NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

QUANTITATIVE RISK ANALYSIS FOR HOMELAND SECURITY RESOURCE ALLOCATION

by

Christopher S. Reifel

December 2006

Thesis Advisor:	Kent Wall
Second Reader:	Raymond Roll

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE: Quantitative Risk Analysis for Homeland Security Resource Allocation	5. FUNDING NUMBERS
6. AUTHOR(S) Christopher S. Reifel	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

Defense against terrorism both at home and abroad has become a priority in the United States. As a result, resource allocation has also increased. However, even as resources increase, they are still finite. So the dilemma becomes how to efficiently allocate these limited resources. Currently the data, while abundant, is confusing. One suggested method is to allocate resources based on risk. However, there is virtually no guidance on how that risk should be defined or what the parameters are in a risk-based approach. Also, there is no flow of information model that outlines how to communicate to decision makers the risk reduction potential of each policy alternative.

This thesis investigates the usefulness of quantitative risk analysis as an approach to determine the allocation of counter-terrorism resources. This approach develops a simulation-based quantitative risk assessment method that allows for subjective elements and uncertainties. The risk assessment information is then integrated with the cost of the alternatives to yield a risk-reduction-cost-tradeoff curve that guides decision makers with resource allocation decisions. This approach is demonstrated by using the Port Security Grant Program as an example. We find that the approach provides the decision maker the information required to discover robust resource allocation solutions.

14. SUBJECT TERMS Homeland security, quantitative risk analysis, risk management, resource allocation, maritime security, port security	15. NUMBER OF PAGES 119
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

QUANTITATIVE RISK ANALYSIS FOR HOMELAND SECURITY RESOURCE ALLOCATION

Christopher S. Reifel
Major, United States Air Force
B.S., Purdue University, 1992
M.S., University of Colorado, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES (HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2006

Author: Christopher Reifel

Approved by: Kent Wall
Thesis Advisor

Raymond Roll
Second Reader

Dr. Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Defense against terrorism both at home and abroad has become a priority in the United States. As a result, resource allocation has also increased. However, even as resources increase, they are still finite. So the dilemma becomes how to efficiently allocate these limited resources. Currently the data, while abundant, is confusing. One suggested method is to allocate resources based on risk. However, there is virtually no guidance on how that risk should be defined or what the parameters are in a risk-based approach. Also, there is no flow of information model that outlines how to communicate to decision makers the risk reduction potential of each policy alternative.

This thesis investigates the usefulness of quantitative risk analysis as an approach to determine the allocation of counter-terrorism resources. This approach develops a simulation-based quantitative risk assessment method that allows for subjective elements and uncertainties. The risk assessment information is then integrated with the cost of the alternatives to yield a risk-reduction-cost-tradeoff curve that guides decision makers with resource allocation decisions. This approach is demonstrated by using the Port Security Grant Program as an example. We find that the approach provides the decision maker the information required to discover robust resource allocation solutions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

CAPPS	Computer Assisted Passenger Pre-Screening System
CBP	Capabilities-based Planning
COTP	Captain of the Port
DHS	Department of Homeland Security
DNI	Director of National Intelligence
GAO	Government Accountability Office
IAIP	Information Analysis and Infrastructure Protection
IED	Improvised Explosive Device
IG	Inspector General
MARAD	Maritime Administration
MARSEC	Maritime Security
MVD	Military Dynamite
ODP	Office of Domestic Preparedness
PDF	Probability Density Function
PMRM	Partitioned Multiobjective Risk Method
PRA	Probabilistic Risk Assessment
PSG	Ports Security Grant Program
OGT	Office of Grants and Training
QDR	Quadrennial Defense Review
QRA	Quantitative Risk Analysis
RMTWG	Risk Management Training Working Group
SBA	Small Boat Attack
SLGCP	State and Local Government Coordination and Preparedness
TIP	Targeted Infrastructure Protection
TNT	Trinitrotoluene
TSA	Transportation Security Agency
UASI	Urban Area Security Initiative
USCG	United States Coast Guard
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank the following for their contributions and support that enabled me to complete this thesis:

My two advisors, Dr. Kent Wall and CDR Ray Roll, for inspiring me with their expertise and guidance.

My family for their tremendous support, encouragement, and patience.

Dr. Ron Brown, from the Naval Postgraduate School and his colleague, Dr. William Walters from the Army Research Lab, for their assistance with blast modeling

The professional experts from the Naval Surface Warfare Center, Indian Head Division, and specifically Arthur Boyers, for their assistance with blast modeling.

The Blast/FX™ professionals at Northrop Grumman and the Transportation Security Administrations for their support and the use of the Blast FX software.

The professional men and women of the United States Coast Guard, Sector San Francisco, for their input on port security issues and their experiences with the Maritime Security Risk Assessment Model.

THIS PAGE INTENTIONALLY LEFT BLANK

I. BACKGROUND

A. THE TERRORIST THREAT TO THE HOMELAND

"We [Office of the Director of National Intelligence (DNI)] assess that al-Qa'ida will continue to pose the greatest threat to the Homeland and U.S. interests abroad by a single terrorist organization. We also assess that the global jihadist movement—which includes al Qa'ida, affiliated and independent terrorist groups, and emerging networks and cells—is spreading and adapting to counterterrorism efforts."[1] The DNI makes it clear that the terrorist threat to the U.S. is still very real and expanding. The document goes on to assess that the number of activists calling themselves jihadists is increasing in both number and worldwide dispersion and that if this trend continues, the threat to the U.S. will intensify. Clearly, terrorism remains a threat that must be taken seriously.

Evidence supporting the DNI's judgment is abundant. The pace and lethality of terrorist attacks have increased substantially since the terrorists attacks against the United States on September 11, 2001 (9/11) as compared to the 1990s.[2] Furthermore, nearly all statistics indicate an exponential increase in worldwide incidents of terrorism since 2002.[3] Indeed, it is only a matter of time before terrorists strike another significant attack on U.S. soil. America was fortunate to have escaped another airline attack in which terrorists were planning to smuggle explosives material onboard U.S.-bound airliners originating in Britain and detonate the explosives over the Atlantic Ocean. The plot was disrupted, in large part, due to successful counterterrorism work by British officials.[4] This instance clearly demonstrates terrorists' continued intent to attack America.

---

[1] Director of National Intelligence, Declassified Key Judgments of the National Intelligence Estimate "Trends in Global Terrorism: Implications for the United States" dated April 2006, available from http://www.dni.gov/press_releases/press_releases.htm (accessed 29 September 2006).

[2] Anonymous, *Imperial Hubris* (Washington, D.C.:Brassey's, 2004), 91.

[3] Derived from multiple databases. For example, see Memorial Institute for the Prevention of Terrorism (MIPT) database at http://www.tkb.org/Home.jsp (accessed 16 September 2006). Also see National Counter Terrorism Center (NCTC) database at http://wits.nctc.gov/ (accessed 18 September 2006)

[4] John Ward and Karen DeYoung, "Plot to Bomb U.S.-Bound Jets is Foiled: Britain Arrests 24 Suspected Conspirators," *The Washington Post Foreign Service*, 11 August 2006, available from http://www.washingtonpost.com/wp-dyn/content/article/2006/08/10/AR2006081000152.html (accessed 25 August 2006).

The threat to America extends beyond the use of airlines as the attack method and includes other methods and weapons, such as weapons of mass destruction, computer viruses, and ships. Other delivery means include the maritime domain, border exploitation, food sources, water supplies, and computer networks. These delivery means create a significant dilemma due to the vast amount of options that exist. The wide range of delivery means are made possible in part by America's open society, which facilitates people entering the United States, and which also facilitates the movement of goods and services to and from the United States. This has led to an increased attention to border security, which includes not only land borders but also water borders. Moreover, the movement of vast amounts of goods demands that cargo flow freely and efficiently into the country either by air, land, or sea transportation modes. All of these transportation methods have inherent vulnerabilities. One can argue that all of these areas of vulnerability deserve security funding. The challenge is to determine how to prioritize and in what proportions to allocate funding.

B. THE RESOURCE ALLOCATION PROBLEM

"America remains dangerously unprepared to prevent and respond to a catastrophic terrorist attack on U.S. Soil." This statement, written by Stephen Flynn in his book *AMERICA the Vulnerable: How Our Government is Failing to Protect Us from Terrorism*, echoes the findings of an independent, bipartisan group formed by the Council on Foreign Relations to evaluate the state of homeland security in the United States.[5] Flynn's main theme is that America needs to do more to protect itself from terrorism. This is not an uncommon theme in the literature. Accordingly, the money spent each year on homeland security is rising at nearly double the rate of inflation.[6] Despite increased spending, homeland security resources are still finite, and there needs to be more focus on how to

[5] Stephen Flynn, *AMERICA the Vulnerable: How Our Government is Failing to Protect Us from Terrorism* (New York: HarperCollins, 2004), ix.

[6] Derived from U.S. Department of Labor Bureau of Labor Statistics and U.S. Department of Homeland Security, *Budget-in-Brief: Fiscal Year 2006*, available from http://www.dhs.gov/xlibrary/assets/Budget_BIB-FY2006.pdf (accessed November 2, 2006). The consumer price index rose 3.4% in 2004 and 3.8% in 2005. For the same years, the DHS budget increased 8.1% and 6.6%, respectively.

effectively utilize these limited resources and less focus on allocating more resources. Moreover, as the homeland security budget continues to rise, so does the public's interest in how this money is being spent.[7]

1. Resource Allocation for Homeland Security

Deciding how to effectively allocate limited resources to improve security is not an easy task. One of the traditional approaches to security planning has been scenario-based planning in which planners determine a likely threat scenario and a suitable means to defend against it. However, scenario-based planning is extremely challenging when defending against the asymmetric threat of terrorism due to its uncertainty as to the specific nature of the threat. To account for this uncertainty, Sharon Caudle, a senior analyst with the U.S. Government Accountability Office's Homeland Security and Justice Team, advocates capabilities-based planning as one of the better approaches to resource allocation and results management.[8] Paul Davis, of the RAND Corporation, defines capabilities-based planning as "planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances, while working within an economic framework."[9] The Department of Defense (DOD) has been using capabilities-based planning for several years, and the Department of Homeland Security (DHS) has recently adopted it as well.[10] According to DHS, capabilities-based planning differs from scenario-based planning and is intended to balance the threat and magnitude of a potential terrorist attack with the resources required to prevent and respond to them.[11] DHS is using this approach to identify required capabilities needed to defend against a wide array of threats and provide a feedback loop to measure success in achieving them.[12]

---

[7] Ralph Perl, *CRS Report for Congress: Combating Terrorism: The Challenge of Measuring Effectiveness* (Washington, D.C.: Congressional Research Service, 2005), 1-2, available from: http://www.opencrs.com/document/RL33160/ (accessed 28 November 2005)

[8] Sharon Caudle, "Homeland Security, Approaches to Results Management," *Public Performance & Management Review* 28 no. 3 (March 2005), 369.

[9] Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation* (Santa Monica, CA: RAND Corporation, 2002), 1.

[10] Ibid.

[11] U.S. Department of Homeland Security, *Fact Sheet: Strengthening National Preparedness: Capabilities-Based Planning*, 1. Available from http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm (accessed December 6, 2005)

[12] Ibid., 1.

In addition to using capabilities-based planning, DHS has endeavored to use risk management to help guide spending efforts. This is partially attributable to the notion that "Risk management has received widespread support and interest from Congress, the President, and the Secretary of DHS as a tool that can help set priorities on how to protect the homeland."[13] Moreover, DHS has been directed to use risk-based planning to help guide spending efforts.[14] This direction is based on an abundance of policy guidance that recommends, directs, or merely supports the idea of a risk-based approach to resource allocation. For example, in Homeland Security Presidential Directive 7 (HSPD-7), the President states: "[I, The President of the United States] encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources."[15] In addition to HSPD-7, several strategy documents have echoed and expanded upon the notion of risk management strategies.

The National Strategy for Homeland Security, released in July 2002, establishes a foundation upon which to organize homeland security efforts and provides initial guidance on how to prioritize related efforts including resource allocation. The Strategy identifies three strategic objectives for homeland security: prevention, protection, and response. These equate to the prevention of terrorist attacks within the United States, protection by reducing America's vulnerability to terrorism, and response in order minimize the damage and effectively recover from attacks that do occur.[16] The benefits of devoting resources to homeland security will be a reduction in risk of future terrorist attacks as well as the consequences should such an attack occur. To assist decision makers on how to prioritize homeland security efforts, the Strategy provides guidance aimed at channeling resource allocation for homeland security.

---

[13] U.S. Government Accountability Office (GAO), *Risk Management, Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure* (Washington, D.C.: GAO, December 2005), 19.

[14] Ibid., 20.

[15] President of the United States, *Homeland Security Presidential Directive/HSPD-7* (December 2003), available from http://www.whitehouse.gov/ (accessed 15 March 2006).

[16] President of the United States, *National Strategy for Homeland Security* (July 2002), 2-3, available from http://www.whitehouse.gov/ (accessed 15 March 2006).

The Strategy defines financial costs as "the amount of money, manpower, equipment, and innovative potential that must be devoted to homeland security."[17] These resources should be allocated with two goals in mind: to devote the right amount of resources to homeland security, and to spend those resources on the correct activities.[18] Furthermore, the Strategy specifies that in order to spend the resources on the correct activities, policymakers should allocate resources in such a way that the value gained is spread evenly across all sectors.[19] This should be done with an attempt to equalize the value of risk mitigation per dollar.[20] The right amount of resources should be determined by evaluating the benefit of reducing risk versus the additional cost while realizing that it is not practical to eliminate all risks. Given the impracticality of eliminating all risks, decision makers need to establish an acceptable level of risk.

The idea that risk cannot be eliminated is further supported in other literature. For example, the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* outlines a plan to reduce America's vulnerability to attacks on critical infrastructure, stating "… we [the U.S. population] must accept some level of terrorist risk as a persisting condition in our daily lives."[21] Likewise, the 9/11 Commission released their final report in 2004 and made several recommendations that involved using a risk-based approach. The Commission states that America can be attacked in many ways and is still very vulnerable, and that no defense or protective measure is perfect. The risks must be calculated in an effort to guide decision makers in making hard choices as to where to allocate resources.[22] One of the specific recommendations made by the 9/11 Commission is in the area of transportation security. The Commission recommends that "the U.S. Government should identify and evaluate transportation assets that need to be protected, set

---

[17] President of the United States, *National Strategy for Homeland Security*, 63.

[18] Ibid., 63.

[19] Ibid., 64.

[20] Ibid., 76.

[21] President of the United States, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003), 13, available from http://www.whitehouse.gov/ (accessed Aug 11, 2006).

[22] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York, NY: W.W. Norton, 2004), 365.

risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort."[23]

2. Critique of Homeland Security Spending

The 9/11 Commission, in the course of providing their recommendations, was quick to point out early fallacies with homeland security spending. One particular example involves how DHS is allocating funds to assist state and local governments in their security efforts. The Commission makes reference to one DHS methodology in which every state receives a minimum amount of funds regardless of any other criteria and another DHS methodology in which funds are allocated based on population size. The Commission cautioned against allowing federal homeland security assistance to remain a program for general revenue sharing. Furthermore, the Commission cautioned that homeland security is too important for "politics as usual," and that Congressional representatives should not use these funds as a "pork barrel" to protect the interests of their home states or districts. In light of this, the 9/11 Commission recommended that "homeland security assistance should be based strictly on an assessment of risks and vulnerabilities."[24]

In December 2005, the 9/11 Public Discourse Project delivered another blow to policymakers regarding the 9/11 Commission's recommendations when they gave Congress and DHS a failing grade on distribution of homeland security funding to states. They found:

> Congress has still not changed the underlying statutory authority for homeland security grants or benchmarks to insure that funds are used wisely. As a result, homeland security funds continue to be distributed without regard for risk, vulnerability, or the consequence of an attack, diluting national security benefits of this important program.[25]

Eben Kaplan, a research associate for the Council on Foreign Relations, further critiques DHS grant spending. He discusses grant program criticisms directed at DHS for wasteful expenditures and also highlights the need for a different approach to resource

---

[23] National Commission on Terrorist Attacks Upon the United States, 391.

[24] Ibid., 396.

[25] 9/11 Public Discourse Project, *Final Report on 9/11 Commission Recommendations* (December, 2005), 1. Available from http://www.9-11pdp.org, accessed 5 October 2006.

allocation.[26] He reviews the old methods for distributing DHS funds that awarded funds using a population-based formula that ensured each state received a minimum amount of funds. Members of Congress capitalized on the old distribution plan to funnel DHS money to their constituents at home. For example, the town of North Pole, AK with a population of 1,700, received a grant of $557,400.[27] In another instance, the city of Santa Clara, CA used DHS funds to purchase a fleet of Segway scooters for their bomb squad.[28] Kaplan goes on to discuss how DHS is acknowledging these shortfalls in its resource allocation methodology and is attempting to move toward an objective risk-based approach. Moreover, Secretary Chertoff is quoted as saying that "as we focus on the reality of what we're trying to protect … we're going to increasingly be looking to … approaches that put politics to one side and talk about real tangible things like risk."[29]

3. Resource Allocation in Maritime Security

Maritime security, specifically port security, is one area where DHS has attempted to implement risk-based resource allocation. One of the challenges with port security resource allocation is the large number stakeholders involved. The federal government has jurisdiction over interstate and foreign commerce and some waterway channels. Jurisdiction over ports resides with state and local governments. Furthermore, ports can be a subsidiary of a public agency or structured under the private sector. As a result, security at the ports varies. Either municipal law enforcement or private port police can be the primary instrument of port security. On the other hand, the consequence of a failure in port security extends well beyond local municipalities and involves numerous federal agencies.[30]

The two primary Federal agencies involved in port security are the U.S. Coast Guard and the Bureau of Customs and Border Protection. The U.S. Coast Guard is the principal maritime law enforcement authority and the lead federal agency for the maritime

---

[26] Eben Kaplan, "Risk-based Homeland Security Spending," Council on Foreign Relations online article, 8 February 2006, available from http://www.cfr.org/publication/9806/ (accessed 27 February 2006)

[27] Kaplan.

[28] Ibid.

[29] Ibid.

[30] John Fritelli, *Port and Maritime Security: Background Issues for Congress* (Washington D.C.: Congressional Research Service, 2005), 9, available from: http://www.mipt.org/pdf/CRS_RL31733.pdf (accessed 16 March 2005).

component of homeland security.[31] Additional players routinely include the Transportation Security Agency (TSA) and the Maritime Administration (MARAD).

It is important to understand the roles and motivations of different stakeholders in maritime security, because each has their own resources and funding. For example, the USCG and TSA both have programs focused on improving port security yet they have unique funding sources. The state and local agencies involved in port security are more complicated. Their funding for port security comes in the form of DHS grant money from a combination of TSA and Office of Domestic Preparedness (ODP) funds. ODP awards grants under Urban Area Security Initiative (UASI), and TSA awards grants through their Port Security Grant Program.[32] The TSA portion of grant awards was eventually taken over by DHS' Information and Analysis and Infrastructure Protection Directorate (IAIP). What remains, are three federal agencies playing key rolls in port security improvement—USCG, TSA, and IAIP. Furthermore, federal law and HSPD-7 call for the use of a risk-based approach for port security resource allocation, [33] but provide limited guidance on what such an approach should look like. Despite this lack of guidance, each the USCG, TSA, and IAIP have taken steps toward implementing a risk-based approach for port security resource allocation.

In December 2005, the GAO evaluated agency progress in adopting a risk-based approach for port security. The GAO found that the USCG, ODP and the IAIP have made some progress, with the USCG making the most progress, in utilizing risk management for resource allocation. However, numerous challenges remain. The GAO found that the USCG has identified strategic goals as they relate to preventing a terrorist attack and vulnerability to terrorism in the maritime domain. The USCG has also made progress by identifying and evaluating security alternatives at the individual port level. Furthermore, the USCG has completed three major security assessments at the port level, which has facilitated an understanding of how to prioritize risks within a port. However, the GAO

---

[31] Fritelli, 9.

[32] U.S. Department of Homeland Security Office of Inspector General, *Review of Port Security Grant Program* (Washington, D.C.: Department of Homeland Security, January 2005), 5.

[33] U.S. Government Accountability Office, *Risk Management, Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, (Washington, D.C.: GAO, December 2005), 5.

concludes that the USCG risk-based approach lacks sufficient information to represent threats, vulnerabilities, and consequences associated with port security. More importantly, the GAO concludes that the USCG risk-based approach falls short in showing how the application of resources can be effective at reducing risk and producing the most favorable cost-benefit outcome.[34]

Similar to the Coast Guard, ODP has made progress in using risk management for resource allocation. They have set broad risk management goals that support a wide range of maritime goals, such as harbors, ports, and coastal approaches. ODP has carried out risk assessments and evaluated mitigation options to help determine which ports should receive priority for grants. Additionally, they have developed a risk-based grant selection process for awarding DHS grant money to corporations involved in homeland security projects. However, the GAO concludes that ODP has fallen short in developing a risk-based approach that allows risks to be compared and prioritized among ports.[35]

IAIP has made limited progress in using risk management for resource allocation. They have experienced difficulty in conducting risk assessments of critical infrastructure to determine the risks of certain types of terrorist attacks. The initial tool for completing this task was the Risk Analysis and Management for Critical Asset Protection, which fell short of accomplishing the task.[36] The IAIP has since begun to develop a National Comparative Risk Assessment that will examine risks within and across various sectors. This assessment is scheduled to produce the initial results by the end of 2006. The IAIP has cited challenges with a risk management approach to resource allocation. The challenge is the lack of information from other federal agencies, specifically, information that assesses the likelihood of various threat scenarios involving critical infrastructure attacks.[37]

In summary, the GAO's report indicated that the USCG, ODP, and IAIP have made progress in adopting a risk management framework for effective resource allocation, but the progress has been limited and challenges remain. One possible reason for this is a lack

[34] U.S. Government Accountability Office, *Risk Management, Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, (Washington D.C.: GAO, December 2005), 10.

[35] Ibid., 11

[36] Ibid., 77-78.

[37] Ibid., 12.

of sufficient guidance on how to implement a risk management framework. Missing from the GAO report is that each of the agencies reviewed do not address the challenge of communicating risk analysis results to a decision maker. This is important since the decision maker needs to make resource allocation decisions based on the risk analysis results. The decision maker may not fully understand the methods employed in risk analysis or how to interpret the results. Thus, it is essential to communicate risk analysis results in a clear manner that leads the decision maker through the assumptions and results.[38]

C. RESEARCH ISSUES TO ADDRESS

There are two primary issues to be addressed concerning the use of a risk-based approach for homeland security resource allocation. First, there has been an abundance of federal-level guidance directing the use of a risk-based methodology but little guidance on what such an approach should look like.[39] Thus, it is necessary to develop a method by which risk can be quantitatively assessed and determine the feasibility of the method for homeland security resource allocation. Specifically, what is needed is a quantitative analysis that incorporates methodology accounting for at least some of the subjectivity and uncertainties that are inherent in risk analysis. Most analysts commonly associate risk quantification with assigning a single value to represent a risk component or the aggregation of several risk components. This is not optimal in that most aspects of homeland security involve uncertainty,[40] or random variables which are better represented using a range of values.[41] This uncertainty and the associated range of values require the use of distribution functions which in turn requires mathematical modeling.[42]

---

[38] David Vose, *Quantitative Risk Analysis: A Guide to Monte Carlo Simulation Modeling* (New York: John Wiley & Sons, 1996), 267-268.

[39] U.S. Government Accountability Office, *Risk Management, Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure* (Washington D.C., GAO, December 2005), 5.

[40] U.S. Department of Homeland Security, *National Preparedness* Guidance (Washington D.C., Department of Homeland Security, April 2005), 5.

[41] James R. Evans and David L. Olson, *Introduction to Simulation and Risk Analysis* (Upper Saddle River, New Jersey: Prentice Hall, 2002), 69.

[42] A distribution is defined as a set of numbers collected from a well-defined universe of possible measurements arising from a property or relationship under study. *The American Heritage Dictionary*, 2d Edition (Boston: Houghton Mifflin Company, 1982), 411. For more information on mathematical modeling and distribution functions, see also Evans and Olson, 3-6 and 69-88.

The second research issue centers on communication. How does an analyst communicate quantitative risk analysis results to a decision maker in such a way as to be understandable and in a manner that allows a decision maker to evaluate risk reduction potential given multiple policy alternatives? The decision maker needs to be able to allocate the budget in such a way that the maximum risk reduction is achieved, given a fixed budget.

Developing a quantitative risk analysis methodology for resource allocation is not without its challenges. This methodology first requires a definition of risk, as there is currently no single agreed upon definition of risk. Given an operational definition for risk, we next must quantify, or measure, the risk. Once given the capability to quantify risk, we can then proceed to assess the risk associated with the various alternatives. This, in turn, requires a way to translate risk into management action. In other words, how do policymakers use quantified risk to evaluate policy alternatives? If these steps can be accomplished and operationalized, then there will exist a way to rationally allocate resources in such a way as to achieve the greatest risk reduction for the given amount of available resources.

