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A system that allows military personnel to track possible threats</td>
<td>This can be done by giving other assets to other vulnerable countries and learning from their advantages and disadvantages.</td>
</tr>
<tr>
<td>Increasing intelligence</td>
<td>The intelligence support at home can be utilized as additional help to those serving abroad</td>
</tr>
<tr>
<td>Continual briefs on intelligence</td>
<td>Every country should share intelligence reports so that they can assess whether or not two or more countries are experiencing similar threats with the same organization.</td>
</tr>
</tbody>
</table>
Task 2: Assess and Monitor These Threats to See How Infrastructure and Personnel Are Impacted

If the ETA or Al-Qaeda makes a threat towards DOD personnel, we will have to consider how we protect our team through determining whether or not our infrastructure is sufficient. We do this by identifying the strategic issues. Strategically, an issue that arises from a situation analysis is that of inner managerial controls. In order to place strategic goals on an international basis we ensure that all internal controls within the DOD are devoid of the internal weaknesses. There is little transparency among governments, and obtaining cooperation from reluctant countries can make it difficult for the United States to enforce its efforts into screening possible terrorist activities, industries and the infrastructure. Another strategic issue is that of the timeline. Previous strategic plans have not gone beyond five years, and given the advancement in technology we must prepare these plans so that we can apply them over a ten year plan.

As administrations change, we have to maintain the strategic plan for at least a decade before we can start seeing results in the long term. The DOD in conjunction with governmental and private security stakeholders both at home and abroad will maintain the strategy. For example, Goldman Sachs has an interest with foreign investments throughout the world. If we can encourage transparency through transactions which occur between countries that are most susceptible terrorism, we can decrease the threat of extremists infiltrating these banking systems and destroying some of the most important aspects of commerce. The same goes for weapons trading and drug trafficking. All these
elements help us develop a better understanding as to which areas the money and/or weapons are transported to, thus giving an idea where an attack might occur. We are responsible for understanding how the infrastructure functions within foreign governments.

Brian Jackson and David Frelinger wrote “Emerging Threats and Security Planning with the A RAND Infrastructure, Safety, and Environmental Program which frames a middle ground approach to addressing possible threats. Meeting halfway in a proposal rather than burdening a country with its own security forces is essential. “Ideally, the national approach to addressing possible future threats should strive to get as many of the advantages of both ends of the spectrum—responding prudently to threats. . . but not allowing doing so to threaten the effectiveness and sustainability of existing security efforts by forcing planners to spend disproportionate time focusing on unlikely terrorist scenarios. Analysts could use techniques such as risk analysis or cost/benefit analysis to assess different threats and use their results as a common denominator to determine how much we should worry about different possible attacks and the advisability of different possible responses to them” (Jackson, Frelinger, 2009).

For example, as reported in FY 2010 Performance and Accountability Report, “Treasury served a leading role in establishing the Afghanistan threat finance cell (ATFAC). This is a Kabul-based task force charged with collection, analysis, and dissemination of
intelligence to disrupt funding and support for the Taliban and other terrorist and insurgent networks in Afghanistan. It provides finance expertise to U.S. civilian and military leaders and assists a

Afghan authorities have investigated insurgent terrorist financing, narcotics trafficking, and government corruption. Through this assistance, ATFC has helped build the capacity of Afghan authorities to operate independently, a key U.S. policy goal in Afghanistan” (Performance and Accountability Report, 2010). The ultimate goal here is to eliminate cyber threats within the infrastructure of our banking and finance industry. For example, there are several strategic factors implemented by the Department of Treasury to eliminate such threats; however, these goals are not 100% preventative, so we must keep an ongoing effort to deter criminal acts from infiltrating our banking infrastructure. This is an example of how we utilize intelligence to protect other personnel from being harmed. It can be utilized in any form of security and infrastructure program.

Task 3: Direct and Engage In an Appropriate Response

The DOD Antiterrorism (AT) Program Directive 2000.12 written in 2003 developed a response as to how we are to evacuate noncombatant civilian employees from areas of threat. Particularly the Defense Intelligence Agency (DIA) AT responsibilities includes:

1. Establish and operate a Joint Intelligence Task Force for Combating Terrorism (DIA/JITF-CT) to direct collection, exploitation, analysis, fusion, and dissemination of all-source intelligence in support of DOD combating terrorism operations, planning, and policy, including DOD AT requirements.
The JITF-CT serves as the single national-level, all-source foreign terrorism intelligence effort within the Department of Defense. The JITF-CT is designated to serve as the central repository of all foreign terrorism-related intelligence for the Department of Defense. Military Department Secretaries and Service Chiefs shall conduct terrorism intelligence activities as a component of or in consonance with the JITF-CT.

2. DIA/JITF-CT shall provide prompt dissemination of intelligence on foreign terrorist threats, including specific warning of threats against DOD personnel (including family members), facilities, and other DOD material resources. Warnings to DOD Personnel (including family members) shall be in accordance with the "No Double Standard" policy as defined in Enclosure 2. The DIA/JITF-CT is the focal point within the Department of Defense for the analysis of data and information pertaining to domestic and foreign terrorist threats to DOD Personnel (excluding threats posed by U.S. persons who have no discernable foreign control or connections).

3. Operate a 24-hour terrorism intelligence Warning and Fusion Center within the JITF-CT; ensure terrorist threat intelligence is disseminated to the appropriate DOD Components.

4. Send a representative to the Interagency Committee on Terrorism, and provide the DOD input to the national intelligence foreign terrorism warning process.

5. Maintain a foreign terrorism database, which includes information on foreign terrorist groups, capabilities, facilities, incidents, biographies, and foreign counterterrorism policies and response capabilities.
6. Subject to the provisions of References (aa) and (ab), assess the foreign terrorist threat worldwide, ensure dissemination to the DOD components, and produce daily foreign terrorist threat awareness reports.

