NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

https://apps.dtic.mil/dtic/tr/fulltext/u2/a527037.pdf (retrieved 20 January 2019)

THESIS

IMPROVING THE COAST GUARD PORTS, WATERWAYS AND COASTAL SECURITY OUTCOME MEASURE

by

Matthew E. Cutts

June 2009

Thesis Advisor:	Robert Josefek
Second Reader:	Manson Brown

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
June 2009

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE Improving the Coast Guard Ports, Waterways and Coastal Security Outcome Measure

5. FUNDING NUMBERS

6. AUTHOR(S) Matthew E. Cutts

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 is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This thesis examines the Coast Guard Ports, Waterways and Coastal Security (PWCS) Outcome Measure. The first goal was to determine if the current measure accurately reflects Coast Guard mission effectiveness in achieving homeland security. The PWCS Outcome Measure provides information on risk reduction due to threat, vulnerability and consequence management by the Coast Guard with respect to 15 maritime terrorism scenarios. While the current measure provides a good sense of Coast Guard effectiveness in reducing the risk of maritime terrorism, there are a number of areas for potential improvements. This finding led to the second goal of the research, which was to provide recommendations to more accurately assess Coast Guard homeland security mission effectiveness. As a formative evaluation of the PWCS Outcome Measure, the research provides insight into recommendations for improving this measure from several experts both inside and outside the Coast Guard. In addition, it outlines considerations to implement these recommendations.

It is critical to optimize the application of limited resources to the issue of maritime terrorism, and this can only occur through accurate measurement of mission effectiveness in preventing terrorism. This study is applicable to the improved assessment of terrorism risk reduction efforts, especially in the maritime environment.

14. SUBJECT TERMS Coast Guard, Risk Analysis, Risk Assessment, Risk Management, Risk Modeling, Expert Judgment, Heuristics and Biases

15. NUMBER OF PAGES
143

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	UU

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 is unlimited

IMPROVING THE COAST GUARD PORTS, WATERWAYS AND COASTAL SECURITY OUTCOME MEASURE

Matthew E. Cutts
Captain, United States Coast Guard
B.S., United States Coast Guard Academy, 1983
M.S., University of Illinois, 1989

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
June 2009

Author: Matthew E. Cutts

Approved by: Robert Josefek
Thesis Advisor

Manson Brown
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines the Coast Guard Ports, Waterways and Coastal Security (PWCS) Outcome Measure. The first goal was to determine if the current measure accurately reflects Coast Guard mission effectiveness in achieving homeland security. The PWCS Outcome Measure provides information on risk reduction due to threat, vulnerability and consequence management by the Coast Guard with respect to 15 maritime terrorism scenarios. While the current measure provides a good sense of Coast Guard effectiveness in reducing the risk of maritime terrorism, there are a number of areas for potential improvements. This finding led to the second goal of the research, which was to provide recommendations to more accurately assess Coast Guard homeland security mission effectiveness. As a formative evaluation of the PWCS Outcome Measure, the research provides insight into recommendations for improving this measure from several experts both inside and outside the Coast Guard. In addition, it outlines considerations to implement these recommendations.

It is critical to optimize the application of limited resources to the issue of maritime terrorism, and this can only occur through accurate measurement of mission effectiveness in preventing terrorism. This study is applicable to the improved assessment of terrorism risk reduction efforts, especially in the maritime environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

It has been a great privilege to be associated with the Center for Homeland Defense and Security over the past 18 months, especially with all the members of cohorts 0705/0706, from whom I have learned so much. Thanks to Chris Bellavita for pulling us into the world of academia, and to Chris and Dave Brannan for helping me make connections with important sources of information and inspiration. To Heather Issvoran, Alana Ringle, Craig Coon, and Kristin Darken, for taking us in like family, and handling every imaginable logistical, computer, and moodle issue with aplomb. To Nadav Morag and Lauren Wollman, who started us on the road toward our theses and helped all along the way. Finally, to my advisor Bob Josefek and second reader Admiral Manson Brown, your guidance and encouragement throughout the entire thesis process made possible what seemed insurmountable at times.

To Lieutenant Commander Brady Downs, Lieutenant Commander Dave Cooper, Lieutenant Commander Jim Moran, and Matt Mowrer, thanks for developing the foundation on which my work is based; I appreciate your many emails and time on the phone discussing things as they are and as they could be. To Captain Will Ellis, Commander Gwyn Johnson, Commander Roger Wykle, Bob Kelly, Pete Steel and Drema Corbett, for your most able assistance maintaining forward motion on every aspect of Coast Guard Pacific Area Resource Management and Force Readiness Command Implementation during my frequent absences.

Most importantly, I want to express heartfelt thanks to my family. To Ellen Wrynn, my bride and constant companion of over 23 years who has supported me in every professional and academic pursuit, you have my most devoted appreciation for your commitment and love. Only because you handled every aspect of our lives from middle school to high school to college, swim teams to music lessons, Girl Scouts to medical appointments, was it possible to complete this program. To Hannah, who sat next to me doing your homework while I did mine and put up with me being gone for school and work: thanks for your patience. To Zach and Josh, who started college the same time as I started at the Naval Postgraduate School: keep up the good work; you'll graduate before you know it!

I. INTRODUCTION

A. PROBLEM STATEMENT

1. Background

The Coast Guard has 11 mission programs that protect the "vital economic and security interests of the United States including the safety and security of the maritime public, our natural and economic resources, the global transportation system, and the integrity of our maritime borders."[1] Of these 11, five mission programs are directly related to homeland security:

1. Drug Interdiction
2. Migrant Interdiction
3. Ports, Waterways, and Coastal Security
4. Other Law Enforcement
5. Defense Readiness

2. Condition

Twelve measures are published in the latest *Program Assessment on the Coast Guard Ports, Waterways, and Coastal Security* (2006) mission-program area. Of these, one is an efficiency measure, seven are output measures, and four are outcome measures. The outcome measures are most indicative of effectiveness in achieving security in the maritime domain. Three of the four outcome measures indicate estimated risk reduction due to Threat, Vulnerability, and Consequence Management. The outcome measure most indicative of the effectiveness in achieving maritime homeland security is the "Annual Percent Reduction in Terrorism-Related Maritime Risk." This measure combines

[1] Thad W. Allen, *Fiscal Year 2009 President's Budget* (statement to the U.S. Senate Committee on Commerce, Science, and Transportation, Sub-committee on Oceans, Atmosphere, Fisheries, and Coast Guard, Washington, D.C., March 6, 2008) U.S. Coast Guard, http://www.uscg.mil/comdt/speeches/docs/CST_FY09_Budget_6_Mar_08.pdf (accessed March 6, 2008).

estimated risk reduction due to threat, vulnerability, and consequence management for 15 different maritime attack scenarios into a proxy for Coast Guard outcome performance in achieving security in the maritime domain. The *Program Assessment* states, "In order to improve the validity and objectivity of the measure in the future, the Coast Guard intends to invite external experts to participate in the evaluation."[2]

3. Costs

Using measures that do not accurately reflect mission effectiveness can give Coast Guard leaders and Congress a false sense of progress toward securing the homeland. It also hampers efforts to optimize resource allocation. Finally, it may lead to a focus on areas that do not need attention, misleading efforts to acquire improved technology, improve tactics, form stronger partnerships, and pursue better intelligence along with other activities in pursuit of improved operations. Too much focus on areas that do not need attention will lead to resource misallocation, leading to the real cost: the danger that this resource misallocation could result in a successful terrorist attack in the U.S. maritime domain.

B. RESEARCH QUESTIONS

The Coast Guard publishes an annual *Performance Summary*, which reports effectiveness in each of the service's 11 mission programs. This research will examine the measures used to report on performance in the Ports, Waterways, and Coastal Security mission-program.

1. Does the current measure accurately reflect Coast Guard mission effectiveness in achieving homeland security?
2. If not, how can the Coast Guard construct a measure to accurately assess homeland security mission effectiveness?

[2] U.S. Office of Management and Budget, *Program Assessment on the Coast Guard Ports, Waterways and Coastal Security, Assessment Year 2006* (Washington, D.C.: Office of Management and Budget, 2006), White House, http://www.whitehouse.gov/omb/expectmore/detail/10003635.2006.html (accessed December 9, 2007).

C. SIGNIFICANCE OF RESEARCH

While an extremely large amount of research has been conducted in the field of risk assessment, a lesser amount of that research has focused on terrorism risk assessment. There exists an even smaller body of work in the field of maritime terrorism risk assessment. As a result, it is difficult for maritime agencies to rationally allocate resources in their quest to reduce maritime terrorism risk. While the incidence of maritime terrorism is significantly lower than land or air based terrorism, the principles underlying terrorism risk assessment in each environment are applicable to other environments.

As previously mentioned, the Coast Guard publishes an annual *Performance Summary* which reports effectiveness in each of the service's 11 mission programs. This formative evaluation of the Coast Guard Ports, Waterways, and Coastal Security Outcome Measure provides insight into recommendations for improving this measure from a number of experts both inside and outside the Coast Guard. In addition, it will provide a plan to implement these recommendations. It will be applicable to each of the three levels outlined above: maritime terrorism risk assessment, terrorism risk assessment, and risk assessment. As a result, this research should be useful to those who wish to optimize resource allocation in their organization. It may also serve as a foundation for further studies in risk assessment, especially those in the area of maritime terrorism.

This research will be of interest to those working in and around all of the nation's 361 seaports. Since 95 percent of all commerce arrives in the United States through those ports, successful prevention of maritime terrorism affects every single person in this country. It is critical to optimize the application of limited resources to the problem of maritime terrorism, and this can only occur through accurate measures of mission effectiveness in preventing terrorism. Homeland security practitioners and national leaders will find this study applicable to the improved assessment of terrorism risk reduction efforts, especially in the maritime environment.

D. LITERATURE REVIEW

1. Background

The study of the measurement of Coast Guard mission effectiveness in achieving homeland security provides insight into the linkage between resource utilization and risk reduction so that the Coast Guard and other organizations can execute their missions while using taxpayer funding wisely by optimizing resource allocation. While the study and implementation of measurement are both extremely important, these activities are not ends in themselves; they are merely means for an organization to ascertain whether it is making progress toward achieving its goals. This is the thesis put forth by William Casey in "Enterprise Excellence: Driving Strategic Results Instead of Metric Mania."[3] The article lays out a path between enterprise-wide goals and individual actions through informed decision making. This requires the use of metrics to inform decision making, without allowing the collection and analysis of metrics to become the new goal of the organization.

The goal of this research is to improve measurement of Coast Guard effectiveness in achieving homeland security. This requires the ability to measure the current level of terrorism-related maritime risk and project the future level of risk given certain Coast Guard activities. There are a number of sub-literatures that are germane to the assessment of terrorism risk and include literature on:

1. Risk Assessment
2. Risk Modeling
3. Expert Judgment
4. Event Trees

[3] William Casey et al., *Enterprise Excellence: Driving Strategic Results Instead of Metric Mania* (Lakewood, CO: Executive Leadership Group, 2006).

2. Risk Assessment

Risk assessment is part of the larger risk management framework. Conventional risk assessment defines risk as the probability of an undesired event multiplied by the cost of that event: R = P x C. Stephen Unwin and many other authors state that the probability of naturally occurring events such as earthquakes or hurricanes typically follows a Poisson distribution.[4] Terrorism risk analysis defines risk as a function of three components: threat (probability that a specific target will be attacked in a specific way during a specified period), vulnerability (probability that damage occurs, given a threat), and consequences (the magnitude and type of damage resulting from a successful terrorist attack).[5] Terrorism risk does not follow a Poisson distribution because terrorists adjust target selection based on the vulnerability of those targets (threat shifting)[6] and terrorists use adaptive learning to modify future attacks in their quest for success.[7] A number of authors have developed the threat shift model, of note is "Insurance, Self-Protection, and the Economics of Terrorism" by Darius Lakdawalla and George Zanjani.

A key part of assessing terrorism risk is assessing the threat. Gary Ackerman reviews various risk assessment methodologies, examines their failure to properly account for threat, and concludes that this failure leads to over/underestimation of risks, overlooking possible synergistic responses, and exclusion of the dynamic nature of terrorist threats.[8]

[4] Stephen D. Unwin, "Adaptability of Conventional Risk-Based Decision Methods to Homeland Defense," (Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2006), Los Alamos National Laboratory, http://risk.lanl.gov/site2k6/archives/pgm2006.html (accessed January 27, 2008).

[5] Henry Willis et al., *Estimating Terrorism Risk* (Santa Monica, CA: RAND Corporation, 2005), xvi, RAND Corporation, http://www.rand.org/pubs/monographs/MG388/ (accessed January 28, 2008).

[6] Dino Falaschetti and Bryan Roberts, "Threat Shifting: A Key Issue in Terrorism Risk Analysis" (Presented at Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2006) Los Alamos National Laboratory, http://risk.lanl.gov/site2k6/archives/pgm2006.html (accessed January 27, 2008).

[7] Gordon Woo, *Understanding Terrorism Risk* (Newark, CA: Risk Management Solutions, 2002), 7, Risk Management Solutions, http://www.rms.com/Publications/UnderstandTerRisk_Woo_RiskReport04.pdf (accessed January 28, 2008).

[8] Gary Ackerman, "Chasing Shadows: Determining the Terrorist Threat," (presented at Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2007), Los Alamos National Laboratory, http://risk.lanl.gov/site2k7/RS2007Presentations.html (accessed January 2008).

A well-accepted method of risk assessment is probabilistic risk analysis. Numerous authors use this method to predict terrorism risk, including Greg Chavez et al. of the Los Alamos National Laboratory Office of Risk Analysis and Decision Support Systems, Carl Southwell of the USC Center for Risk and Economic Analysis of Terrorism Events, and Rajan Batta et al of the State University of New York at Buffalo. Willis and others have pointed out that a problem with using probabilistic risk analysis is the paucity of terrorism events compared to natural disasters.[9] Improvements in probabilistic risk analysis in the assessment of terrorism risk will only be made when it is possible to more accurately quantify the dynamic nature of terrorist attacks, especially the effects of threat shifting. Just as the analysis of a moving weight on a beam is more difficult than the analysis of a dead weight on that same beam, analysis of an asymmetric terrorist attack is more difficult than analysis of symmetric warfare. Research into the causative factors of threat shifting and their results will lead to more accurate probabilistic risk analysis of terrorism risk.

3. Risk Modeling

Since there is a shortage of data on which to base probabilistic risk analysis, researchers have sought alternative means to assess terrorism risk. Among several authors, Seth Guikema offers game theory as a way to assess terrorism risk by modeling terrorist actions. Game theory models the interaction between terrorists (attackers) and defenders, is based on utility maximization, and allows development of a probabilistic statement of risk.[10] Guikema points out three game theory assumptions: Instrumental Rationality, Consistently Aligned Beliefs, and Knowledge of the Rules. He shows that many decision makers do not exhibit Instrumental Rationality, terrorists and defenders do not hold Consistently Aligned Beliefs, and not all players know all possible actions (complete Knowledge of the Rules). While using game theory with the preceding

[9] Henry Willis et al., *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*, (Santa Monica, CA: RAND Corporation, MG-388-R TR-386-DHS, 2007), 6, RAND Corporation, http://www.rand.org/pubs/technical_reports/2007/RAND_TR386.sum.pdf, (accessed January 28, 2008).