D. THE PROPOSED APPROACH

This thesis will investigate the usefulness of quantitative risk analysis as an approach to support decision makers in the allocation of counterterrorism resources. Furthermore, this approach will present a cost tradeoff analysis that highlights the robustness of resource allocation alternatives. To explore these concepts, the author uses the Port Security Grant Program (PSG) as a resource allocation case study.

This research is important because misallocation of homeland security resources can have serious implications. Allocating resources based solely on equity considerations, as has been done in the past,[43] gives insufficient protection to high-risk targets while providing overabundant protection to very low risk targets. Homeland security policymakers should have the means to connect resources allocated to risk. Specifically, they need a way to assess how resource allocation affects risk reduction. Risks can be

[43] Shawn Reese, *Homeland Security Grants: Evolution of Program Guidance and Grant Allocation* Methods (Washington, D.C.: Congressional Research Service, 2006), 22.

difficult to eliminate, but risks can be reduced to acceptable levels.[44] Ultimately, policymakers must determine the level of risk they can accept and allocate available resources to reduce the risks to achieve this.

In addition to risk reduction, policymakers need to find allocations that are robust to changes in the threat. Take for example the terrorist threat involving WMD, which can take at least three forms: nuclear, biological or chemical. Allocating resources to achieve an acceptable level of risk with respect to nuclear threats may lead to unacceptable levels of risk from the other two forms of threat. If the biological or chemical threat manifests itself, then the nation may experience unacceptable damage. Policymakers need to have a way to investigate this robustness concern. Importantly, policymakers need to know if there are resource allocations that yield acceptable levels of risk across a range of threats since it is difficult to predict what threat might prevail.

[44] President of the United States, *The National Strategy for Homeland Security*, 2.

II. LITERATURE REVIEW

A. OVERVIEW

This chapter presents a review of the risk literature and existing methodologies. The review begins with a descriptive analysis of the basic definitions of risk and its historical origins. Next the author examines the evolution of risk within specific industries, notably addressing the key industries in which risk analysis methodologies have played a key role and are still present to this day. The author then describes and evaluates attempts to implement risk-based methodologies in homeland security. Finally, the author provides and analysis of the Port Security Grant Program which is a specific program within DHS that utilizes QRA.

B. DEFINING RISK

Existing approaches to risk management hinge upon the how risk is defined. Several definitions of risk can be found in the literature. The word risk itself comes from the Italian word *risicare* (to dare).[45] The American Heritage Dictionary defines risk as "The possibility of suffering harm or loss; danger; a factor, element, or course involving uncertain danger; hazard."[46] The Society for Risk Analysis defines risk as "The potential for realization of unwanted, adverse consequences to human life, health, property, or the environment; estimation of risk is usually based on the expected value of the conditional probability of the event occurring times the consequence of the event given that it has occurred."[47] One other way to view risk is "any uncertainty that affects a system in an unknown fashion whereby the ramifications are also unknown but bears with it great fluctuation in value and outcome."[48] While these definitions use different wording, the theme is consistent in that risk involves an undesirable event that leads to unwanted consequences.

---

[45] Peter L Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: John Wiley & Sons, 1996), 8.

[46] *The American Heritage Dictionary*, Second College Edition (Boston: Houghton Mifflin Company, 1982), 1065.

[47] Society of Risk Analysis, available from http://www.sra.org/resources_glossary_p-r.php (accessed 20 July 2006).

[48] Johnathan Mun, *Applied Risk Analysis: Moving Beyond Uncertainty in Business* (Hoboken, New Jersey: John Wiley & Sons, 2004), 26-27.

Beyond the basic definition of risk itself, some experts have offered definitions for the broader concept of risk analysis. Vlasta Molak, in *Fundamentals of Risk Analysis and Risk Management* offers the following: "Risk analysis is a body of knowledge (methodology) that evaluates and derives a probability of an adverse effect of an agent (chemical, physical, or other), industrial process, technology, or natural process."[49] She goes on to point out that an "adverse effect" can be defined in many different ways. Some examples include fatalities, injures, a failure of an industrial component such as a power plant, or a loss of revenue.[50]

Another term often used synonymously with risk analysis is risk management. While not specifically defining risk management separately, Molak provides a distinction in that risk management deals with overall strategies for handling risk not just assessing risk.[51] She refers to the insurance industry as one of the early examples where risk management strategies emerged.[52] In a slightly different perspective, Peter Bernstein offers a way to look at risk management which is to focus on "areas where we have some control over the outcome while minimizing the areas we have absolutely no control over the outcome and the linkage between effect and cause is hidden from us."[53]

C. THE HISTORY OF RISK

Given the definitions of risk and the associated risk analysis and risk management spin offs, the reader can gain additional insight from a review the fundamental origins of risk. Some date early acknowledgment of the existence of risk back to the Athenians over 2400 years ago. Terje Aven, in *Foundations of Risk Analysis*, quotes an excerpt from Pericle's Funeral Oration in Thurcydidas' "History of the Peloponnesian War":

> We Athenians in our persons, take our decisions on policy and submit them to proper discussion. The worst thing is to rush into action before consequences have been properly debated. And this is another point where we differ from other people. We are capable at the same time of taking risks and assessing them beforehand. Others are brave out of ignorance; and

[49] Vlasta Molak, "Introduction and Overview," in *Fundamentals of Risk Analysis and Risk Management* ed. Vlasta Molak (New York: Lewis Publishers, 1996), 1.

[50] Molak, 1.

[51] Ibid., 4.

[52] Ibid.

[53] Bernstein, 197.

> when they stop to think, they begin to fear. But the man who can most truly be accounted brave is he who best knows the meaning of what is sweet in life, and what is terrible, and he then goes out undeterred to meet what is to come.[54]

While the Athenians showed a basic understanding of risk, they had no real way to measure risk since they had no real number system. In the words of Bernstein, "the only way to deal with risk [in those days] is to appeal to the gods and their fates."[55]

As risk analysis grew over the years it has become more rooted in probability theory.[56] Part of this is due to the Hindu-Arabic numbering system which provided the roots for today's modern conception of risk.[57] Additionally, there were several key milestones that have led to the incorporation of more probability theory in risk analysis. In the 1600s, Blaise Pascal introduced probability theory and Edmond Halley came up with the concept of life-expectancy tables. Then in 1792, Pierre Simon de LaPlace used a rudimentary form of quantitative analysis to determine the likelihood of death without a smallpox shot.[58] As risk analysis continued to grow into the 20th century, there emerges obvious distinctions in the various applications of risk. These various distinctions are embraced by key applications, some of which are examined in the next section.

D. KEY APPLICATIONS

This section examines a sample of the key industries containing significant risk analysis work. The author explores three primary industries: finance, nuclear, and defense. In most cases, risk concepts found their way into each of these industries as a result of scholarly research or safety studies and the concepts remain present to this day.

1. Finance Industry

Much of the early work with respect to risk and the financial industry can be attributed to Harry Markowitz:

> In, 1952, Nobel Laureate Harry Markowitz, then a young graduate student studying operations research at the University of Chicago, demonstrated

[54] Terje Aven, *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective* (England: John Wiley & Sons, 2003), 1

[55] Bernstein, xxiii.

[56] Molak, 4.

[57] Bernstein, 3.

[58] Molak, 4.

> mathematically why putting all your eggs in one basket is an unacceptably risky strategy and why diversification is the nearest an investor or business manager can ever come to a free lunch. [59]

Markowitz made his name in the financial industry when we published an article in the *Journal of Finance* entitled "Portfolio Selection." The paper was so influential that it earned Markowitz a Nobel Price in Economic Science in 1990. The premise of his paper was that investors should focus on the complete wealth strategy and not just on individual security holdings. The primary objective of his "Portfolio Selection" was to present investors with the thought that "expected return is a desirable thing and variance of return an undesirable thing."[60] While Markowitz made no specific mention of the word risk, it has since become synonymous with variance, or the "undesirable thing."[61] Markowitz's work would end up providing the foundation for all future theoretical finance work.[62]

The concepts introduced by Markowitz were further expanded upon by experts such as William Sharpe and others. Sharpe is responsible for introducing the *Capital Asset Pricing Model*, which essentially expresses the concept that higher levels of risk equate to higher expected returns.[63] The combined work of Markowitz and Sharpe brought forth the concept of an optimally balanced portfolio, in which an investor could choose a portfolio that provided the best bang for the buck given their risk tolerance. To analyze this concept of a balance between risk and return required a method by which risk could be measured.[64] This idea of measuring risk is discussed in greater detail later in this chapter.

2. Department of Defense

Risk management has been used in the Department of Defense (DOD) for years but has been illuminated even more recently with the release of the 2001 Quadrennial Defense Review (QDR).[65] This report was significant in that the Department presented a new strategy-driven risk management framework that formed the foundation for much of the

[59] Bernstein., 6.

[60] Ibid., 252.

[61] Ibid.

[62] Ibid., 257.

[63] Mun, 28.

[64] Ibid.

[65] U.S. Department of Defense, *Quadrennial Defense Review Report* (30 September 2001), 64, available from http://www.defenselink.mil/qdr/ (accessed October 27, 2006).

QDR defense program.[66] The framework is introduced with the following excerpt highlighting the importance of the new framework:

> Managing risk is a central element of the defense strategy. It involves balancing the demands of the present against preparations for the future consistent with the strategy's priorities. It entails assuring allies and friends, deterring threats of coercion and aggression, and, when necessary, defeating adversaries. It involves maintaining military advantages and developing new military competencies while dissuading future military competitors.[67]

The DoD framework consists of four related dimensions:[68]

- Force management [risk] – the ability to recruit, retain, train, and equip sufficient numbers of quality personnel and sustain the readiness of the force while accomplishing its many operational tasks;
- Operational [risk] – the ability to achieve military objectives in a near-term conflict or other contingency;
- Future challenges [risk] – the ability to invest in new capabilities and develop new operational concepts needed to dissuade or defeat mid-to long-term military challenges; and
- Institutional [risk] – the ability to develop management practices and controls that use resource efficiency and promote the effective operation of the Defense establishment.

The general strategy for implementing this framework is to identify the risks within each dimension and then determine how to mitigate them. The framework facilitates tradeoff analysis among basic objectives and resource constraints. Furthermore, by evaluating DoD in these dimensions, the DoD is focusing on issues concerning force development, key capabilities, and force sustainability.[69]

The subsequent QDR, released on February 6, 2006, references the previously established risk management framework in the context of "balancing near-term demands against preparations for the future."[70] Furthermore the Department is evaluating an option to incorporate a risk-based approach into the acquisition process in place of the current

[66] U.S. Department of Defense, *Quadrennial Defense Review Report* (30 September 2001), 64, available from http://www.defenselink.mil/qdr/ (accessed October 27, 2006).

[67] Ibid., 57.

[68] Ibid., 57-58.

[69] Ibid., 58.

[70] U.S. Department of Defense, *Quadrennial Defense Review Report*, (6 February 2006), 70, available from http://www.defenselink.mil/qdr/ (accessed October 27, 2006).

cost-based approach.[71] The Chairman's Assessment summarizes the Departments overall position on risk assessment as a necessary component of the QDR Strategy given the uncertain nature of the security environment of 2025. He states "we must hedge against this uncertainty by identifying and developing a broad range of capabilities."[72] In other words, we accept risk when assessing which capabilities to pursue in the face of an uncertain future.

3. Nuclear Industry

Risk management principles have touched other industries beyond finance. Molak breaks some of these down and offers six types of risk analysis: chemical risk analysis, cancer risk analysis, epidemiologic risk analysis, probabilistic risk analysis (chemical or nuclear safety), and qualitative risk analysis. Of these, the nuclear power industry provided the most relevant contribution for the study conducted in this thesis—it provided the source for concepts in probabilistic risk assessment. In doing so, the nuclear power industry provides some of the early examples through the use of full-scope risk assessments. The term "full-scope" implies that these assessments combined engineering modeling to quantify the threat and also an analysis of the undesirable outcomes.[73] Similar terms have since become widely used, one of which is quantitative risk analysis (QRA).

E. QUANTITATIVE RISK ANALYSIS

Initial risk concepts in industry were primarily qualitative and have since evolved into more quantitative. This section analyzes existing quantitative risk analysis methodologies beginning with the prominent pioneers in the field and includes a descriptive analysis of the associated academic literature.

QRA is a concept originally developed based on a nuclear reactor safety study sponsored by the Nuclear Regulatory Commission in 1975.[74] Stanley Kaplan and John Garrick are two of the original pioneers of QRA and ventured to analyze risk by attempting

---

[71] U.S. Department of Defense, *Quadrennial Defense Review Report*, (6 February 2006), 71, available from http://www.defenselink.mil/qdr/ (accessed October 27, 2006).

[72] Ibid., A-6

[73] B. John Garrick "Risk Management of the Nuclear Power Industry," in *Fundamentals of Risk Analysis and Risk Management*, ed. Vlasta Molak (New York: Lewis Publishers, 1996), 328.

[74] Ibid., 334

to determine what the future will entail given a certain course of action (or inaction).[75] They define risk as a "triple {e, p, x}" whose values are given by the answer to three questions: (1) "What can happen?" (2) "How likely is it to happen?" (3) "If it does happen, what are the consequences?"[76] To answer these questions, one must develop a list of scenarios and for each, identify the probability of that scenario occurring and then identify the consequence should that scenario occur. For example, one might consider the undesirable event of a hurricane. The scenarios for a hurricane can be represented by the categories one through five with five being the worst. The likelihood of occurrence and associated consequences can be derived from historical data which shows that higher category hurricanes are less probable than lower category storms. Conversely, the consequences run opposite to the probabilities. The higher category storm yields the worse consequences and the lowest category storm yields the least consequences. Given all the possible scenarios, the probabilities can be combined to represent a cumulative probability which is then used to generate the combined risk of hurricane damage.

Kaplan and Garrick also point out an important distinction when considering the ideas of probability and consequences in that it is common to hear risk described as a product of probability and consequence (probability x consequence).[77] They suggest that this is misleading and recommend thinking in terms of the probability distribution of the consequence. One way to conceptualize this point is to go back to the hurricane example. If one were to take a low probability/high consequence scenario and a high probability/low consequence scenario, the product of probability and consequence in both cases could be the same. In reality, the two cases are quite different.

Since Kaplan and Garrick established a portion of the founding framework for quantitative risk analysis, others have gone on to build upon and expand on their work. One particular case is the work of E. Pate-Cornell who addresses a way to view uncertainty and offers six levels of risk analysis. She approaches the uncertainty challenge in risk

---

[75] Stanley Kaplan and B. John Garrick, "On the Quantitative Definition of Risk," *Risk Analysis* 1, no. 1 (1981), 13.

[76] Ibid., 13.

[77] Ibid.

analysis by dividing uncertainty into two categories: epistemic and aleatory.[78] Epistemic uncertainty results from a lack of fundamental knowledge or lack of a commonly accepted approach.[79] For example, an epistemic uncertainty exists when two analysts derive different casual predictions for a nuclear event using their own respective approaches. Aleatory uncertainty reflects the randomness in well known phenomenon.[80] For example, an aleatory uncertainty exists when an analyst specifies weather conditions for the nuclear event. The weather variable for a hypothetical event in the future is an accepted random uncertainty.

Pate-Cornell presents six levels of complexity in the characterization of risk that account for epistemic and aleatory uncertainty to varying degrees of detail:[81] Level zero analysis consists of the identification of an unwanted event which is basically the identification of a threat. For example, an unwanted event might include an airplane flying into a building, a nuclear event at a port or an improvised explosive device (IED) on a ferryboat. This level is sufficient if the threat is known and can be characterized.

Level one analysis builds upon the previous level and is used when not only when the hazard or threat is known, but one can also attempt to identify an upper bound on various outcomes should the threat manifest itself. This level of analysis is only feasible if the value of the upper bound is known. The applicability of this level of analysis will also depend on what outcome the analyst is interested in exploring. For example, an analyst may choose to explore fatalities associated with a nuclear event. In this case, the upper bound outcome might be described in terms of projected loss of life. In the case of a nuclear event in a small town, the upper bound on loss of life becomes the population of that town.

Level two analysis centers on the difficulty in trying to define a plausible worst-case scenario for cases where the upper bound isn't nearly as clear. In the case of a nuclear detonation near a large metropolitan city, the worst-case outcome is not that clear. The

78 Elisabeth Pate-Cornell, "Risk and Uncertainty Analysis in Government Safety Decisions," *Risk Analysis* 22, no. 3 (June 2002), 8.

79 Ibid.

80 Ibid.

81 Ibid, 8-12.

worst case might be defined as a ten kiloton weapon in the heart of the city with high winds of 10 miles per hour which complicate the fall-out problem. One can say that an even worst case would be a 100 kiloton weapon with 50 mile per hour winds blowing from the detonation location directly toward the city. As this thought process progresses, the probabilities obviously become more unrealistic.

Thus, the concept of this level of analysis is to define plausible upper bounds to the worst case scenario. The question then becomes: "What is the maximum probable loss of life from a nuclear event?" In some cases, this type of data is available. For example, the consulting firm Abt Associates has conducted studies that projected fatalities associated with a nuclear attack at a seaport. In their report they predict one million fatalities as a maximum "plausible" upper bound.[82] The challenge at this level of analysis is the upper bound can be subjective. For instance, the term "plausible" might mean something different based on how the term is being used. A maximum plausible loss of life as a result of a nuclear explosion for a small city will likely vary significantly from a larger city. Thus, it is desirable to reduce this uncertainty.

With level three analysis the objective is to produce a "best-estimate" analysis. This is accomplished by attempting to quantify probability estimates that lie near the middle of the probability distribution. In other words, this level uses the median or expected value. An important element of this level of analysis is the definition of the distribution. Outcomes will not always fall in the center of the distribution function and may fall closer to the tails of the distribution. The distribution can be defined in such a way that there is a higher distribution of outcomes that fall in the center but will still account for the variance in the tails.

Level four and five analysis involves the use of Bayesian analysis which involves organizing the various scenarios into a group of mutually exclusive elements. This type of analysis uses Bayesian statistics which are used to determine posteriori distributions of a variable by combining a priori opinion with observed data.[83] While Pate-Cornell

[82] Abt Associates, *The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability* (Cambridge, MA: Abt Associates, 30 April 2003), 7, available from http://www.abtassociates.com/report/ES-Economic_Impact_of_Nuclear_Terrorist_Attacks.pdf (accessed 30 May 2006).

[83] Vose, 28.

incorporates Bayesian analysis into her analysis levels, risk analysts are divided on the utility of Bayesian statistics.[84] Furthermore, Bayesian analysis exceeds the scope of this study.[85]

Other work in the area of QRA is found in the abundance of academic texts. In most cases, the academic literature strives to present how to implement the theories presented by risk experts such as Kaplan and Garrick. David Vose describes quantitative risk analysis as an approach that not only examines 'what if' scenarios, but goes one step further to essentially account for every possible value that each variable within a model could take and weights each possible scenario using a probability of occurrence.[86] Quantitative risk analysis achieves this by modeling each uncertain variable using a probability distribution. According to Vose, the goal of a quantitative risk analysis model is to calculate the combined impact of multiple uncertainties with some problem and generate a probability distribution of possible model outcomes.[87] This represents the primary difference from a deterministic model which uses a single discrete value as opposed to a distribution of values.

The importance of distribution functions is further illuminated by Aven in which he first presents the basic element of risk analysis using what he calls the "classical approach based on best estimates."[88] The underlying premise of this approach is that all input data are real and observed which is in accordance with traditional statistical modeling.[89] Thus, to determine weight and probability, one is required to perform measurements. For example, if the objective were to estimate the probability of an aircraft breaking in two as a result of an air to air missile attack, the analyst would conduct missile shoots against drones over and over again until the probability of the drone breaking in two can be accurately estimated.

---

[84] Vose, 28.

[85] For a detailed discussion of Bayesian Analysis, see Tim Bedford and Roger Cooke, *Probabilistic Risk Analysis* (Cambridge, UK: Cambridge University Press, 2001), 61-82.

[86] Ibid., 8.

[87] Ibid., 9.

[88] Aven, 14-15.

[89] Aven, 14.

Unfortunately, given the nature of many scenarios such as consequences resulting from a terrorist attacks, it is not feasible to generate real measurements. A better approach is to represent uncertainty by using known quantities combined with experience and building distribution functions that represent the range of values that uncertain variables might take.[90] Multiple uncertainty variables are then integrated together to generate a combined output distribution. This can be accomplished through simulation.

Johnathan Mun in *Applied Risk Analysis*, offers a simple view of simulation. He states "A simulation calculates numerous scenarios of a model by repeatedly picking values from a user-predefined *probability distribution* for the uncertain variables and using those values for the model."[91] Mun discusses the importance of simulation and distributions to avoid the "flaw of averages" trap.[92] By this, he is referring to a situation where an analyst uses a series of data points and calculates the average of the data. Furthermore, the analyst suggests that this average is representative of all the data sources. For example if the analyst is examining salaries within a company where top management makes significantly more income than most of the employees, then the distribution of wages is obviously skewed. An average of this data would not be representative of the average salary for an employee at this company.

F. RISK-BASED METHODOLOGY FOR HOMELAND SECURITY

Soon after 9/11, the GAO offered an approach to risk management with application to homeland security. They begin by offering several definitions of a risk management approach. First, they describe the approach as consisting of "a systematic, analytical process to consider the likelihood that a threat will harm an asset or individuals and to identify actions that reduce the risk and mitigate the consequences of an attack or event."[93] Furthermore, they define a risk-based approach as one that uses a step-by-step methodology for assessing threats, risks, requirements, and includes information on how to

[90] Aven, 48-49.

[91] Mun, 61.

[92] Mun, 62.

[93] U.S. Government Accountability Office, *Homeland Security, A Risk Management Approach Can Guide Preparedness Efforts*, 7.

prioritize resource allocation.[94] The GAO approach is founded on three pillars: threat assessment, vulnerability assessment, and criticality assessment.[95] The threat assessment is based on several factors which include terrorist capability, intention, and consequences. The vulnerability assessment identifies weaknesses in physical structures, personnel protection, and processes that might be capitalized on by a terrorist. The criticality assessment is designed to identify and evaluate high value assets and infrastructure such as power plants, computer networks, and government buildings.

While the GAO suggest in their report that "risk management is the best approach to guide program and responses to better prepare against terrorism and other threats,"[96] their framework merely offers a starting point and is mostly qualitative in nature. The GAO makes an occasional reference to assigning loss values to key assets which, hints at a more quantitative approach, but provides limited guidance on how to objectively assign the loss values.[97]

Shawn Reese, an analyst in the American National Government, Government and Finance Division of the Congressional Research Service, discusses the details pertaining to the risk factors that should be considered when allocating DHS funding. These include perceived threats, homeland security capabilities, population size, and critical infrastructure. Reese offers a non-comprehensive list of threats, a portion of which are considered significant. Some of the list includes critical infrastructure items such as power plants, bridges, and computer networks. Reese also suggests that risk analysts use a population factor described in terms of different densities across various cities when evaluating risk-related consequences.[98] Furthermore, Reese discusses capabilities in terms of prevention and response and how capabilities can reduce risk.

---

[94] U.S. Government Accountability Office, *Homeland Security, A Risk Management Approach Can Guide Preparedness Efforts*, 6.

[95] Ibid., 8

[96] Government Accountability Office, *Homeland Security, A Risk Management Approach Can Guide Preparedness Efforts*, 11.

[97] Ibid.

[98] Reese, *Risk-based Funding in Homeland Security Grant Legislation: Issues for the 109th Congress*, 17.

In addition to the GAO and CRS, other institutions have endeavored to apply risk-based methodologies to homeland security. One example is the work completed by Elisabeth Pate-Cornell and Seth Guikema in the area of homeland security in which they offer an approach to the modeling of terrorist threats.[99] They perform an extensive analysis of threat scenarios, terrorist groups, probabilities, consequences, and time periods. They evaluate capabilities in the general sense of merely protecting the targets analyzed in their scenarios. Additionally, they develop a quantitative model of terrorist threats which is heavily dependent on expert opinion to aid in determining quantitative values based on professional subject matter authority.[100]

The work of Pate-Cornell and Guikema provides extensive emphasis on the risk analysis piece but their analysis is overly reliant on expert opinion, which can be subjective. Also, it would be more complete if their work went one step further by incorporating how their risk results can be used to evaluate and prioritize policy options given limited resources.