7. Provide a member to the DOD Antiterrorism Coordinating Committee (ATCC) and subcommittees.

8. Function as the DOD Executive Agency for diplomatic security matters.” (Directive 2000.12)

All these responsibilities listed in the directives are a prime example of how we are to establish protection for any noncombatant federal employees and their families from threats of terrorism. There are controls in place for an evacuation. But prior to evacuating such employees, we have to acknowledge the fact that we have learn to deter the possibility of physical harm to these individuals. The Annual Report to Congress on Foreign Economic Collection & Espionage of 2008 indicates, “The threat to the United States from foreign economic intelligence collection and industrial espionage has continued unabated since the publication of the Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2007. Economic espionage cases went up slightly and nearly every day brought reports—in the press and in the classified world—of new cyber-attacks against U.S. government and business entities. Additionally, the increasing use of new modes of communication and social networking provided uncharted opportunities for transferring information and spying on the part of enterprising foreign intelligence services.” (http://cdse.dss.mil/counterintel)
They also address the threat of technologies which in return can threaten the well-being of DOD employees. Because of newly emerging technologies that are still in premature stages, they are vulnerable to attacks. “Many of these constitute Critical National Assets, defined as systems, processes, technologies, or information that are of broad overriding importance to the survival, safety, or vitality of the United States and that, if stolen, modified, or manipulated by an adversary, would seriously threaten US national or economic security. Often these technologies are difficult to identify in their early phases.” (Annual Report to Congress on Foreign Economic Collection and Industrial Espionage)

These examples are critical not only to protect our infrastructure but to also protect our personnel. Military and noncombatant DOD personnel are severely at risk should one of our infrastructures be infiltrated or destroyed in a country such as Spain. The Spanish government will have to coordinate with U.S. military personnel in order to protect assets of all types.

Conclusion

The security measures are an attempt to increase security abroad in order to increase security at home, and it best to keep in mind that this is not only for the benefit for the U.S. but also for other countries. We cannot simply set goals and objectives and expect them to be followed by bodies outside of the United States. In 2008 the Department of Defense (DOD) implemented a strategy to promote security on an international level. Particularly they emphasize the importance of promoting security to prevent war. The DOD seeks to prevent warfare by a strategy with the idea that “the best way to achieve
security is to prevent war when possible and to encourage peaceful change within the international system” (National Defense Strategy, Department of Defense). The protection of our noncombatant employees is an active approach consistent with other security measures. The United States in its many attempts to deter terrorism worldwide must take measures to ensure that more strategies are being developed to address better security measures.
References


Security Threat Assessment for the New York City Metropolitan Transit Authority’s Subway System and the Security Risks Posed to Its Riders

New York City Police Department Joint Terrorism Task Force

Intelligence Gathering

Introduction

In response to specific intelligence reports provided to the New York City Police Department’s Joint Terrorism Task Force (NYPD JTTF), the Department of Homeland Security has determined that more security measures are required for major metropolitan subway systems including New York City’s Metropolitan Transit Authority (MTA). These measures are a result of intelligence gathered by the DHS and the Federal Bureau of Investigation. Based on this specific threat information, the DHS and FBI have determined implementation of new security measures will be deemed necessary for the MTA and its riders. The completion of a threat assessment is necessary among available agencies involved with the NYPD JTTF to counter such threats.

These measures are a result of assessments made by individuals connected to operations of intelligence gathering within the DHS. Available information leads us to believe that several groups either of or related to Al Qaeda terrorist organization are considering multiple attacks at major MTA subway hubs. Specifically, Grand Central, Brooklyn Bridge/City Hall, and Penn Station have been listed as main targets for the attack. The
NYPD JTTF will conduct these assessments by comparing intelligence reports against available law enforcement anti-terrorism databases and records.

Intelligence Overview
The following information is collected from the DHS and FBI for the individuals who have pledged allegiance to Al Qaeda and are involved with the threat assessments: full name, aliases, date of birth, social security number (if any).

The information being collected is to facilitate security threat assessments within the MTA subway systems. Individuals involved with this threat are vital in providing further information as to whether or not there is similar danger to other mass transit systems in the New York City vicinity and across the country. This information is to be used to determine when these individuals intend to carry out such Mumbai-like attacks at the aforementioned subway stations.

Knowns/Unknowns
We know these terrorists are capable of obtaining low-grade weaponry with an ability to maneuver through subway stations in a swift manner. We have reason to believe their ability to maneuver through the city is based on mapping and constant traveling on the MTA subway systems prior to the date of attack. We must also consider the idea that bomb making materials may be used in small backpack carry-ons and left on trains and/or other areas of subway stations.
We are unable to confirm whether or not these threats are affiliated with Al Qaeda or a similar organization who shares the same ideology. We are also unable to identify how many individuals are expected to attack, if they are of U.S. citizenship status, or if intelligence reports suggest that these terrorists plan on attacking any other metropolitan transit system in the country.

Lessons Learned from Mumbai Attacks

On December 13, 2001 terrorists entered the Indian Parliament; they claimed to be part of Lashkar-e-Taiba (LeT). Although Pakistan denied that such a group is based in its country, many Indians believe that the politicians needed to take a bigger role on handling the issues coming out of Pakistan. Specifically, India declared that it will take on a serious role in response to the terrorist attacks which affected hundreds of locals and tourists. This even meant military force if necessary. The long standoff between Indian and Pakistan has created concerns among the international community, and a military action from India to Pakistan could lead to a massive war. The United States understands the self-defense approach India would take should they attack Pakistan; but only if they had failed in all attempts with diplomatic measures.

This terrorist organization is on the list of foreign organizations which the United States government has included in its reports. In addition to Lashkar-e-Taibe, another terrorist group, Jaish-E-Mohammed was also at the root of the Mumbai attacks (Lessons, 2009).
LeT Ideology and Modus Operandi/Tactics:

LeT has made it clear that they are another strand of an Al-Qaeda like terrorist platform. Their ideals are similar to Al-Qaeda: terrorize globally without hesitation and to enforce ideals onto Western societies that do not share the same values or ideologies as their Islamic faith.