[10] Seth Guikema, “A Critical Assessment of Game Theory in Terrorist Risk Assessment” (Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2006), Los Alamos National Laboratory, http://risk.lanl.gov/site2k6/archives/pgm2006.html (accessed January 2008).

assumptions does not perfectly model terrorism risk, its utility is undeniable. Among other things, game theory allows for the analysis of the previously discussed phenomenon of threat shifting or target substitution. Guikema indicates that an area worthy of future research is the adjustment of game theory assumptions.

One commercial terrorism risk model is the AIR Terrorism Loss Estimation Model developed by AIR Worldwide Corporation. The predominant commercial terrorism risk model was developed by Risk Management Solutions (RMS). Gordon Woo is called "the chief architect of the RMS terrorism model" in the RMS publication ***Managing Terrorism Risk.***[11] This publication indicates that RMS calculates insurance losses attributable to terrorist attacks using extensive high resolution U. S. building data combined with event based models, including explosion modeling, dispersion modeling, disease modeling, business interruption modeling, and casualty modeling. In "Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection," Willis et al. recommend that DHS should "consider investing in the extensions of [the RMS] insurance-industry model…to improve the usefulness of this approach to homeland security analyses."[12]

As previously mentioned, while game theory can be used to model potential terrorist actions, current models assume that both defenders and attackers (terrorists) hold Consistently Aligned Beliefs and have complete Knowledge of the Rules. Neither assumption is true and improvements in terrorism risk analysis using game theory will only occur through development of models with assumptions that more closely match real world situations concerning terrorists' state of mind. Both the AIR Terrorism Loss Estimation Model and the RMS terrorism risk model were developed by the insurance industry in their quest for profit. These models provide a useful starting point, but will require significant work to shift their emphasis from commercial insurance calculations toward terrorism risk assessment.

[11] Risk Management Solutions, *Managing Terrorism Risk* (Newark, CA: Risk Management Solutions, 2003), Risk Management Solutions, http://www.rms.com/publications/terrorism_risk_modeling.pdf (accessed January 28, 2008).

[12] Willis et al., *Terrorism Risk Modeling*, xv.

4. Expert Judgment

Economic incentives have driven insurance companies and other commercial entities to conduct risk research, especially in the area of terrorism-related risk. In "The Evolution of Terrorism Risk Modeling," Gordon Woo states that the insurance industry used expert judgment long before using modern computational tools for risk analysis.[13] Using individual expert judgments can be dangerous, as individual experts may not always have complete information on a situation. To address this issue, panels of experts are often formed to provide more complete information. This introduces a new issue, that of aggregating expert opinions. There is a large amount of literature on this panel aggregation problem. Linear averaging is a simple way to aggregate expert opinions, but does not provide useful aggregation when those opinions are incomplete or incoherent. Predd et al. suggest a method to increase the coherence of expert panels in their paper "Scalable Algorithms for Aggregating Disparate Forecasts of Probability." They refer to the Coherent Approximation Principle (CAP) created by Osherson and Vardi. While the CAP can be used to increase coherence in expert forecasts, it is extremely computationally intensive and, therefore, slow. This is because all events are grouped into a single subset. Predd proposes grouping events in subsets of no more than three events to reduce computational requirements, while approximating results gained through CAP. This is accomplished through selection of event subsets according their logical relationships.[14] The authors test their algorithm against five data sets to compare their results to full CAP aggregate results. They find that it is possible to complete calculations within seconds versus hours for full CAP calculations "while achieving competitive forecasting gains."[15]

A simpler approach to panel aggregation is proposed by Tastle and Wierman. They apply weights to both experts' assessment of the value of a random variable and to

[13] Gordon Woo, "The Evolution of Terrorism Risk Modeling," *Journal of Reinsurance* 10, no. 3 (2003): 1.

[14] J. B. Predd et al., "Scalable Algorithms for Aggregating Disparate Forecasts of Probability" (Proceedings of the Ninth International Conference on Information Fusion, Florence, Italy, 2006), 5.

[15] Ibid., 7.

the degree of importance placed on each expert's opinion. In their paper "Determining Risk Assessment Using the Weighted Ordinal Agreement Measure," the authors apply their approach to Homeland Security Threat Categories, but this approach could potentially be applied to other areas, including expert assessment of the probability of occurrence of certain events. When this paper was presented at the 2007 Los Alamos National Laboratory Risk Symposium, they indicated that it was rejected by the *Journal of Statistics* and that considerable work would be required before this approach would be widely accepted.[16] Nonetheless, it will be valuable to consider the utility of this approach in the assessment of terrorism risk using expert opinion. Without assigning numerical weights to expert judgment, Gordon Woo follows a similar line of reasoning to that of Tastle and Wierman when he outlines the basis for choosing "the most informed terrorism experts."[17]

Predd et al. suggest that their scalable algorithm technique to reduce computational requirements in the aggregation of expert judgment approaches the accuracy of full CAP results by showing that their results from one data set compare favorably with full CAP results. The paper indicates that five data sets were analyzed using scalable algorithms. Unfortunately, the authors only compare results from one of the five data sets used. The validity of scalable algorithms would be better supported through a more rigorous comparison of scalable algorithm aggregation results with full CAP results. Tastle and Wierman suggest a technique for weighting Likert categories in their proposed process for determining risk assessment, but acknowledge that further research is required to assign suitable values to these weights.

5. Event Trees

In "Quantifying Insurance Terrorism Risk," Gordon Woo indicates that an event tree "can be used…to estimate the probability that a planned terrorist attack results in a

[16] William J. Tastle and Mark J. Wierman, "Determining Risk Assessment Using the Weighted Ordinal Agreement Measure," *Journal of Homeland Security*, June 2007, Homeland Security Institute, http://www.homelandsecurity.org/newjournal/Articles/displayArticle2.asp?article=157 (accessed January 2008).

[17] Woo, "The Evolution of Terrorism Risk Modeling," 3.

notable loss."[18] Event trees are found throughout terrorism risk literature, notably in the work of Bilal Ayyub and Niyazi Bakir. Detlof von Winterfeldt is the Director of the Homeland Security Center for Risk and Economic Analysis of Terrorism Events (CREATE). He uses Project Risk Analysis to create an event tree that can then be used to provide insight into actions that can be taken to prevent terrorism.[19]

John Harrald et al. use event chains to analyze terrorist attacks on U.S. ports and waterways,[20] as do James Moran and Dave Cooper in their documentation of Coast Guard Risk Assessment and Risk Reduction.[21] While the use of event chains simplifies the required analysis, it seems that more accurate modeling of terrorism risks could be achieved through the use of event trees, and work on creating event trees to describe terrorism-related maritime risk would be worthwhile. As demonstrated by Predd et al. there is great potential to reduce computational requirements through adjustments to the way in which calculations are made. Unfortunately, implementing event trees in lieu of event chains would also require more data input from field commands on possible outcomes for a much larger number of scenarios. However, this is another source of information on terrorist threat shifting that should not be ignored.

6. Conclusion

Four sub-literatures were covered in this literature review. Risk analysis is a well developed and broad field of study. Narrowing the focus of this research to several

[18] Gordon Woo, "Quantifying Insurance Terrorism Risk" (working paper. National Bureau of Economic Research, Cambridge, MA, 2002), 11, Risk Management Solutions, http://www.rms.com/newspress/quantifying_insurance_terrorism_risk.pdf (accessed January 28, 2008).

[19] Detlof von Winterfeldt and Heather Rosoff, "Using Project Risk Analysis to Counter Terrorism," (presented at USC Symposium on Terrorism Risk Analysis, Los Angeles, CA, 2005), University of Southern California, http://www.usc.edu/dept/create/assets/002/51845.pdf (accessed January 28, 2008).

[20] John R. Harrald, Hugh W. Stephens, and Johann Rene van Dorp, "A Framework for Sustainable Port Security," *Journal of Homeland Security and Emergency Management* 1, no. 2 (2004), Berkeley Electronic Press, http://www.bepress.com/jhsem/vol1/iss2/12/ (accessed January 27, 2008).

[21] James Moran, "Maritime Security Risk Assessment Process" (presented at Los Alamos National Laboratory Risk Symposium, Santa FE, NM, 2007), Los Alamos National Laboratory, http://risk.lanl.gov/site2k7/RS2007Presentations.html (accessed January 27, 2008); Dave Cooper, "How the Coast Guard Attempts to Optimize Mission Execution through Risk Reduction Return on Investment," (presented at Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2007), Los Alamos National Laboratory, http://risk.lanl.gov/site2k7/RS2007Presentations.html (accessed January 27, 2008).

aspects of the included field of risk assessment allows the opportunity to examine avenues for improving measurement of Coast Guard mission effectiveness in achieving homeland security in greater detail. Terrorism risk assessment requires quantification of threat, vulnerability, and consequences. Techniques that allow refinement in the assessment of each of these three components will lead to more accurate assessment of terrorism risk. Risk modeling allows the use of probabilistic risk analysis even when data sets of previous terrorism events are incomplete. An examination of the underlying assumptions of game theory and determination of the effects of altering these assumptions could lead to better risk analysis. The oldest method of assessing terrorism risk is the use of expert judgment, which is now used as an input to probabilistic risk analysis, risk modeling, and event trees. While the problem of panel aggregation has been exhaustively studied, methods to speed up or simplify aggregation while maintaining or enhancing the value of the aggregated expert judgment call for further study. Finally, the event chains currently used by the Coast Guard and others allow assessment of terrorism-related maritime risk. However, the development of these event chains into event trees has the potential to improve measurement of Coast Guard mission effectiveness, as event trees should provide a better approximation of the dynamic nature terrorist attacks.

While a there are a number of gaps and issues in the literature relating to terrorism risk assessment, the area that provides the greatest opportunity for improvement seems to be the improvement of expert judgment used by the Coast Guard to assess terrorism-related maritime risk and to assess the effectiveness of Coast Guard efforts to address that risk.

E. ARGUMENT

The model used to assess Coast Guard impact on terrorism-related maritime risk would benefit from refinement of several components in order to more accurately represent Coast Guard effectiveness in reducing this risk. Those components are: analysis of threat shifting combined with improved modeling, properly elicited and aggregated expert opinions, and event trees.

Terrorism risk analysis defines risk as a function of three components: ***threat, vulnerability***, and *consequences*[22] Better threat assessment will improve the risk assessment calculated with that threat input. Terrorists adjust target selection based on the vulnerability of those targets (threat shifting)[23] and use adaptive learning to modify future attacks in their quest for success.[24] A thorough examination of threat shifting will allow improved risk assessment, finally resulting in a more accurate reflection of Coast Guard mission effectiveness in achieving homeland security.

Compared to land-based terrorist attacks, there is a shortage of maritime terrorist attack data on which to base risk analysis, but modeling can be used to address this data shortfall. In his monograph *The Maritime Dimension of International Security*, Peter Chalk states, "Indeed, according to the RAND Terrorism Database, strikes on maritime targets and assets have constituted only 2 percent of all international incidents over the last 30 years…[nonetheless] there has been a modest yet highly discernible spike in high-profile terrorist incidents at sea over the past six years."[25] This includes attacks on the French oil tanker Limburg and the Philippine SuperFerry 14, along with numerous attacks by the Tamil Tigers on Sri Lankan naval vessels. The maturation of the models used to arrive at the Ports, Waterways, and Coastal Security Outcome Measure will allow more accurate assessment of terrorism-related maritime risk so that the Coast Guard can improve homeland security effectiveness measurement.

Expert opinions can be used to assess terrorism risk, and if numerous expert opinions are properly aggregated, the resultant risk assessment will be more accurate than that arrived at through consideration of only one information source. Current Coast Guard assessment of terrorism risk is achieved by considering expert opinions generally

[22] Henry Willis et al., *Estimating Terrorism Risk*, xvi.

[23] Falaschetti and Roberts, "Threat Shifting."

[24] Gordon Woo, *Understanding Terrorism Risk*, (Newark, CA: Risk Management Solutions, 2002), 7, Risk Management Solutions, http://www.rms.com/Publications/UnderstandTerRisk_Woo_RiskReport04.pdf (accessed January 28, 2008).

[25] Peter Chalk, *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States* (Santa Monica, CA: RAND Corporation, 2008), 19-20, RAND Corporation, http://www.rand.org/pubs/monographs/2008/RAND_MG697.pdf (accessed February 9, 2009).

within the Coast Guard. Measurement of homeland security effectiveness will be significantly improved through inclusion of outside experts in addition to Coast Guard opinions and by considering the use of advanced panel aggregation techniques to provide the best input on the Reduction in Terrorism-Related Maritime Risk outcome measure.

The Coast Guard Ports, Waterways, and Coastal Security Outcome Measure can be improved through the use of improved threat shifting, inclusion of outside experts and improved expert judgment, and maturation of models to more accurately depict terrorism-related maritime risk and Coast Guard impact on that risk.

Potential issues or challenges include the difficulty of constructing event trees to replace the current event chains, collecting better source data from a larger number of sources, and then mobilizing the resources to complete the computations in a timely, yet accurate manner so as to accurately assess terrorism risk. However, none of these issues are insurmountable. Research into terrorist threat shifts will provide insight to more accurately model terrorist activities during attacks, streamlined reporting techniques will allow the collection of more expert opinions without a significantly greater burden on those providing those opinions, and the use of computational techniques to reduce required processing time while maintaining a comparable level of accuracy will permit the swift processing of much larger data sets.

F. THESIS OUTLINE

Chapter II of this project reviews guidance from the General Accountability Office on risk management framework and provides an overview of the Coast Guard risk-based decision-making guidelines. In addition, it contains information from a number of sources on the terrorism risk assessment, an important component in both the risk management framework and the risk-based decision-making guidelines. Chapter III examines the data sources used in the Ports, Waterways, and Coastal Security (PWCS) outcome measure, the structure of the model, and the mechanics of how the model determines the value of the measure. Chapter IV describes the research methodology and reviews the qualitative data collection results, pointing out areas of convergence and divergence between the experts consulted. Chapter V points out the need for outside input to the PWCS Outcome Measure and suggests a number of potential contributors to the assessment of Coast Guard effectiveness in reducing the risk of maritime terrorism. It also considers issues that adversely affect expert judgment, ideas to address these issues, and concludes with an appraisal of various methods of expert judgment aggregation. Chapter VI presents a summary of recommendations for improvement to the PWCS outcome measure, an implementation plan and recommendations for future research, and conclusions.

II. MARITIME TERRORISM RISK MANAGEMENT AND ASSESSMENT

A. BACKGROUND

As the lead federal agency for maritime homeland security, the Coast Guard is responsible for deploying its personnel and platforms so as to obtain the maximum reduction in the risk of maritime terrorism. From its beginnings as the Revenue Cutter Service in 1790, the Coast Guard has played an integral part in "protecting the coast, trade, and maritime interests of our nation."[26] Three previous pieces of legislation laid the foundation for the Coast Guard Port Security mission.