Author Carl Roper, in his book on risk management for security professionals, describes a risk management process originally developed by the Risk Management Training Working Group (RMTWG) of the U.S. Security Policy Board, of which he was a member. Roper's begins by defining risk as a function of impact, threat and vulnerability. He defines risk and the elements as follows[101]:

Risk = Impact x (Threat x Vulnerability)

Threat x Vulnerability = Probability

Impact = Expected Impact (Asset Value)

---

99 Elisabeth Pate-Cornell and Seth Guikema, "Quantitative Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures," *Military Operations Research* 7 no. 4 (2002), 1.

100 Ibid., 5.

101 Carl Roper, *Risk Management for Security Professionals*, (Woburn, MA: Butterworth-Heinemann, 1999), 17

Roper goes on to describe risk management as the process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.[102] To do this, he offers five steps to risk management:[103]

1. Asset Assessment – Identify critical assets, undesirable events and expected impacts, value/prioritize assets based on the consequence of loss.
2. Threat Assessment – Identify threat adversaries, intent and motivation, capability, frequency, and degree relative to each critical asset
3. Vulnerability Assessment – Identify potential vulnerabilities or undesirable events, identify existing countermeasures in place and their level of effectiveness in reducing vulnerabilities.
4. Risk Assessment – Likelihood of an attack, likelihood of vulnerability exploitation, and multiply the two previous.
5. Countermeasure Assessment – Identify countermeasures, costs, and tradeoffs, and select an appropriate protection strategy.

Roper, while presenting his risk management process, reminds the reader that as with most quantitative risk methodologies, one of the difficult challenges lies in how to quantify risk. The first four steps in Roper's methodology are focused on this task. One way to do this is to assign general levels such as "low", "medium", "high", or "critical". Another option might be to use a one to ten scale. The basis on which to assign these ratings is somewhat subjective but can be aided by some description as to what constitutes each of the ratings. Being able to quantify risk, whichever approach is used, is a useful step to facilitate policy options analysis.

Beyond the need for quantification, Roper discusses the costs associated with various policy options. Essentially, every countermeasure has a cost associated with it that can be measured in terms of dollars, inconvenience, time, or personnel. In order to select the best countermeasure option, the cost associated with each countermeasure must be

[102] Roper, 17.

[103] Ibid., 20-21.

determined.[104] Consideration is given not only to the cost of tangible materials, but also to the on-going operational costs associated with a countermeasure and its implementation.

Once the costs are known, Roper advocates a two step "analyze and prioritize" process. The first piece of the analyze step examines how the asset value compares to the proposed cost of protection. For example, does a low value asset require a lot of money to protect? The second piece of the "analyze" step is to look at what policy option provides the best protection at the lowest cost.[105] Finally, based upon the results of risk assessment, the last step is to determine whether a policy option will mitigate risk to an acceptable or conditionally acceptable level as defined by the decision maker.

The second step is "prioritize." Roper recommends policymakers look at counter measures that address more than one undesirable event and also look at how the combination of countermeasure can collectively lower the risk for all the events identified.[106] This is done using a matrix assigning risk reduction potential for various counter measures and then deriving a cumulative risk reduction potential.

The next instance of a risk-based methodology for homeland security was offered by the RAND Corporation in 2005. The RAND Corporation Center for Terrorism Risk Management and Policy defines risk in terms of the same three components introduced by Kaplan and Garrick back in the 1980s and others, but add the component of vulnerability.[107] Vulnerability is defined as the probability that damage occurs, given an attack occurs. With the addition of vulnerability, Rand defines the components of threat and consequences in a slightly different way. Threat is defined as the probability that a specific target is attacked using a specific method during a specific time period and consequences are the magnitude and type of damage resulting from a successful terrorist attack.[108] Essentially, by incorporating vulnerability, RAND introduces consideration of how well a target is hardened or protected.

---

[104] Roper, 82.

[105] Ibid., 85.

[106] Ibid.

[107] Henry H. Willis, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby, *Estimating Terrorism Risk* (Santa Monica, California: RAND Corporation, 2005), xvi.

[108] Ibid., iii.

One of the contributions of the RAND Corporation's methodology is consideration of a wide range of possible threats in an uncertain environment. The approach also attempts to address the problem of evaluating the risk for individual cities. Resource allocation decisions have been made in the past without adequate consideration to factors that differentiate cities as being likely targets over others.[109] For example, one would logically think that a city with a population 8 million should receive more resource consideration than a city with a population of 20 thousand. The RAND monologue shows that risk estimates can be fashioned based on population factors such as density-weighting that can apply across a wide range of threat scenarios. This is demonstrated by comparing their results of risk underestimation errors with that of other approaches. While the approach presented by the RAND Corporation has significant relevance and goes one step farther than Kaplan and Garrick, it does fall short in that it does not demonstrate how policymakers can use a risk management approach to make resource allocation decisions in the resource limited environment of homeland security.

One critique of the RAND methodology is the use of a "best estimate" approach to consequences combined with the likelihood of occurrence. This approach can be summarized by the following formula:

$$\text{Risk} = P\{A\} * P\{S|A\} * E\{\text{consequence}\}$$

$$= P\{\text{occurrence}\} * E\{\text{consequence}\}$$

In this formula, the threat is represented by P{A}, the probability that an attack occurs. Vulnerability is represented by the term P{S|A}, the probability that damage will occur given that an attack occurs. Vulnerability here is the physical weakness of structures and facilities, as well as, security short falls that might be exploited by terrorists. Finally, the consequence is represented by the term E{consequence}, the expected value of the consequence. This component represents a value such as the expected fatalities or expected economic loss given a successful attack. The RAND methodology allows management action to focus on any one of these risk components. Management action however, can affect both consequence and vulnerability which makes it difficult to assess policy option effects against a single risk component.

[109] Willis et al., xv.

RAND acknowledges that consequences are determined by many uncertain factors and that these uncertainties can be accounted for using a full distribution of potential consequences or specific points contained therein. They decided however, to simplify consequences using only the expected value of the distribution of damage.[110] The expected value of a variable generally corresponds to the notion of the mean, or average.[111] Additionally, RAND indicates that the tails of the distributions are very dependent upon assumptions when considering events like terrorism due to lack of supporting data.

Some experts such as Yacov Haimes, argue that using an expected value is an incomplete approach and that accurate risk assessments need to consider the entire distribution to include the tails, as opposed to an expected value.[112] Furthermore, the expected value of risk does not adequately represent a measure that truly conveys the decision maker's objectives. However, Haimes offers one exception to the expected value argument in which the analyst can use a "conditional expected value" generated by the partitioned multi-objective risk method (PMRM).[113] This method, instead of using the traditional expected value of risk, generates numerous conditional expected-value functions which represent the risk given that the outcome falls within specific ranges in which probabilities are exceeded.[114]

A common theme in the homeland security risk methodology literature is the concept of breaking up risk into various components such as threat, vulnerability, and consequence. The primary challenge with these components is obtaining the necessary data to quantify them. While it is feasible to quantify consequence data, quantifying threat and vulnerability data faces more challenges. This difficulty in quantifying threat and vulnerability data is expanded on below.

The threat component of the risk formula presents a significant challenge. RAND's discussion of the threat component stimulates several questions as to what type of data is

---

110 Willis et al., 9

111 Evans and Olson, 70.

112 Yacov Y. Haimes, *Risk Modeling, Assessment, and Management* (New York: John Wiley & Sons, 1998), 309-312.

113 Ibid., 309.

114 Ibid., 312.

required to define a threat in terms of the method of attack:[115] What are the attacker's objectives? Has the attacker indicated a desire to carry out the type of attack in question? Does the attacker have the capability in terms of manpower, equipment or capability to carry out an attack? One way to package these questions is to think of the threat as a combination of attacker intent and capability.[116]

One of the difficulties with threat and vulnerability is that they are difficult to assess in enough detail to assign a value to them. One can argue that the previous occurrence of a particular attack method lends itself to a higher likelihood of occurrence in the future. Likewise, intelligence data suggesting a potential attack method leads to higher probability values for that attack method. While this makes intuitive sense, what threat values to assign in these cases does not. For example, terrorists have shown a desire to use a ship as a weapon, as seen by the attack against the USS Cole that occurred in Yemen on October 12, 2000.[117] As a result, analysts will likely assign higher threat probabilities to future scenarios involving boats as weapons. Once again, it is difficult to specify how much greater the probability might be.

The same challenge occurs with attempting to assess capability. One could argue that it is not difficult for terrorists to obtain small explosives and rent a power boat. Others might argue that terrorists are not capable of obtaining explosives within the U.S. nor do they have the capability to rent a power boat. Furthermore, one can make the argument that the capability exists once it has been confirmed either by demonstration or by reliable intelligence sources. Despite the options for determining capability, the challenge of quantification still remains. For example, is the best option to take a Boolean approach and quantify using a one or zero? Or, should an analyst attempt to quantify using various levels of capability? Once again, subjective interpretation plays a role here.

Quantifying vulnerability presents similar challenges to quantifying threats. Vulnerability is defined to represent the probability or likelihood of an attack being

---

[115] Willis et al., 6.

[116] Ibid.

[117] Yemen Gateway, "Attack on the USS Cole," 17 December 2001, available from http://www.al-bab.com/yemen/cole2.htm (accessed 19 September 2006).

successful given its attempt.[118] Vulnerability is often times a function of target hardness or a function of what security measures have been taken to prevent a successful attack.[119] Existing security measures are important because they help establish existing, or baseline risk. Once the baseline risk is established, one can evaluate the impacts of future policy alternatives, thereby making the effects of policy alternatives cumulative.

Similar to threat quantification, vulnerability values are likely to be subjective. One method to approach vulnerability is to assess what characteristics will facilitate or allow the attacker to carryout the desired method of attack. For example, if the attacker has the ability to carry out a suicide attack on a boat by placing a bomb in a backpack and if passengers are allowed to carry unscreened bags onboard the boat then this becomes an area of vulnerability. Likewise, if an attacker has the ability to attack a ferryboat by placing an explosive inside a vehicle to be transported on the ferry and if the vehicles are not screened for explosives then this too becomes an area of vulnerability.

In summary, while all the quantitative risk analysis methodologies do not specifically contain the components of threat, vulnerability, and consequence exactly, most are founded upon the basic concepts of risk pioneers such as Kaplan and Garrick. From a conceptual viewpoint, all the methodologies acknowledge that uncertainties exist about the possibility of an unwanted event and that bad things can happen which are represented by some type of loss. The methodologies provide a good foundation for the incorporation of quantitative risk analysis into homeland security decision resource allocation but could be more complete. The methodology proposed here attempts to offer a clearer picture of QRA and in doing so, explores its application to the Port Security Grant Program.

G. RISK-BASED METHODOLOGY FOR THE PORT SECURITY GRANT PROGRAM

1. Background

Prior to describing the specifics of the Port Security Grant Program, the author provides the reader with a brief overview of the importance of the maritime domain and the associated maritime threats to maritime security. This background information provides the motivation for using the PSG as our case study.

[118] Willis et al., 7-8.

[119] Ibid.

In today's global economy, more than 80 percent of world trade travels by water via a global maritime link.[120] The international system includes 30 megaports that form the hubs of the world's trade network. Over 75 percent of the global maritime trade and more than half of the world's daily oil consumption pass through a limited number of strategic international straits and canals.[121] Additionally, the U.S. maritime system includes over 3,700 cargo and passenger terminals operating out of more than 300 sea and river ports.[122] The marine geography under U.S. jurisdiction covers nearly 98,000 miles of coastline and over 3.5 million square miles of ocean area.[123]

The expansive maritime system provides a backbone for the uninterrupted flow of shipping. Many companies rely on the maritime system to support their just-in-time delivery approach for goods and services.[124] Companies avoid stockpiling or maintaining a reserve of energy, raw materials, and key components, which means that any interruption in the flow of goods can have implications for the national and global economies.[125] While maritime security has recently come under national and international scrutiny, the idea of disrupting the flow of maritime goods has been around for some time. For example in 1956, Egyptian forces shut down the Suez Canal for over a year by sinking ships in the narrow waterway.[126] While at the time the global trade impacts were minimal, presumably, a similar event today would have a much larger effect since nearly 14 percent of the world's trade passes through the canal.[127] Furthermore, the consequences of a

---

120 President of the United States, *National Strategy for Maritime Security* (Washington, D.C.: The White House, September 2005), 1.

121 Ibid., 1.

122 John Fritelli, *Port and Maritime Security: Background Issues for Congress*, (Washington, D.C.: Congressional Research Service, 2005), 2, available from: http://www.mipt.org/pdf/CRS_RL31733.pdf (accessed 16 March, 2005).

123 U.S. Coast Guard, *Maritime Strategy for Homeland Security* (Washington, D.C.: U.S. Coast Guard Headquarters, 2002), 18.

124 President of the United States, *National Strategy for Maritime Security*, 8.

125 Ibid., 8.

126 Jonathan Howland, "Hazardous Seas," *JINSA online*, (April 2004), available from http://www.jinsa.org (accessed 10 November 2006).

127 Jean-Paul Rodrigue, Claude Comtois, and Brian Slack, *The Strategic Space of International Transportation*, (New York: Routledge, 2006) available from http://people.hofstra.edu/geotrans/eng/ch5en/conc5en/ch5c1en.html (accessed September 18, 2006).

current day attack could include damage to port facilities, loss of life, a spike in oil prices, increased shipping costs, port delays, environmental hazards, and lost revenue for business unable to receive their products.

There is reason to be concerned that terrorist groups such as Al Qaeda might engage maritime targets directly or use the maritime domain to support their activity. Al Qaeda has a history of exploiting the maritime domain to support their efforts including creating fraudulent documents such as seaman's licenses that allow them travel to ports without a visa.[128] They have been known to raise money through arms smuggling, drugs trafficking, and slavery.[129] Coalition naval forces have interdicted over a hundred Al Qaeda operatives who were using working sail boats to transport weapons and drugs in the Persian Gulf.[130] Additionally, the intelligence community has discovered that Al Qaeda owns and operates a fleet of vessels used to ferry operatives, bombs, money, and commodities using the maritime domain.[131] It is believed that an Al Qaeda owned ship was used to deliver the explosives used for a car bomb that killed five Americans in Saudi Arabia in November of 1995.[132]

The maritime domain provides not only a medium for transit but also presents an array of targets that fit terrorist objectives. Ports are potential targets because of their economic and symbolic importance.[133] Security experts are concerned that terrorists could use the maritime transportation system to smuggle personnel, weapons of mass destruction (WMD), or other hazardous materials into the United States. The specific threat scenarios are numerous and include using maritime vessels as weapons against ships carrying people or chemicals, launching a cruise missile from a freighter off the U.S. coast, subsurface attacks using SCUBA equipment, and mines in shipping channels. The CIA warned that Al Qaeda was focused on advancing their maritime capabilities. In May 2002, a joint

[128] Christian Weber, *Maritime Terrorist Threat* (New York: The New York State Office of Homeland Security focus report, 21 February 2006), 5.

[129] Fay Bowers and Peter Grier, "How Al Qaeda Might Strike the U.S. by Sea," *The Christian Science Monitor* (14 May 2003), available from http://www.csmonitor.com/2003/0515/p02s02-usgn.html (accessed 10 October 2006).

[130] Weber, 5.

[131] Ibid., 6.

[132] Ibid., 5.

[133] Ibid, 9.

Moroccan-CIA operation disrupted an al Qaeda plot to attack U.S. and British ships in the Strait of Gibraltar using speedboats loaded with explosives. During this operation the CIA seized an al Qaeda maritime manual detailing the best locations to strike different types of ships and the quantity of explosives needed to cause critical damage.[134]

It is clear that maritime security ought to be a priority for homeland security decision makers as the maritime domain offers attackers an avenue to either execute or facilitate and attack against the United States. The U.S. Coast Guard in particular has created the largest port security effort since World War II.[135] One particular piece of the port security effort is the Port Security Grant Program. This program primarily focuses on the threat to passenger and vehicle ferries.[136] Ferries have been considered by terrorists as a ripe target with the potential for a large number of casualties. Most recently, in February 2004, terrorists detonated eight pounds of Trinitrotoluene (TNT) onboard a Philippines' *Superferry 14* killing 116 people.[137]

2. The Port Security Grant Program Overview

The DHS Appropriations Act of 2005 provides $150 million for port security grants.[138] DHS developed the PSG program and charged its Office of State and Local Government Coordination and Preparedness (SLGCP) with program administration. SLGCP's Office of Domestic Preparedness, which has now become the Office of Grants and Training (OGT), currently administers the program.[139] The grants provide funding for projects that improve the physical security in the Nation's most at-risk seaports. The program mirrors the intent of Congress and the Administration to protect critical infrastructure from terrorism involving the use of explosives and non-conventional threats that would cause major interruptions in the flow of commerce and substantial fatalities.[140] Additionally, the administrators of the program place a strong emphasis on prevention and

134 Weber, 2-3.

135 Fritelli, 10.

136 U.S. Department of Homeland Security, *Fiscal Year 2005 Port Security Grant Program* (Washington, D.C.: Department of Homeland Security, 2005), iii.

137 Weber, 11.

138 U.S. Department of Homeland Security, *Fiscal Year 2005 Port Security Grant Program*, iii.

139 U.S. Department of Homeland Security Office of Inspector General, *Follow Up Review of the Port Security Grant Program* (Washington, D.C.: Department of Homeland Security, February 2006), 3.

140 U.S. Department of Homeland Security, *Fiscal Year 2005 Port Security Grant Program*, iii

detection against the threat of an IED delivered via small craft, or onboard a ferry using a carrying device such as a backpack or vehicle.[141]

In order to determine how best to appropriate funds under the program, DHS administrators developed a risk-based methodology to determine the most at-risk seaports. While the methodology shows progress in the use of QRA, it is not without its challenges and shortcomings. The Office of Domestic Preparedness (ODP) in concert with the U.S. Coast Guard (USCG) and the Information Analysis and Infrastructure Directorate (IAIP) developed the following formula:[142]

Risk = Consequence x Vulnerability x Threat

Consequence includes the potential effects on people, economic damage, national security, and impacts associated with possible hazardous materials that might be involved. Vulnerability considers factors such as the distance from the open water and the number of port calls. Threat considers any existing threat information such as intelligence estimates provided by the USCG and the intelligence community. Threat also considers the number of previous incidents at a given port and vessels of interest. The formula was applied to the Nation's 129 largest volume ports and 66 port areas were identified as at-risk.[143]

Grant awards for the 66 ports were first determined by dividing the ports into four tiers. Tier one represented those ports with the highest risk and tier four represented those ports with the lower risk.[144] ODP allocated grant money to each tier and then ports within each tier competed for the funds. Part of the evaluation to award grant money to port projects consisted of a field review process. This process was managed by the applicable USCG Captain of the Port (COTP) for which the project applies and considered four primary factors. First, the COTP considered how well the project supported the priority to protect against the IED threat. Second, the COTP considered how well the project addressed the priorities outlined in the Area Maritime Security Plan which is a plan that

141 U.S. Department of Homeland Security, *Fiscal Year 2005 Port Security Grant Program*, 7.

142 Ibid., 3.

143 Ibid.

144 U.S. Government Accountability Office, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure* (Washington, D.C.: GAO, December 2005), 57-58.

outlines operational and physical measures associated with each of the maritime security (MARSEC) levels.[145] Third, the COTP considered how the project coincided with security priorities for the specific port area based on personal expertise and experience. Finally, the COTP performed a cost-benefit analysis to determine the potential risk reduction given the cost of the project. The overall objective of the last step is to award grants that offer the highest potential for risk reduction for the least cost.

3. Critique of the Port Security Grant Program

In February 2006, the DHS Inspector General (IG) conducted an evaluation of the PSG and identified several shortcomings in their risk-based methodology. The DHS IG analyzed details regarding how decision makers evaluated potential risk reduction for the national priority threats and the potential risk reduction for the least cost. The details are presented in Table 1 which depicts the scoring system used for the Field Review Process. The COTP was individually responsible for awarding the scores and often did so, based on personal experience and knowledge of his port area.[146]

Criterion	Score
Risk reduction potential	20 pts*
Prevention/detection of underwater IED attack (10 pts)	
Prevention/detection of IED attacks by small craft (10 pts)	
Prevention/detection of vehicle born IEDs on ferries (10 pts)	
Consistency with Area Maritime Security Plan	5 pts
Applicability to local security priorities	5 pts
Potential risk reduction for least cost	5 pts
Total possible score	35 pts

*The National Review Process subsequently awarded points for either a combination of underwater and small craft attacks or vehicle born IEDs, but not both.

Table 1 Port Security Grant Program Field Review Scoring System[147]

[145] U.S. Coast Guard, *Overview of Area Maritime Security Regulations, 33 CFR Part 103* (October 2003), available from http://www.aapa-ports.org/govrelations/ (accessed 22 May 2006).

[146] U.S. Department of Homeland Security Inspector General, *Follow Up Review of the Port Security Grant Program*, 8.

[147] Ibid., 8.

The DHS IG reported that there were issues regarding how field reviewers scored projects relative to each other. The report noted that COTPs tended to award project scores differently, resulting in a wide range of scores between ports. For example the Houston port area projects scores ranged from 9 being the lowest to 30 being the highest.[148] Whereas the port of New York/New Jersey, also in the same risk tier had scores that ranged from 3 being the lowest to 17 being the highest.[149] The report highlighted the fact that subjectivity is inherent in the process and relies heavily on the judgment of those assigning the scores.[150] The IG recommended that program administrators enhance the standardization of the field review scoring methodology.

The GAO further critiqued the PSG methodology as being limited in the ability to compare benefits of security measures and their potential for risk reduction.[151] Additionally, the GAO suggested that the values being used for consequence data might not accurately represent the possibilities of damages from a terrorist attack. For example, one method currently used to evaluate potential consequences of an attack on a ferry is to use the average number of daily passengers.[152] This alone, does not accurately represent the full range of consequences in terms of impact on people.

Another recent study involved several agencies who worked together on a project to develop a mission oriented risk and design analysis of critical information systems.[153] One of the key findings from this study was the challenge in how to conduct an effective cost-benefit analysis after having used a risk-based methodology. The paper highlights the fact that in traditional cost-benefit analysis, policy alternatives are considered independent of each other. This limits the ability to compare risk-reduction potential across a wide range

148 U.S. Department of Homeland Security Inspector General, *Follow Up Review of the Port Security Grant Program*, 15

149 Ibid.

150 Ibid., 16

151 U.S. Government Accountability Office, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, 62.

152 Ibid., 61.

153 Donald L. Buckshaw, Gregory S. Parnell, William L. Unkenholz, Donald L. Parks, James M. Wallner, and O. Sami Saydjari, "Mission Oriented Risk and Design Analysis of Critical Information Systems, *Military Operations Research* 10, no. 2, (2005), 34.

of policy alternatives given their associated cost. The findings of this study echo one of the shortcomings in the current PSG program methodology as critiqued by the DHS IG and GAO.

In summary, the Port Security Grant (PSG) program is one of the more recent examples where decision makers attempt to use a risk-based approach for resource allocation and specifically attempt to apply quantitative risk analysis (QRA). DHS has made it a priority to use a risk-based methodology to ensure that funds are available to the Nation's highest risk ports.[154] While their efforts have shown significant strides to effectively utilizing such an approach, shortfalls still exist. These seem to exist for two primary reasons. First, insufficient efforts were made to account for the subjectivity and uncertainties that often accompany risk-based methodologies. Second, DHS evaluators involved in the review process where scores were assigned to various criteria often scored projects differently. DHS evaluators also lacked an efficient method to evaluate the tradeoff between risk reduction and project cost.

[154] U.S. Department of Homeland Security, *Fiscal Year 2005 Port Security Grant Program: Program Guidelines and Application Kit*, 3.

III. FORMULATION OF THE RISK-BASED RESOURCE ALLOCATION PROBLEM

A. INTRODUCTION

This chapter presents a conceptual model of a risk-based approach to the resource allocation problem confronting decision makers managing homeland security programs directed at reducing terrorist risk. It provides an operational definition of risk that serves as a basis for resource allocation decisions that respond to the potential for risk reduction of each policy alternative. In doing so, the mathematical notation for the remainder of this thesis is established. Next, the chapter sets out the process to be followed in order to obtain the quantitative information necessary for the risk-based approach presented and identifies the key information and data requirements to do so. The chapter concludes with a schematic to help the reader visualize the conceptual model.

B. THE DECISION MAKER'S OBJECTIVE

This methodology assumes decision makers want to maximize risk reduction and make resource allocation decisions consistent with this objective. Thus, decision makers are assumed to allocate homeland security and defense resources so as to achieve the greatest reduction in risk relative to the current situation and existing security measures (baseline risk).