Their motive for executing such an attack is to demonstrate how simple their tactics may be in order to spread a message. They used low-tech weapons that produce vastly disproportionate results. The Mumbai attack was sequential, highly mobile. It was a departure from the by-now-common suicide bombings. But the tactics themselves were simple—armed assaults, carjackings, and drive-by shootings, building take-overs, barricades and hostage situations, things that we have seen before, but put together in this impressive complex of attacks. The attack was carried out by just 10 men, armed with easily obtained assault weapons, pistols, hand grenades, simple improvised explosive devices, little more than the arsenal of a 1940s infantryman, except they had with them 21st century communications technology—cell phones, satellite phones, BlackBerrys, and GPS locators. The attackers embedded themselves among civilians, using them not only as hostages, but as shields to impede the responders and to maximize civilian casualties. This is a tactic that we have seen elsewhere and that now we have to be prepared for, that is, terrorists deliberately embedding themselves with civilians to increase the ultimate body count as the response takes place” (Lessons, 2009).
Furthermore, according to analysis that was done by the Mineta Transportation Institute, “two-thirds of all of the terrorist attacks on surface transportation over the last 40 years were intended to kill, and 37 percent of those attacks resulted in fatalities. Now that compares with about 20 to 25 percent of terrorist attacks overall, suggesting that when terrorists come to surface transportation, they do view it primarily as a killing zone. Indeed, 75 percent of the fatal attacks involved multiple fatalities and 28 percent involved 10 or more fatalities. So the intent here clearly is slaughter” (Lessons, 2009).

Lessons and Implications

Hearings in Congress in 2009 specifically laid out the implications of the Mumbai attack. There are at least four implications that led to a disastrous ending to the attacks:

1) The terrorists were in the hotel for several months, and posing as different guests; they were taking picture and thus learning the layout of the hotel;

2) Police responders were not familiar with the hotel, which therefore made it difficult to maneuver throughout the facility;

3) Management did not increase security measures despite threats that may have been given by intelligence analysts;

4) There were many entrances and open stairways; making it easy for anyone to roam through the hotel freely.

To counter such situations management and law enforcement should have in place the following:

1) Advanced training for employees in the layout of the hotel and how to identify suspicious activity;
2) There must be coordination with local law enforcement and management/employees of the hotel in order to disseminate information quickly as a threat develops;

3) Security must be increased, and the security personnel must be able to analyze intelligence reports and even develop them so they can be communicated to law enforcement;

4) Areas should be strictly monitored and secured. There should not be any open stairways and doorways. Cameras and security guards should be in place in areas which are not regularly checked.

The implications and lessons that need to be learned from the attack in Mumbai are that we need to ensure emergency response to be as quick as possible. The Interagency Threat Assessment and Coordination Group annual report to Congress in 2011 offers ways in which we can maintain a strong force, better communication, and safer grounds in areas such as subway systems.

Strengthen and Manage Oversight

Here the ITACG suggests that, “The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, established the position of a Program Manager to ‘plan for and oversee the implementation of, and manage’ the Information Sharing Environment (ISE), and to be ‘responsible for information sharing across the Federal Government.’” Consistent with the direction and policies issued by the President, the Director of National Intelligence (DNI), and the Director of the Office of Management and Budget
(OMB), the Program Manager, Information Sharing Environment (PM/ISE) issue
government-wide procedures, guidelines, instructions, and functional standards, as
appropriate, for the management, development, and proper operation of the ISE. In
strengthening the management and oversight of the ISE, the PM/ISE actively governs,
integrates performance and investment, engages stakeholders, and encourages a culture of
information sharing” (Paul, 2011).
This means the DHS, MTA, the NY DOT, and the NYPD JTTF must coordinate with
other local, state and tribal law enforcement authorities. Typically, non-federal
organizations do work with other subcommittees: the ITACG report states three such
entities which are non-federal organizations who coordinate closely with select ISA IPC
Sub-Committees and working groups (Paul, 2009):
• Criminal Intelligence Coordinating Committee (CICC) – Fusion Center Sub-Committee
and the
SAR Sub-Committee
• Global Justice Information Sharing Initiative (GLOBAL) – Fusion Center
Sub-Committee, SAR
Sub-Committee, Information Integration Sub-Committee (Standards Working Group)
• Regional Information Sharing Systems (RISS) – Information Integration
Sub-Committee
(Assured SBU Network Interoperability Working Group)

Improve Information Sharing and Establish Standards for Responsible Information
Sharing and Protection
This report states that “the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) makes it clear the PMISE’s responsibilities extend to addressing and facilitating improved information sharing between and among the components of the Intelligence Community (IC), the Department of Defense (DoD), as well as the Homeland Security and law enforcement communities. In addition, the PMISE is required to address and facilitate responsible information sharing between federal departments and agencies and state, local and tribal governments; federal departments and agencies and the private sector; and federal departments and agencies and foreign partners and allies. While ensuring responsible information sharing between all of these mission partners, the PMISE must also ensure the protection of privacy, civil rights, and civil liberties (P/CR/CL)” (Paul, 2009)’ This guidance is to ensure that stakeholders, the DHS, and the NYPD JTTF are coordinating in such a way that all information sharing is received at the same time. Information sharing also includes the public in the way the MTA has campaigned for with the campaign “If you see something say something.” This not only engages the private sector stakeholders but also the public who all take part in initiating information sharing among law enforcement and MTA staff.

Intelligence Cycle, the Intelligence Community, and Fusing Law Enforcement

The intelligence cycle process consists of five steps: planning and direction, collection, processing, analysis and production, and dissemination. This cycle is provided as a means for assisting analysts, policymakers, and managers alike. The idea here is to have policymakers pay attention to intelligence reports which may indicate imminent danger. Too often we find that policymakers are compelled to reject certain intelligence
information from the Intelligence Community (IC) simply because it does not contain 

enough information to convince a policy maker of a decision. Human Intelligence is a 
crucial part of what makes the Intelligence Cycle function, according to Mark Lowenthal, 
author of “Intelligence: From Secrets to Security.” Lowenthal depicts the IC as one that 
does not receive much feedback from policymakers. He has indicated that as a means of 
furthering information through the IC and the intelligence cycle that we create these 
fusion centers such as the NYPD JTTF. He specifically states, “The legal difficulty 
encountered in the United States is inherent in the federal system, which places 
responsibility for local law enforcement on the states and their cities or counties. As a 
means of improving liaison between the federal and local levels, a series of fusion 
centers, called Joint Terrorism Task Forces (JTTFs), have been formed, although the 
majority of them tend to be staffed by state law enforcement personnel. These are in 
a rather early state of development and their ability to provide the desired liaison and 
integration and future remains uncertain” (Lowenthal, p. 257). The increasing of JTTFs is 
an efficient way to create a better communication center. We have created many since 
September 11th and we are still in the process of revamping and renewing certain ideas so 
that more information is streamlined.