1. The Espionage Act, Magnuson Act, and Ports and Waterways Safety Act

On July 30, 1916, German saboteurs set fire to a boxcar full of explosives at Black Tom Island in Jersey City, New Jersey. The U.S. had started to support the Allied Powers in World War I and allowed the purchase of U.S. ammunition as long as it was not carried to Europe in American vessels. Much of this ammunition passed through the Jersey Central Railroad Terminal on Black Tom Island. The sabotage caused over $40 million in damage to the facility and to buildings throughout Northern New Jersey, Manhattan, Staten Island, and Brooklyn. This catastrophe prompted passage of the Espionage Act of 1917 and placed the Coast Guard in charge of port security to regulate vessels in U.S. waters during national security emergencies. The Korean Conflict and the "Red Scare" both started in 1950. That same year, Congress passed the Magnuson Act. This expanded Coast Guard authority to cover harbors, ports, and waterway facilities. Due to several large oil spills and vessel groundings, Congress enacted the Ports and

[26] Robert Scheina, "The U.S. Coast Guard at War: A History," U.S. Coast Guard, http://www.uscg.mil/History/articles/h_CGatwar.asp (accessed November 11, 2007).

Waterways Safety Act of 1972. This further expanded the Coast Guard's Espionage and Magnuson Act authorities to cover peacetime maritime safety.[27]

2. The Maritime Transportation Security Act and the Security and Accountability for Every Port Act

The Coast Guard role in port security was greatly enlarged by Congress in response to the attacks on USS COLE, of 9/11 and against the French tanker Limburg that urgently indicated the need for greater oversight of the maritime domain to protect the U.S. population and economy. Recent legislation concerning the Coast Guard's role in maritime homeland security include the Maritime Transportation Security Act of 2002 (MTSA) and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act). This legislation combined with guidance from the Department of Homeland Security provides direction for the Coast Guard to assume the role "as the "lead federal agency" and/or "executive agent for maritime security" as indicated in the Coast Guard Combating Maritime Terrorism Strategic and Performance Plan.[28] As such, the Coast Guard is charged with reduction of the risk of maritime terrorism, and the General Accountability Office (GAO) has provided specific recommendations on this issue.

B. GAO RISK MANAGEMENT FRAMEWORK

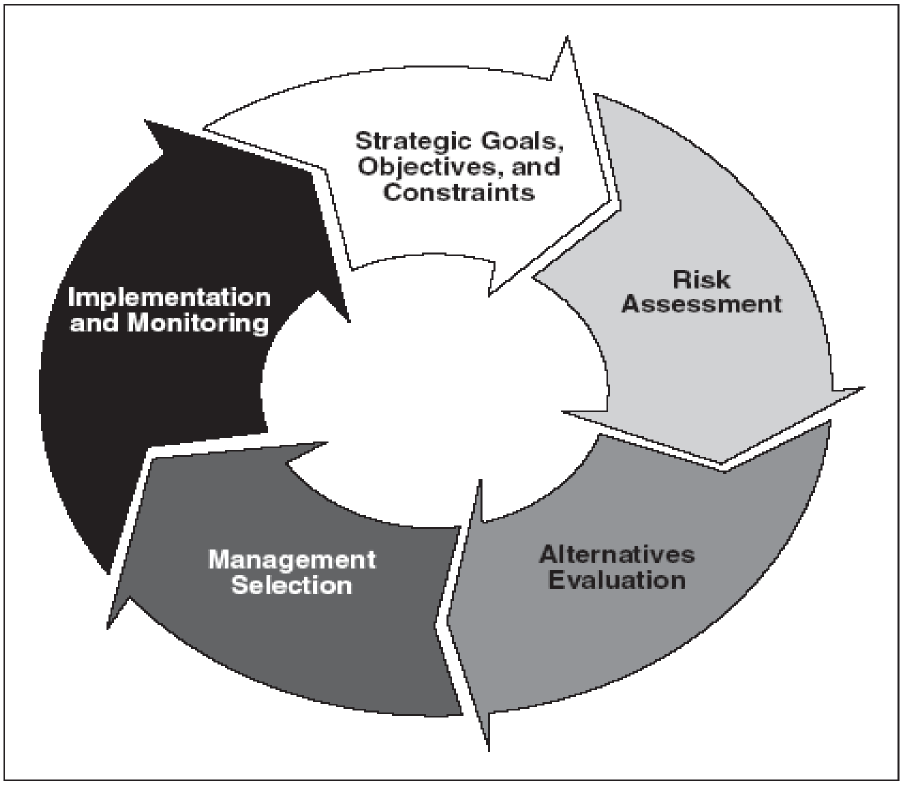
The GAO risk management framework was published in the 2005 report, "Risk Management: Further Refinements Needed to assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure." This framework was created since there "is no established universally agreed upon set of requirements or processes for a

[27] Dennis Bryant, "Port Security: A Historical Perspective," Marine Link (March 8, 2004), http://www.marinelink.com/Story/Column:+Port+Security:+A+Historical+Perspective-13883.html (accessed November 28, 2007).

[28] Brian M. Salerno, *Combating Maritime Terrorism Strategic and Performance Plan* (Washington, D.C.: United States Coast Guard, 2008), 5.

risk management framework specifically related to homeland security and combating terrorism."[29] It is shown in Figure 1 and contains five phases:

1. Strategic goals, objectives, and constraints,
2. Risk assessment,
3. Alternative evaluation,
4. Management selection,
5. Implementation and monitoring.


Strategic Goals, Objectives, and Constraints
Risk Assessment
Alternatives Evaluation
Management Selection
Implementation and Monitoring

Source: GAO.

Figure 1. GAO Risk Management Framework[30]

[29] Margaret Wrightson, *Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure* (Washington, D.C.: U.S. Government Accountability Office, 2005), 100, U.S. Government Accountability Office, http://www.gao.gov/new.items/d0691.pdf (accessed January 27, 2008).

[30] Norman J. Rabkin, *Strengthening the Use of Risk Management Principles in Homeland Security*, (statement to U.S. House of Representative Committee on Homeland Security. Washington, D.C.: U.S. Government Accountability Office, GAO-08-904T, 2008). Committee on Homeland Security. http://homeland.house.gov/SiteDocuments/20080625151226-90211.pdf (accessed January 27, 2008).

The strategic goals, objectives, and constraints phase uses the Government Performance and Results Act of 1993 as a source of evaluation criteria. The elements of this phase include a clear delineation of the desired end state, a "hierarchy of strategic goals, subordinate objectives, and specific activities to achieve results,"[31] creation of "priorities, milestones and outcome-related performance measures," and "limitations or constraints that affect outcomes."[32] The Coast Guard Combating Maritime Terrorism Strategic and Performance Plan address each of these components.

The second phase is risk assessment, which requires identification of the sources of risk, and quantification of that risk. The Coast Guard Maritime Security Risk Analysis Model is used by each Coast Guard Captain of the Port to conduct a local risk assessment, which is combined with results from other ports to compile a national maritime security risk assessment.

The third phase is the alternative evaluation, which uses the risk assessment to provide information on the scenarios and targets with the highest risk. This is used to identify countermeasures that are then assessed for their expected effectiveness and subjected to cost-benefit analysis. In addition to agency countermeasure implementation costs, opportunity costs imposed by the countermeasures must be considered. The Coast Guard Combating Maritime Terrorism Strategic Risk Model is used to evaluate alternatives for maritime terrorism risk reduction.

The fourth phase is management selection, informed by the alternative evaluation and resource availability. The decisions on strategy implementation made during this phase depend on management value judgments of risk tolerance and the desired risk reduction profile; should risk reduction measures focus on a few of the highest threat targets, or should they be spread as widely as possible?

The final phase is implementation and monitoring of the management selection to achieve the results identified in the strategic goals, objectives, and constraints phase. The

[31] Wrightson, *Further Refinements Needed*, 103.

[32] Ibid.

effectiveness of chosen countermeasures must be assessed through testing or exercises and measured at the local level. Unintended consequences must also be identified and addressed in this phase.

C. RISK MANAGEMENT IN THE UNITED STATES COAST GUARD

The Coast Guard was formed in 1915 as a combination of the Revenue Cutter Service and the Lifesaving Service. The Lighthouse Service became part of the Coast Guard in 1939, and in 1942 the Navigation and Steamboat Inspection Service was added. All of these agencies played a part in maritime risk management, which the Coast Guard continues to this day. Through the years, service personnel have worked to reduce threat through protection executed with security patrols and other actions, to reduce vulnerability through prevention accomplished by regulating maritime activities, and to reduce consequences through timely response and recover actions during search and recue operations.

Coast Guard experience with risk management was combined with risk management theory and codified in a comprehensive document in the 1997 edition of the Coast Guard Risk-Based Decision Making Guidelines.[33] The guidelines use a process that is similar to the GAO risk management framework and contain four steps shown in Figure 2 that occur in sequence but allow for feedback throughout the process between each step and also allow feedback through a separate risk communication step:

1. Frame the decision structure,
2. Complete the risk assessment,
3. Conduct risk management,
4. Implement impact assessment.

[33] Joseph Myers, “Risk-Based Decision Making,” *Proceedings of the Marine Safety & Security Council* 64, no. 1 (2007): 6-9.

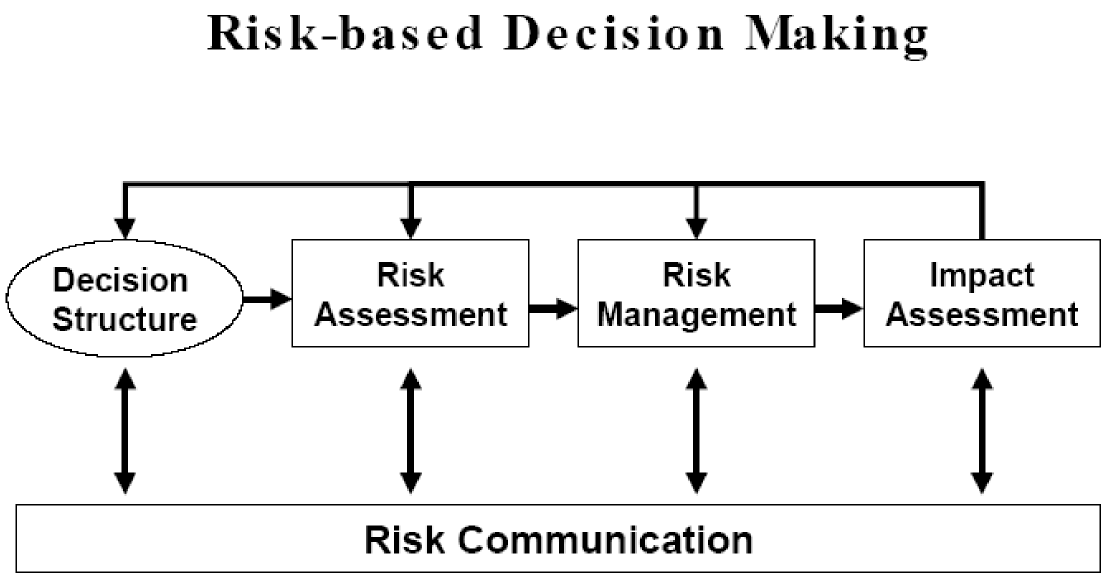


Figure 2. Risk-Based Decision-Making Process[34]

Roughly analogous to the strategic objectives, outcomes, and constraints phase of the risk management framework is the decision structure step in the guidelines. The problems that are to be addressed through the process are identified, which is basically an identification of the strategic goals and outcomes. Influencing factors are also delineated in this step and correspond to identification of constraints.

Both models contain a risk assessment step. The risk-based decision-making guidelines include an extensive list of available risk assessment tools, including pareto analysis, checklist analysis, relative ranking/risk indexing, preliminary risk analysis, change analysis, what-if analysis, failure modes and effects analysis, hazard and operability analysis, fault tree analysis, event tree analysis, event and causal factor charting, and preliminary hazard analysis. The guidelines include recommendations on when and how to use each tool with examples of how to use the tools.

[34] Bert Macesker et al., "Quick-reference Guide to Risk-based Decision Making (RBDM): A Step-by-step Example of the RBDM Process in the Field," 2, Air University, http://www.au.af.mil/au/awc/awcgate/uscg/risk-qrg.pdf (accessed October 25, 2008).

The risk management step of the guidelines encompasses both the alternative evaluation and management selection of the GAO risk management framework. This step uses the results of the risk assessment to provide information to decision makers on risk management options. The Coast Guard policy and procedures for Operational Risk Management provides a list of five potential risk control options.[35] Once all risk control options are analyzed, then recommendations are made to senior leadership and a management selection is made. The risk control options include:

1. *Spread out the risk.* This is accomplished by spreading out the activity over time or space.

2. *Transfer the risk.* Risk transfer is accomplished by enlisting the assistance of other entities who can assume some of the risk through contracts or partnerships.

3. *Avoid the risk.* It may be possible to avoid some port security risks by not allowing certain vessels or cargoes into the port. However, in addition to Ports, Waterways, and Coastal Security mission, the Marine Safety mission drives the Coast Guard to facilitate commerce, so it is very rare that the Coast Guard would take such an action.

4. *Accept the risk.* If the cost-benefit calculations indicate other organizational risk reduction investments should be made first, then the most appropriate course of action may be to accept the risk in the analyzed case.

5. *Reduce the risk.* This can be accomplished through application of Coast Guard and other resources to reduce the threat, vulnerability, or consequences.

Finally, impact assessment in the guidelines includes the same activities as implementation and monitoring in the risk management framework.

Throughout each step of the risk-based decision-making guidelines is the requirement to initiate and continue risk communication with stakeholders, customers, suppliers who may be affected by the operations to gather information for the risk assessment and to cultivate buy-in for the eventual Coast Guard decision.

[35] U.S. Coast Guard Headquarters Human Factors Division, "Operational Risk Management," *Commandant Instruction 3500.3* (Washington, D.C.: U.S. Coast Guard, 2000), 8, U.S. Coast Guard, http://www.uscg.mil/directives/ci/3000-3999/CI_3500_3.pdf (accessed October 25, 2008).

D. RISK ASSESSMENT

Before one can assess risk, the term “risk” must be defined. Robert Ross cites 17 different definitions for risk in his paper “Risk and Decision-Making in Homeland Security,” including the three risk assessment questions posed by Kaplan and Gerrick:

1. What can go wrong?
2. What is the likelihood that it would go wrong?
3. What are the consequences?[36]

Although there are numerous variations, most definitions state that risk is a **function of the probability of the occurrence of an unwanted future event and the consequences of that event.**

Risk = f(Probability, Consequences)

Ross states that “risk, no matter how well founded in reality, is a mental and emotional construct rather than a physical reality.”[37] The subjectivity of risk is seen in the preceding definition by the inclusion of the word “unwanted.” There are many events which are wanted by one party and unwanted by another party; a germane example would be the success or failure of a maritime terrorist attack.

1. System Definition

The response to the first question, “What can go wrong?” requires an examination, definition, and delineation of the system within which the Coast Guard is operating and wishes to reduce risk. Three applicable activities outlined by Bilal Ayyub to define a system for subsequent risk assessment are:

[36] Stanley Kaplan and B. John. Garrick, “On the Quantitative Definition of Risk,” *Risk Analysis* 1, no. 1 (1981): 14.

[37] Robert Ross, “Risk and Decision-Making in Homeland Security” (unpublished paper, Department of Homeland Security, Washington, D.C., 2006), 4.