C. THE DEFINITION OF RISK

Following the work of Kaplan and Garrick, Pate-Cornell and others, risk is defined here as the likelihood, or probability, of an "unwanted" event (consequence) occurring. This event is characterized by consequence, or losses, that are beyond what the decision maker can tolerate or deems acceptable. The consequences are denoted by the random variable C and maximum acceptable value by c^*. Risk, R, is then defined by the probability of the event in which the consequences exceed the maximum acceptable value denoted by:

$$R = P\{C \geq c^*\}.$$

For example, consider a decision maker whose primary concern is the potential casualties resulting from a bomb attack at a major U.S. port facility located near a large

metropolitan city. In this case, C represents the magnitude of casualties resulting from the attack and is random because it is difficult to predict with certainty the exact level of casualties. The maximum acceptable value c^*, on the other hand, is known to the decision maker and in this case represents a threshold level of casualties. In other words, the decision maker cannot tolerate casualties in excess of this value so the event described by $C \geq c^*$ is to be avoided. Note that, if this event is *highly unlikely* to occur meaning a low probability (P) of occurrence, then the decision maker may treat the event as one of "acceptable risk." Conversely, if the event is considered highly likely or even likely to occur, then the decision maker would be inclined to treat the event as one of "unacceptable risk," and would take some action to reduce the risk to an "acceptable level."

Figure 1 shows risk represented in terms of the probability density function (PDF) for C. We denote this PDF by $f_C(c)$. The x-axis represents the outcome variable such as fatalities from attack, and the y-axis represents the probability weighting for the outcome. Therefore, an analyst would interpret the distribution function considering where c^* is plotted and examines the area under the curve to the right. This area represents the probability that C is equal to or greater than the decision maker's acceptable outcome level c^*. This area is the risk (R) and represents the probability that casualties will exceed that level indicated by c^*.

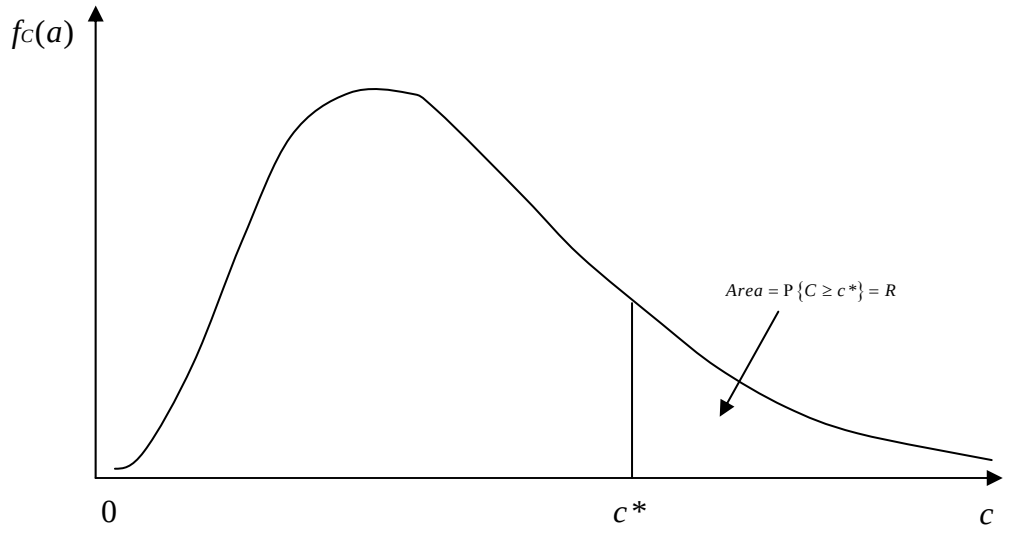

Figure 1 Distribution Function.

D. MANAGEMENT ACTION AND THE ASSOCIATED RESOURCE ALLOCATION PROBLEM

As previously established, it is not feasible to completely eliminate all risk. Risk is dynamic and is subject to change as a result of management action. Decision makers implement policy alternatives with the goal of reducing risk. This is the basis for most interpretations of risk management.[155] Management action is expressed as a set of policy alternatives denoted by A that is composed of N objects:

$$A = \{a_1, a_2, a_3, ..., a_N\}$$

Associated with each of these alternatives is a cost. Thus, each alternative has an associated budget which is denoted by b_n. Therefore, the budgets corresponding with the identified set of alternatives is defined by the set B composed of N objects:

$$B = \{b_1, b_2, b_3, ..., b_N\}$$

In the bomb attack at a port example, consider four possible policy alternatives. The first uses funds to install a fence around all port facilities with gated access and thus reduces vulnerability. The second purchases a contract for armed security personnel to patrol the grounds at regular intervals and thus also reduces vulnerability. The third purchases security cameras to monitor port facilities and fence lines. The fourth provides funds to local emergency response authorities to improve response time and capability that would, in turn, reduce consequences resulting from an attack.

Given the proposed set of alternatives and associated budgets, the decision to allocate or not allocate funds can be denoted by D composed of N objects:

$$D = \{d_1, d_2, d_3, ..., d_N\}.$$

Therefore, $d_n = 1$ if a_n is chosen for implementation. Conversely, $d_n = 0$ if a_n is not chosen for implementation.

Finally, most decision makers are under budget constraints in one form or another. Thus every resource allocation decision will be subject to these budget constraints. To

[155] U.S. Government Accountability Office, *Homeland Security, A Risk Management Approach Can Guide Preparedness Efforts*, 7.

represent this, F denotes the total budget available to the decision maker for the security program. All resource allocation decision must satisfy the following:

$$\sum_{n=1}^{n=N} d_n b_n \leq F$$

E. MANAGEMENT ACTION AND RISK

Each resource allocation decision will have some affect on risk. Furthermore, one can assume that each policy alternative is effectual; i.e., $\partial C\left(a_n\right)/\partial a_n < 0$. This implies a connection between risk and management action. This critical interaction is represented by showing the dependency between the risk R and the decision variable D:

$$R = R(D) = P\{C(A(D)) \geq c^*\}$$

Finally, the current situation, or baseline risk, represents the "do nothing" approach and is denoted by $D = \{0, 0, ..., 0\}$ and is represented by $R(0)$.

F. RISK REDUCTION

Assuming that all possible policy alternatives are effectual further assumes that $R(D) \leq R(0)$. So the reduction in risk is represented by:

$$\Delta R(D) = R(0) - R(D) = P\{C(0) \geq c^*\} - P\{C(A(D)) \geq c^*\}.$$

This equation shows that the change in risk is a function of the decision maker's choice to implement a policy option. The policy option will reduce risk by some amount below the existing baseline level. This change also equates to a corresponding change in consequence outcome.

G. RISK-BASED RESOURCE ALLOCATION PROBLEM

Risk-based resource allocation can now be formulated in terms of maximizing risk reduction. The decision maker desires an allocation of funds so as to maximize risk reduction:

$$\max_D \Delta R(D) \text{ subject to the funding constraint } \sum_{n=1}^{n=N} d_n b_n \leq F.$$

H. REQUIREMENTS OF THE RISK-BASED APPROACH

The key to implementing a risk-based approach is contained in the risk reduction formulation $\Delta R(D) = R(0) - R(D)$. The analyst must calculate $R(D)$ and, implicitly, $\partial C(a_n)/\partial a_n$. In other words, how much is risk reduced as a function of the decision to implement a policy alternative. Determining this amount of risk reduction is the fundamental problem in a "risk-based" approach. Given this amount of risk reduction, it is a relatively simple task for an analyst to calculate the optimal allocation using established results from the field of mathematical programming.

The computation of $R(D)$ requires the probability density function $f_C(D)$ (equivalently the cumulative distribution function). This, in turn, requires the model describing the consequences function of the implemented alternative, $C(A(D))$. In principle this can be done by theoretical manipulations of the probability models representing the uncertainties inherent in $C(A(D))$.[156] Thus, the necessary data and information to implement a risk-based approach is that required for the construction of $C(A(D))$ and the specification of the probability models for its uncertain components.

I. FORMULATION SUMMARY

The process of risk-based resource allocation is depicted in Figure 2. The schematic can be read from top to bottom. The process begins with decision maker identification of the consequence of concern C. The magnitude of these consequences is a function of the various policy alternatives and thus becomes $C(A(D))$. Next the analyst determines areas of uncertainty and specifies the associated probability models. These models are then used to derive $f_c(D)$. Next, given the decision maker's risk maximum accepted value of risk (c^*), the analyst derives risk $R(D)$. Finally, the decision maker incorporates the total budget (F), the cost to implement the chosen alternative combination $B(D)$, and the associated impacts on risk reduction $\Delta R(D)$, to make resource allocation decisions. This final step whereby the decision makers desire to maximize risk reduction given the funding constraint is once again denoted by:

[156] A. Papoulis, *Probability, Random Variables and Stochastic Processes*, (New York: McGraw-Hill, 1965), chapters 5-7.

$\max_{D} \Delta R(D)$ subject to the funding constraint $\sum_{n=1}^{n=N} d_n b_n \leq F$.

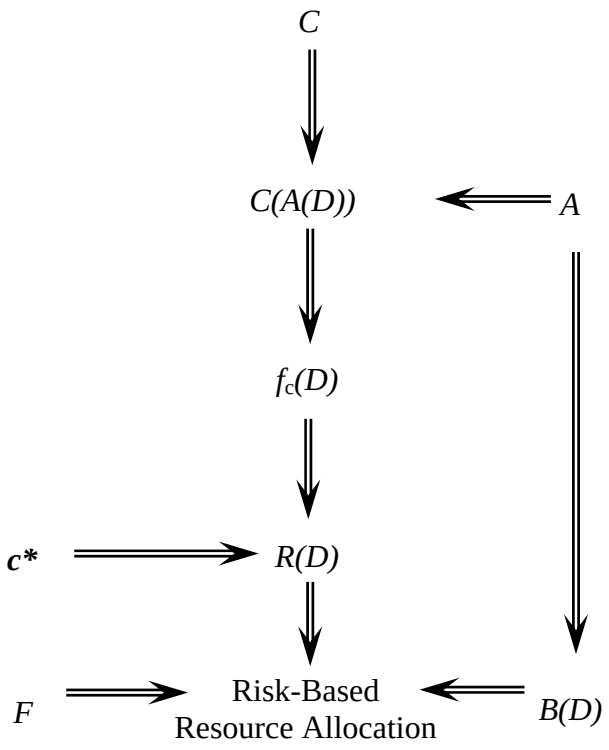

Figure 2 Risk-based Resource Allocation Methodology

IV. QUANTITATIVE RISK ANALYSIS USING SIMULATION

A. INTRODUCTION

This chapter presents derivation of $f_c(D)$ by means of simulation (Figure 3). The derivation of $R(D)$ from purely theoretical considerations using probability theory is impractical because of the complexity of the relationships. However, it is feasible to utilize a simulation-based approach. Simulation is an established tool for quantitative risk assessment that has proven very useful in many areas of decision making when a large amount of uncertainty exists.[157] Exploring the applicability of simulation in resource allocation decision making related to homeland security and defense is a central theme of this thesis.

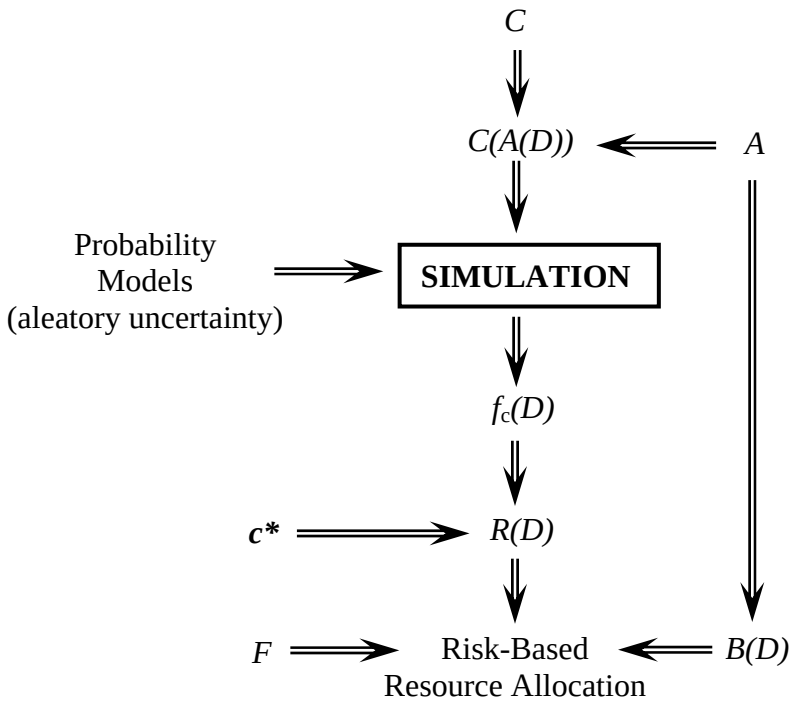

Figure 3 Risk-based Methodology, Simulation Piece

[157] James R. Evans and David L. Olson, *Introduction to Simulation and Risk Analysis* (Upper Saddle River, New Jersey: Prentice Hall, 2002), 2-3.

B. SIMULATION EXAMPLE

To introduce the concepts of simulation the author presents a step by step example using the scenario of an explosive device detonated onboard a passenger boat. Following the concepts introduced in the previous chapter, the first step is to identify what undesirable event and associated outcomes are of concern to the decision maker. For this example, the undesirable event is the loss of life due to a bomb explosion onboard a passenger boat. Therefore, the decision maker is interested in policy alternatives that could potentially minimize loss of life. Next, the analyst needs to quantify the potential fatalities given a bomb explosion onboard a passenger boat.

The number of fatalities will be dependent on several factors, but the three most important are passenger load, explosive size, and location of the explosive relative to passenger concentration. The first part of passenger load is to determine the passenger capacity of the boat. The analyst can obtain this if the type of boat is known. This example will look at one boat with a passenger capacity of 500 people. Next, the analyst should attempt to obtain historical data that shows how many people are typically on the boat. One approach is to obtain an historical average, keeping mind that there are instances when the boat has more or less passengers onboard. For this example, the average number of passengers is 250.

Now that a maximum passenger capacity and average passenger load data have been obtained, it is possible to define a passenger distribution using modeling software such as Excel or Crystal Ball. For example, suppose the available data suggests a normal distribution with a mean of 250, truncated between 0 and 500, represents the number of passengers on board. Figure 4 shows the probability density function for this distribution when the standard deviation equals 100 which is set to represent a wide range of passenger loads.[158] If y denotes the number of passengers then $y \sim N(250,100;1,500)$.

[158] The standard deviation is normally calculated based on actual data. Given the absence of actual data, the figure used here is an assumption.

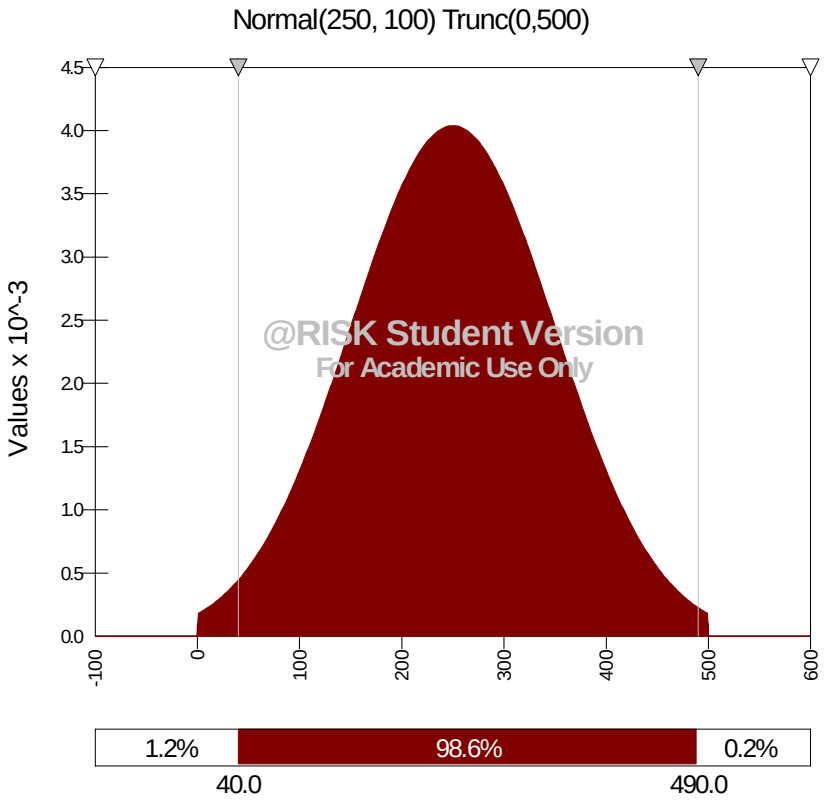

Figure 4 Example Model Passenger Distribution

The second factor that will affect fatalities onboard the boat is the size of the explosive itself. Once again, there are several factors that will determine how big an explosive might be. For this example, the company operating the boat does not allow passengers to carry any baggage onboard but does routinely transport shipping packages on its storage deck. Therefore, the most feasible attack method is to hide an explosive in one of these containers onboard the boat. The analyst can then use the maximum package size allowed on the boat to help define how large the explosive might be. Another factor to consider is the explosive type. Blast yields vary depending on explosive types and how the explosives are packaged. A given weight of one type of explosive may have a much higher yield than the same weight of another explosive. For this example, the analyst will assume the explosive type is TNT. Even though explosives can be constructed using different using different compounds, most can generally be converted to a TNT equivalent weight.

Now that the analyst has established the maximum package size and the explosive type, it is possible to define an explosive size distribution. For this example, the analyst has determined that the maximum TNT explosive size is 50 pounds. Since not all packages are capable of packaging an explosive of this size, the analyst will specify a probability distribution for package size. This may reveal that the boat predominantly carries packages that will conceal a 30 pound bomb. Furthermore, assume the analyst believes another Normal distribution with a mean of 30, standard deviation of 10 and truncated between 0 and 50 is sufficient to represent the uncertainty in bomb size (Figure 5). If x denotes the explosive size then $x \sim N(30,10;1,50)$.

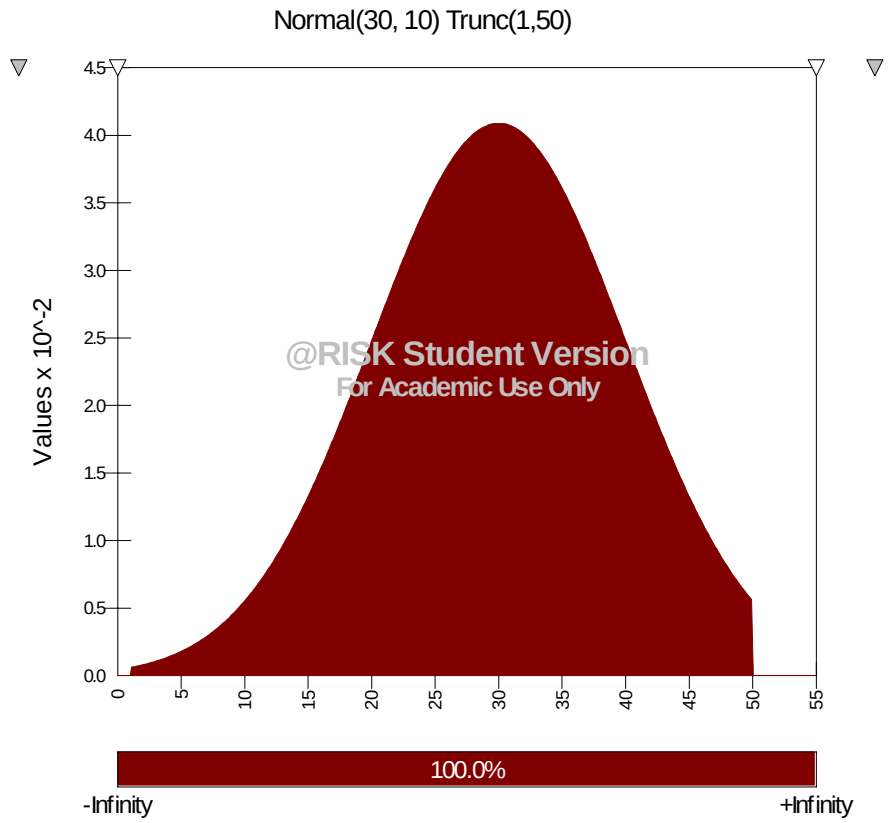

Figure 5 Example Model Explosive Distribution

The next step in the model construction is to define a relationship between the passenger fatalities and the explosive distribution. To do this requires an analysis of blast effects to establish a relationship between explosive size and lethal distance. Many factors go into this such as explosive casing and structures surrounding the explosive itself which

might include containers, flooring, walls etc. Several blast effect tools are available that can aid an analyst in determining this relationship which can be defined in terms of a lethal radius. Knowing the lethal radius as a function of the explosive size allows the calculation of the number of expected casualties based on the number of passengers within the lethal radius. This function is denoted by:

$$r(x) = a + bx + cx^2$$

Where E is the size of explosive and a, b and c are constants derived using explosive size and corresponding lethal radius data. Using the lethal radius, one now calculates the lethal area using the formula πr^2.

Next, the analyst uses this lethal area to calculate passenger casualties. One approach is to determine the passenger area onboard the ship. Here, the assumption is made that passengers are uniformly distributed within the passenger compartment.[159] Given the total number of passengers and further assuming a notional two feet between passengers, it is possible to calculate the passenger area which is denoted by S. The maximum passenger area is constrained by the total passenger capacity. Finally, casualties are calculated by multiplying the ratio of lethal area to passenger area by the total number of passengers. Thus, the equation for passenger casualties is:

$$C = \frac{\pi r^2(x)}{S} \bullet y$$

The computation of the probability density function for fatalities via simulation is accomplished by repeating the following steps many times. Each pass through these steps is called a *trial* (or run of the simulation model). Step 1: Draw a number, y, (sample) from the passenger distribution and another number, x, (sample) from the explosive distribution. Step 2: Compute the lethal radius, r, for the explosion using $r(x) = a + bx + cx^2$ and the lethal blast area, $\pi r^2(x)$. Step 3: compute the fatalities, C, by multiplying the number of

[159] This assumption is used to simplify this example model. The author acknowledges that this is a simplifying assumption and further notes that the effects of clustering are partially accounted for in the final model described in the next chapter.

passengers on board, y, with the fraction of passenger area that is in the blast of the explosion (S denotes passenger area on the ship):

The total number of trials the model runs depends on the degree of reliability one desires in the result. Usually, 1000-5000 trials are sufficient to obtain a reliable estimate of the probability density function for the consequence. An example probability density function for fatalities is shown in Figure 6. This corresponds to the probability density function introduced in Figure 1 on page 40.

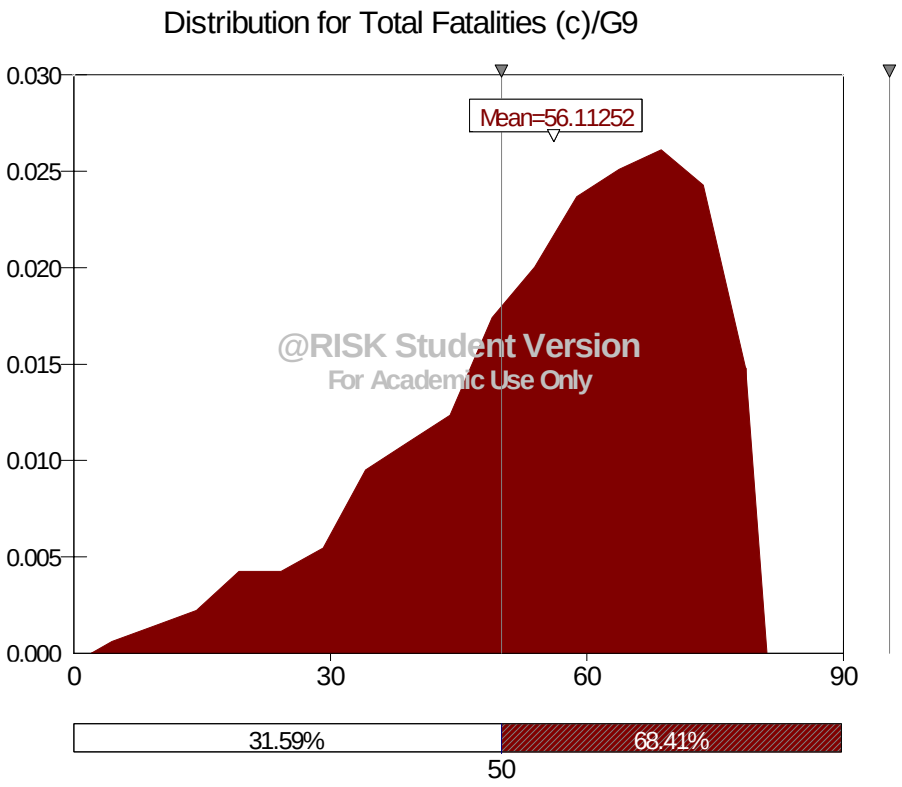

Figure 6 Output Probability Distribution Function (Fatalities)

The next step is to construct a risk curve from the distribution function. This is accomplished by plotting values from the distribution function onto a graph with outcome and risk probability values. Referring back to Figure 1, the area represented by R represents the percentage of the distribution that exceeds c^*. This is one slice of the distribution and represents a data point for the risk curve. Figure 7 shows an example of how one data point is plotted using c^k and its corresponding r^k. This process is then

repeated to show a representation of multiple data points from the distribution function plotted together to form the remainder of the risk curve (Figure 8). More data points of course result in a higher fidelity risk curve.