Results and Outline of Security Measures of Threat Assessment on MTA Subway System 

We must gather all JTTFs and create a public awareness so that they are integrated with 
the communication and with law enforcement including the stakeholders. There needs to 
be upgraded presence of law enforcement on both the NYPD JTTF and FBI governing 
levels. There is a need to keep a close eye on suspicious activity through the security
monitoring system developed by the NYPD. All subway systems vulnerable to such Mumbai-like attacks will need to be dealt with swiftly by means of quick communication via the IC and the public. We must address, at minimum, the following emergency responses set in place in underground areas of the MTA subway systems in case of ANY emergency: fire systems and procedures, exits in case of natural disasters, how to handle evacuations, what to do with a power failure, reporting these emergencies, and how to increase security with the threat of terrorism.
References


https://www.hsold.org/?view&did=444384


CHAPTER X

The United States Department of Homeland Security

Evaluating the Critical Infrastructure Program

Introduction

One of the nation’s top priorities is the safety and stability of the United States’ infrastructure both at home and abroad. As technology advanced throughout the years, different components of infrastructure became closely linked. Prior to technological advances, systems of our infrastructure were independent of one another. There was very little linkage among them. However, with today’s advances in technology they have become linked through computer systems. Critical infrastructures such as oil, telecommunication, gas, electricity, banking, nuclear plants, law enforcement and emergency services are at a high risk should there be a cyber-attack on systems responsible for maintaining these elements. The Cyberterrorism Defense Analysis Center (CDAC) states that “the threat of cyberterrorism to our technical infrastructure is real and immediate. Computers and servers in the United States are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency, and sophistication each year. As our nation’s critical infrastructure grows more reliant on information technologies, it also becomes more exposed to attackers, both foreign and domestic. These attacks can threaten our nation’s economy, public works, communication systems, and computer networks.” (FEMA)
This report will evaluate the banking infrastructure of our nation, an element that is extremely vulnerable to terrorist activities. The financing of terrorism has been an aim of terrorists by laundering funds from one account to another. We need to make sure that the threats have been strategically minimized; in order to determine that, we have to evaluate the safety mechanisms already in place. The oversight of such areas falls under the watchful eye of the U.S. Department of Treasury. It is extremely crucial for this country and for others alike to secure and maintain the economy around the world. We will have to strengthen relationships with stakeholders both on a domestic and international level. Private sector entities responsible for protecting the areas of cyberspace and contracts with the United States government will have to be improved.

Purpose
We will define four evaluation methods to determine whether or not the banking infrastructure has in fact been improved since the attacks of September 11th.

Evaluation Overview
These evaluations are designed to improve the regulatory arrangements that are in place. Because our time and resources are limited, it is necessary to obtain external research to determine if there is improvement in security. According to the World Bank’s Handbook for Evaluating Infrastructure Regulatory Systems, “A quick evaluation may take up to 5 person-days and could cost up to US$15,000” (Brown, Stern, Tenenbaum). Therefore we will have to determine how to evaluate the banking infrastructure without spending too many tax dollars.

First Evaluation Method: Collecting Data
Collecting data is the simplest form of evaluation. When collecting data within the banking system, you are essentially compiling information that is already stored in banking databases. This requires only technical skill. Furthermore FDIC rules and regulations require banks to collect certain information since September 11th. Title 31 of the Money and Finance Law relates to the National Money Laundering and Related Financial Crimes Strategy; it addresses enhancement of the role of the private financial sector in prevention through partnerships between the private financial sector and law enforcement agencies, including incentives to strengthen internal controls and to adopt more effective policies industry wide. It also addresses the enhancement of intergovernmental cooperation between the federal government and state and local officials, including prosecutors and other law enforcement officials (GPO). This is very effective in allowing agencies to collect data in order to find out which individuals, groups, or companies are conducting illegal activities. The Treasury Department is working with public and private sector partners to develop a method to continue to monitor the activities of investors and banking clients. The Department of Homeland Security and Department of Treasury’s Banking and Finance Critical Infrastructure and Key Resources Sector-Specific Plan as an input to the National Infrastructure Protection Plan conducted in 2007 states, “The process for developing these metrics will incorporate collaboration and insights from sector participants, regulators, as well as other sectors’ government and sector coordinating councils as appropriate. These include processes for developing metrics to address vulnerabilities stemming from gaps in sector dependencies, continuous improvement to the information-sharing framework, and unique challenges posed by cyber-crime. The Treasury Department will coordinate with the FBIIC agencies
and the FSSCC to validate, update, and implement these metrics” (DHS-Banking and Finance).

Second Evaluation Method: Conducting an Analysis of Outside Stakeholders

For the FY 2012, the Treasury Department’s new budget reflects a plan coordinated by the government to seek more clearly developed objectives. Specifically, “The Presidential Policy Directive on Global Development – the culmination of months of interagency research and debate – concludes that we should ‘redouble our efforts to support, reform, and modernize multilateral development organizations most critical to our interests,’ and to that end, ‘renew our leadership in the multilateral development banks.’”

Figure 1.1 reflects the budget requests and appropriations by the Department:

<table>
<thead>
<tr>
<th>Poverty Reduction and Economic Growth (MDBs)</th>
<th>FY 2010 Approp.</th>
<th>FY 2011 CR Level</th>
<th>FY 2012 Request</th>
<th>FY 2012 Request Full Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Development Association (IDA)</td>
<td>1,262.5</td>
<td>1,262.5</td>
<td>1,358.5</td>
<td>1,358,500,000</td>
</tr>
<tr>
<td>Int’l Bank for Reconstruction and</td>
<td>117.4</td>
<td></td>
<td>117,364,344</td>
<td></td>
</tr>
</tbody>
</table>
Over the course of five years the intention is to improve strategic performance goals in hopes of increasing international oversight while risks are minimized. Between $10 billion and $20 billion will be required. This number is based on estimated totals for 2010. An estimated $2 billion a year needed for development of stricter security measures which require more personnel and contractors to oversee the process. Not only