1. Define the goal and objectives of the analysis.
2. Define the system boundaries.
3. Define the success criteria in terms of measureable performances.[38]

The goal and objectives of any risk assessment should be to ascertain potential sources of risk in the system with the goal of reducing the risk to an acceptable level. Defining the system boundaries will restrict the area of consideration for the risk assessment to enable an in-depth consideration of applicable issues and factors. Finally, defining success criteria should also result in the identification of failure criteria. Failure in the prevention of terrorism can be defined as an attack that results in damage to the intended target. Failure scenarios that describe potential attacks should be created at this point for later assessment.

2. Probability

To answer the question "What is the likelihood that it would go wrong?" one needs to consider the components of probability of the occurrence of a given event. In the field of terrorism risk assessment, this probability can be broken down into a function of threat and vulnerability:

$$\text{Probability} = f(\text{Threat, Vulnerability})$$

The combination of this equation for probability with that above for risk results in risk being a function of threat, vulnerability, and consequences:

$$\text{Risk} = f(\text{Threat, Vulnerability, Consequences})$$

3. Threat

Threat can be further broken down into a function of terrorist capability and intent:

$$\text{Threat} = f(\text{Capability, Intent})$$

[38] Bilal Ayyub, *Risk Analysis in Engineering and Economics* (Boca Raton, FL: Taylor and Francis, Inc, 2003), 45.

Terrorist capability is defined as the ability of the adversary to conduct an attack. This depends on resource availability, including trained and willing personnel, operational equipment, funding and logistical networks to plan, support and execute an attack. Terrorist intent is the intention of a terrorist to conduct an attack. Information on both capability and intent can be gained through intelligence collection and processing.

In "Estimating Terrorism Risk," Willis et al. develop the equations above to quantify risk. Willis states that threat can be quantified as "The probability that a specific target is attacked in a specific way during a specified time period."[39]

$$\text{Threat} = P(\text{attack occurs})$$

4. Vulnerability

Vulnerability to a terrorist attack is a measurement of the likelihood of a successful attack from the terrorists' point of view. This will depend on the scenario under consideration along with the security systems in place to defend against a successful terrorist operation. Willis states that vulnerability can be quantified as "The probability that damage (where damages may involve fatalities, injuries, property damage, or other consequences) occur, given a specific attack type, at a specific time, on a given target."[40]

$$\text{Vulnerability} = P(\text{attack results in damage} \mid \text{attack occurs})$$

5. Consequences

The final question is "What are the consequences?" Willis states that consequences can be quantified as "The expected magnitude of damage (e.g. deaths, injuries, or property damage), given a specific attack type, at a specific time, that results in damage to a specific target."[41]

$$\text{Consequences} = E(\text{damage} \mid \text{attack occurs and results in damage})$$

[39] Henry Willis et al., *Estimating Terrorism Risk*, 6.

[40] Ibid., 8.

[41] Ibid., 9.

6. Risk Quantification

Combining the three equations developed by Willis results in the following definition of risk for a specific target: “the expected consequence of an existent threat…for a given target, attack mode, and damage type.”[42]

As above, risk is a function of threat, vulnerability and consequences, but Willis’ equations allow one to quantify that risk:

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Consequences}$$

$$\begin{aligned} \text{Risk} = {} & P(\text{attack occurs}) \\ & * P(\text{attack results in damage} \mid \text{attack occurs}) \\ & * E(\text{damage} \mid \text{attack occurs and results in damage}) \end{aligned}$$[43]

One of the main reasons for terrorism is to achieve political ends through the creation of fear in the country under attack. Since this often does result, the assessment of the consequences of terrorism must include more than a tally of the immediate physical damage of a particular attack. Immediate outcomes could include the destruction of a building or the death of targeted personnel and/or innocent bystanders. Long-term outcomes could include disruption of the delivery of utilities and other aspects of critical infrastructure or loss of faith in one or more segments of the economy (such as aviation). These long-term outcomes are estimated through secondary economic affects.

E. TERRORISM-RELATED MARITIME RISK ASSESSMENT

1. Port Security Risk Analysis Tool (PSRAT)

The Coast Guard was tasked with executing the port security mission by the Espionage Act of 1917 and the Magnuson Act of 1950. However, Coast Guard records contained in the Abstract of Operations database show that only a small amount of

[42] Henry Willis, *Guiding Resource Allocations Based on Terrorism Risk* (Santa Monica, CA: RAND, 2006), 11, RAND Corporation, http://www.rand.org/pubs/working_papers/2006/RAND_WR371.pdf (accessed January 28, 2008).

[43] Henry Willis et al., *Estimating Terrorism Risk* (Santa Monica, CA: RAND Corporation, 2005), 13, http://www.rand.org/pubs/monographs/2005/RAND_MG388.pdf (accessed January 28, 2008).

resource hours were devoted to ports, waterways and coastal security (PWCS) from 1998-2000.[44] Figure 3 contains a Lowess plot with a break between fiscal year 2001, third and fourth quarter (FY01 Q3 and FY01 Q4) which illustrates the jump in PWCS resource hours after 9/11. Because of the need to secure 361 U.S. ports and 95,000 miles of shoreline, the Coast Guard applied every available resource to Ports, Waterways, and Coastal Security after 9/11. There was a huge increase which peaked at almost 100,000 resource hours in the last quarter of 2001.[45] Because this level of operations was unsustainable, the Coast Guard had to focus resources in areas with the greatest security needs.

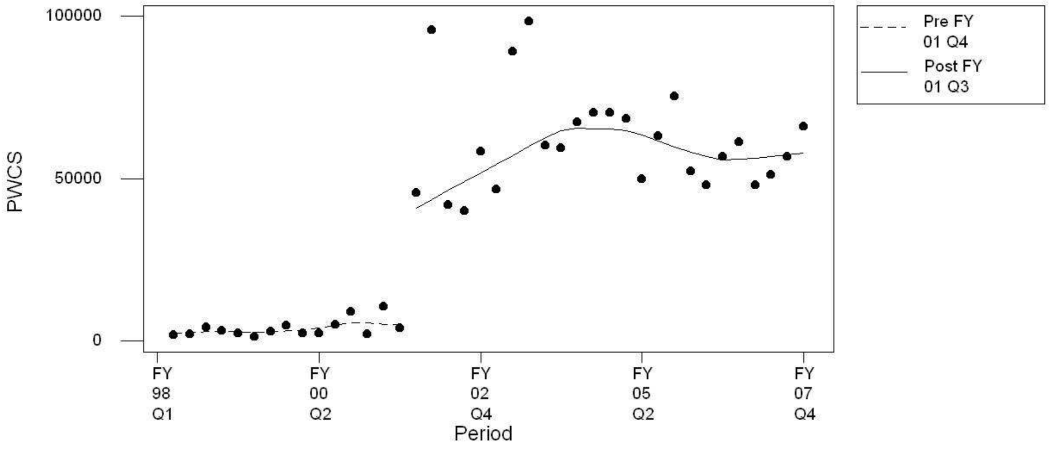


Figure 3. U.S. Coast Guard Ports, Waterways and Coastal Security Resource Hours[46]

Admiral Allen, who was then the Coast Guard Atlantic Area Commander, initiated development of a computer program so each Captain of the Port (COTP) could quantify security risk and locate areas with the highest security risk in U.S. ports. A team of employees from Coast Guard headquarters, the Coast Guard Research and

[44] U.S. Coast Guard, *Abstract of Operations* (Washington, D.C.: U.S. Coast Guard, 2007).

[45] Ibid.

[46] Ibid.

Development Center, and ABS Consulting developed the first version of the Port Security Risk Analysis Tool to meet these criteria. The program was fielded in November 2001.

In alignment with numerous risk assessment guidelines, the PSRAT defines risk as the product of Probability and Consequence. Navigation and Vessel Inspection Circular 9-02 specifies that:[47]

> Risk = Probability X Consequence, or R = P X C
>
> R = risk score for a given security breach
>
> P = probability - probability of a security breach
>
> C = consequence - the sum of possible consequences associated with a successful security breach. Consequences may be based on impacts to life, economic security, symbolic value, and national defense.

The probability of a security breach can be broken down into the product of threat (T) and vulnerability (V). Threat is defined as the likelihood of attack against a given asset or location, and vulnerability is defined as weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach. (NVIC enclosure (3) pages 1-2) This results in the following formula:

Risk = Threat X Vulnerability X Consequence.

The Port Security Risk Analysis Tool provided each COTP the ability to capture a local assessment of threat, vulnerability, and consequences of specific attack scenarios against assets and infrastructure in the port.[48] The risk algorithm within PSRAT calculated a relative risk score for each asset or infrastructure, which then allowed the COTP to set priorities within that port. However, estimates of threat, vulnerability, and consequences were made on a local level. The threat components used in PSRAT were local intelligence estimates of the potential for attack on each asset or infrastructure

[47] Brian Salerno, "Navigation and Vessel Inspection Circular No. 9-02" (Washington, D.C.: U.S. Coast Guard, 2008), 3-1, Assistant Commandant for Marine Safety, Security, and Stewardship (CG-5), http://www.uscg.mil/hq/cg5/NVIC/pdf/2002/NVIC_09_02_Change_3.pdf (accessed July 8, 2008).

[48] U.S. Coast Guard Headquarters Port Safety and Security Division, *USCG Port Security Risk Assessment Tool* (Version 2) Users' Manual (Washington, D.C.: U.S. Coast Guard, 2002), 1.

within that port. Wide variations in threat, vulnerability, and consequence assessments occurred because of local differences and varying levels of rigor required in each COTP zone. While PSRAT provided valuable risk information so individual COTPs could set priorities within an individual port, these port risk assessments were not standardized. As a result, it was not possible to compare security risks between different ports, nor was it possible to assess overall port security risk within each Coast Guard district, area, or on a nationwide basis.[49] A new version of PSRAT was released in 2002 which allowed further refinement of the consequence components by including the ability to capture the affect of mitigation in the form of recoverability and redundancy.

2. Maritime Security Risk Analysis Model (MSRAM)

In December 2004, the Coast Guard started developing a new program called the Maritime Security Risk Analysis Model (MSRAM) to build on the foundation and experience gained through the use of PSRAT. This development addressed the issues outlined above with PSRAT along with feedback from the General Accountability Office and the Department of Homeland Security. MSRAM uses threat information from the Coast Guard Intelligence Coordination Center (ICC), which "provides strategic intelligence support [and] serves as the Coast Guard's primary interface with the collection, production, and dissemination elements of the national intelligence and law enforcement communities."[50] The ICC threat assessment separates terrorist intent and capability, and it also provides threat estimates for each attack scenario against each type of target contained in the model. In addition, the new program drives consistency in vulnerability and consequence assessments through user training, a help desk, recommended ranges for factor scoring and benchmark data, and a review process to identify anomalies and outlier data. Vulnerability assessments are linked to specific target attributes and include specific guidance for scoring interdiction capabilities of the

[49] Brady Downs, "The Maritime Security Risk Analysis Model," *Proceedings of the Marine Safety & Security Council* 64, no. 1 (Spring 2007): 36, 37.

[50] Department of the Navy, *Naval Doctrine Publication 2: Naval Intelligence*, Naval Warfare Development Command, http://www.nwdc.navy.mil/content/Library/Documents/NDPs/ndp2/ndp20007.htm (accessed September 1, 2008).

owner/operator, local law enforcement, and the Coast Guard. Consequence assessments have been revised in an attempt to achieve equivalency between death/injury, economic losses, environmental impacts, national security degradation, and symbolic damage to national landmarks. The new model also considers the secondary economic impact of terrorist attacks. Additional consistency is gained through the requirement to assess the same terrorist attack scenarios in each port, while allowing the ability to analyze optional scenarios.[51] The field level risk assessment data collection with MSRAM was initiated in February 2006, and data collection continues on an annual basis. In addition, MSRAM has been updated to incorporate improvements suggested by field units and headquarters personnel, especially the recently added blast calculator, which allows better estimation of the consequences of maritime terrorism to improve risk assessment.

[51] Brady Downs, "The Maritime Security Risk Analysis Model," 36.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE COMBATING MARITIME TERRORISM STRATEGIC RISK MODEL

A. BACKGROUND

The Coast Guard Ports, Waterways, and Coastal Security (PWCS) outcome measure is arrived at in two steps. The first step is an assessment of the risk of maritime terrorism arrived at through the Maritime Security Risk Analysis Model (MSRAM), an assessment of the risk level within each Coast Guard Captain of the Port Zone. This provides the raw risk level, assuming no Coast Guard activity to prevent terrorism. The second step is an assessment of the effectiveness of Coast Guard activities designed to prevent, protect, respond, and recover from maritime terrorism. This is accomplished through the construction of potential maritime terrorist attack scenarios and an assessment by Coast Guard experts on the probability of failure of Coast Guard activities to prevent a successful terrorist attack in each scenario. This assessment is used in the Combating Maritime Terrorism Strategic Risk Model (called the LROI model) to calculate the risk reduction achieved by the Coast Guard, which is reported as the PWCS outcome measure. The LROI model was created by ABS Consulting in conjunction with personnel from Coast Guard headquarters in 2005.

B. RISK QUANTIFICATION

As outlined in Chapter II, Kaplan and Gerrick pose three risk assessment questions which guide the quantification of risk. This chapter will review how each of these three questions are addressed in MSRAM and the LROI model. Then it will examine the data sources used in the models and how the LROI model determines the value of the PWCS outcome measure.

1. Question 1: What Can Go Wrong?

Responding to the first risk assessment question: What can go wrong?” requires one to define and delineate the system within which operations are conducted as the first step to reduce risk. The Coast Guard does this by defining 15 different maritime terrorism scenarios in three overall groups: transfer, direct attack, and exploitation. Each of these scenarios is within the maritime domain which the Coast Guard is charged protecting in its role as lead federal agency for maritime homeland security. The definitions below are taken from the Coast Guard Combating Maritime Terrorism Strategic and Performance Plan. Two groups of direct attack scenarios (vessels and facilities) are included so that the list below matches the numbering system in the LROI model.

Transfer – Includes the transfer of terrorists and/or weapons of mass destruction (WMD) into the United States where exploited vessels en route from foreign countries are used as a means of conveyance.

1. Vessels/Transfer of Terrorists: Transfer of terrorist(s) into the United States with the intent and capability to carry out terror attacks within the United States where exploited vessels en route from foreign countries are used as a means of conveyance.

2. Vessels/Transfer of WMD: Transfer of WMD (e.g., chemical, biological, radiological, nuclear) into the United States to support ongoing terrorist operations where exploited vessels en route from foreign countries are used as a means of conveyance.

Direct Attack – Includes various attack modes and/or weapons against identified high value and/or critical targets. Targets may be vessels of various types.

3. Vessels/Waterside Attack: Waterborne explosive attacks against high-value vessels or barges. This scenario does not include subsurface attacks such as mines or swimmer/diver attacks.

4. Vessels/Shoreside Attack: Shoreside explosive attacks delivered against high-capacity passenger vessels (e.g., passenger ferries, cruise ships, and RO/RO ferries).

5. Vessels/Aircraft Attack: Independently obtained private aircraft for use in a suicide-style attack against vessel/barge. Plane size limited by what one individual can commercially obtain and pilot.

6. Vessels/Stand-off Weapons: A weapon fired from a short distance at a moored or moving vessel.

7. Vessel/Chemical Biological Radiological (CBR): Delivery of CBR materials against a high-capacity passenger vessel (e.g., passenger ferries, cruise ships, and RO/RO ferries).