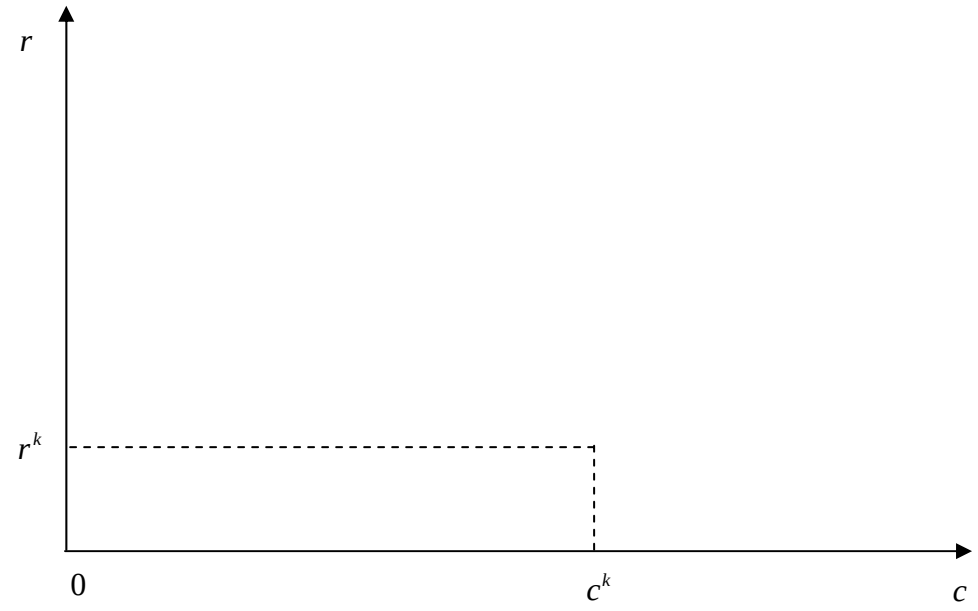

Figure 7 Risk Curve Construction Showing a Single r^k and c^k Plot

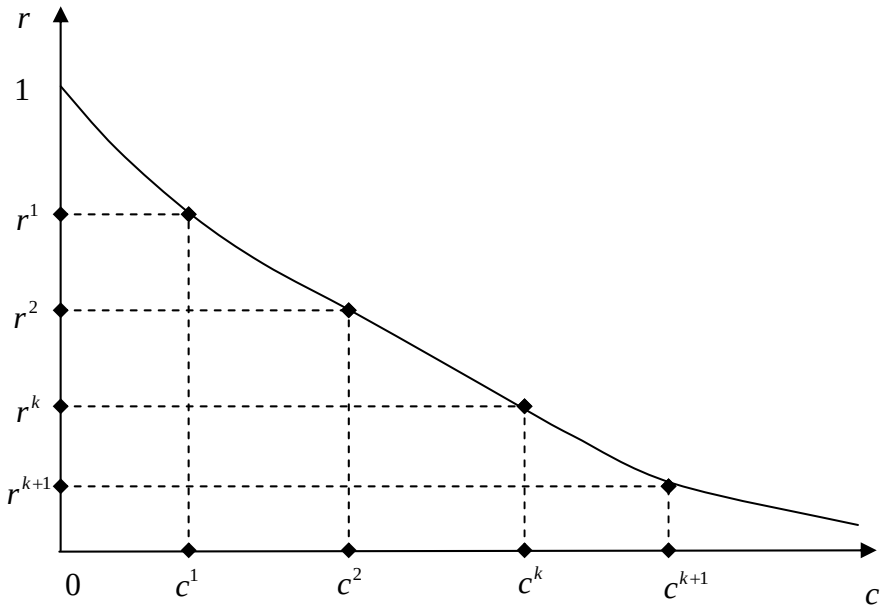

Figure 8 Completed Risk Curve Plot of Multiple r^k and c^k Values

We now apply the risk curve construction step to the example model. For this example the decision maker has set a threshold of 50 fatalities. This equates to the c^k value discussed previously discussed. The data bar underneath the distribution annotated by a percentage in the white block and another percentage in the solid block shows the analyst to determine the r^k value. In this snapshot, the c^k value is set at 50 and the R value is 68.41 percent (point A). Repeating this construction for $c = 10, 20, 30...$ gives the curve presented in Figure 9.

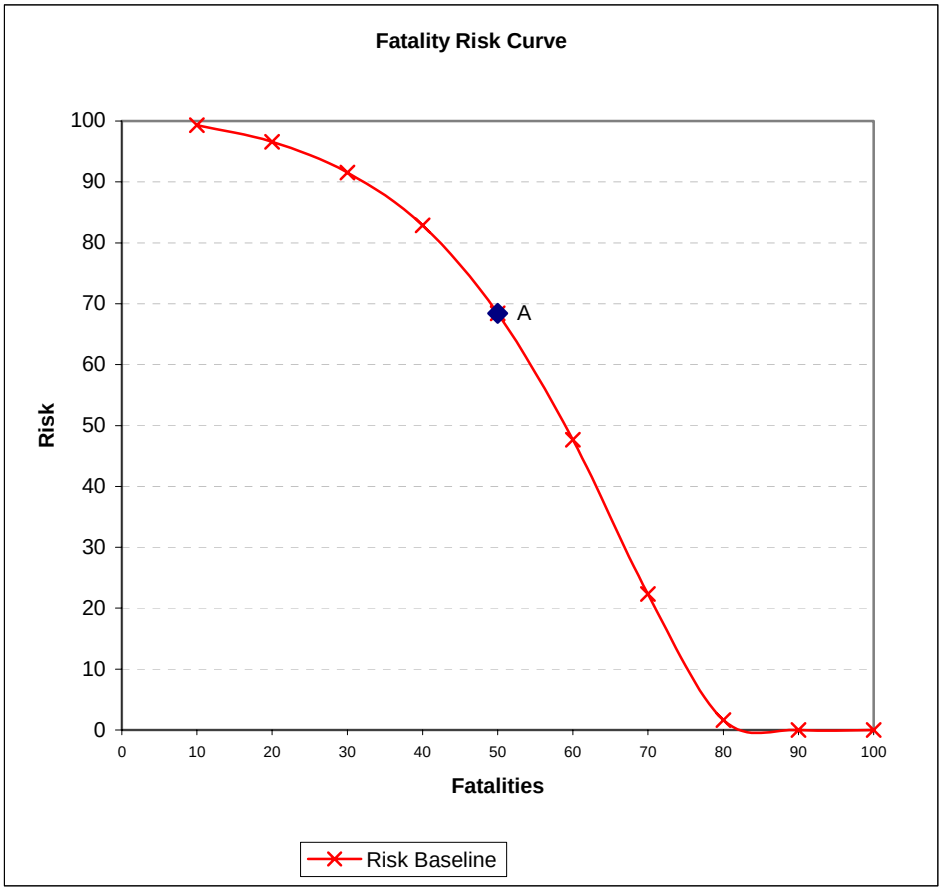

Figure 9 Example Model Baseline Risk Curve

Now that the baseline risk curve has been set, the analyst can incorporate policy alternatives. For demonstration purposes, this example model incorporates one policy alternative in which the boat company limits the number of passengers their boats. While this may seem unrealistic, it will convey the conceptual point.

To model this policy alternative the analyst will need several pieces of information. The first is updated or projected passenger data that needs to include projected maximum capacities and projected average number of patrons. The projected maximum capacity is straight forward which is the new maximum allowed capacity. The average number of riders can be calculated by assuming that the maximum number of patrons will not change but they will be distributed over a greater number of scheduled trips. Thus, the resulting figures might be a maximum passenger size of 300 and an average passenger load of 150. To implement this in the model requires changing the previously defined passenger distribution. Figure 10 depicts a side by side comparison of the original and modified distributions. While the two distributions share a similar shape, the values associated with the revised distribution are smaller.

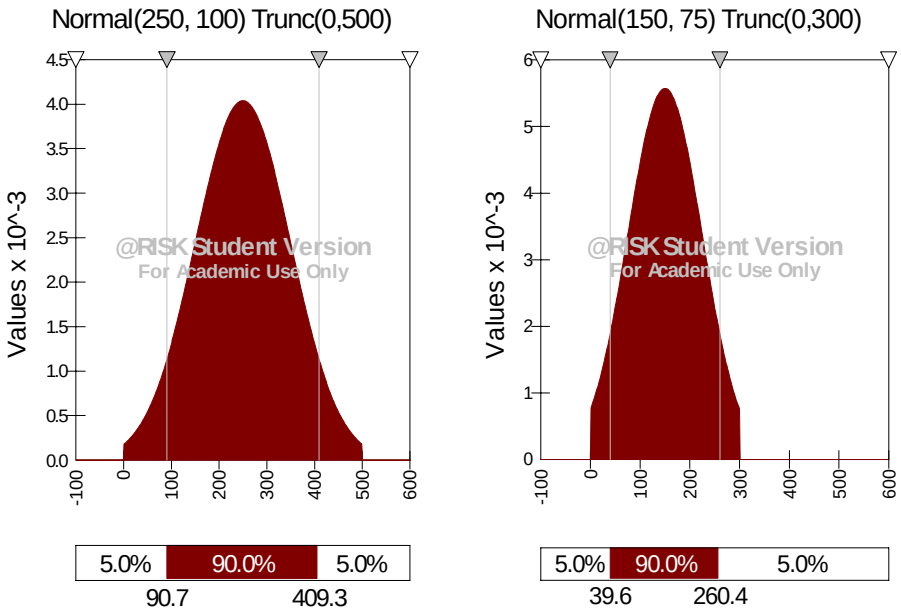

Figure 10 Example Model Passenger Distribution Comparison

Now that the passenger distributions have been modified, the next step is to run the model again. Once again, the analyst is interested in reviewing the probability density function for the defined outcome pertaining to the number of fatalities. Figure 11 depicts a side by side comparison of the pre-policy option output and the post policy option output. The analyst is able to examine the output and note the reduction in the mean fatalities from 55.5 to 48.2.

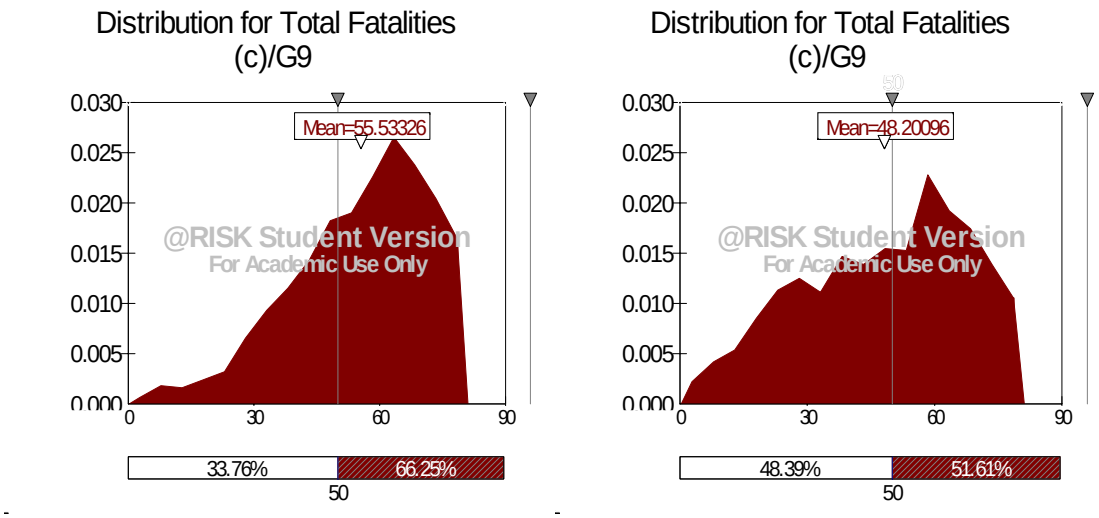

Figure 11 Output Probability Density Function Comparisons (Fatalities)

These distributions are then used to construct the pre-policy option risk curve and the post policy option risk curve for comparison purposes. Figure 12 depicts a graph with both the pre-policy alternative risk curve and the post-policy alternative risk curve. The comparison between the two reveals a reduction in risk: with $c^* = 50$, $R = 0.51$ with the policy option in place whereas without the policy option $R = 0.68$.

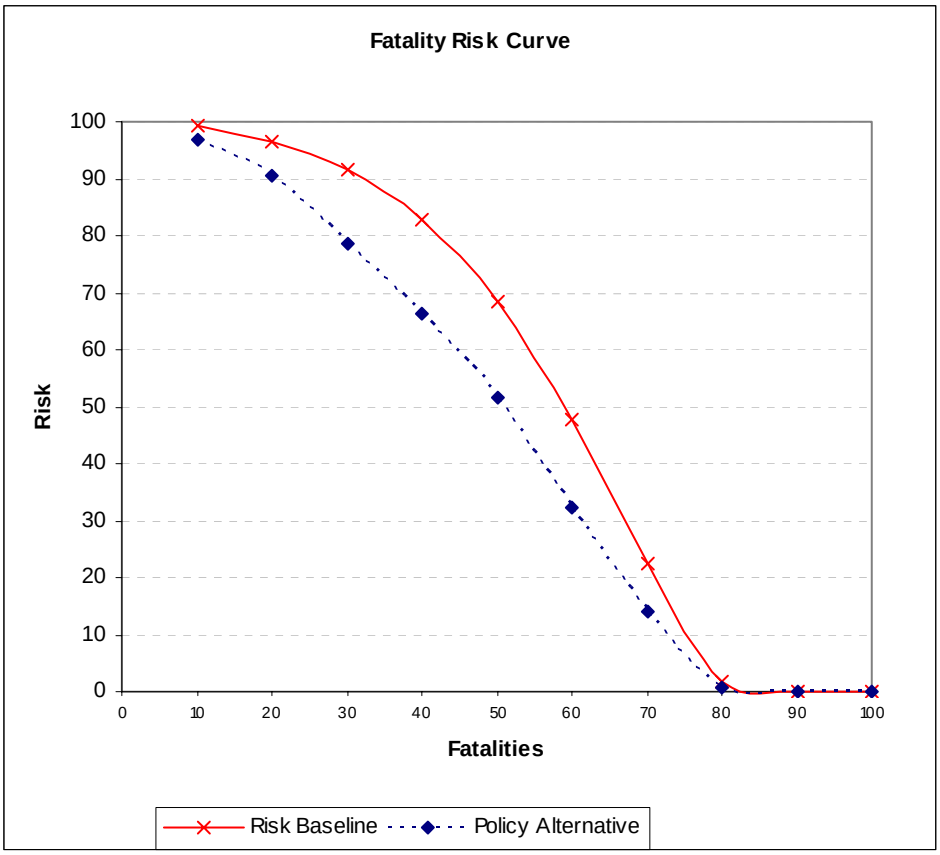

Figure 12 Model Example Risk Curve Comparison

The last remaining step is to plot the risk curves on a graph with their corresponding costs. The cost of the alternative presented here is driven by the cost of obtaining the smaller boats and the associated operating costs. While the example incorporates only one policy option, the same methodology could be applied for multiple policy options. The objective of the final plot (not included here) is to allow the decision maker to compare multiple policy alternatives, given their associated costs, and their impact on risk reduction.

C. SIMULATION DATA AND ASSUMPTIONS

The example model presented so far has yet to address the required data to construct such a model. The required data might not always be available or may be of suspect quality. This will require the analyst to make assumptions along the way. It is important to make note of data quality and assumptions so that decision makers have an accurate picture of the quality of the analysis on which they are making their decision. This section discusses the data necessary to construct a quantitative risk analysis model and addresses areas where assumptions are likely to be necessary.

1. Consequence Data

Consequence data is more feasible to gather and quantify for incorporation into a risk model than threat and vulnerability data because it is easier to measure and often times already exists. One approach to gathering this data is to first categorize the outcomes. For example, if an explosive device were detonated within a city, different types of outcomes will occur. These might include fatalities, injuries, tangible destruction of structure and equipment, or various types of economic loss. Categorizing the outcomes allows the decision maker to focus efforts on distinct categories depending on where the greatest concern exists. For example, the decision maker might care a great deal about loss of life or injuries and less about specific property damage.

After defining the categories, it is necessary to determine what data is required to quantify the outcomes within each category. For example, to quantify the potential damage to a structure or vessel, one must analyze the destructive potential of the explosive in question. Specifically, if the analyst is concerned with a backpack bomb carried onto and detonated aboard a boat, one would have to know the type, quantity, and packing of the explosive. Furthermore, one would have to know the structural damage that might result from the blast effects.

Another element of the outcome data is the maximum potential losses for each category in question. If the analyst wishes to evaluate potential fatalities resulting from an attack on a particular city, the maximum potential fatalities can be defined as the size of the population. Or, if the analyst wishes to evaluate potential fatalities resulting from an attack on a ferryboat, the maximum potential fatalities can be defined as the passenger capacity of that ferryboat. Furthermore, the analyst is also likely to know the average number of passengers on a ferryboat and can further refine the data set.

Finally, the above data and information must be converted into a math model that explicitly identifies the uncertainties and suggest a probability model for each.

2. Policy Alternative Data

Once the consequence data is obtained, the next step is to obtain policy alternative data. The required data for the policy alternatives falls into two categories. The first and most obvious is the associated cost of each alternative. This data is required as it will

ultimately be used by the decision maker to perform the risk versus cost analysis. Generally, this data is readily available since it is usually presented up front when a project or policy option is submitted for evaluation. One additional consideration with cost data is the differentiation between immediate or "one time" costs, and maintenance or recurring costs. A project such as installing security lights or cameras would consist of upfront costs for equipment and installation and minimal maintenance costs. Conversely, a project such as a passenger/baggage screening service that utilizes security personnel to perform the screening will consist of some upfront costs to put the screeners in place and significant ongoing costs to keep the service in place.

The second policy alternative data category involves determining how the various alternatives impact risk. This data becomes slightly more problematic and requires more analysis. First, in the words of Bruce Schneier, "security is a weakest-link problem [and therefore] attackers are more likely to attack a system at its weak points."[160] To that end, security alternatives generally focus on these weak points that equate to areas of vulnerability. Therefore, for each alternative, an input is required to determine how the alternative will reduce vulnerability. For example, consider an alternative involving human interaction such as a security service which will inspect bags to be carried on a ship, one must assess how much this reduces vulnerability. It becomes subjective in that one can take a perfect world approach and say that the screeners will be 100 percent effective at catching a backpack bomb before it is carried onto a boat. A more realistic approach is to accept the fact that screeners are human and are prone to oversights which means there is still a chance that a backpack bomb will make its way onto a boat. Either way, the requirement is to obtain data that describes the effectiveness of the alternative under consideration.

3. Assumptions

When constructing a quantitative risk analysis model, an analyst will likely find areas where data is lacking.[161] One way to fill these data gaps is to make assumptions which in turn need to be communicated clearly to the decision maker. Additionally, an

[160] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York, NY: Copernicus Books, 2003), 103.

[161] Molak, 9.

analyst should determine the ramifications of the assumptions and what model deficiencies might result. One way to do this is to conduct a sensitivity analysis. A sensitivity analysis allows the analyst to examine the impacts of variable assumptions on forecasts.[162] Significant changes between runs indicates that the assumption needs to be refined by acquiring additional data or leaving the assumed component out of the equation altogether.

Realizing the assumptions cannot be completely eliminated, the analyst should attempt to characterize them as another variable of uncertainty and at least represent them using a distribution.[163] This is conceivable given that the analyst most likely knows the lower and upper bounds of the data in question. Once the lower and upper bounds are identified, the analyst can then specify the distribution shape that best characterizes the range of uncertainty.

[162] Evans and Olson, 130.

[163] Ibid., 69.

V. QUANTITATIVE RISK ANALYSIS MODEL APPLIED TO THE PORT SECURITY GRANT PROGRAM

A. INTRODUCTION

This chapter provides an illustration of our approach to the Port Security Grant Program (PSG). Given the PSG emphasis on the improvised explosive device (IED) threat to ferryboats, this chapter first begins with an overview of ferryboats and their role in the maritime domain. The remainder of the chapter focuses on the model construction to include a section on each of the threats: backpack IED, vehicle IED, and a small boat attack (SBA) IED.

B. FERRYBOAT BACKGROUND

Ferryboats, similar to other public transportation vessels, represent a potential target with prevention and protection challenges. Ferryboats come in many shapes and sizes, have varying degrees of passenger capacity, operate in many different ports, have dynamic schedules, and are often owned by private companies. Also, some ferryboats have the capacity to carry vehicles as well as passengers. Additionally, the location of various ports directly affects the quantity, type, and accessibility of civil boat traffic. All of this information is relevant in one form or another to constructing a model that can accurately represent potential consequences of an IED attack against a ferryboat.

Another important aspect of the ferryboat scenario is the terrorist's objectives. This study assumes that if a terrorist is to attack a ferryboat using an IED, one of their objectives is to maximize loss of life or injuries. To that end, the terrorist is likely to carry out the attack in such a manner as to achieve this objective. For example, in the IED in a backpack scenario, the attacker is likely to choose a ferryboat at or near maximum passenger capacity, use the biggest explosive charge conceivable in a backpack, and detonate the explosive near the biggest cluster of passengers on the boat.

C. BACKPACK IED THREAT

One of the objectives of the model is to quantify the risk associated with the backpack IED attack on a ferryboat. The model developed here focuses exclusively on outcomes related to immediate fatalities but can easily be adapted to economic damage,

hazardous materials, or other consequences. This section will discuss the various components of the model: required data, output generation, and risk curves.

1. Required Data

To generate a probability distribution function for fatalities resulting from an IED onboard a ferry requires the analyst to consider what factors contribute to the number fatalities. The two most obvious factors are passenger data and explosive size. Passenger data includes passenger capacity, actual passenger load, and passenger density. While passenger capacity is a constant, passenger load and density are variables and need to be represented by a data distribution. One source of this data is historical passenger loads from which, one can fit this distribution.

The first two pieces of passenger data are passenger capacity and actual passenger load. The data used for this model comes from the Blue and Gold Ferry Fleet, which operates in the San Francisco Bay area.[164] The company possesses 14 passenger and tour vessels that range in capacity from 300 to 700 passengers. On the basis of this data, the model uses a maximum boat capacity of 500 which falls in the middle of this range. Furthermore, research conducted in 2002 suggests that ferryboats operating in the San Francisco Bay typically operate at an average of 33 percent of their capacity.[165] Given that the need for mass transportation has risen in the San Francisco Bay area since 2002, and that an attack would likely take place during a high volume time, it is more realistic to use a higher passenger capacity percentage. Thus, this model assumes the quantity of passengers to be a random variable, y, with a minimum quantity of zero passengers and a maximum quantity of 500 passengers. The probability model representing y is a truncated Gaussian distribution with (expected value) $\mu = 400$ passengers and (standard deviation) $\sigma = 100$ passengers.[166]

$$y \sim N(400,100;0,500).$$

---

[164] Blue and Gold Fleet, available from: http://www.blueandgoldfleet.com/Information.htm (accessed 12 September 2006).

[165] CALSTART, *Passenger Ferries, Air Quality, and Greenhouse Gases: Can System Expansion Result in Fewer Emissions in the San Francisco Bay Area?* (California: CALSTART, 23 July 2003), 6.

[166] Similar to the example model presented in the previous chapter, the standard deviation is assumed and intended to represent a wide range of passenger loads. This figure can be calculated if actual passenger data were available.

The final piece of passenger data is passenger density. Typically, this is a function of passenger compartment size and layout. For simplicity, this model assumes a single passenger compartment. In reality, a ferryboat is likely to have many passenger compartments to include passenger space outside along the perimeter areas of the vessel. This model uses the approach of calculating a passenger density. To do this, it was assumed that the passenger compartment was large enough to accommodate its capacity, given an assumed minimum required spacing of two feet between passengers. Therefore, the passenger area was calculated using the number of passengers for a given run and a radius of two feet.

The physical distribution of passengers within a passenger compartment can vary. One approach is to assume that all the passengers on the boat are evenly spaced throughout the passenger compartments on the vessel. However, it is more likely that passengers will cluster at various locations on the vessel. This becomes important because one can also assume that an attacker would tend to gravitate toward clusters containing higher concentrations of people in order to maximize attack effectiveness. Therefore, the model does consider some limited effects of clustering. To do this, the model acknowledges that clustering can occur and represents this phenomenon by drawing a random percentage of the total passenger load and placing them into a single cluster. The cluster is further defined by a passenger density in which each person is separated from the other passengers by a space of two feet.