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Development (IBRD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inter-American Development Bank (IDB and FSO)</td>
<td>102.0</td>
<td></td>
<td></td>
<td>102,018,035</td>
</tr>
<tr>
<td>Multilateral Investment Fund (MIF)</td>
<td>25.0</td>
<td>25.0</td>
<td>25.0</td>
<td>25,000,000</td>
</tr>
<tr>
<td>Inter-American Investment Corporation (IIC)</td>
<td>4.7</td>
<td>4.7</td>
<td>20.4</td>
<td>20,428,519</td>
</tr>
<tr>
<td>Asian Development Bank (AsDB)</td>
<td>0.0</td>
<td>106.6</td>
<td></td>
<td>106,585,848</td>
</tr>
<tr>
<td>Asian Development Fund (AsDF)</td>
<td>105.0</td>
<td>105.0</td>
<td>115.3</td>
<td>115,250,000</td>
</tr>
<tr>
<td>African Development Bank (AfDB)</td>
<td></td>
<td></td>
<td>32.4</td>
<td>32,417,720</td>
</tr>
<tr>
<td>African Development Fund (AfDF)</td>
<td>155.0</td>
<td>155.0</td>
<td>195.0</td>
<td>195,000,000</td>
</tr>
<tr>
<td>European Bank for Reconstruction &amp; Development (EBRD)</td>
<td>0.0</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Subtotal</td>
<td>1,552.2</td>
<td>1,552.2</td>
<td>2,072.6</td>
<td>2,072,564,466</td>
</tr>
</tbody>
</table>

(Intermediate, 2010)
are we sustaining the security of banks in other countries, but we have to ensure that commerce and other legitimate trades done through our banking systems does not negatively affect the nation’s economy.

In order to conduct an evaluation on an area like this we must evaluate the external stakeholders who are responsible for coordinating with the U.S. government in securing our banking infrastructure. Stakeholders include entities such as banks, investment firms, hedge funds, and other entities both local and international. The method to evaluate success in this is a survey to find out whether or not they have put effective regulations in place post September 11th. The following is a list of questions for such a survey:

1. What is the main function of this entity?
   a. Banking
   b. Investment Advisor/Manager
   c. Hedge Fund
   d. Governmental Agency

2. How many Suspicious Activity Reports (SAR) were filed with the Financial Crimes Enforcement Network (FinCen) last year?
   a. 10,000 or fewer; if so, the approximate number_______
   b. 10,001-15,000
   c. 15,001-20,000
   d. 20,001 or more; if so, the approximate number_______

3. Of the Suspicious Activity Reports issued to FinCen approximately how many were follow up by a governmental agency?
a. fewer than 10; if so, the approximate number ________
b. 101-500
c. 501-1000
d. 1001 or more; if so, the approximate number ________

5. Does the firm or governmental agency have a written document pertaining to the Bank Secrecy Act? If you are a governmental agency, is there a Memorandum of Understanding with the appropriate agency?

6. How much is currently spent on upholding current FDIC rules and regulations?

7. Were there any indications of a terrorist activity within the past year? If so, explain.

8. Has the government opened investigations pursuant to possible terrorism activity?

9. How many individuals are assigned to detecting fraudulent activity within your firm, agency?

10. How many managers are in charge of overseeing the operations of these security measures?

11. Do you receive federal funding in order to enforce any of these rules and regulations? If so, how much did the entity receive in the last fiscal year?

12. If the entity received funds, how much was used to enforce the regulations?

13. If the entity received funds, did you need to request more funding? If so, why?

14. How often do you report to the appropriate agency for updates and reports?
15. What kinds of training are in place for personnel?

16. What are the credentials are required of an entry level candidate to work in the fraud
detection department?

17. What are the approximate salaries for individuals in these departments?

18. How often are you audited by FINRA or other government agency?

19. Is there documentation that must be provided as a result of the audit?

20. How many foreign clients do you have and in what countries?

21. How many open inquiries are there regarding suspicious activity?

22. Are you a fiduciary to any foreign investment accounts? If so, please attach
documents pertaining to fiduciary accounts.

23. Have there been any anonymous tips outside the firm/agency? If so, how many?
What was the subject of the tips?

24. Who are the outside auditors, and are they paid through private or tax dollars?

25. Are you aware of any suspicious activities involving funds being invested with hedge
funds and feeder funds?

These questions require the respective agency and/or firm to conduct a thorough analysis.
With the information compiled by these entities we will be able to develop an
understanding as to whether or not tax payer dollars have been well spent. This
procedure should be conducted on an annual basis in order to ensure not only compliance
with how tax dollars are spent but also to determine if more or fewer tax dollars are needed. These questions relate not only to counterrorism but also to financial fraud. Bernie Madoff is an example of how he practically dismantled the economy with the economic downfall of 2008. Every government agency involved with financial fraud detected the investment red flags post-Madoff and was put on high alert thereafter. Such red flag areas include:

a. Obscure auditors: feeder funds did not have an outside performance audit

b. Unusual fee structures: no management fee for the Madoff funds, unusual for a hedge fund’s operations

c. Family influence: many of these family members controlled and operated in key positions, thus keeping the fraudulent activities quiet

d. Inadequate staff: Madoff had nearly $17 billion under management with only a few staff members

e. No registration with the Securities and Exchange Commission (SEC) after 2006

f. Lack of Transparency: on site due diligence inspections for investors were limited or even denied; no answers to questions regarding the business or his investment strategies.

g. Unusual transfers: Towards year end, Madoff would invest the assets in Treasury bills, a very unusual practice for hedge funds.
Surveying areas of financial firms is not only important to ensure that funding terrorism is eradicated but that the white collar crimes committed by individuals within this country are also eradicated. Continuous surveying of these areas can keep us up to speed with information and we can determine which controls need to be set in place in order to ensure that these occurrences are minimized.

Third Evaluation Method: Collecting Basic Data through Practical Evaluation

When we attempt to compare data we have to first collect data that is both qualitative and quantitative. The “Handbook of Practical Program” discusses the various types of evaluations that can be done. One practical evaluation method is the use of logic models. Specifically, a logic model “is a draft document that captures how the program works” (Hatry, Wholey, Newcomer). Figure 1.2.
Outcome

Figure 1.2 is a basic model utilized to estimate whether or not the goal in fact was reached. Because we do not have exact numbers at hand, we will input numbers to determine if the cost was well measured and if we utilized the resources thoroughly.

This basic model can be extremely complex when dealing with large areas of the infrastructure. The table above is a basic representation of how we can utilize this model in order to ensure that ration of cost and goals are equal and successful.