8. Vessel/Sub-Surface Attack: Subsurface explosive attacks delivered against high-value vessels or barges.

Exploitation – Includes terrorists taking control of a vessel of opportunity to be used as a weapon against other maritime targets; potential targets are other vessels and/or facilities/infrastructure.

9. Vessel/Exploitation/Internal Forces: Internal forces taking control of a vessel of opportunity to be used as a weapon against other targets.

10. Vessel/Exploitation/External Forces: External forces taking control of a vessel of opportunity to be used as a weapon against other targets.

Direct Attack – Includes various attack modes and/or weapons against identified high value and/or critical targets. Targets may be maritime related facilities/infrastructure.

11. Facilities/Waterside Attack: Waterborne explosive attacks delivered on a subset of high-value facilities/infrastructure/key resources.

12. Facilities/Shoreside Attack: Shoreside explosive attacks delivered against facilities/infrastructure/key resources.

13. Facilities/Aircraft Attack: Independently obtained private aircraft for use in a suicide-style attack against facility/infrastructure/key resources. Plane size limited by what one individual can commercially obtain and pilot.

14. Facilities/Stand-off Weapons: A weapon fired from a short distance at stadiums/airports, Marine Transfer Facilities (MTFs), and Maritime Critical Infrastructure/Key Resources (MCI/KR).

15. Facilities/Sub-Surface Attack: Subsurface explosive attacks delivered against facility/infrastructure/key resources.[52]

The LROI Model uses maritime terrorism risk information from the Maritime Security Risk Analysis Model. The 13 direct attack/exploitation scenarios listed above are contained within MSRAM, each of which is a combination of an attack/exploitation

[52] Salerno, *Combating Maritime Terrorism*, D-11-12.

mode and a specific target class (either vessel or shoreside facility). MSRAM targets include vessels and facilities that are maritime critical infrastructure/key resources. The model further breaks these down into 62 target classes with associated required scenarios for each target class. The two transfer scenarios in the LROI model are not in MSRAM. As a result, the Coast Guard conducts annual meetings to acquire information from Coast Guard subject matter experts (SME) on the risk of occurrence of these events and the estimated effectiveness of Coast Guard activities to prevent the events. Risk data from previous years is provided to personnel who are assessing the risk of transfer of terrorists and WMD. Other source data that is considered includes the National Maritime Security Risk Profile, the National Maritime Transportation Security Plan risk assessment, and information from the Coast Guard Intelligence Coordination Center. The transfer scenarios have the highest risk of the 15 scenarios in the LROI model.[53]

2. Question 2: What is the Likelihood That It Would go Wrong?

Answering the question "What is the likelihood that it would go wrong?" requires an assessment of the probability of occurrence of an event. As outlined by Kaplan and Gerrick, the Coast Guard quantifies this probability by breaking it down into the two components shown in the formula below; threat and vulnerability.

$$\text{Probability} = f(\text{Threat, Vulnerability})$$

a. Threat

Threat is defined as the likelihood of a specific terrorist attack on a particular target, which is characterized by the Coast Guard Intelligence Coordination Center and further broken down into the three factors that are shown below and represent intent, capability, and geography. ICC uses the geography factor to account for terrorists' relative preference for attacks in one area vs. another. The formula for threat is:

$$\text{Threat} = \text{Intent} * \text{Capability} * \text{Geography}$$[54]

[53] Salerno, *Combating Maritime Terrorism*, D-4.

[54] U.S. Coast Guard, *Maritime Security Risk Analysis Model*, 142.

b. Vulnerability

Vulnerability is defined as the likelihood that a terrorist attack will be successful, and MSRAM uses the following information to calculate this value. The Coast Guard sector personnel characterize the achievability of each attack scenario in the absence of all security measures, which is the probability that terrorists could successfully complete that attack. They also assess system security and characterize the expected failure rate to interdict the attack with assets of the Coast Guard, other government agencies, or the owner/operator. Finally, sector personnel assess target hardness or the probability that a given target will fail to withstand an attack. These factors are combined into vulnerability as shown below.

$$\text{Vulnerability} = \text{Achievability} * (1\text{-System Security}_{CG}) * (1\text{-System Security}_{OG}) * (1\text{-System Security}_{O/O}) * (1\text{- Target Hardness}).$$[55]

c. Threat Shifting

As indicated by Woo, “A cornerstone of terrorist targeting is target substitution.”[56] This phenomenon is also referred to as threat shifting and risk shifting. Similar to criminals who focus efforts on the least protected targets within an area of interest, terrorists seek maximum damage with minimum energy expenditure. To this end, Al Qaeda and associated jihadist terrorists conduct extensive research on all aspects of available targets and execute attacks on those targets that present the lowest level of defense. This is evident in numerous instances, including the Irish Republican Army (IRA) shift from a planned bombing of London to Manchester in response to heightened security in the capital, the 2003 attack on the British embassy in Istanbul in favor of the more secure American embassy, the 2005 Bali attack on the nightclubs with the poorest security, and the Jemaah Islamiyah embassy attack in Singapore instead of a more

[55] U.S. Coast Guard, *Maritime Security Risk Analysis Model,* 143.

[56] Gordon Woo, “Terrorism Risk,” in *Wiley Handbook of Science and Technology for Homeland Security*, ed. John G. Voeller, 2 (London: John Wiley and Sons, Inc., 2007).

heavily fortified embassy in the Philippines.[57] The MSRAM vulnerability formula above takes into account threat shifting by assigning higher risk to targets with higher attack achievability, lower system security, and lower target hardness.

3. Question 3: What are the Consequences?

Both the primary and secondary consequences are calculated in MSRAM. This requires an assessment by each COTP of the level of impact associated with a successful attack. The primary consequence characterization includes five categories: the expected number of deaths or injuries; the primary economic impact made up of expected property damage and business interruptions; environmental impact, defined by the number of barrels of oil or hazardous material spilled; national security impact of the attack, or measure of degradation in the U.S. ability to respond to a theater/regional crisis; symbolic impact, quantifying damage to landmarks. In addition, the consequence calculation includes an assessment of response capability of the Coast Guard, other government agencies, or the owner/operator which results in consequence reduction. The calculation for primary consequence is:

$$\text{Consequence}_{\text{primary}} = [\text{Death/Injury} + \text{Economic}_{\text{primary}} + \text{Environmental} + \text{Nat'l Defense} + \text{Symbolic}] * (1\text{-Response Capability}_{\text{CG}}) * (1\text{- Response Capability}_{\text{OG}}) * (1\text{- Response Capability}_{\text{O/O}})$$[58]

MSRAM aggregates the severity scoring for each of the six aspects of consequence to calculate the RIN for each target-scenario pair.

Secondary consequence is a categorization of the impact of a successful attack on the local, regional, or national economy, and considers redundancy and recoverability. This is combined with the primary consequences to calculate overall consequences and overall risk for each specific scenario – target pair is calculated as shown below:

[57] Gordon Woo, “Terrorism Risk,” 2.

[58] U.S. Coast Guard, *Maritime Security Risk Analysis* Model, 147.

$$\text{Consequence}_{\text{overall}} = \text{Consequence}_{\text{primary}} + \text{Consequence}_{\text{secondary}}$$[59]

$$\text{Risk}_{\text{overall}} = \text{Threat} * \text{Vulnerability}* \text{Consequence}_{\text{overall}}$$[60]

4. Event Frequency

MSRAM data collected by each COTP indicates the relative risk for all scenarios—target pairs in that sector. Individual sector data is Sensitive Security Information and when more than one sector's information is collected into a common database, it must be safeguarded at the SECRET classification level. This data is collected by Coast Guard headquarters into a nationwide database that allows review and analysis. However, since the data reflects relative risk information, it cannot be combined to reflect national maritime risk. As a result, the Coast Guard translates the relative risk data into expected loss by distributing expected attack frequency among all 15 scenarios. The Coast Guard headquarters planning team consulted accessible intelligence and estimated attack frequency at one direct attack/exploitation every year distributed across all 15 scenarios. This distribution is based on the threat level provided by the Coast Guard Intelligence Coordination Center and target attractiveness. The issue of threat shifting is addressed by assigning more threat to higher value, less protected targets that are more attractive to attack. Once this attack frequency is applied to the relative risk data, expected losses can be added to calculate the raw risk of each scenario, which is the risk level before any Coast Guard intervention. The headquarters planning team conducted additional research with the ICC and other sources to estimate the frequency of the two transfer scenarios. They arrived at the following frequencies as a result of this research: one transfer of terrorists every 10 years and one transfer of weapons of mass destruction every 20 years.[61]

Mr. Gary Ackerman, Research Director of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) recently conducted a survey of 20 experts concerning the potential for a WMD attack. On the question of the probability of

[59] U.S. Coast Guard, *Maritime Security Risk Analysis Model*, 147.

[60] Ibid.

[61] Salerno, *Combating Maritime Terrorism*, D-4.

an attack within the next 10 years, the mean probability was 53 percent and the median was 50 percent. There was a large standard deviation because of the large amount of uncertainty associated with this issue: no consensus formed among the experts. One expert estimated the probability at less than 5 percent while others estimated the probability at over 90 percent. The responses to successive survey questions indicated that "most experts expect the probability of a jihadist WMD attack to rise dramatically between 10 and 25 years' time."[62] While the Ackerman results are not restricted to transfer of WMD within U.S. ports, as is the preceding Coast Guard estimate, these two estimates of the probability of terrorist activity associated with WMD seem to be of the same order of magnitude. This is an area that deserves further examination and update if it is to reflect the latest available information.

5. Risk Ownership

The Coast Guard portion of risk ownership for each of the 15 scenarios was arrived at through consultation with Coast Guard personnel who participated in the 2005 risk-based PWCS outcome measure effort and is shown in Table 1, Risk Ownership Summary. While the Coast Guard is the lead federal agency for maritime homeland security, there are a number of other organizations involved with securing U.S. ports against terrorism. Because there have been changes in laws, regulations, policies, and partnerships since 2005, the Coast Guard portion of risk ownership should be reassessed.

[62] Gary Ackerman, "The Future of Jihadists and WMD," in *Jihadists and Weapons of Mass Destruction*, ed. Gary Ackerman and Jeremy Tamsett, 365-366 (Boca Raton, FL: CRC Press, 2008).

Table 1. Risk Ownership Summary[63]

Scenario	Estimated CG Threat Ownership	The following partners share the responsibility for mitigating the **Threat** of this Scenario	Estimated CG Vulnerability Ownership	The following partners share the responsibility for mitigating the **Vulnerability** of this Scenario	Estimated CG Consequence Ownership	The following partners share the responsibility for mitigating the **Consequence** of this Scenario	Overall CG Risk Ownership
1. Transfer through the Maritime Domain of Terrorists	0% to 10%	CIS, CBP, DOE, TSA Nat’l Intelligence Community Originating State Owner Operator Int’l LE Community	10% to 35%	State and Local LE CBP, CIS, FBI , TSA Nat’l Intelligence Community Owner Operator Int’l LE Community	10% to 35%	FEMA is the major owner after large-scale attack State and Local Responders also major owners	**43%**
2. Transfer through the Maritime Domain of WMD	0% to 10%	DOD & CBP are major owners CIS, DOE Nat’l Intelligence Community Originating State Owner Operator Int’l LE Community	10% to 35%	State and Local LE CBP is a major owner Nat’l Intelligence Community DOE, FBI, CIS Owner Operator Int’l LE Community	10% to 35%	FEMA is the major owner after WMD State and Local First Responders also major owners	**43%**
3. Waterside attack on Vessel	10% to 35%	State & Local Law Enforcement FBI Nat’l Intelligence Community	35% to 65%	State and Local Authorities Owner Operator of Vessel	10% to 35%	State and Local First Responders	**70%**
4. Shoreside Attack on Vessel	0% to 10%	State & Local Law Enforcement FBI Nat’l Intelligence Community	0% to 10%	State and Local Authorities Owner Operator of Vessel	35% to 65%	State and Local First Responders	**55%**
5. Aircraft attack on Vessel	0% to 10%	DOD is the major owner FAA, DOT State & Local Law Enforcement Nat’l Intelligence Community	0% to 10%	TSA is the Major Owner FAA DOT	10% to 35%	State and Local First Responders	**30%**
6. Stand-off Weapons Attack on Vessel	0% to 10%	Nat’l Intelligence Community FBI	35% to 65%	Owner Operator of Vessel	10% to 35%	State and Local First Responders	**63%**
7. CBRNE Attack on Vessel	0% to 10%	HHS, TSA, CBP, FBI, DNDO Owner Operator Nat’l Intelligence Community State & Local Law Enforcement	0% to 10%	State & Local Law Enforcement Owner Operator of Vessel HHS	0% to 10%	HHS Owner Operator State and Local Hospitals and First Responders	**14%**

[63] U.S. Coast Guard Headquarters Office of Plans and Policy, *Combating Maritime Terrorism - Definitions*, (Washington, D.C.: Coast Guard Headquarters Office of Plans and Policy, 2006), 16.

Scenario	Estimated CG Threat Ownership	The following partners share the responsibility for mitigating the Threat of this Scenario	Estimated CG Vulnerability Ownership	The following partners share the responsibility for mitigating the Vulnerability of this Scenario	Estimated CG Consequence Ownership	The following partners share the responsibility for mitigating the Consequence of this Scenario	Overall CG Risk Ownership
8. Sub-surface Attack on Vessel	10% to 35%	State & Local Law Enforcement FBI Nat'l Intelligence Community	35% to 65%	State and Local Authorities Owner Operator of Vessel	10% to 35%	State and Local First Responders	**70%**
9. Use of Vessel as Weapon - Exploitation by Internal Forces	0% to 10%	Nat'l Intelligence Community Flag State of Vessel International Maritime Community Owner Operator of Vessel	65% to 90%	Owner Operator of Target DOD IAIP	0% to 10%	State and Local First Responders	**80%**
10. Use of Vessel as Weapon - Exploitation by External Forces	0% to 10%	Nat'l Intelligence Community Flag State of Vessel International Maritime Community Owner Operator of Vessel	65% to 90%	Owner Operator of Target DOD IAIP	0% to 10%	State and Local First Responders	**80%**
11. Waterside attack on Facility	0% to 10%	State and Local Law Enforcement	10% to 35%	Owner Operator of Facility	10% to 35%	State and Local First Responders	**43%**
12. Shoreside attack on Facility	0% to 10%	State and Local Law Enforcement	35% to 65%	Owner Operator of Facility	10% to 35%	State and Local First Responders	**63%**
13. Aircraft attack on Facility	0% to 10%	DOD is the major owner FAA, DOT State & Local Law Enforcement Nat'l Intelligence Community	0% to 10%	TSA is the Major Owner FAA DOT	10% to 35%	State and Local First Responders	**30%**
14. Stand-off weapons attack on Facility	0% to 10%	State & Local Law Enforcement Nat'l Intelligence Community FBI	0% to 10%	Owner Operator of Facility	0% to 10%	State and Local First Responders	**14%**
15. Sub-surface Attack on Facility	0% to 10%	State & Local Law Enforcement FBI Nat'l Intelligence Community	0% to 10%	State & Local Authorities Owner Operator	0% to 10%	State and Local First Responders	**14%**

6. Risk Reduction Calculation

LROI uses fault trees to model the risk reduction achieved by Coast Guard maritime homeland security activities for each of the 15 scenarios. The same process is used for calculation of risk reduction for both direct and exploitation attacks (Scenarios 3 through 15). This section will review how risk reduction is calculated for a representative scenario. Once this is complete, the methodology of risk reduction calculations for Scenarios 1 and 2 (Transfer of Terrorists and Transfer of WMD) will be reviewed.