The second major input to the model is the explosives data. The analyst needs to consider several characteristics regarding explosives. The first is the size of the explosive. When considering explosives carried in a backpack, the size of the explosive is limited by the size of the backpack and the attacker's desire to conceal the explosive. This model makes the assumption that a backpack capable of carrying 50 pounds of explosives represents a reasonable upper bound for the backpack size. To model this, the size of the explosive device by weight is assumed to be a random variable, x, with a minimum size of one pound and a maximum size of 50 pounds. The probability model representing x is assumed to be a truncated Gaussian distribution with (expected value) $\mu = 35$ pounds and σ (standard deviation) 10 pounds: $x \sim N(35,10;1,50)$.

The attacker makes a conscious trade-off between explosive size and the likelihood of detection but gravitates toward larger explosives sizes. To represent this, the model calculates the mean using 70 percent of the maximum explosive size. Thus, using an explosive size of 50 pounds, the mean is 35 (.70 * 50).

The next piece of the explosives data is a relationship between the size of the explosive and associated fatalities resulting from the explosion. Blast effect analysis shows how the impact of an explosion on a human body is a function of the level of overpressure at the point the blast wave reaches the human body. The anatomically affected area leading to death is typically the lungs.[167] Lung damage is a result of gas-tissue interface where spalling and tearing can occur, and the degree of damage is a function of positive pulse duration and peak overpressure associated with the blast.[168] Another component of the blast that leads to fatalities and injures is fragmentation. Fragmentation depends on the explosive casing and contents packaged with the explosive. In some cases fragmentation can cause more damage than the overpressure. Using the combined effects of overpressure and fragmentation, it is possible to determine a radius within which, a human is likely to sustain fatal injuries. BlastFX™, Explosive Effects Analysis Software is used to compute the lethal radii where expected fatalities are predicted to occur.[169] This data is then input into MATLAB® 7.1 to obtain a least squares for using a quadratic function. The function representing the lethal radius for the backpack IED is:

$$r = -.002818x^2 + .3634x + 6.89$$

Where $r(x)$ is the lethal radius as a function of explosive size x.

2. Output Generation

The initial output of the model is the outcome distribution for fatalities. In order to run the simulation and generate this output distribution, a final relationship is required. The output is defined in terms of the number of fatalities resulting from a backpack IED on a ferry. The basic approach involved using a relationship between lethal area and boat

[167] Paul W. Cooper, *Explosives Engineering* (New York: Wiley-VCH, 1996), 417.

[168] Ibid., 417.

[169] Blast/FX™ Explosives Effects Analysis Software was created by Northrop Grumman for the Transportation Security Administration's (TSA) Systems Engineering Branch. The software was designed for security and engineering professionals concerned about the threat of explosions to facilities and their occupants. For more information, see http://www.blastfx.com/ (accessed 1 November, 2006).

area. The lethal area is calculated given the lethal radius, which is calculated using the equation generated using blast modeling and data fitting tools. Next, the passenger area (or density) is calculated using a uniform dispersion of passengers with a minimum of two feet between them. As mentioned previously, the effects of one cluster of passengers is also incorporated. The number of passengers clustering is drawn as a random percentage of the total passenger load. Finally, given the lethal area with the explosion centered in the passenger cluster, the number of fatalities is calculated by the percentage of total passengers that fall within the lethal area. Therefore, the equation relating casualties to lethal radius and total passengers on-board at the time of the blast is

$$C = \frac{\pi r(x)^2}{S} \bullet y$$

where C denotes casualties, S denotes the total area onboard devoted to passenger accommodation, r denotes the lethal radius as a function of explosive size x and y denotes the number of actual passengers.

Now that the input relationship is defined, the model is set to run. Running the model requires that the analyst specify the number of trials to run. The number of trials becomes important in determining the overall fidelity of the output. It is feasible to run the model multiple times using a range of iterations and examine its behavior to determine the point of diminishing returns. For this model, the consequence probably distribution function is generated by running the model with 1,000 trials. As the model steps through each trial, a data point from each input distribution (passenger load and explosive size) is taken, and a fatality figure is calculated. In the end, these data points are used to construct a frequency histogram that is an estimate of the output PDF for fatalities.

3. Construction of Risk Curve

Once the output distribution of fatalities is generated from the 1000 trials, it is then possible to construct the risk curve using the same steps discussed in the previous chapter. Here we compute fatalities from 0 to 100 with an interval of 25. At each of these data points, the percentage of the remaining distribution is used as a data point for the risk curve. The resulting risk curve is shown in Figure 13

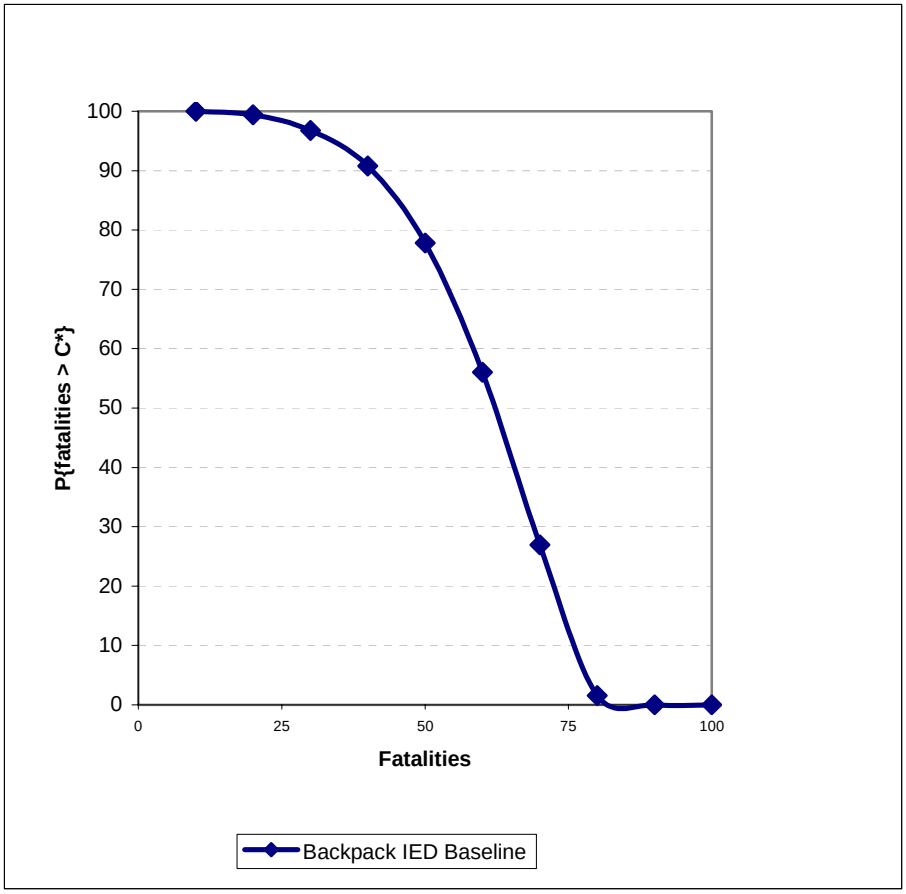

Figure 13 Backpack IED Baseline Risk Curve

4. Validation and Verification

After running the model and prior to using the results for management action, it is important to validate and verify the output. One method is to determine if the output is reasonably consistent with expectations. Doing this requires an analysis of the raw output data containing the sampled explosive size. The analyst must first ensure that the sampled data makes sense based on the defined input distribution for explosive size. And second, the analyst determines if the resulting lethal radius fit the provided equation. For this model, the analysis showed consistency in both cases.

Another method is to modify the input distributions, re-run the model and determine that the change in the output distribution is consistent with expectations. To accomplish this, the maximum explosive size is increased from 50 pounds to 75 pounds. The expected result is more fatalities, or a higher mean for the outcome distribution. The observed

behavior is consistent with expected results as the mean increased from 59.8 to 76.6 (Figure 14). Another expected result is a risk curve showing a higher level of risk. This behavior is observed and is depicted in Figure 15. As depicted, the increased explosive size shows a higher level of risk.

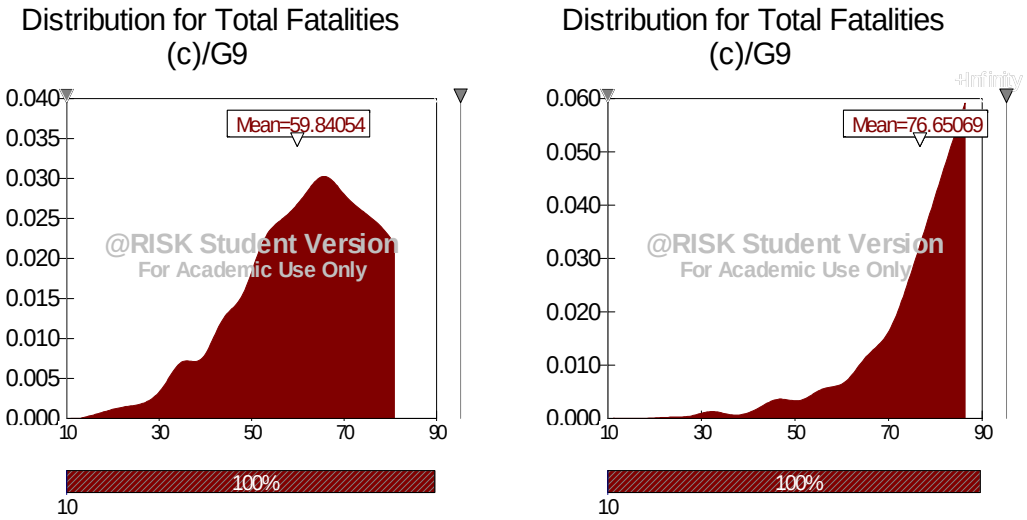

Figure 14 Sensitivity Analysis, Increase in Maximum Explosive Size

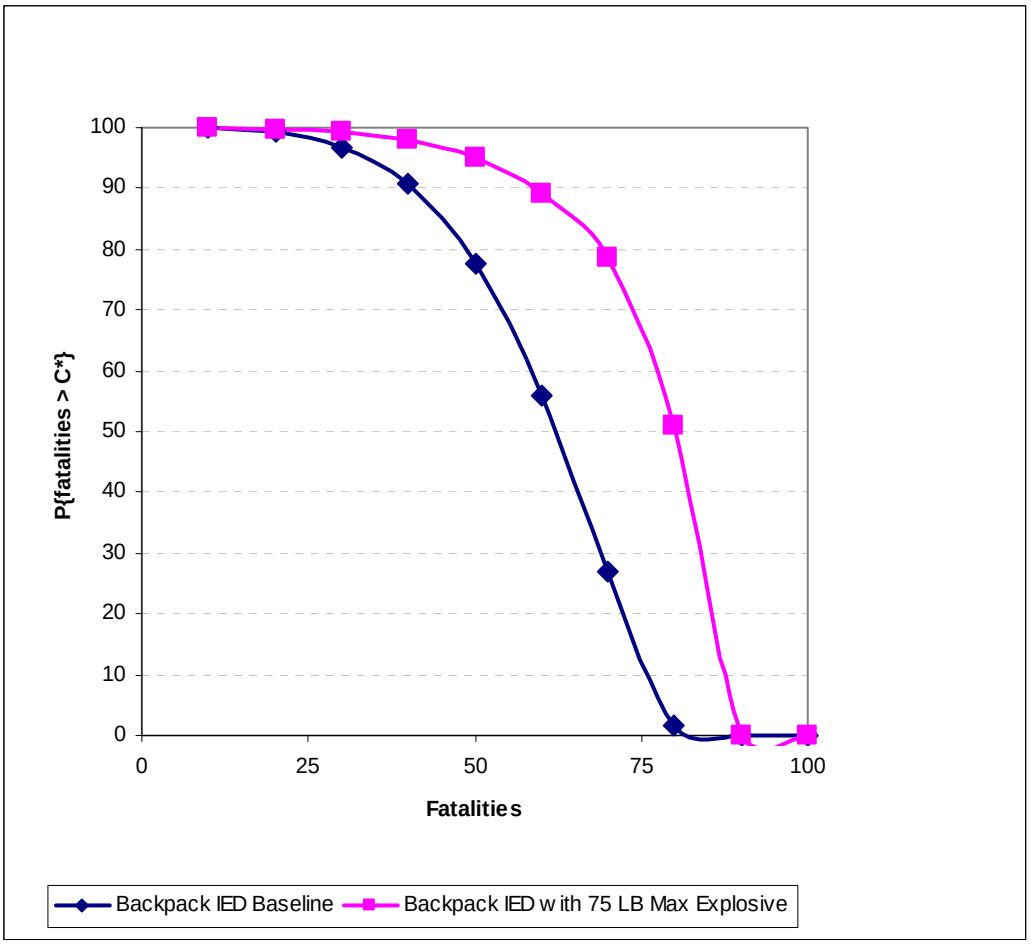

Figure 15 Sensitivity Analysis, Change in Backpack IED Risk Curve

D. VEHICLE IED THREAT

The next threat simulated in the model is an IED placed in a vehicle onboard a ferry capable of transporting vehicles. As with the backpack IED, the focus is exclusively on the outcome of fatalities resulting from the attack.

Two significant differences were incorporated into the model to account for the vehicle IED threat. First, the size of the explosive capable of being placed in a vehicle is much larger than that which can be placed in a backpack. The most likely location to place a vehicle IED is in the trunk to minimize chances for detection. This model assumes that the average trunk in a sedan style vehicle can conceal approximately 100 pounds of explosives. Thus the Gaussian distribution was modified to have a mean $\mu_X = 70$ pounds and standard deviation σ 20 pounds: $x \sim N(70, 20; 1, 100)$.

Once again, the skewed distribution toward the higher explosive size represents the likelihood that an attacker would gravitate toward the higher end of the explosive spectrum.

The second significant difference with a vehicle IED is the ferry compartment layout. Vehicle compartments are typically located on their own level below the passenger level. Therefore, the explosive effects are not only limited by the metal comprising the trunk itself but are also limited by the structure separating the two floors. This phenomenon was represented by constructing a similar structural layout within the blast effects simulation in order to calculate the area of expected casualties. Additionally, it was assumed that the attacker would not have any input on the placement of the vehicle onboard the ferry, and therefore the vehicle explosion was placed at the center of mass on the ferryboat by default. The resulting function for the vehicle IED lethal radius function is:

$$r = .05x + 13$$

From here, the output probability distributing function is generated using the same formula for C described previously. Thus, the resulting risk curve is found at Figure 16.

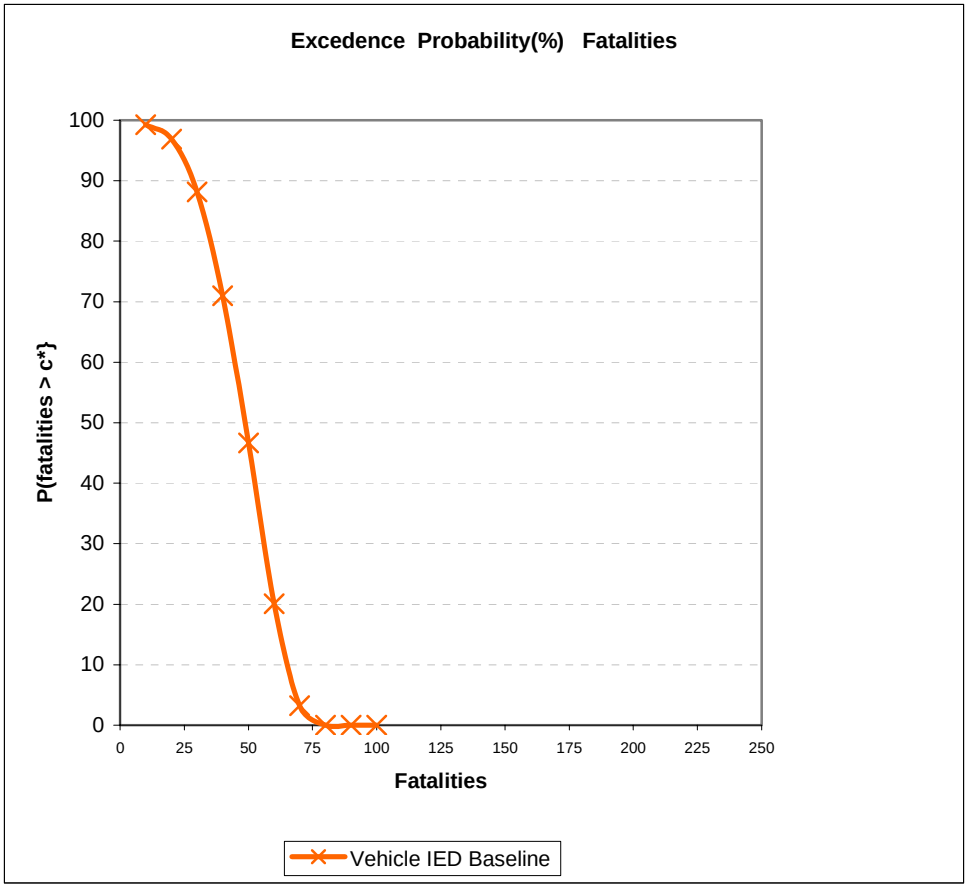

Figure 16 Vehicle IED Baseline Risk Curve

E. SBA IED MODEL COMPONENT

The final threat simulated in the model is an IED placed onboard a small boat and used to ram a ferry. As with the backpack IED and the vehicle IED, the focus is exclusively on the outcome of fatalities resulting from the attack.

The SBA IED threat introduces several dynamics that significantly increase model complexity. The effects of a SBA are a function of several factors, which include the size of the boat, speed of the boat, impact location, hull penetration, etc. It is possible that a SBA would merely puncture a hole in the vessels thereby causing it to take on water as opposed to causing a significant number of fatalities. Conversely, with the correct combination of factors such as hull penetration, delayed fusing, and a large enough explosive, it is feasible that numerous fatalities could result.

The USS Cole bombing provides one point of reference for this analysis. Reports suggest that the attackers used a rubber style boat, similar to a zodiac, loaded with several hundred pounds explosives for the attack. It is unclear if the ramming boat actually penetrated the hull of the USS Cole or merely pulled alongside it. If a rubber style boat was used, it is unlikely that it penetrated the hull before detonating. Regardless, the explosion created a 40-foot hole, killing 17 sailors and injuring 38 others.[170]

From an input perspective, the SBA introduces complex modeling challenges. The potential size of the explosive is relatively straight forward and bound by the size of the ramming boat. The next factor deals with the origin of the blast itself. The effects of a blast initiated outside the hull of the target vs. being initiated after hull penetration, are quite different. For simplicity, this model assumes that the ramming boat penetrates the ferry before the explosive detonates. This is feasible given that the attacking boat is a speedboat ramming a ferryboat with an aluminum superstructure which is not uncommon.

To model the explosion from a small boat impact, the maximum explosive size was increased to 300 lbs with a mean of 200. Thus the Gaussian distribution was modified to have a mean $\mu_X = 200$ pounds and standard deviation σ 70 pounds.

$$x \sim N(200, 70; 1, 300).$$

As discussed previously, the skewed distribution toward the higher end represented the likelihood that an attack would lean toward the higher end of the explosive spectrum.

The other significant change is the origination of the blast. With the backpack IED, for instance, it was assumed that the attacker would detonate the explosive at the center of mass of the largest cluster of people. With a small boat attack, the attacker is not likely to have flexibility in choosing the impact point corresponding to the location of the greatest passenger concentration. Therefore, the blast origin for the model was placed at the midpoint alongside the boat. The resulting function for the SBA IED lethal radius function is:

$$r = 1.786_x 10^{-5} x^2 + .05043x + 20$$

[170] Yemen Gateway, "Attack on the USS Cole," 17 December 2001, available from http://www.al-bab.com/yemen/cole2.htm (accessed 19 September 2006).

From here, the output probability distributing function is generated using the same formula for C described previously. Thus, the resulting SBA IED risk curve is plotted in Figure 17.

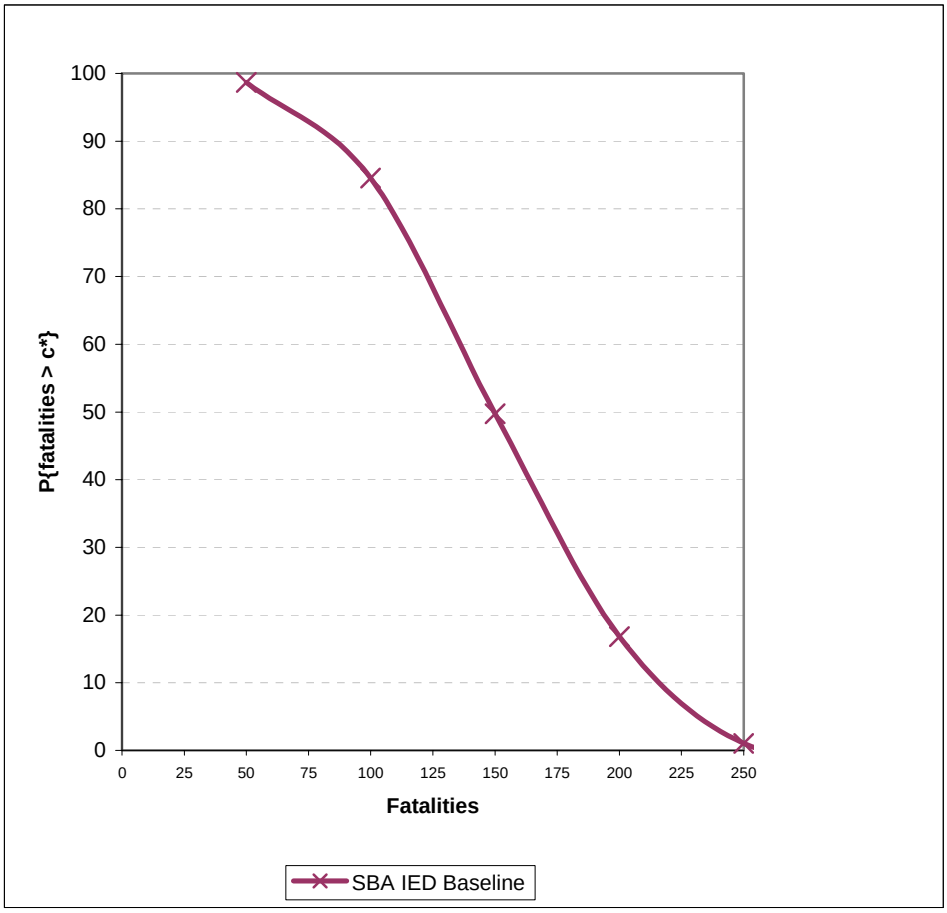

Figure 17 SBA IED Baseline Risk Curve

F. INCORPORATION OF ALTERNATIVES

Alternatives, or policy options, will ultimately reduce risk. The extent to which an alternative reduces risk is the key to decisions based on risk reduction. To model this requires information about the alternative. This information includes a description of the alternative, intended effects, and potential effectiveness data. In some cases, these data may be difficult to predict and require drawing on the past performance of similar programs.

The first alternative ($a1$) is strictly focused on reducing the risk associated with a backpack IED. One version of this alternative might be to reduce the size of carry-on bags

or completely eliminate the option for passengers to carry bags on the ferry. The latter is on the extreme end of the security countermeasure spectrum and may seem unrealistic. Limiting the size of a carry-on, however, is somewhat more realistic and can be done in a similar fashion to the airline industry in which the carry-on must fit inside a specifically sized container. The ultimate effect of this type of alternative would be a reduction in the size of explosive that a potential terrorist could carry in a backpack on a ferry.

To model this alternative requires adjusting the explosive's size distribution to account for the smaller carry-on bag. To represent this, the alternative defines a maximum backpack size that in turn reduces the maximum explosive size from 50 pounds to 40 pounds. Thus, the resulting distribution function is

$$x \sim N(28,10;1,40).$$

A second alternative ($a2$), is a screening program with two components. The first component involves some type of x-ray device to scan carry-on bags. The second component involves the inspection of vehicles by a security screener. As with any security program or procedure, there is the question of effectiveness. If an x-ray device were 100 percent effective in detecting explosives in carry-on bags, the risk of a backpack IED would effectively be reduced to zero. However, this is usually not the case as x-ray machines are not 100 percent effective. For this alternative historical data from a similar program is useful. Studies conducted on weapons detection have shown that x-ray machines can be up to 95 percent effective.[171] However, the weaker element in the screening process is the human screener who screens the vehicles or interprets the x-rays. The Federal Aviation Administration has conducted studies in which inspectors have attempted to smuggle weapons onboard airlines, and they report an 80 percent detection rate.[172] This seems to indicate a 15 percent reduction in detection (from 95 percent) based on the human element.

With this kind of data in hand, the risk analyst can incorporate the alternative effectiveness factor to determine the effect on risk. For modeling purposes, the analyst

[171] William A. Crenshaw, "Civil Aviation: Target for Terrorism," *Annals of the American Academy of Political Science* 498, (Jul, 1988), 64.