Conclusion

Evaluating a governmental infrastructure is quite complex and requires a multitude of procedures. In this case, I have described three which I believe best suit the banking infrastructure. We must make sure that our goals are not overfunded or underfunded; additionally, we will have to acknowledge the fact that we will need to be transparent in our findings to the public. They need to be aware of all the funding going to various aspects of a governmental security measures.
References


INTRODUCTION

In recent years, terrorists have become more sophisticated with their tactics involving improvised explosive devices (IEDs), technology, and their advancement in the training and smuggling of persons and weapons through techniques including money laundering, illegal immigration, and fraud. For the purposes of sustaining healthy human life amongst communities, particularly the United States, we have become increasingly more concerned with the threat of biological weapons being transported via cargo vessels.

Maritime security has been an area which has caused great concern and debate amongst politicians as to how secure our nation’s ports are and if we are doing enough to protect our maritime infrastructure. This last chapter discusses the implications of a potential bioterrorist attack. The United States will need to evaluate the following:

1. Most vulnerable ports and effects to homeland security and our nation’s citizens;
2. Security measures the Department of Homeland Security (DHS), U.S. Coast Guard (USCG), and other stakeholders are implementing into our maritime ports.

Threats of bio-nuclear and bio-chemical attacks could prove to be one of the most devastating events to hit since September 11th, 2001. Extremists have been using
technology and other methods to create chaos amongst western countries. The United States has become concerned with the possibility that a similar attack could occur on U.S. soil using devices similar to the IED’s used in the Madrid and London attacks. New techniques involve smaller attacks which occur simultaneously at multiple locations. We cannot dismiss potential threats even if they seem to be “far-fetched.” The following sections will give insight into the threats, the potential effects on human life and our maritime borders.

I. VULNERABILITY OF OUR PORTS

On April 6, 2012, the Government Accountability Office (GAO) issued a report on maritime security and its efforts to address reinforced security measures to our nation’s ports. It stated that the DHS predicts our ports support more than $700 billion of commerce each year. Any disruption could severely impact the economic health of this country and alter relationships with countries we trade with the most.

The USCG and the DHS are responsible for maintaining strategies implemented along our ports. Other stakeholders include private trading companies and worldwide governmental agencies which are responsible for securing the cargo as it ships to the United States. However, human error does happen and we cannot be certain that every container arriving into the United States has been checked for bombs, weapons, drugs, or other chemicals. The 2012 GAO report indicates that “As the lead federal agency for the Marine Transportation System (MTS), the U.S. Coast Guard is responsible for facilitating the recovery of the MTS following a significant transportation disruption, such as a
security incident or natural disaster, and working with maritime stakeholders for the expeditious resumption of trade. Area Maritime Security (AMS) Plans, which are developed by the Coast Guard with input from applicable governmental and private entities, serve as the primary means to identify and coordinate Coast Guard procedures related to prevention, protection, and security response, as well as facilitation of MTS recovery. In the aftermath of Hurricane Katrina, the Coast Guard conducted efforts to identify additional recovery-related elements and incorporate them within its AMS Plans to help ensure a consistent approach to MTS recovery and trade resumption. In addition, the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) required that AMS Plans include a Salvage Response Plan to ensure that waterways are cleared and port commerce is reestablished as efficiently and quickly as possible following a transportation security incident (TSI), among other things” (GAO, Maritime 2012).

This report makes clear that the DHS and the USCG among other stakeholders have a good handle on how to maintain security throughout our coastlines. However, we must understand and evaluate how human life is affected should there be an incident involving explosives, or bio-chemical weapons. This includes medical emergency response, communication response, evacuation response, and stakeholder mitigation response. Radiological blasts entering dense area coasts such as New York and New Jersey could be disastrous for a population at large.

With an estimated eight to ten million New Yorkers in the metropolitan area including, Manhattan, the Bronx, Brooklyn, Queens, Staten Island, and areas along New Jersey,
there are obvious concerns as to how we will be able to deliver emergency responses to these communities. With the population outnumbering emergency response centers by the millions, there is no way to tell how long it will take to dispatch and rescue countless number of citizens that could be affected by a bio-chemical or radiological attack. Given the close proximity of the ports to these dense populations, there is a need to acquire proper emergency response systems to mitigate a disaster site of this magnitude.

II. DIRECTIVES AND THREATS

The way chemical attacks infiltrate one internal system could be difficult to determine. Unlike explosive attacks, chemical attacks may not be visible to physical well-being. Predicting the outcome of a bio-nuclear attack is dependent upon information provided by intelligence agencies. The National Security Presidential Directive-43 (NSPD) and the Homeland Security presidential Directive-14 (HSPD) responds to any given domestic nuclear threats and the detections of such threats. There are specific goals in maintaining the safety and deterrence of having such attack occur: “To protect against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material in the United States, and to protect against attack using such devices or materials against the people, territory, or interests of the United States” (NSPD, 2005)

Figure 1.1

| NSPD-43 AND HSPD-14 (NSPD, 2005) | Continue to develop, deploy, and enhance | Threats to maritime will increase if we fall |
In addition to these directives, former president George W. Bush signed the HSPD-18 in 2007 regarding countermeasures against Weapons of Mass Destruction (WMD) which include chemical, biological, radiological, and nuclear agents (CBRN). Biodefense in the 21ST century has been growing rapidly. HSPD-18 addresses the countermeasures that should be implemented in a way without giving way to panic amongst government agencies. We must acknowledge that any form of detection, deterrence, and advancement in nuclear weapons must be treated differently as each scenario may require unique responses. This directive addresses such matters in that, “It is not presently feasible to develop and stockpile medical countermeasures against every possible threat. The development of vaccines and drugs to prevent or mitigate adverse health effects
caused by exposure to biological agents, chemicals, or radiation is a time-consuming and costly process.” In other words, we have to ensure that each countermeasure and its researching efforts build on the nation’s objectives in combating such threats. In doing so, the HSDP-18 suggests four objectives which address the countermeasures of WMDs:

Figure 1.2 (HSPD-18)

<table>
<thead>
<tr>
<th>Target threats that have potential for catastrophic impact on our public health and are subject to medical mitigation</th>
<th>In maritime area threats include the smuggling to weapons onto cargo ships from international ports that have weak security measures in place</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yield a rapidly deployable and flexible capability to address both existing and evolving threats</td>
<td>The USCG is the front line responder guarding our waters so must acquire advance knowledge on CBRN’s and the threat of exposure to these CBRN’s</td>
</tr>
<tr>
<td>Are part of an integrated WMD consequence management approach informed by current risk assessments of threats, vulnerabilities, and capabilities</td>
<td>Experts of WMDs may assist the USCG on board if necessary</td>
</tr>
<tr>
<td>Include the development of effective, feasible, and pragmatic concepts of operation for responding to and recovering from an attack</td>
<td>The communication lines between medical emergency response agencies and the DHS are crucial in order to sustain best emergency response times</td>
</tr>
</tbody>
</table>

Simply put, many objectives, visions, and strategies have been discussed throughout these preparations; however, we must focus on how we could mitigate an attack should it occur on U.S. soil. The response time and administration of emergency services depends on the communication, and transportation of vehicles, equipment, and personnel.