The LROI model is used to calculate the PWCS outcome measure through the following process. Each of the 15 scenarios is associated with several Lines of Assurance that have the potential to reduce the risk (threat, vulnerability, or consequence) of that particular scenario. There are 21 Lines of Assurance (LOA) that are made up of one or more activities from the complete list of 29 activities conducted to reduce the risk of maritime terrorism. These activities are grouped into three categories shown below. A full listing is contained in the appendix, which indicates the linkage between activities and Lines of Assurance. It also indicates the risk component that each activity addresses; threat, vulnerability, or consequence. Finally, it indicates whether each is an independent, dependent, or supporting activity. Independent activities such as patrolling do not require intelligence cuing to succeed, as the assets executing these activities are already on scene. Dependent activities, such as investigating anomalies, are dependent on intelligence cuing to prompt execution of the activity to reduce the risk of maritime terrorism. Supporting activities include collection, processing, and dissemination of intelligence, along with other activities that are important to the reduction of maritime terrorism risk reduction, but do not directly do so. Coast Guard experts, specializing in each of the three categories, assess the probability of success of each of the 29 activities. The three categories and corresponding expert areas of specialization are:

1. Achieve Maritime Domain Awareness – This includes the collection, processing, analysis, and production of intelligence, and disseminating that intelligence and information.
2. Lead and Conduct Effective Maritime Security and Response Operations – This includes conducting patrols, conducting boardings, and enforcing security zones.

3. Create and Oversee an Effective Maritime Security Regime – This includes review, approval and enforcement of vessel and facility security plans, and execution of the International Port Security Program.[64]

LROI combines the failure probability (1-effectiveness) for each activity to calculate the failure probability of the LOA. Then the failure probabilities of all LOAs that may stop a particular scenario are combined to calculate the risk reduction that the Coast Guard can achieve for that scenario. Finally, LROI combines the risk reduction achieved across all scenarios to arrive at the final PWCS outcome measure. The following sections will illustrate the process used to calculate risk reduction for direct attack and exploitation using Scenario 4 as an example and will examine the same process for transfer of terrorists and weapons of mass destruction.

a. Calculation of Risk Reduction for Direct Attack and Exploitation

Figure 4 is the fault tree for scenario 4, Shoreside Attack against Vessel. This fault tree shows the overall success probability for this scenario that the Coast Guard will succeed in reducing the risk of maritime terrorism through any one of the seven Lines of Assurance shown in Figure 4 (see below). This is represented by the “or” gate at the top of the fault tree. Line of Assurance F depends on successful intelligence cuing to prompt Activity 16, Investigate Anomalies, and this is shown in the fault tree by an “and” gate between the intelligence activities (Activities 3 and 4) and Activity 16, Investigate Anomalies. This means that no risk reduction will be achieved unless intelligence cuing is received in time to investigate anomalies. One step further down in the fault tree is the “or” gate between Activities 3 and 4, signifying that intelligence cuing can come from a source either inside or outside the Coast Guard. Line of Assurance M, Intervene by Specialized Use of Force, also requires intelligence cuing. This means that Activity 18, Specialized Use of Force, requires intelligence cuing to be effective. Since they are made up of independent activities, none of the other five Lines of Assurance in Scenario 4 require external intelligence cuing, so the probability of effectiveness for each of these is the same as the underlying activity, as shown in Table 2 following the fault tree.

[64] Office of Plans and Policy, *Combating Maritime Terrorism*, 16.

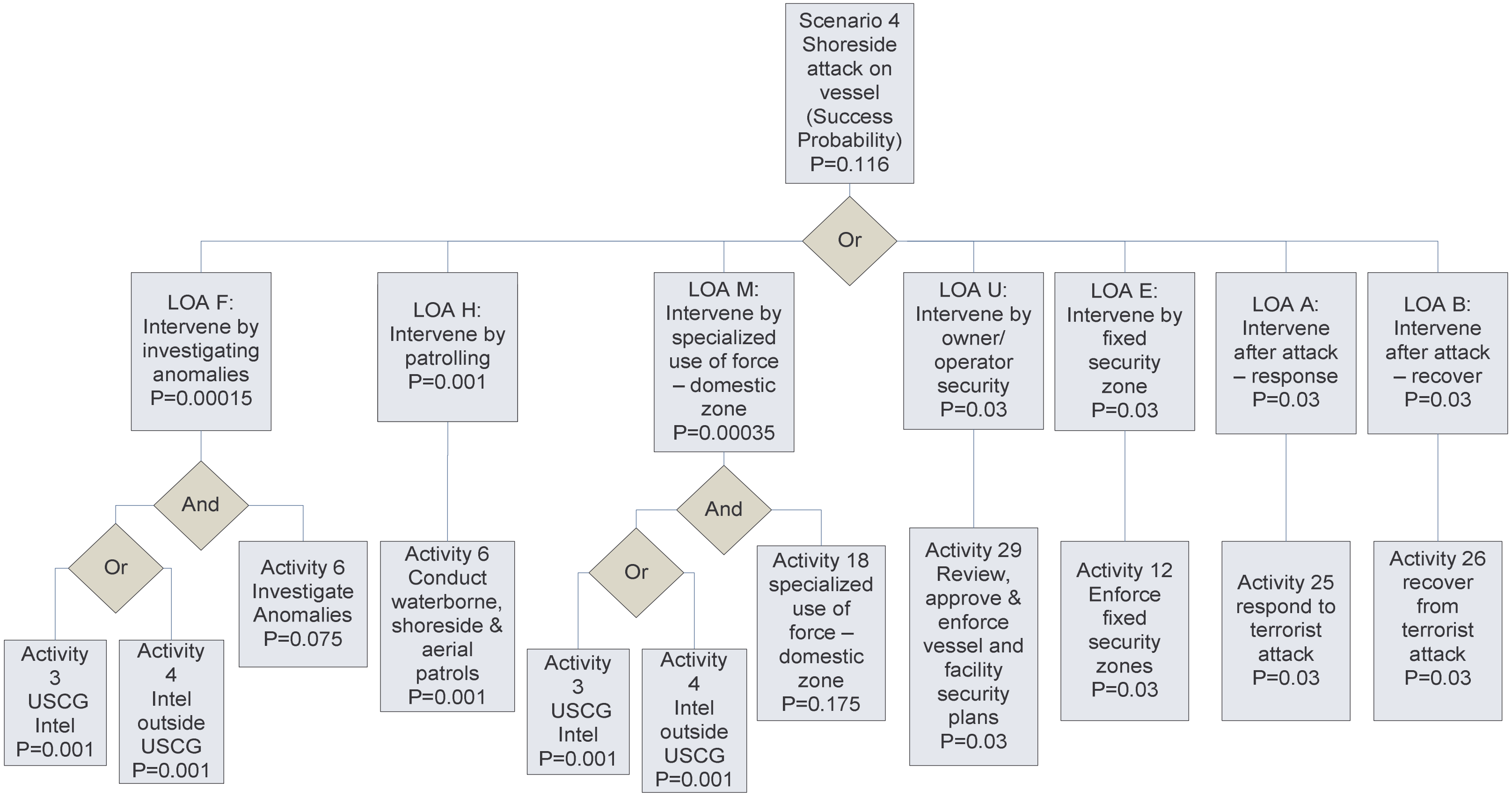

Scenario 4 Shoreside attack on vessel (Success Probability) P=0.116
Or
LOA F: Intervene by investigating anomalies P=0.00015
LOA H: Intervene by patrolling P=0.001
LOA M: Intervene by specialized use of force – domestic zone P=0.00035
LOA U: Intervene by owner/ operator security P=0.03
LOA E: Intervene by fixed security zone P=0.03
LOA A: Intervene after attack – response P=0.03
LOA B: Intervene after attack – recover P=0.03
And
Or
Activity 6 Investigate Anomalies P=0.075
Activity 3 USCG Intel P=0.001
Activity 4 Intel outside USCG P=0.001
Activity 6 Conduct waterborne, shoreside & aerial patrols P=0.001
And
Or
Activity 18 specialized use of force – domestic zone P=0.175
Activity 3 USCG Intel P=0.001
Activity 4 Intel outside USCG P=0.001
Activity 29 Review, approve & enforce vessel and facility security plans P=0.03
Activity 12 Enforce fixed security zones P=0.03
Activity 25 respond to terrorist attack P=0.03
Activity 26 recover from terrorist attack P=0.03

Figure 4. Scenario 4 Fault Tree, Success Probability

Table 2. Scenario 4 Line of Assurance—Activity Map[65]

Line of Assurance	Activity	Psuccess	Pfailure
F - Intervene by investigating anomalies	16 - Investigate Anomalies, 3 – USCG Intelligence Cuing, 4 - Non-USCG Intelligence Cuing	0.00015	0.99985
H - Intervene by patrolling	7 - Conduct Waterborne, Shoreside, and Aerial Patrols	0.001	0.999
M - Intervene by specialized use of force – domestic zone	18 - Specialized Use of Force - Domestic Zone, 3 - USCG Intelligence Cuing, 4 - Non-USCG Intelligence Cuing	0.00035	0.99965
U - Intervene by owner/operator security	29 - Review, Approve, and Enforce Compliance with Domestic Vessel, Facility and Outer Continental Shelf (OCS) Facility Security Plans	0.03	0.97
E - Intervene by fixed security zone	12 - Enforce Fixed Security Zones	0.03	0.97
A - Intervene after attack - recovery	25 - Respond to Terrorist Attack	0.03	0.97
B - Intervene after attack - response	26 - Recover from Terrorist Attack	0.03	0.97

LROI performs calculations on the basis of probability of failure, so the effectiveness estimations (Probability of Success = P_s) provided by Coast Guard experts are converted to Probability of Failure (P_f) as follows: $P_f = 1 - P_s$. From this viewpoint, the fault tree for Scenario 4, Shoreside Attack against Vessel, shows that the overall failure probability for this scenario that the Coast Guard will fail to reduce the risk of maritime terrorism through any one of the seven Lines of Assurance is represented by an "and" gate at the top of the fault tree shown in Figure 5 (see below). The failure of Line of Assurance F is contingent upon failure of either intelligence cuing (Activities 3 and 4) or Activity 16, Investigate Anomalies. This is shown in the fault tree by an "or" gate

[65] U.S. Coast Guard Headquarters Office of Policy and Planning Integration "LROI Model" (Washington, D.C.: U.S. Coast Guard Headquarters Office of Performance Management and Assessment, 2008).

between the intelligence activities (Activities 3 and 4) and Activity 16, Investigate Anomalies, and signifies that no risk reduction will be achieved if there is a failure in either intelligence cuing or action to investigate anomalies. One step further down in the fault tree is the “and” gate between Activities 3 and 4, signifying that a failure of intelligence cuing occurs when that failure occurs both inside and outside the Coast Guard. Line of Assurance M also requires intelligence cuing, and the failure probabilities are calculated using the same logic. None of the other five Lines of Assurance in Scenario 4 require external intelligence cuing, so the probability of failure for each of these is the same as the underlying activity, as above.

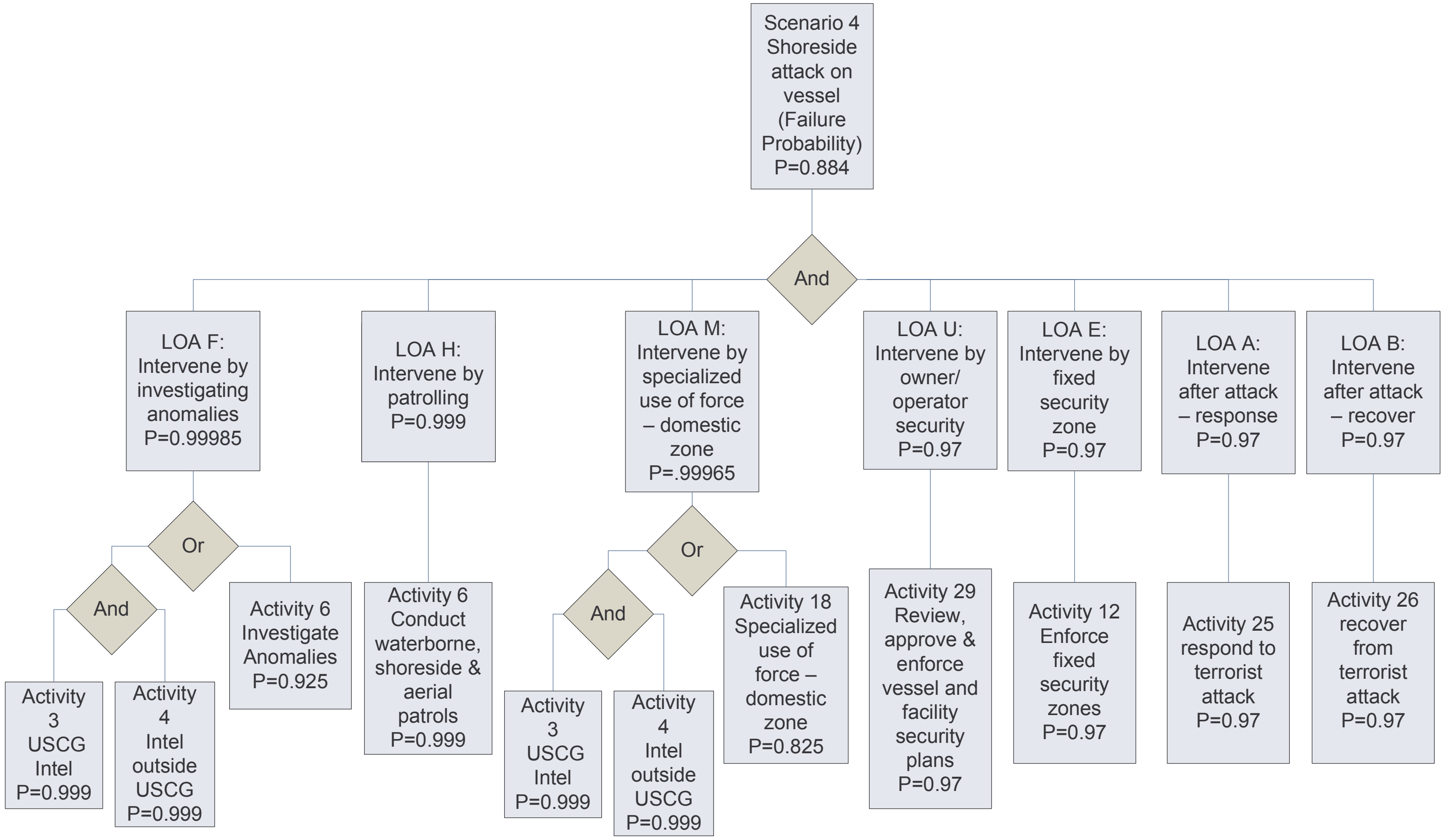

Scenario 4 Shoreside attack on vessel (Failure Probability) P=0.884
And
LOA F: Intervene by investigating anomalies P=0.99985
LOA H: Intervene by patrolling P=0.999
LOA M: Intervene by specialized use of force – domestic zone P=.99965
LOA U: Intervene by owner/ operator security P=0.97
LOA E: Intervene by fixed security zone P=0.97
LOA A: Intervene after attack – response P=0.97
LOA B: Intervene after attack – recover P=0.97
Or
And
Activity 3 USCG Intel P=0.999
Activity 4 Intel outside USCG P=0.999
Activity 6 Investigate Anomalies P=0.925
Activity 6 Conduct waterborne, shoreside & aerial patrols P=0.999
Or
And
Activity 3 USCG Intel P=0.999
Activity 4 Intel outside USCG P=0.999
Activity 18 Specialized use of force – domestic zone P=0.825
Activity 29 Review, approve & enforce vessel and facility security plans P=0.97
Activity 12 Enforce fixed security zones P=0.97
Activity 25 respond to terrorist attack P=0.97
Activity 26 recover from terrorist attack P=0.97