[172] Ibid., 65.

must now consider that given an IED attack in a backpack, what is the likelihood that the screening process will detect the explosive and stop the attack? By incorporating this into the model, a new risk curve can be developed that represents the reduction in risk resulting from the incorporation of the alternative at hand.

The third alternative ($a3$), is a ferry passenger and boat rental patron screening system that is similar to the Computer Assisted Passenger Pre-Screening System (CAPPS) system. CAPPS is a system that attempts to screen individuals based on travel patterns, financial transactions, personal records, and law enforcement and intelligence databases.[173] For simplicity, this alternative simply runs a background check to determine if the person is on the Terrorism Watch List, has an outstanding arrest warrant, or has been flagged by the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) system. US-VISIT is supposed to provide a mechanism to track non-immigrants who overstayed their visas.[174] Modeling this alternative poses the greatest challenge of the three in that there is little open source data that indicates how effective a system like this might be. This is mostly due to the similar systems mentioned being relatively new with little history upon which to draw effectiveness data.

The problem facing the manager of the Port Security Grant Program is to decide which, if any, of these alternatives is to be funded. A risk-based approach requires that the decisions be a function of the extent to which each alternative reduces risk. In terms of the notation of Chapter III, the set of alternatives contain three elements:

$$A = \{a_1, a_2, a_3\}.$$

Each of these requires a budget, so the budget requests are contained in another set of three elements:

$$B = \{b_1, b_2, b_3\}.$$

The decision to be made by the manager is now expressed by the values assigned to the three elements of the decision set:

---

[173] Mitchel A. Sollenberger, *Sensitive Security Information and Transportation Security: Background and Controversies*, (Washington D.C.: Congressional Research Service, 5 February 2005), 4.

[174] Lisa M Seghett and Stephen R. Vina, *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*, (Washington D.C.: Congressional Research Service, 26 January 2006), 1.

$$D = \{d_1, d_2, d_3\}.$$

For example, if the manager decides on funding all three alternatives then $D = \{1,1,1\}$. To solve the decision problem, the manager requires three risk measures: $R(D_1), R(D_2), R(D_3)$ where for notional convenience we use $R(D_1)$ to denote $R(D)$ when $D = \{1,0,0\}$, $R(D_2)$ to denote $R(D)$ when $D = \{0,1,0\}$, and $R(D_3)$ to denote $R(D)$ when $D = \{0,0,1\}$. These risk measures then give rise to three risk reductions: $\Delta R(D_1), \Delta R(D_2)$, and $\Delta R(D_3)$ that serve as the basis upon which the decisions are made. The next step is to compute each alternative's risk measure and the associated risk reduction (relative to the baseline or "do nothing" situation). To accomplish this, re-compute the fatalities under each of the alternatives.

The model for casualties C is dependent on the alternatives and is expressed as:

$$C(D) = \frac{\pi r(x(D))^2}{S} \bullet y.$$

Where $x(D)$ signifies the dependency of the explosive weight (size) on the decision. If $d_1 = 1$ then, then policy option a_1 is implemented and the size restriction limits the explosive to no more than 40 pounds.

Furthermore, if $d_2 = 1$ then policy option a_2 is also implemented and:

$x = 0$ with probability P_d while

$x \sim N(28,10;1,40)$ with probability $1 - P_d$

Where P_d is the probability of detection of the x-ray process. This includes two factors: the effectiveness of the x-ray machine and the effectiveness of the human screener. If the explosive is detected then $x = 0$ which means there is no explosive. However, detection probability is not known with certainty and is only an estimate. To capture this effect, P_d is treated as uncertain and is modeled using a Beta(p,q) distributed random variable. Numbers from this distribution range between 0 and 1 with mean value = p/(p+q).

In summary, this type of analysis is then repeated for all additional alternatives being considered. It is also important to consider the possibility that an alternative is effective at reducing the risk for more than one threat. This model incorporates the three

alternatives previously discussed. The first alternative is aimed only at preventing the backpack IED threat. The second alternative is aimed at preventing the backpack IED threat and the IED in a vehicle threat since the screening system screens carry-on bags and vehicles. The third alternative is aimed at preventing all three IED threats: the backpack IED threat, the IED in a vehicle threat, and the small boat IED attack. The third alternative accomplishes this by screening all potential ferryboat passengers and may prevent them from boarding the boat. Also, the third alternative screens potential boat renters in the general vicinity of a port and may prevent them from renting a boat.

The resulting risk curves for the backpack IED threat for all three alternatives are presented in Figure 18. Prior to analyzing the risk curves, the decision maker must specify c^* (maximum accepted value of risk). For this example, it is assumed that the decision maker has set $c^* = 50$. An analysis of the risk curves shows that each of the alternatives has some risk reducing effect for the backpack IED. Moreover, alternatives a_2 and a_3 are the more effective with alternative a_2 being the most effective. These results are consistent, given that alternatives a_2 and a_3 are screening programs that may prevent an attacker from placing an IED onto a ferryboat. However, the difference in risk reduction between a_2 and a_3 is indicative of the projected effectiveness of the programs.

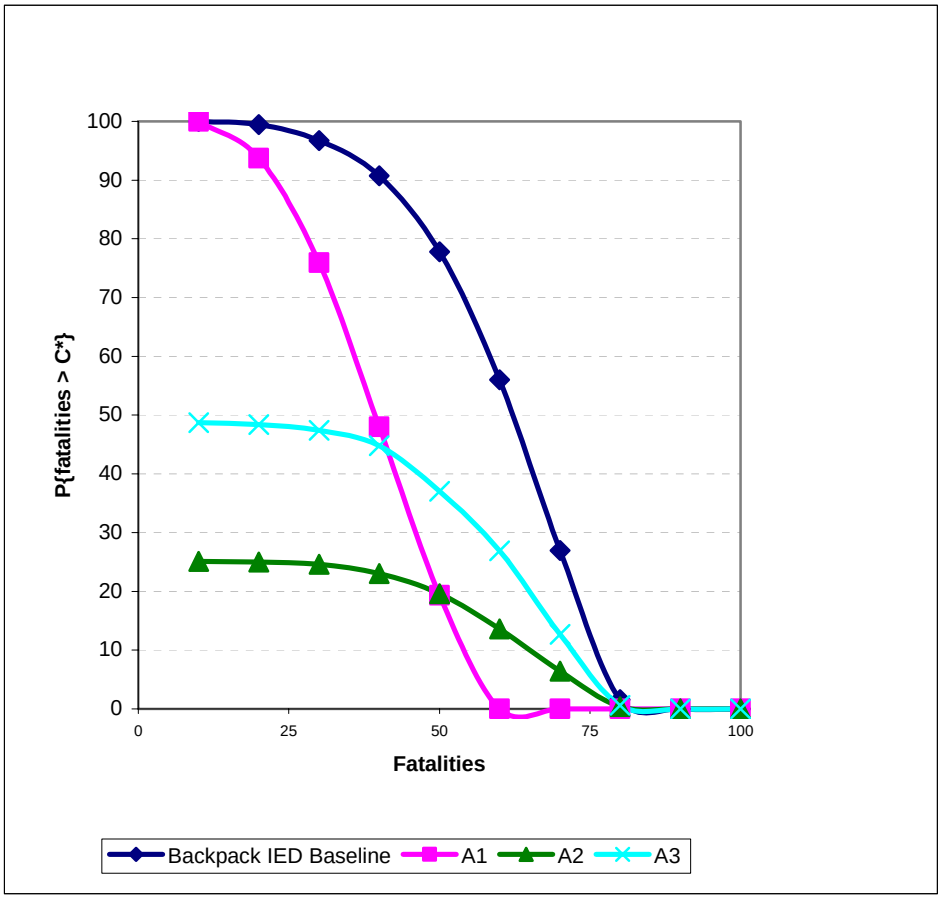

Figure 18 Risk Curves: Backpack IED Baseline and Alternatives

The resulting risk curves for the vehicle IED threat for alternatives a_2 and a_3 are presented in Figure 19. Alternative a_1 is not shown, as it has no effect against the vehicle IED threat. An analysis of the risk curves shows that both alternatives a_2 and a_3 have some risk reducing effect for the vehicle IED. Furthermore, alternatives a_2 indicates a more risk reduction than alternative a_3. This is consistent, given that alternative a_2 advertises a slightly higher effectiveness rate than alternative a_3.

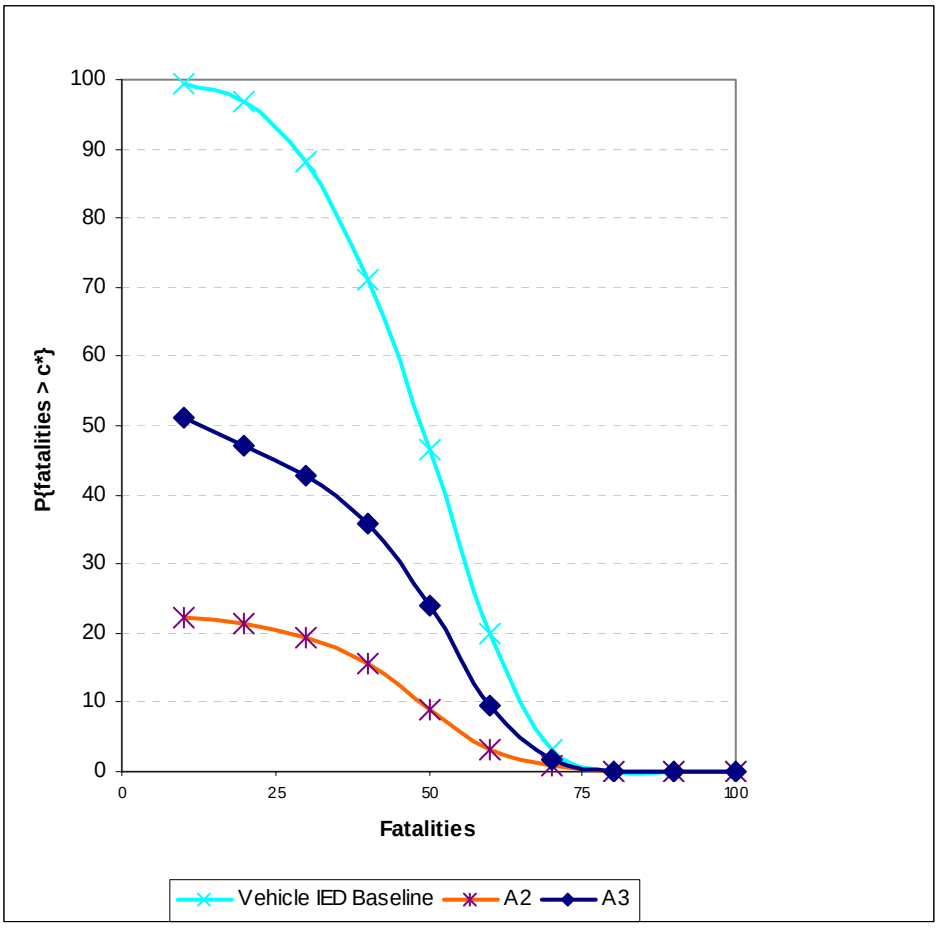

Figure 19 Risk Curves: Vehicle IED Baseline and Alternatives

The resulting risk curve for the SBA IED threat for alternative a_3 is presented in Figure 20. Alternative a_1 and a_2 are not shown as they have no effect against the SBA IED threat. An analysis of the risk curve shows that alternative a_3 is effective at reducing the risk for the vehicle IED, which once again is consistent given that the probability of detecting an attacker (P_d) is not 100 percent.

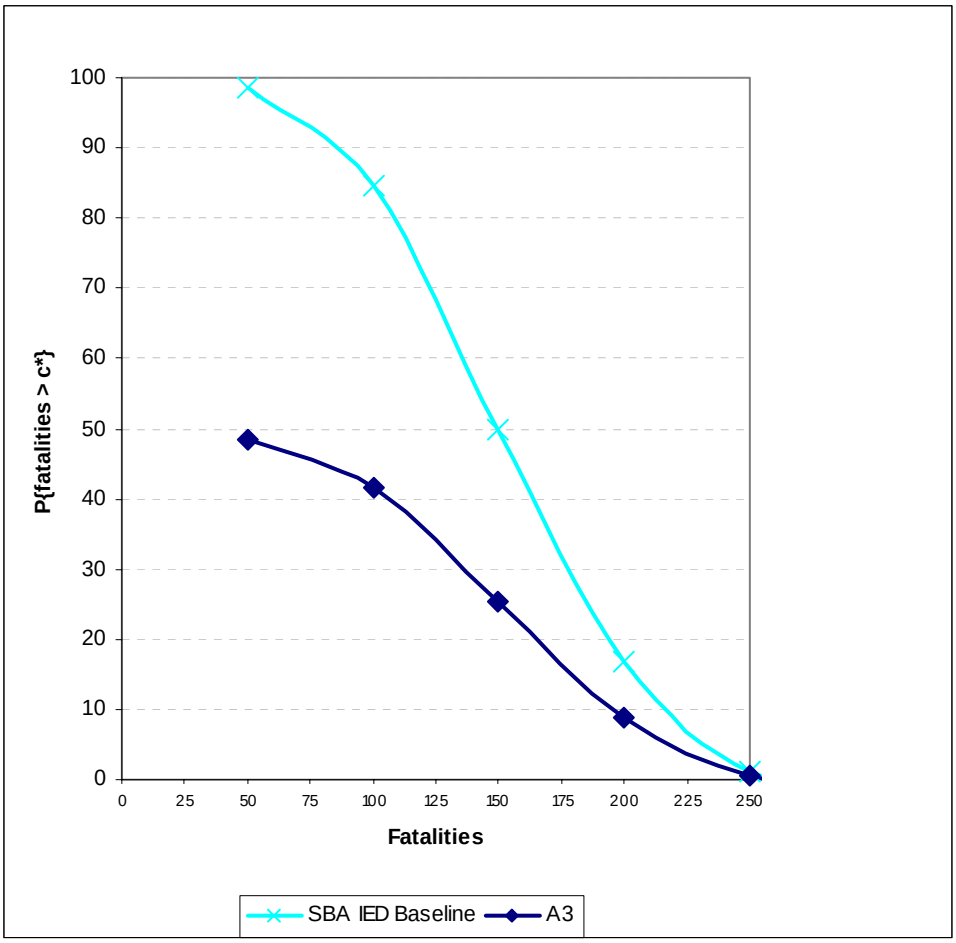

Figure 20 Risk Curves: SBA IED Baseline and Alternative *a*3

G. POLICY OPTIONS ANALYSIS

Having explored various aspects of applying a model to the Port Security Grant program, the final step is to present the output in a manner that allows the decision maker to evaluate the risk reduction potential given the cost involved. A risk analysis model, despite the level of detail, is of no value unless the results are understandable, believable, and tailored to the problem at hand.[175] Moreover, considering that QRA uses complex models involving probability distributions and statistics, understanding QRA results can be a challenge for decision makers. It is therefore imperative that the results of a model be presented in a form that is clearly understood by the decision maker and aids in the decision making problem.

[175] Vose, 267.

The research objectives of this study were to present a methodology that meets the criteria outlined by the abundance of policy guidance documents and to present an alternative approach to using a single number when attempting to quantify risk. The approach presented here utilizes distribution functions to better inform the decision maker on the nature of the uncertainty and the risk. A final objective of this study was to incorporate an approach that allows a cost tradeoff analysis and highlights the robustness of resource allocation in the area of port security. Homeland security policymakers should have the means to connect the risk to the resources allocated. This section addresses the final research objective and shows how risks and costs can be connected in order for the decision maker to make resource allocation decisions.

1. Identification of Costs Associated with Identified Alternatives

Each of the policy alternatives presented to the decision maker will have a required budget (cost). Some costs may involve a one-time purchase and installation of equipment such as a fence or a lock. Other costs may be more long-term, such as a contract that includes security personnel or maintenance of a system. Additionally, there are indirect costs associated with security alternatives. For example, Schneier discusses security costs for the air travel and states that "most countermeasures that increase the security of air travel certainly cost us significantly more money, and will cost us in terms of time and convenience."[176] Schneier makes the point that the mere loss of time also equates to loss of money.

Given all the potential types of costs, a determination is required to distinguish what costs to include into the risk versus cost analysis. The inclusion of upfront costs such as the costs associated with the purchase and installation of equipment is a good starting point. One way to capture the long-term costs is to use life-cycle cost. This concept includes both one-time and recurring cost such as annual labor and operations expenses.

Generally, projected costs are provided upfront when a contractor is bidding for a project. In the case of the Port Security Grant Program, applicants are required to specify

[176] Schneier, 18.

their projected costs as part of the grant application.[177] The applicant guidance kit provides a budget detail worksheet to be submitted with their application.

The costs of the three policy alternatives that are incorporated into the model for this project are notional and are for example only. The notional costs for each of the alternatives are listed in Table 2. Policy alternative a_1 will incur a slight upfront cost to install a mechanism for checking bag size. However, most of the cost associated with this alternative will instead come in the form of lost revenue for the ferry company as a result of patrons choosing other forms of transportation for the inconvenience. Policy alternative a_2 does involve both up front costs in terms of x-ray equipment and a contract to pay the screeners. Policy alternative a_3 involves contracting a company to construct a computer system and the costs of installing the system and associated networking components at all the ferry terminals and boat rental locations for a given port resulting in the highest price tag.

Policy Alternative	**Cost**
Maximum Carry-on Policy (a_1)	\$100,000 (b_1)
Bag and Vehicle Screening Program (a_2)	\$500,000 (b_2)
Personnel Screening System (a_3)	\$700,000 (b_3)

Table 2 Policy Alternative Costs

2. Construction of Risk versus Cost Plots

Once the cost for each of the alternatives is obtained, the data can be plotted on a graph along with the corresponding risk. The risk values are taken from the model simulation as discussed in the previous section.

Next the risk and cost are plotted on one graphic so that the decision maker can compare cost and risk among multiple alternatives (Figure 21). This plot shows each of the alternatives plotted where the x-axis represents the cost and the y-axis represents the risk. Additionally, the baseline data points are plotted for reference purposes to show the existing risk level with none of the current alternatives being implemented. The analyst

[177] U.S. Department of Homeland Security, *Fiscal Year 2005 Port Security Grant Program: Program Guidelines and Application Kit*, D-1.

must remember that the data risks plotted are associated with the consequence type and threshold defined by the decision maker. In this scenario, the consequence type is fatalities and the threshold is 50. This number is set by the preferences of the decision maker to represent the unacceptable outcome.

The following provide several examples to the reader as to how to read and interpret the graph. Once again, when referring to risk, it referrers to the risk of fatalities exceeding 50. Thus the baseline risk of a backpack IED attack, a vehicle IED attack and an SBA IED attack is .78, .47, and .97, respectively. The same logic applies to reading the risk for each attack type given the policy options a_1, a_2, and a_3. For example, given policy option $a3$, the risk of a backpack IED attack, a vehicle IED attack and an SBA IED attack are .38, .24, and .48 respectively. Additionally, the cost to implement the alternatives can be read on the x-axis.

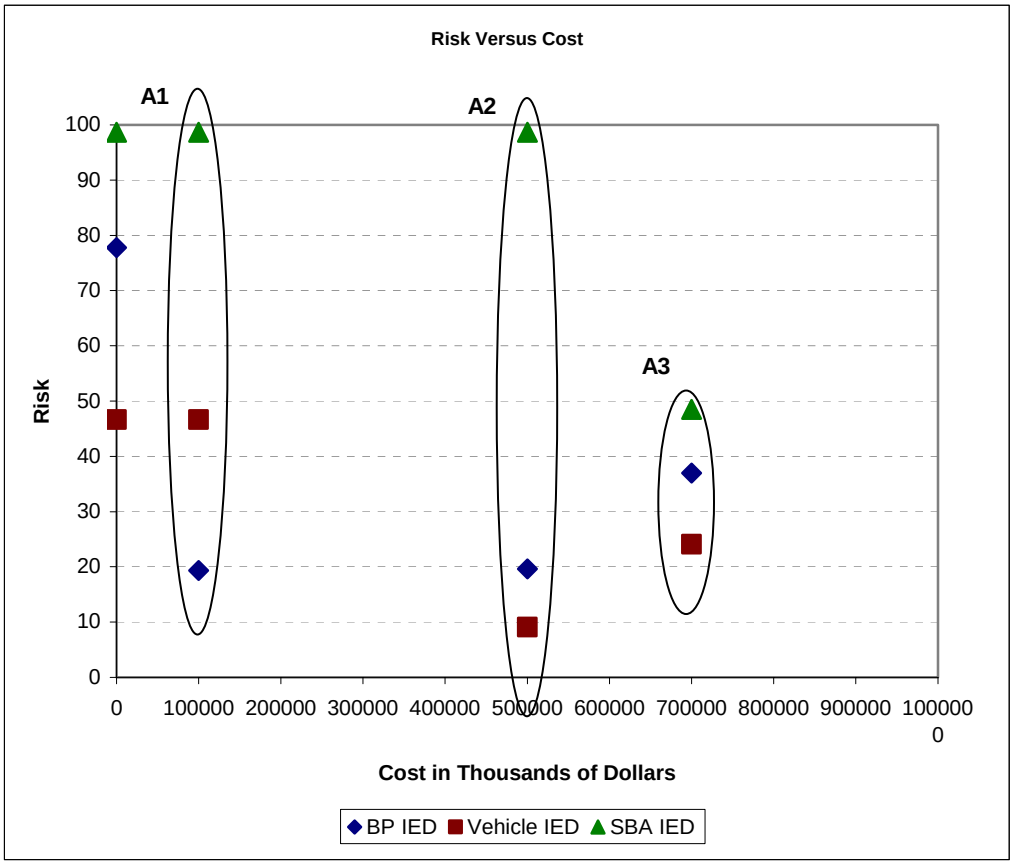

Figure 21 Risk versus Cost Plot

Figure 21 indicates that all three alternatives are somewhat effective at reducing the risk associated with a backpack IED attack. Also, only alternatives a_2 and a_3 are effective at reducing the risk of a vehicle IED. While, only alternative a_3 has any effect on reducing the risk of a small boat attack.

If the decision maker's priority is a robust policy option that reduced the risk of all three threats, the best option would be alternative a_3. This alternative, however, comes with the highest price tag. On the other hand, alternative a_2 might look more attractive given either of two conditions. First, the decision maker is more concerned about the backpack and the vehicle IED threat and not as much about the small boat attack IED threat. Or second, the decision maker is budget constrained and only has $500,000 to allocate to the port security grant program. In the first condition, the decision maker concern is driven by likelihood of occurrence. Importantly, this is not factored into model and can be subjective. As previously discussed, the risk presented here is strictly in terms of consequences.

This policy options analysis approach clearly offers a way for the decision maker to view risk versus cost tradeoffs in one product. The decision maker is able to evaluate and prioritize policy alternatives in an effort to maximize robustness and achieve the greatest risk reduction for the given costs. This fulfills the final research objective and offers one possible answer to one of the DHS IG's critiques of the PSG. Additionally, the approach addresses recommendations made from the 9/11 Commission pertaining to effective resource allocation based on risk.

H. MODEL OMISSIONS

The model constructed for this thesis was designed to provide a simple yet accurate representation of the required steps to perform a quantitative risk analysis. Therefore, there were several details that were intentionally omitted in an effort to reduce the complexity. The omitted details were not necessarily due to lack of data availability but in most cases is due to lack of data access. The details omitted on the basis of simplicity warrant a brief overview.

First, in order to model the effects of an explosion onboard a ferryboat, the exact layout of the vessel should be represented. This includes the various passenger levels,

placement of compartments, construction of walls and floors between compartments, location of glass windows, etc. The model here examined immediate fatalities that directly resulted from the explosion itself as a function of overpressure and explosive casing fragmentation. Other factors can certainly contribute to fatalities such as the possibility of drowning, ensuing fires following an explosion, or person who initially receive serious injuries that lead to a delayed death.

Second, various types of explosives can be used for an IED. The model here incorporated only TNT. A more detailed model would include the spectrum of explosives such as Ammonium Picrate, HBX-3, Military Dynamite (MVD), Pentolite, Torpex, and Tritonal, just to name a few.[178] The ability exists to model other explosives from a blast effects perspective by converting the explosive type into a TNT equivalent weight.

Finally, the present model incorporates only one possible outcome resulting from an IED attack on a ferry—fatalities. A decision maker might be interested in other outcomes such as injuries, immediate and long-term economic damages, and psychological effects. Each of these components could be incorporated into the model using the same steps described previously. The injury component is fairly straightforward and not difficult to model. One challenge with injuries however, is that they can vary in range of severity and the analyst must decide how to characterize the injuries.