**III. HOW WE RESPOND TO AN ATTACK**

Structurally, our emergency response teams are trained to go into the field and sustain injuries to individuals in the shortest time possible. Timing is crucial. During September 11th, the FDNY and NYPD were criticized for having poor emergency communication
channels open which caused chaos amongst the injured. Part of the reason internal communication channels were inoperable was because the number of calls dialing into the emergency response systems were overriding the systems and causing a jam. Emergency channels used the same towers as used by the general public. Between the use of cell phones, land lines, and emergency communication channels it was nearly impossible to answer every call that was coming into these response centers.

CBRN’s are one of the most dangerous weapons known to man. The spread of radioactive material is extremely dangerous and we have to be able to respond to a threat that may be seen in the future. Other biological and chemical threats are toxic enough to spread viruses across stateliness. HSPD-18 addresses these types of agents and the impact of how dangerous it is to a human population.
### BIOLOGICAL THREATS:

(a) **Traditional Agents**: Naturally occurring toxins such as anthrax

(b) **Enhanced Agents**: Modified agents made from natural toxins.

(c) **Emerging Agents**: Unrecognized pathogens that might be naturally occurring such as the Severe Acute Respiratory Syndrome (SARS).

(d) **Advanced Agents**: Of biological nature that engineered in a laboratory to bypass traditional countermeasures or produce a more severe or otherwise enhanced spectrum of disease.

<table>
<thead>
<tr>
<th>RESULT:</th>
<th>Mass casualties.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Difficulty to eradicate</td>
</tr>
<tr>
<td>Threat to human life with minimal tools available to mitigate these agents.</td>
<td></td>
</tr>
<tr>
<td>Tools are not developed yet to detect and control man-made agents thus causing severe outbreaks with little treatment.</td>
<td></td>
</tr>
</tbody>
</table>

### NUCLEAR AND RADIOLOGICAL AGENTS:

(a) **Improvised Nuclear Devices**: Radioactive materials designed to result in the formation of a nuclear-yield reaction.

(b) **Radiological Dispersal Devices**: Devices, other than a nuclear explosive device, designed to disseminate radioactive material.

(c) **Intentional Damage or Destruction of a Nuclear Power Plant**: Damage to a reactor core and destruction of the containment facility of a nuclear reactor could contaminate a wide geographic area with radioactive material.

<table>
<thead>
<tr>
<th>RESULT:</th>
<th>Creating mass nuclear reaction reaching more areas than a localized community.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Creates chaos and pressures emergency crews to mitigate the situation.</td>
</tr>
<tr>
<td>Could cause nationwide contamination.</td>
<td></td>
</tr>
</tbody>
</table>

### CHEMICAL THREATS:

(a) **Toxic Industrial Materials and Chemicals**: Solid, liquid, or gaseous form

| Infiltration of these chemicals could lead to simultaneous attacks in a metropolitan |
that are used or stored for use for military or commercial purposes.

(b) **Traditional Chemical Warfare Agents:** Nerve agents historically developed for warfighter use.

(c) **Non-traditional Agents:** Chemical threat agents or toxicants requiring adapted countermeasures.

Physically debilitating materials could also be used on simultaneous attacks. Similar to warfare agents, this requires developing countermeasures.

If we are faced with an attack like this, the two most important elements are emergency response times and emergency response teams. Triage facilities, hospital vacancies, communication channels between government agencies and emergency response centers are crucial in addressing the most severe cases. We cannot afford to lose communication amongst these entities because of the time constraints and difficulty of managing a CBRN attack. There are four key factors which must work in order to facilitate a disaster site:

1. Hospitals must have plans;
2. Emergency call centers must have ample space to communicate amongst emergency response teams and government offices;
3. USCG must be able to stop incoming shipments from sea to prevent any possible future attacks;
4. We must have an abundance of vaccinations, tools, and equipment on site to work a triage center during a disaster.
The GAO’s report on hospital preparedness addresses the capacity for bioterrorism response. It also addresses the limited training personnel have to identify and diagnose biological agents. “Almost all hospitals reported participating in a local, state, or regional interagency disaster preparedness committee. In addition, most hospitals reported having provided at least some training to their personnel on identification and diagnosis of disease caused by biological agents considered likely to be used in a bioterrorist attack, such as anthrax or botulism” (GAO, Hospital 2003).

These reports are a cause for concern when dealing with response time and treatment.

Figure 1.4 below addresses what the staffing facility maintained:

**Urban Hospitals with Medical Equipment Capabilities, per 100 Staffed Beds**

(GAO, Hospital 2003)

<table>
<thead>
<tr>
<th>Ventilators</th>
<th>Percentage of Hospitals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 2</td>
<td>9%</td>
</tr>
<tr>
<td>2 to less than 5</td>
<td>33.9%</td>
</tr>
<tr>
<td>5 to less than 10 ventilators</td>
<td>39.7%</td>
</tr>
<tr>
<td>10 or more ventilators</td>
<td>17.4%</td>
</tr>
<tr>
<td><strong>Total Percentage of Hospitals</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal Protective Equipment (PPE) suits</th>
<th>Percentage of Hospitals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 2 PPE suits</td>
<td>38.2%</td>
</tr>
</tbody>
</table>
### PPE Suits Availability

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 to less than 5 PPE suits</td>
<td>24.8%</td>
</tr>
<tr>
<td>5 to less than 10 PPE suits</td>
<td>16.6%</td>
</tr>
<tr>
<td>10 or more PPE suits</td>
<td>20.3%</td>
</tr>
<tr>
<td><strong>Total Percentage of Hospitals</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