Figure 5. Scenario 4 Fault Tree, Failure Probability

The calculation of failure to achieve risk reduction is as follows:

Failure of intelligence cuing, “and” gate

$P_{fi} = P_{fA3} * P_{fA4}$

$P_{fi} = 0.999 * 0.999$

$P_{fi} = 0.998001$

Failure of Line of Assurance F, “or” gate

$P_{fLF} = 1 – [(1 – P_{fi)} * (1 – P_{fA16})]$

$P_{fLF} = 1 – [(1 - 0.998001)* (1 - 0.925)]$

$P_{fLF} = 0.999855$

Failure of Risk Reduction in Scenario 4, “and” gate

$P_{fS4} = P_{fLF} * P_{fLH} * P_{fLM} * P_{fLU} * P_{fLE} * P_{fLA} * P_{fB}$

$P_{fS4} = 0.99985 * 0.999 * 0.99965 * 0.97 * 0.97 * 0.97 * 0.97$

$P_{fS4} = 0.884$

This indicates that the probability of failure of all seven Lines of Assurance associated with Scenario 4 to reduce the risk of maritime terrorism is 88.4 percent. Therefore, the overall Raw Risk Reduction Factor (RR_{rf}) achieved by Coast Guard PWCS activity in Scenario 4 is 1.0 – 0.884 = 0.116, or RR_{rf} = 11.6%.

Given a Raw Risk RIN of 1,463 for Scenario 4 results in the following:

Scenario 4 RR RIN = 1463

Raw Risk Reduction, RR_r

RR_r RIN = RR_{rf} * RR RIN

RR_r RIN = 0.116 * 1463

RR_r RIN = 170

As indicated in the Risk Ownership Summary (Table 1), the Coast Guard Owned Risk Factor ($CGOR_f$) for this scenario is 55 percent of the raw risk, or $CGOR_f$ = 55%. This is used to calculate the portion of the risk that is owned by the Coast Guard.

Coast Guard Owned Risk, CGOR

CGOR RIN = $CGOR_f$ * RR RIN

CGOR RIN = 0.55 * 1463

CGOR RIN = 810

The Coast Guard Owned Risk Reduction Factor is calculated by dividing the Raw Risk Reduction by the Coast Guard Owned Risk.

Coast Guard Owned Risk Reduction Factor, $CGOR_{rf}$

$CGOR_{rf}$ = RR_r RIN / CGOR RIN

$CGOR_{rf}$ = 170 / 810

$CGOR_{rf}$ = 21%

This results in a Coast Guard Owned Risk Reduction Factor for scenario 4 of 21 percent. Once Risk Reduction Factors are calculated for each scenario, they can be combined to calculate the total risk reduction due to Coast Guard activities, which is the PWCS Outcome Measure. The Coast Guard then uses these results to assess the return on investment of each Line of Assurance and underlying activities to inform plans to acquire the platforms and bring on the personnel and to execute those activities.

b. Calculation of Risk Reduction for Transfer of Terrorists and Weapons of Mass Destruction

Scenarios 1 and 2: Calculations of risk reduction associated with the two transfer scenarios achieved through Coast Guard activities start out with a characterization of the overall risk associated with Transfer of Terrorists or Transfer of Weapons of Mass Destruction. As previously indicated, the overall risk levels of the transfer of terrorists or WMD in the maritime domain are estimated through analysis of the National Maritime Strategic Risk Profile and the National Maritime Transportation Security Plan risk assessment, combined with information from the Coast Guard Intelligence Coordination Center. Each of the two transfer scenarios is subdivided into 16 sub-scenarios to account for vessel type, crew compliance/non-compliance with Coast Guard direction, and level of warning provided concerning arrival of these vessels. As shown below in Figure 6 and Figure 7 (see below), the overall risk for Scenario 1, Transfer of Terrorists, is then subdivided among its 16 sub-scenarios, and the overall risk for Scenario 2, Transfer of Weapons of Mass Destruction, is subdivided among its 16 sub-scenarios. A fault tree is constructed for each of the 16 sub-scenarios, and risk reduction is calculated in the same manner as the previous example, Scenario 4.

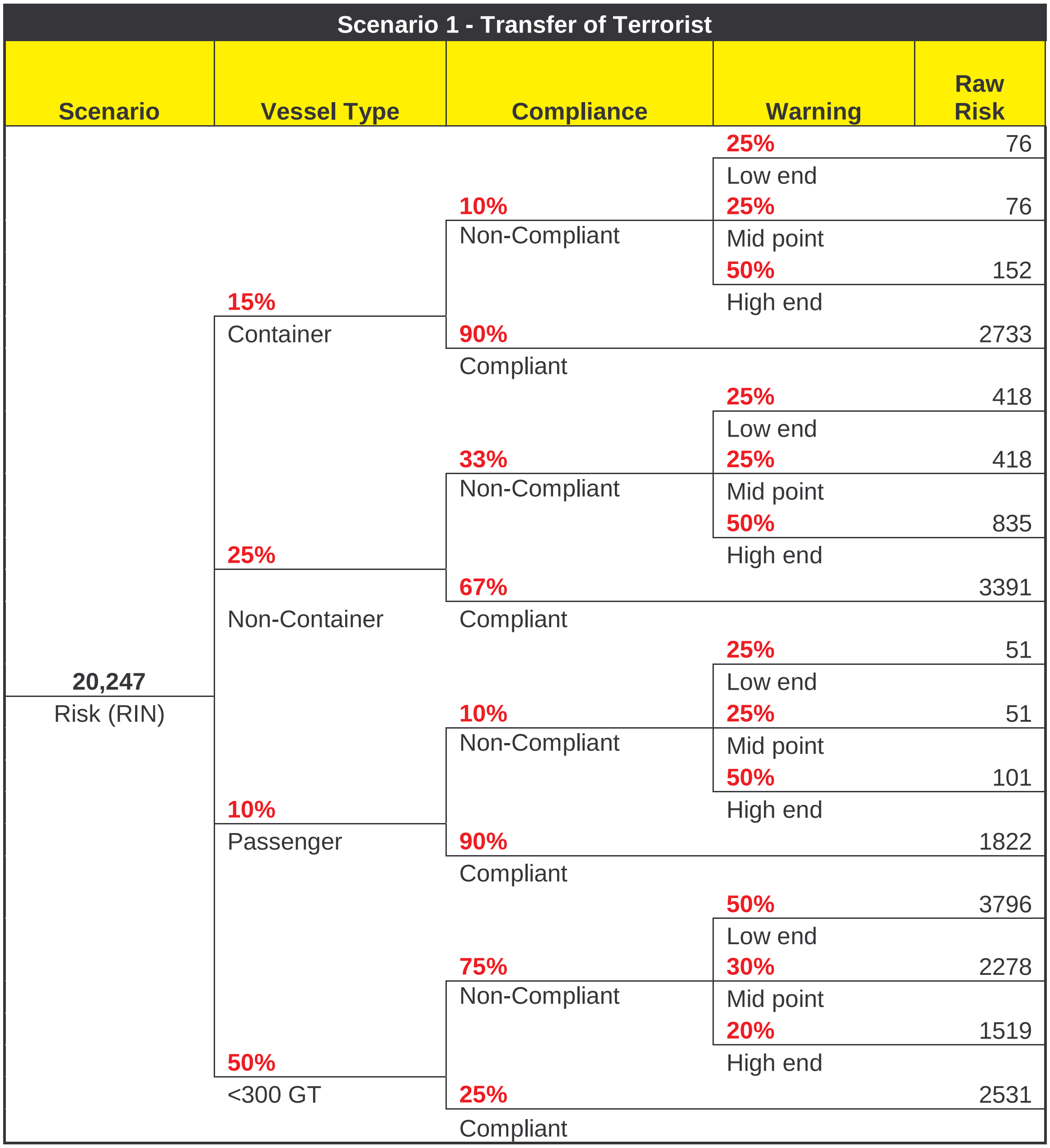


Figure 6. Transfer of Terrorist Scenario Assumption Tree[66]

[66] Office of Policy and Planning Integration, “LROI Model.”

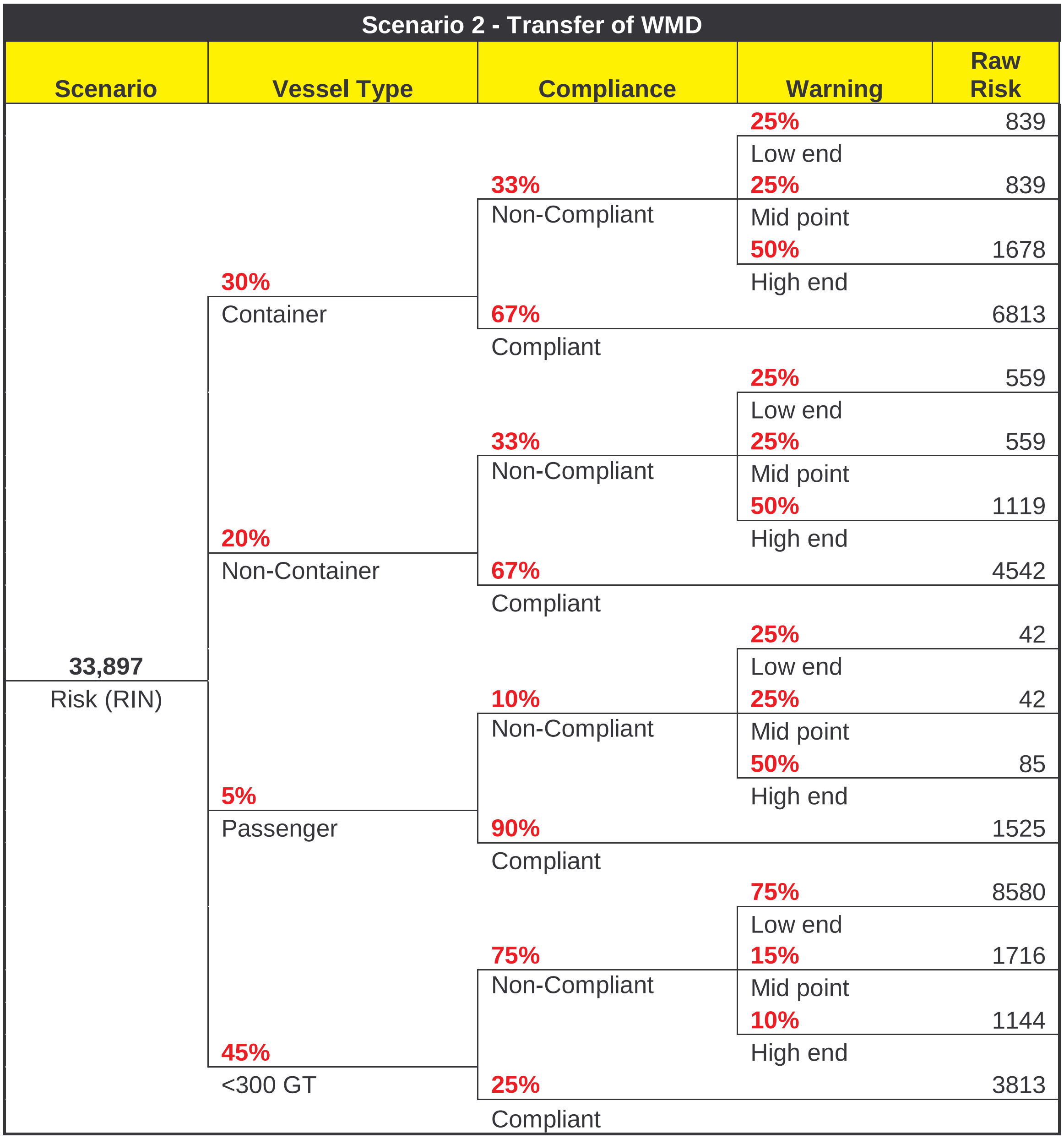


Figure 7. Transfer of WMD Scenario Assumption Tree[67]

c. Overall Risk Reduction – PWCS Outcome Measure

The previous two sections described the process used to calculate the risk reduction for each of the 15 scenarios. The total reduction in the risk of maritime terrorism is found by summing the risk reduction for each scenario, as shown in Table 3

[67] Office of Policy and Planning Integration, "LROI Model."

below. The PWCS Outcome Measure is then found by dividing the risk reduction by the Coast Guard owned risk. Each activity is classified as to whether it reduces threat, vulnerability, or consequence, so the risk reduction due to reduced threat, vulnerability, or consequence can also be calculated. In FY08, the PWCS Outcome Measure indicated that Coast Guard activities reduced the risk of maritime terrorism by 20 percent. As a result of this performance, the Coast Guard exceeded goals for overall risk reduction, threat reduction, and vulnerability reduction.

Table 3. FY08 PWCS Outcome Measure[68]

Scenario Description	CG Owned Risk, RIN	Risk Reduction, RIN	Risk Reduction %	Threat Reduction, RIN	Vulnerability Reduction, RIN	Consequence Reduction, RIN	Threat Reduction, %	Vulnerability Reduction, %	Consequence Reduction, %
1 - Terrorist Transfer	8755	2541	29%	897	1645	0	10%	19%	0%
2 - WMD Transfer	14658	1738	12%	641	1098	0	4%	7%	0%
3 - Vessels/ Waterside attack	1836	523	28%	11	257	255	1%	14%	14%
4 - Vessels/ Shoreside Attack	810	170	21%	2	84	84	0%	10%	10%
5 - Vessels/ Aircraft attack	322	107	33%	0	0	107	0%	0%	33%
6 - Vessels/ Stand-off Weapons	673	153	23%	34	60	60	5%	9%	9%
7 - Vessel/CBR	0	0	0%	0	0	0	0%	0%	0%
8 - Vessel/Sub-surface Attack	469	60	13%	1	20	39	0%	4%	8%
9 - Vessel/ Exploitation/ Internal Forces	1736	317	18%	11	182	123	1%	11%	7%
10 - Vessel/ Exploitation/ External Forces	3808	887	23%	29	590	269	1%	15%	7%
11 - Facilities/ Waterside attack	1503	521	35%	12	165	344	1%	11%	23%
12 - Facilities/ Shoreside attack	6093	1112	18%	10	551	551	0%	9%	9%
13 - Facilities/ Aircraft attack	378	73	19%	0	0	73	0%	0%	19%
14 - Facilities/Stand-off weapons	190	112	59%	5	37	70	3%	19%	37%
15 - Facilities/Sub-surface Attack	223	130	58%	5	43	82	2%	19%	37%
FY08 Grand Total	41454	8444	20%	1657	4732	2057	4%	11%	5%
FY08 Targets			17%				1%	10%	6%

https://apps.dtic.mil/dtic/tr/fulltext/u2/a527037.pdf (retrieved 20 January 2019)

[68] Matthew Mowrer, "2008 Risk Change and Margin of Error.xls" (internal document, U.S. Coast Guard Headquarters Office of Performance Management and Assessment, Washington, D.C., 2008).