The ability to model economic damages is not as straight forward. Immediate economic damage such as the cost of the boat itself either in terms or repair or replacement costs, is easily quantifiable. The long-term economic damages are more challenging to measure. These might include aspects such as loss of revenue over some period of time resulting from the loss of a ferryboat and the reluctance of the population to utilize that mode of transportation both at the affected port and at other ports across the country.

In summary, the model omissions were a function of simplification and data availability. Every scenario that an analyst attempts to model will have unique characteristics. The scope of analysis will drive the level of detail required. The bottom line is that if the decision maker wishes to use QRA, a comprehensive model can be constructed with the applicable details included assuming access to the required data is

[178] Cooper, 406.

available. In situations where the required data is not available, assumptions or approximations are required and thus, need to be clearly communicated to the decision maker.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. RESEARCH IMPLICATIONS AND FINDINGS

This study explores two research areas. First, it presents a methodology by which risk is quantitatively assessed and determines its feasibility for homeland security resource allocation. In doing so, this study presents a quantifiable definition of risk. This study also showed that uncertain variables can be represented using a range of values (distribution function) as opposed to single point estimates. Addressing the second research area—communication of risk to decision makers—this study demonstrates that it is possible to translate the effects of policy alternatives on risk into management action so that decision makers can effectively allocate limited counter terrorism resources. In exploring these areas, this study has shown that there are benefits and challenges to using QRA for homeland security resource allocation. This section summarizes these benefits and shortcomings and provides recommendations for homeland security policymakers considering using or mandating a risk-based approach for allocating resources.

1. Benefits of Quantitative Risk Analysis for Homeland Security Resource Allocation

There are numerous advantages for using quantitative risk analysis for homeland security resource allocation. QRA offers a systematic analytical process that provides policymakers with estimated risk reduction potential associated with policy alternatives. The process acknowledges that while risk generally cannot be eliminated, measures can be taken to help reduce it.

Risk analysis has a proven track record. Many industries with characteristics similar to homeland security have successfully used QRA. These typically include industries focused on improving safety, including environmental or nuclear plant safety.[179] The insurance industry also uses QRA to evaluate relationships between smokers and lung cancer.[180] The same analysis can apply to areas of homeland security when evaluating relationships between terrorist attacks and consequences.

[179] Molak, 6-7.

[180] Ibid., 7.

One of the primary advantages of quantitative risk analysis is that it provides the ability to address significant amounts of uncertainty. The primary source of uncertainty includes the variations and errors that occur in the attempt to assign estimated values to threat, vulnerability, and consequence.[181] This uncertainty is best represented through probability distribution functions as opposed to single point estimates. Furthermore, using a probability density function reduces the effects of subjective judgment by representing variables using a range of possible values as opposed to a single value.

A risk-based methodology can also help the decision maker perform a cost benefit analysis by showing the tradeoffs between resource allocation and risk reduction.[182] This study demonstrates this by showing how decision makers can view the risk versus cost trade-off for a given policy option in a single dimension. Furthermore, the methodology developed here gives decision makers a tool for analyzing multiple policy options on one product so that they can make decisions as to what combinations of policy alternatives represent the most effective use of limited resources.

Finally, as the 9/11 Commission concluded, a risk-based approach to resource allocation can help reduce organizational and political bias that can sometimes influence decisions.[183] Most state and local officials would argue that more resources are needed for homeland security, but not all sectors or cities face equal risk of being the target of a future terrorist attack. A risk-based approach can help reduce political bias and guide decision makers toward more objective reasoning.

2. Challenges with a Quantitative Risk Analysis for Homeland Security Resource Allocation

The first challenge is inherent to the definition of risk itself. First, there is a distinction between qualitative versus quantitative risk. This study focused on quantitative risk and highlighted in detail the many variations of its definition of risk. Most of the definitions presented here use the concepts of threat, vulnerability, and consequence in one form or another. Breaking risk into the components of threat, vulnerability, and consequence is problematic. Regarding the threat component, there is a distinct difference

181 Willis et al., xvii

182 U.S. Government Accountability Office, *Homeland Security, A Risk Management Approach Can Guide Preparedness Efforts*, 2.

183 National Commission on Terrorist Attacks Upon the United States, 396.

between identifying what bad things can happen and assigning a likelihood value to the possibility of that event occurring. Initial attempts to quantify the threats for this research proved futile. Most threat data comes from intelligence channels but are often times vague and subjective. A better approach is to view the threat as what bad things can happen and, more importantly, what the outcome would be should an attack happen. Thus, it is more feasible to focus on vulnerability and consequence.

While it makes some sense to separate vulnerability and consequence, they are intertwined. For example, a policy option that limits the size of an explosion will obviously limit how many people get killed or injured. On the other hand, a policy option that might thwart an attack altogether not only reduces vulnerability but also, by default, reduces consequences since the attack doesn't happen. Therefore, a better solution is to not waste time differentiating the two and accept the fact that they are intertwined. This results in modeling them together during the QRA process.

Another challenge with QRA is the necessary detail and the amount of data required to implement it. The process of generating the necessary data distributions and constructing the required databases takes time. Furthermore, the data can sometimes be difficult to obtain and, where data is not available or cannot be obtained, one is forced to make assumptions. This was the case in this study, primarily due to the lack of access to data. The data required to remove the assumptions made in this PSG model is generally available, given the required access. The level of effort required to implement QRA for homeland security may seem high, but it can be done if decision makers are willing to do so.

Part of the reason for gathering the required data and generating distribution functions is to reduce subjectivity. However, despite efforts to reduce subjectivity, it cannot be eliminated. This is evident during the construction of the model when, despite reasonably available data that described the upper and lower ends of the distributions, assumptions still must be made in regards to the shape or type of distributions to appropriately characterize the data. Furthermore, assumptions were made as to how the attacker would carry out the attack. For example, would the attacker always detonate an explosive near the biggest cluster of people? Or using a SBA attack, would the attacker

always try to impact the target boat center of mass? While these questions represent only a sample of areas where assumptions are required, decision makers using QRA need to realize that subjectivity cannot be completely eliminated.

If decision makers choose to use QRA, analysts need a way to present the results so that decision makers can interpret and evaluate them. Since quantitative risk analysis is heavily reliant on mathematics, the challenge is to present the data in such a way that a decision maker can interpret the results and thus, make effective policy decisions. One solution is to "black box" the inner workings of the methodology and present decision makers with easy-to-read output graphs. However, it is also necessary that the decision maker understand the assumptions and limitations with the methodology, which demands some level of understanding of how the black box functions.

One example of the black boxing concern is found with the USCG and their Maritime Security Risk Assessment Model (MSRAM). MSRAM is a tool used to calculate risks for threats to individual ports using the components of threat, vulnerability, and consequence.[184] The user primarily interacts with the system by assigning vulnerability and consequence values to threat scenarios. When interviewed, USCG end users clearly described their interface to the system and its output, but the inner workings of the system were not as clear. For example, when asked about the origins of the threat data, the response was "Higher headquarters assigns those," and there is little information as to where the numbers originate.[185]

3. Recommendations for Policymakers

Having reviewed the advantages and challenges of QRA, several conclusions can be drawn. First, QRA can be an effective decision support tool. QRA offers one method for conducting a cost-effectiveness analysis with the measure of effectiveness being an estimated risk reduction. The general concept of risk analysis seems to be widely accepted for helping policymakers make resource allocation decisions in a resource limited

[184] Interviews between U.S. Coast Guard Officials and the author on the topic of port risk assessments and MSRAM, 14 April 2006.

[185] Ibid.

environment.[186] Others contend "Risk analysis can be a very valuable tool to bring all the available facts to the discussion table."[187]

Nonetheless, while risk analysis is a valuable tool, it must be used with caution. The level of caution should be proportional to the uncertainty of calculations and degree of assumptions. A carefully performed risk analysis must be accompanied with all the assumptions and uncertainties clearly defined. Too many assumptions and too much uncertainty can become problematic and can only complicate the decision making process. For this reason, analysts should only apply QRA to areas were enough data is available to adequately define the distributions used in constructing models. Based on this study, the type of data that is generally more available is consequence data, as opposed to probability of occurrence (threat) data. Importantly, this allows decision makers to use QRA for applications beyond terrorism such as natural disasters since the focus is on the undesirable outcome and not the cause. It is widely accepted that risk management has applications to natural disasters as well as terrorism.[188] When considering an undesirable event, the outcomes may be the same regardless of whether terrorism was the cause or a natural disaster was the cause. Therefore it makes sense to channel efforts to reduce vulnerabilities and mitigate consequences.

Next, homeland security resources should not be allocated exclusively based on QRA results. QRA should be used in combination with or in addition to other resource allocation methodologies. This allows the decision maker to make decisions based upon data from more than one source. Therefore, policy makes should use caution when attempting to "mandate" a risk-based approach as the sole method for allocating resources. Molak echoes a similar thought:

> The other group of people, represented in Congress and federal government agencies, is very much enamored with risk analysis and is trying to pass laws and establish regulations that would mandate risk-benefit analysis. In such proposals, risk analysis is treated as a panacea, as if the results of risk

[186] U.S. Government Accountability Office, *Risk Management, Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, (December 2005), 16.

[187] Vlasta Molak, "Conclusion," in *Fundamentals of Risk Analysis and Risk Management* ed. Vlasta Molak (New York: Lewis Publishers, 1996), 426.

[188] Government Accountability Office, *Risk Management, Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, (December 2005), 3.

> analysis are not subject to uncertainty inherent in complex social systems. The overuse and over-trust in numbers derived from such risk analysis could be very dangerous for general democratic processes and may gridlock the decision-making process.[189]

One example of combining methodologies can be found in the DHS National Preparedness Guidance. This guidance provides direction on how to implement the National Preparedness Goal which serves the purpose of "establish[ing] measurable priorities, targets, standards for preparedness assessments and strategies, and a system for assessing the Nation's overall level of preparedness."[190] The National Preparedness Guidance recommends a capabilities-based planning approach consisting of ten steps to meet the National Preparedness Goal. While each of these steps will not be discussed in detail here, a common theme found throughout the steps is that the type and level of identified capabilities is proportional to their ability to reduce risk.[191] Thus, using the approach presented in this study, QRA can be combined with capabilities-based planning to direct efforts in the context of capabilities as opposed to dollars.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

The model constructed for this study provides a basic example of QRA and demonstrates the feasibility of the methodology. There are numerous areas where model enhancements can improve its accuracy and usefulness. Additionally, it is valuable to consider applications for QRA beyond the Port Security Grant Program. To that end, the author concludes with a discussion on implications for expanding the scope of analysis for the QRA methodology presented in this study.

1. Model Refinement

First off, numerous assumptions are made either for simplicity or due to insufficient access to data. One area is the ferryboat structure itself. The model here assumed a single passenger compartment when, in reality, there are multiple passenger compartments separated by various structures such as walls and glass. These items would certainly have an effect on the blast effects associated with a detonation of an explosive onboard a ferryboat.

---

[189] Molak, "Conclusion," 425.

[190] Department of Homeland Security, *National Preparedness Guidance* (Washington, D.C.: Department of Homeland Security, 27 April 2005), 1.

[191] Ibid., 7-9.

Another area for model refinement is the data distributions themselves. Most of the distributions used here were normal distributions. A more thorough way to specify the distributions is to obtain actual data and perform a data fit. An example of this is the ferry boat utilization rate. This data is generally available given the proper "need to know." Using historical data, where they exist, the analyst can define a more accurate distribution that better represents the range of uncertainty.

2. Incorporation of Multiple Consequence Types

The model constructed here focuses exclusively on a single representation of consequence: fatalities. It is reasonable to expect that a decision maker would also be concerned about injuries, structural damage, economic losses, and psychological effects on the population. Future expansion of the model can include these other factors. This would allow the decision maker to look at the cost versus risk tradeoff for individual consequences or to look at an aggregate risk value representative of multiple consequences.

3. Policy Analyst Interface

The model described thus far and the policy alternative analysis is done using the student version of the Microsoft Excel "add-in" program @Risk. For this type of model to be useable for an average policy options analyst, a simple end-user interface is necessary. This would most likely consist of some type of graphical user interface (GUI) where the user would simply input data into an input screen. This GUI would act as the interface to a "back box" that would perform the risk number crunching and then display the results to the analyst in a user friendly interactive manner.

Adding a GUI to the model developed here requires modifications but is feasible. In addition to the GUI, it is necessary to incorporate a database containing several different types of data. One piece of required data is the threat information. In this context, threat information consists of a list of threats selectable by the analyst as opposed to likelihood of occurrence. For example, they might include: SBA IED attack, Backpack IED attack, and Vehicle IED attack. Furthermore, each of the threats may require amplifying information. For example, if the analyst selected the SBA attack, he might also specify boat type, explosive type and quantity, and impact parameters. Ultimately, the level of model detail is dependent on the specifications provided by the end-user.

Beyond the threat data, the analyst will also need to provide information about the consequences of concern. Once again, these might include fatalities, injuries, immediate damages, and potential long-term economic damages. The analyst would not only need to specify the consequence type, but also a threshold level for analysis.[192]

The final input concerns policy options and costs. The analyst would need to provide the system with enough information about the projects to redefine the affected data distributions in order to calculate updated risk curves. For example, a policy option consisting of a screening component would require an estimate of effectiveness. This estimate may or may not be readily available bases on similar screening components used previously. Finally, the analyst would need to provide the system with cost data associated with the policy options.

In addition to the user inputs, the system would need to contain several databases or have access to them. These databases would include information such as ferry boat types, boat configuration data, and passenger capacity. Another database might include explosives and blast effects. Since the number of explosive types varies considerably, a database is the best option to maintain a complete list.

Regarding outputs, the system would automatically generate the risk versus cost curves for the decision maker. The system would provide various options for formatting the data, such as the ability to plot a single policy alternative or a combination of selected policy alternatives. This data would be plotted on a graph similar to the one shown in Figure 21.

4. Implications for Expanding the Scope of Analysis

The research presented here focuses exclusively on the Port Security Grant Program, which is primarily concerned with the IED threat to ferryboats. This represents only a small subset of the port security threat. Other port security concerns include container security, land-based attacks against port facilities, and sea-based attacks against

[192] The threshold level for analysis equates to the c^* notation presented in Chapter III.

liquefied natural gas vessels.[193] Resources are being applied in these areas in addition to the PSG program.[194] Thus, decision makers at this level face the same problem of how to effectively allocate finite resources.

The QRA approach presented here demonstrates that an analyst can determine changes in risk associated with policy options. This application is not restricted to the Port Security Grant Program and can be extended to include other areas in port security and even maritime security as a collective. Expanding the level of analysis to include the entire scope of maritime security encompasses other maritime threats that are not necessarily port related. For example, these include areas such as maritime domain awareness, cruise missiles, mines, and underwater attacks using SCUBA gear.[195] Expanding the scope of analysis to these other areas does not significantly change the resource allocation problem and the methodology still applies. One could even consider applying the methodology beyond maritime security to other areas of homeland security.

While expanding the scope of analysis for QRA seems feasible on the surface, making that transition is not without challenges. For instance, as the elements of risk are examined at higher levels, the bounds of the associated distributions expand greatly. Using an extreme example at the homeland security level, one could argue that the range of consequences spans from zero to the entire population of the United States. Granted, this is unlikely and the associated probability is quite low the possibility exists. Importantly, policymakers should note that as the scope broadens, the bounds of uncertainty expand as well.

In conclusion, the risk-based approach presented in this study showed that QRA can be an effective decision aid for homeland security resource allocation. This requires data and mathematical modeling of factors and uncertainty which is not a simple feat. However, just because it is difficult does not mean that it should not be done. QRA can direct the decision maker's focus on the relevant factors required to effectively allocate limited resources. Furthermore, it forces decision makers to think about the problem and minimize the effects of external factors, such as political pressures.

[193] Frittelli, 6.

[194] Ibid., 15-16.

[195] Ibid., 6.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

9/11 Public Discourse Project. 2006. *Final Report on 9/11 Commission Recommendations*. Available from http://www.9-11pdp.org (accessed March 8, 2006).

Abt Associates. 2003. *The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability*. Cambridge: Abt Associates (30 April), Available from http://www.abtassociates.com/reports/ES-Economic_Impact_of_Nuclear_Terrorist_Attacks.pdf (accessed May 30, 2006)

Anonymous. 2004. *Imperial Hubris.* Washington D.C.: Brassey's.

Aven, Terje. 2003. *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective.* England: John Wiley & Sons, Ltd.

Bedford, Tim and Roger Cooke 2001. *Probabilistic Risk Analysis.* Cambridge, UK: Cambridge University Press.

Bernstein, Peter L. 1996. *Against The Gods: The Remarkable Story of Risk.* New York: John Wiley & Sons.

Bowers, Fay and Peter Grier. 2003. "How Al Qaeda Might Strike the U.S. by Sea." *The Christian Science Monitor* (14 May), available from http://www.csmonitor.com/2003/0515/p02s02-usgn.html (accessed 10 October 2006).

Buckshaw, Donald L., Gregory S. Parnell, William L. Unkenholz, Donald L. Parks, James M. Wallner, and O. Sami Saydjari. 2005. "Mission Oriented Risk and Design Analysis of Critical Information Systems." *Military Operations Research* 28: 19-39.

CALSTART 2003. *Passenger Ferries, Air Quality, and Greenhouse Gases: Can System Expansion Result in Fewer Emissions in the San Francisco Bay Area?*. California: CALSTART.

Caudle, Sharon 2005 "Homeland Security, Approaches to Results Management." *Public Performance & Management Review* 28 no. 3: 352-375.

Cooper, Paul W. 1996. *Explosives Engineering.* New York: Wiley-VCH.

Crenshaw, William A. 1988. “Civil Aviation: Target for Terrorism.” *Annals of the American Academy of Political and Social Science* 498:60-69.

Director of National Intelligence. 2006. “Trends in Global Terrorism: Implications for the United States” Available from: http://www.dni.gov/press_releases/press_releases.htm (accessed 29 September 2006)

Evans, James R. and David L. Olson. 2002. *Introduction to Simulation and Risk Analysis.* Upper Saddle River, NJ: Prentice Hall.

Flynn, Stephen 2004. *AMERICA the Vulnerable: How Our Government is Failing to Protect Us from Terrorism.* New York: HarperCollins Publishers.

Frittelli, John F. 2003 *Port and Maritime Security: Background and Issues for Congress*. Washington: Congressional Research Service.

Garrick, B. John. 1997. “Risk Management of the Nuclear Power Industry.” In *Fundamentals of Risk Analysis and Risk Management,* ed. Vlasta Molak, 327-339. New York: Lewis Publishers.

Haimes, Yacov Y. 1998. *Risk Modeling, Assessment, and Management.* New York: John Wiley & Sons.

Howland, Jonathan 2004 “Hazardous Seas.” *Jinsa Online*. Available from http://www.jinsa.org/ (accessed 10 November 2006)

Kaplan, Eban 2006 *Risk-Based Homeland Security Spending*. Council on Foreign Relations. Available from http://www.cfr.org (accessed February 27, 2006).

Kaplan, Stanley and B. John Garrick, 1981 “On the Quantitative Definition of Risk.” *Risk Analysis* 1 no 1:11-27.

Molak, Vlasta. 1997. “Introduction and Overview.” In *Fundamentals of Risk Analysis and Risk Management,* ed. Vlasta Molak, 1-10. New York: Lewis Publishers.

———. 1997. “Conclusion.” In *Fundamentals of Risk Analysis and Risk Management,* ed. Vlasta Molak, 423-426. New York: Lewis Publishers.

Mun, Johnathan. 2004. *Applied Risk Analysis: Moving Beyond Uncertainty in Business.* Hoboken: John Wiley & Sons.

National Commission on Terrorist Attacks Upon the United States 2004. *The 9/11 Commission Report.* New York: W.W. Norton.

Papoulis, A. 1965. *Probability, Random Variables and Stochastic Processes.* New York: McGraw-Hill.

Pate-Cornell, Elisabeth and Seth Guikema 2002 "Quantitative Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures" *Military Operations Research* 7 no. 4: 5-23.

Pate-Cornell, Elisabeth 2002 "Risk and Uncertainty Analysis in Government Safety Decisions." *Risk Analysis* 22 no. 3: 633.

Perl, Ralph 2005 *Combating Terrorism: The Challenge of Measuring Effectiveness.* Washington: Congressional Research Service.

President of the United States 2003 *Homeland Security Presidential Directive/Hspd-7.* Available from http://www.whitehouse.gov/ (accessed March 15, 2006).

———. 2005. *National Strategy for Homeland Security.* Available from http://www.whitehouse.gov/ (accessed March 15, 2006).

———. 2005. *National Strategy for Maritime Security.* Available from http://www.whitehouse.gov/ (accessed March 15, 2006).

———. 2003. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Available from http://www.whitehouse.gov/ (accessed March 15, 2006).

Reese, Shawn. 2005. *Risk-Based Funding in Homeland Security Grant Legislation: Issues for the 109th Congress*. Washington: Congressional Research Service.

———. 2006. *Homeland Security Grants: Evolution of Program Guidance and Grant Allocation Methods*. Washington: Congressional Research Service.

Rodrigue, Jean-Paul, Claude Comtois, and Brian Slack 2006. *The Strategic Space of International Transportation*. New York: Routledge.

Roper, Carl A. 1999 *Risk Management for Security Professionals*. Woburn, MA: Butterworth-Heinemann.

Schneier, Bruce 2003. *Beyond Fear, Thinking Sensibly About Security in an Uncertain World.* New York: Copernicus Books.

Seghett, Lisa M. and Stephen R. Vina. 2006 *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*. Washington: Congressional Research Service.

Sollenberger, Mitchel A. 2004 *Sensitive Security Information and Transportation Security: Background and Controversies*. Washington: Congressional Research Service.

Strohm, Chris and Darren Goode 2006 "House Lawmakers Introduce Security Bill." *Congress Daily* (14 March).

U.S. Coast Guard. 2002 *The U.S. Coast Guard Maritime Strategy for Homeland Security*. available from http://www.uscg.mil/news/reportsandbudget/Maritime_strategy/ (accessed 16 March 2006).

———.2003. *Overview of Area Maritime Security Regulations, 33 CFR Part 103*, (October), available from http://www.aapa-ports.org/govrelations/ (accessed 22 May 2006)

U.S. Department of Defense 2001. *Quadrennial Defense Review Report.* Available from http://www.defenselink.mil/qdr/ (accessed 27 October 2006).

———. *Quadrennial Defense Review Report.* Available from http://www.defenselink.mil/qdr/ (accessed 27 October 2006).

U.S. Department of Homeland Security. 2005. *National Preparedness Guidance.* Available from http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm (accessed 5 December 2005).

———. 2005 *Fact Sheet: Strengthening National Preparedness: Capabilities-based Planning.* Washington: Department of Homeland Security.

———. 2005. *Fiscal Year 2005 Port Security Grant Program: Program Guidelines and Application Kit.* Washington: Department of Homeland Security.

———. 2005. *Budget-in-brief, Fiscal Year 2006.* Available from http://www.dhs.gov/dhspublic/display?theme=12 (accessed 25 January 2006).

———. 2004. *Fiscal Year 2004 Urban Area Security Initiative Grant Program: Program Guidelines and Application Kit.* Washington: Department of Homeland Security.

U.S. Department of Homeland Security Office of Inspector General. 2005 *Review of Port Security Grant Program.* Washington: Department of Homeland Security, January.

U.S. Department of Homeland Security Office of Inspector General. 2006 *Follow Up Review of Port Security Grant Program.* Washington: Department of Homeland Security, February.

U.S. Government Accountability Office. 2001 *Homeland Security, A Risk Management Approach Can Guide Preparedness Efforts*. Washington: United States Government Printing Office, October.

———. 2005 *Risk Management, Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*. Washington: United States Government Printing Office, October.

Vose, David 1996. *Quantitative Risk Analysis: A Guide to Monte Carlo Simulation Modelling*. New York: John Wiley & Sons.

Ward, John and Keren DeYoung, 2006. "Plot to Bomb U.S.-Bound Jets is Foiled: Britain Arrests 24 Suspected Conspirators." *The Washington Post Foreign Service* (11 August). Available from http://www.washingtonpost.com/wp-dyn/content/article/2006/08/10/AR2006081000152.html (accessed 25 August 2006).

Weber, Christian 2006. *Maritime Terrorist Threat*. New York: New York State Office of Homeland Security.

Willis, Henry, Andrew Morral, Terrence Kelly, and Jamison Medby. 2005 *Estimating Terrorism Risk.* Santa Monica: RAND Corporation.

Yemen Gateway. 2001. "Attack on the USS Cole." *Yemen Gateway*. (14 March). Available from http://www.al-bab.com/yemen/cole2.htm (accessed 19 September 2006).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Diane Miller (diane.miller@dhs.gov)
   Transportation Security Administration (DHS)
   Washington, D.C.

4. Ryan Owens (ryan.owens@dhs.gov)
   Office of Grants and Training
   Washington, D.C.