### Isolation Beds Availability

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 2 isolation beds</td>
<td>18.6%</td>
</tr>
<tr>
<td>2 to less than 5 isolation beds</td>
<td>47.3%</td>
</tr>
<tr>
<td>5 to less than 10 isolation beds</td>
<td>24.6%</td>
</tr>
<tr>
<td>10 or more isolation beds</td>
<td>9.5%</td>
</tr>
<tr>
<td><strong>Total Percentage of Hospitals</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

### Patient Load Through Decontamination Shower

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 2 patients per hour</td>
<td>15.3%</td>
</tr>
<tr>
<td>2 to less than 5 patients per hour</td>
<td>25.8%</td>
</tr>
<tr>
<td>5 to less than 10 patients per hour</td>
<td>28.4%</td>
</tr>
<tr>
<td>10 or more patients per hour</td>
<td>30.5%</td>
</tr>
<tr>
<td><strong>Total Percentage of Hospitals</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Almost ten years after this survey, there is still a concern as to whether hospitals have the capacity to accommodate victims of CBRN attacks.
IV. **USCG, DHS, & STAKEHOLDER RESPONSE.**

Private stakeholders can only be effective if government agencies effectively provide updated information to them. The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets (NSPPCIKA) drafted by the White House discusses challenges with guarding shipment cargos entering the United States. With over three hundred seaports in the United States, it will take more than just the USCG and DHS to secure the nation’s assets. This report suggests that much of the seaport areas represent a “significant protection challenge, particularly in the case of high consequence cargo. Physical and operational security guidelines have undergone a comprehensive review, from which DoT and DHS will issue guidance and recommendations for appropriate protective actions.”

Agreements among international authorities such as the International Maritime Organization (IMO) often provide support to the United States and help implement the rules and practices U.S. agencies use in order to protect our waters. The Department of Transportation (DOT) has recommended that there be “guidelines for passenger vessel and terminal security, including passenger and baggage screening and training of crews. The industry requires R&D for cost-effective technologies for the rapid detection of explosives and other hazardous substances, as well as for new vessel designs to minimize the likelihood of a ship sinking if it were attacked” (National, 2008). The DOT and USCG have initiated what is known was the Sea Marshal program and Maritime Safety and Security Team to assist in assessing and securing vessels at sea and the seaports. DOT has also participated with expediting “compliance with international standards to
enhance port, vessel and facility security. DOT is also working with U.S. Customs Service to implement the Container Security Initiative to ensure the security of shipping supply chain. Shipper who do not comply with outlined rules and regulations will be subject to greater scrutiny and delays when entering U.S. ports” (National, 2008) DHS and DOT have identified six initiatives to enhance maritime security. The six are included in the figure below:

Figure 1.5 (National, 2008)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Identify vulnerabilities, interdependencies, best practices, and remediation requirements</td>
</tr>
<tr>
<td>2.</td>
<td>Develop a plan for implementing security measures corresponding to varying threat levels</td>
</tr>
<tr>
<td>3.</td>
<td>Develop processes to enhance maritime domain awareness and gain international cooperation</td>
</tr>
<tr>
<td>4.</td>
<td>Develop a template for improving physical and operational port security</td>
</tr>
<tr>
<td>5.</td>
<td>Develop security and protection guidelines and technologies for cargo and passenger ships</td>
</tr>
<tr>
<td>6.</td>
<td>Improve waterway security</td>
</tr>
</tbody>
</table>

Each initiative builds upon previous strategies drafted by the White House and through Presidential Directives. The DHS and DOT have agreed to work closely in addressing security assessments in order to identify the vulnerabilities, and to work with other agencies involving “appropriate federal departments and agencies, port security committees, an private-sector owners and operators to develop or facilitate the establishment of security plans to minimize security risks to ports, vessels, and other maritime facilities” (National, 2008). Networking with other governmental agencies and other stakeholders improves the physical security of this nation’s maritime areas. With regards to international maritime challenges, DHS and DOT will work with “international
maritime organizations and industry to study and develop appropriate guidelines and technology requirements for the security of cargo and passenger ships” (National, 2008). These initiatives help improve the safety and security of our nation’s people and infrastructure. The development of relationships with organizations within the United States and abroad is critical to sustaining human life. The DHS, DOT, USCG and private stakeholders including hospitals, port operators, and nuclear scientists must work together in order to see change with the said initiatives.

Conclusion

The development of strategies, objectives, and goals are primarily depends on how the U.S. government implements security measures. In order for us to maintain the safety of our maritime infrastructure we must reach out to international organizations for assistance. This is a global effort and an attack does not only have an effect on our ports but it also affects those who live abroad. The United States’ economy is intertwined with the global economy. September 11th caused economic disaster resulting in a domino effect of economic disasters around the world. We have to be careful, we have to be vigilante, and we always have to be on our toes ready for anything. We may not be able to predict an imminent attack, but we can certainly gain intelligence by being transparent with stakeholders and government agencies. Public health affected by a possible bioterrorist attack could result in mass casualties, irreparable structural damage, and massive economic downfalls. We cannot sustain human life if we cannot sustain the risks involved in understanding and maintaining the security of our maritime infrastructure.
References


CONCLUSION

At the end of this project one may conclude that there are a multitude of infrastructures at risk. From a security standpoint there are still issues that clearly need to be addressed, and there are several components of our infrastructures that need to be closely analyzed. It is important to note that as years go by, technology gets more advanced, people get smarter, and information will be more readily available. If sensitive information and WMDs have fallen into the wrong hands, then we will have to do our best to foil an attack before it happens. Should an attack occur, then we will have to mitigate the effects. With innocent lives at risk there is no room for dismissive actions or political agendas. Terrorists have been responsible for wreaking havoc and killing thousands of lives. The lives lost in America and abroad are a direct result of terrorists able to fund, train, and develop smarter ways to attack our soldiers and innocent civilians. We must make it known to the terrorists that we have not become complacent and that our ties to other countries are stronger than ever. The awareness amongst the public is stronger and the assistance received by other agencies and other stakeholders has multiplied. Men and women in the government solemnly swear to “protect this country from all enemies both foreign and domestic.” This has been apparent even within the general public who take it upon themselves to notify authorities of suspicious activities. We are in this together, and together we can combat terrorism. With that said I leave you with this: the question is not if another attack will occur, but rather, when it does occur, will we be ready?