IV. ASSESSMENT OF COAST GUARD IMPACT ON TERRORISM-RELATED MARITIME RISK

A. METHOD

The purpose of this research is to conduct a formative evaluation of Coast Guard measurement of effectiveness in achieving maritime homeland security that is reported in the Ports, Waterways and Coastal Security (PWCS) Outcome Measure. This thesis:

1. Examines in detail how the Coast Guard currently measures effectiveness in achieving maritime homeland security,
2. Examines how this measurement could be improved, and
3. Makes specific recommendations to improve measurement of effectiveness in achieving maritime homeland security.

The focus of this study is to ascertain strengths in the existing Coast Guard measurement of effectiveness in achieving maritime homeland security and to point out areas for improvement. The desired result is to improve this measurement by using existing Coast Guard expertise and with information from other experts in the field of terrorism risk assessment.

This research examines the mechanisms by which the existing measurement program operates and why these mechanisms operate in their current manner. As such, it is a process evaluation of Coast Guard measurement of effectiveness in achieving maritime homeland security.

The Coast Guard's method for measurement of effectiveness in achieving maritime homeland security is prescribed for Coast Guard field units nationwide. Interviews were conducted with personnel at Coast Guard and DHS headquarters in Washington, D.C., along with personnel on the Coast Guard Pacific Area staff and the Eleventh Coast Guard District staff in Alameda, California. Interviews were conducted with those executing Coast Guard policy concerning maritime homeland security and with those tasked with measurement of the effectiveness of those policies. This pool of interviewees was chosen in an attempt to cover all levels of the spectrum of personnel involved with the measurement of effectiveness in achieving maritime homeland security. In addition to DHS personnel, the author interviewed personnel at University of Maryland National Consortium for the Study of Terrorism and Responses to Terrorism, RAND Corporation and American Bureau of Shipping Risk Consulting Division to gain the perspective of outside subject matter experts.

Correspondence and qualitative interviews were used to collect information from Coast Guard personnel and outside experts in the field of terrorism risk assessment. No qualitative data was collected by conducting observational fieldwork. The literature review has revealed potential areas to improve measurement of effectiveness in achieving maritime homeland security. The interviews provided expert insight into additional areas for improvement from Coast Guard personnel who are using the current metric and from risk assessment experts outside the Coast Guard. Overlaps are identified indicating convergence between interviewees, along with differences and dissent indicating divergence. The qualitative data that was collected is reviewed in this chapter and successive chapters propose how the Coast Guard can apply that information to improve measurement of effectiveness in achieving maritime homeland security.

Purposeful sampling strategies were used since there is a select group of personnel with expertise and involvement in this area of Coast Guard operations. Advocates of the existing measurement program were interviewed, along with those who propose changes to the current methodology.

Qualitative data was collected describing how the Coast Guard currently measures effectiveness in achieving maritime homeland security. A preliminary review of Coast Guard guidance for this measurement was accomplished before conducting the interviews to ensure understanding of current procedures. This project proposes refinements to the metric in question. Recommendations for maintaining the current metric or transitioning to a new metric are addressed in the implementation plan.

B. INTERVIEW QUESTIONS AND FINDINGS

Each of the interviewees was asked a similar set of questions, which are listed in Table 4, though they evolved through the course of the interview process. Those ending in “a” refer to questions on the Maritime Security Risk Analysis Model (MSRAM), while those ending in “b” refer to questions on the PWCS Outcome Measure. The following eight sections of this chapter provide information on responses received from interviewees with a listing of important findings focused on improving the PWCS Outcome Measure. The eight sections are linked directly to the eight questions. The chapter concludes with a summary section that highlights the important observations and suggestions.

Table 4. Interview Questions

Chapter Section	Interview Questions
1. Accuracy of the PWCS Outcome Measure	1.b. Do you think the current measure accurately reflects Coast Guard mission effectiveness in achieving homeland security?
2. Level of Inaccuracy of the PWCS Outcome Measure	2.b. If the current measure does not accurately reflect Coast Guard mission effectiveness in achieving homeland security, can you characterize the level of inaccuracy to indicate if current measures are relatively close, or if they are very far off?
3. Causes of Inaccuracy in the PWCS Outcome Measure	3.b. Can you explain what you think causes the variance between an accurate measure and the Coast Guard’s current measure of mission effectiveness in achieving homeland security?
4. Improving Assessment of Maritime Homeland Security Mission Effectiveness	4.a. How do you think the Coast Guard can improve assessment of maritime terrorism risk? 4.b. How do you think the Coast Guard can improve assessment of mission effectiveness in achieving homeland security?
5. Risk Modeling	5.a. What impact do you think the use of Risk Modeling would have on Coast Guard assessment of maritime terrorism risk? 5.b. What impact do you think the use of Risk Modeling would have on Coast Guard assessment of mission effectiveness in achieving homeland security?
6. Expert Judgment	6.a. What impact do you think the use of Expert Judgment would have on Coast Guard assessment of maritime terrorism risk? 6.b. What impact do you think the use of Expert Judgment would have on Coast Guard assessment of mission effectiveness in achieving homeland security?
7. Expert Judgment Aggregation	7.a. What impact do you think the use of Expert Judgment Aggregation would have on Coast Guard assessment of maritime terrorism risk? 7.b. What impact do you think the use of Expert Judgment Aggregation would have on Coast Guard assessment of mission effectiveness in achieving homeland security?

Chapter Section	Interview Questions
8. Event Trees	8.a. What impact do you think the use of Event Trees would have on Coast Guard assessment of maritime terrorism risk? 8.b. What impact do you think the use of Event Trees would have on Coast Guard assessment of mission effectiveness in achieving homeland security?

1. Accuracy of the PWCS Outcome Measure

Opinions on the current PWCS Outcome Measure ranged from a relatively strong endorsement of the measure to an expression of concern: “I am skeptical of the existing measure of PWCS mission effectiveness because it just seems to be an educated guess.” This interviewee expressed concern because of experience participating in an elicitation of expert judgment for the PWCS Outcome Measure with only Coast Guard personnel present. One Coast Guard officer stated, “The current measure is not accurate enough… [it] shows how we’re doing relative to previous years, but the absolute measure is not as precise as desired.” He offered ideas for achieving better accuracy when responding to the subsequent question on improving the measure. Another officer said, “The accuracy or inaccuracy of the measure can be driven by the alpha—the most forceful person in the group.” He went on to discuss this further when addressing the expert judgment question. The most positive endorsement came from a terrorism expert after an initial examination of the measure and the expert elicitation process: “The measure does seem to reflect actual mission effectiveness well. It incorporates risk reduction with multiple meta-scenarios to cover the threat space; separates threat, vulnerability and consequence; and represents layers of defense through prevention and response.” Several of those interviewed were not familiar enough with the measure to offer a view. Coast Guard personnel with the most knowledge of the measure were convinced that it provides good information concerning Coast Guard mission effectiveness in achieving maritime homeland security in the maritime domain, but also acknowledged the need for improvement. Each interviewee made recommendations for improvement to both the assessment of terrorism-related maritime risk with MSRAM and Coast Guard effectiveness in reducing that risk with the LROI model. These recommendations are enumerated later in this chapter.

2. Level of Inaccuracy of the PWCS Outcome Measure

When asked to characterize the level of inaccuracy, responses ranged from a seemingly overconfident 2.4 percent margin of error to a conservative estimate of within an order of magnitude; one officer stated, “It’s probably in the ballpark” and estimated the PWCS Outcome Measure is within a 70 percent confidence interval. An outside expert said, “The current measure looks like it is already a relatively good reflection of Coast Guard mission effectiveness.” Everyone who was familiar with both MSRAM and the PWCS Outcome Measure voiced the opinion that the risk levels indicated by MSRAM were more accurate than the PWCS Outcome Measure, such as: “MSRAM provides good data,” and “We have a much better assessment of existing risk levels than we do of our effectiveness reducing that risk.” This is because the current risk level in MSRAM is largely based on vulnerability and consequences assessed by local Coast Guard personnel with a much higher degree of certainty than the estimated ability of Coast Guard activities to prevent maritime terrorism in the LROI model. MSRAM data is collected by personnel at each of the 35 Coast Guard sectors throughout the United States and combined to gain understanding of the risk levels in each of those ports. MSRAM data includes judgments on the effectiveness of Coast Guard personnel to prevent terrorism for some, but not all of the 29 activities that the LROI model uses to calculate the PWCS Outcome Measure. By collecting data on a nationwide basis, there is a potential to reduce biases that could adversely affect the PWCS Outcome Measure results. However, to populate the LROI model, the Coast Guard uses unstructured groups to acquire data for activities not included in the robust data collection process required for MSRAM. Skepticism concerning the measure came from experience and concerns with previous mission effectiveness data collection processes. As previously indicated, this prompted apprehension that the accuracy of the measure could be driven by the most forceful person in the group. These concerns combined with the desire to improve the PWCS Outcome Measure prompted additional research into the expert elicitation process.

3. Causes of Inaccuracy in the PWCS Outcome Measure

There was a wide range of ideas put forth on the causes of inaccuracy in the PWCS Outcome Measure. One expert stated, “There is no supportable way of measuring either the level of maritime terrorism risk, or the Coast Guard capability to reduce that risk. There is no way to measure the outcome.” However, the expert went on to suggest the ways in which the Coast Guard could improve assessment of maritime terrorism risk and assessment of Coast Guard activities in reducing that risk.

As previously mentioned, the PWCS Outcome Measure is based on a preliminary assessment of the existing level of risk in the U.S. maritime domain through MSRAM. In reference to MSRAM results, one interviewee stated that “The largest inaccuracy with the risk assessment is probably the transfer scenarios [of terrorists and WMD] – neither is in MSRAM yet,” though a forthcoming version will include them. Another interviewee said, “The biggest driver of inaccuracy in the current measure is the lack of knowledge of the actual capability of the adversary, and lack of knowledge of the actual intent of the adversary. Since threat is a function of capability and intent, this lack of knowledge results in imprecise threat estimation, which then provides inaccurate risk estimation.” This issue leads to inaccuracy in the PWCS Outcome Measure.

Specifically addressing concerns with the PWCS Outcome Measure, the interviewee went on to indicate, “Another source of inaccuracy is the fact that we are making assumptions on the level of intelligence cueing, which then impacts the assessment of the reduction in maritime terrorism risk, since many Lines of Assurance (LOAs) incorporate assumptions on intelligence cueing and its impact on successfully stopping terrorist attacks.” This was emphasized by another respondent who indicated that this lack of knowledge of intelligence cueing is the greatest driver of inaccuracy in the model.

A Coast Guard officer stated that the variance between an accurate PWCS Outcome Measure and the current measure “is caused by bias: we think we’re doing better than we’re actually doing. We expect results from our labor — we expect Coast Guard presence and actions to deter terrorism.”

When referring to the assessment of activity effectiveness within the LROI model, another officer indicated:

> The variance between an accurate measure and our current measure is due to the fact that the Coast Guard is looking at a high level of mission effectiveness, for example, the effectiveness of an entire unit such as a Marine Safety and Security Team. To reduce this variance, the Coast Guard needs to break down that effectiveness into individual components, and then measure those components. One potential breakdown of components is contained in the Coast Guard's Combating Maritime Terrorism (CMT) guidance: ACCCP: Authorities, Capabilities, Capacities, Competencies, Partnerships.

Along a similar line of thought, he also stated, "The Coast Guard needs to gain a better understanding of individual components that contribute to reduced maritime terrorism risk: weapons, night vision goggles, training, etc." Another possibility is to use the six facets of readiness: people, equipment, supplies, training, information, and infrastructure. The MSRAM team worked with the Deployable Operations Group to measure the effectiveness of various Coast Guard adaptive force packages and could provide valuable insight into improving activity effectiveness assessments.

One respondent offered the following list of causes of inaccuracy in the PWCS Outcome Measure:

1. Lack of validation of a full list of activities that reduce maritime terrorism risk.
2. Lack of mapping [Operation Neptune Shield (ONS)] activities to (MSRAM) scenarios
3. Differences between local and national SME assessment of effectiveness in activities that reduce maritime terrorism risk.
4. Lack of outside SMEs in the process used to assess effectiveness in activities that reduce maritime terrorism risk.

In alignment with Item 2 above, another respondent said, "ONS reporting is based on activity, not results, and ONS activities are not directly linked to maritime terrorism risk reduction in MSRAM or in reality." Other interviewees indicated that the poor linkage between Operation Neptune Shield activities (ONS), MSRAM Coast Guard activities and the 29 maritime terrorism prevention activities contained in the LROI model make it difficult to use ONS and MSRAM information to populate the LROI model.

4. Improving Assessment of Maritime Homeland Security Mission Effectiveness

The first step in improving assessment of maritime homeland security mission effectiveness is to improve MSRAM results, and the first step in improving MSRAM results is to ensure accurate target lists are available. One suggestion to do that was “to improve targeting of what is of interest from a security standpoint.” Periodic updating of the target lists will ensure the risk assessment is conducted on the facilities and vessels that are actually in each Coast Guard Captain of the Port (COTP) Zone.

A terrorism expert stated that MSRAM:

> …should allow updates with new threats, new targets, and general environment updates, including regulatory, physical, etc. Examples: sea level rises by two feet, which causes national security implications. New levees built after Katrina could be new targets which could be blown up by terrorists.

A Coast Guard officer suggested, “One way to improve assessment of maritime terrorism risk is to conduct Maritime Transportation Security Act (MTSA) spot checks” to populate MSRAM. This would provide information collected in person on target vulnerability and consequence. He continued:

> Another way is to create ironclad processes for new personnel that are using MSRAM to assess maritime terrorism risk. This would include developing job aids for MSRAM and conducting more training to ensure that those inputting data are familiar with the program and requirements for risk assessment. An additional concern raised was differences between local and national SME assessment of effectiveness in activities that reduce maritime terrorism risk.

These differences would be minimized through the training program described above. In fact, the MSRAM team has a help desk to address field questions on the system, has already created job aids and video training modules and is working to implement MSRAM training at several Coast Guard training centers.

Another Coast Guard officer echoed the drive for more training when he said:

> The best way to improve assessment of maritime terrorism risk is to follow the Commandant's guidance…to institutionalize MSRAM within the Coast Guard…By increasing the number of people who are familiar with the tool, the Coast Guard will be able to better assess maritime terrorism risk, and better use that information to reduce the risk of maritime terrorism.

One respondent stated: "The Coast Guard can improve assessment of maritime terrorism risk through improved understanding of threat and consequence." Improved threat assessments would need to address the lack of knowledge of the actual capability and intent of the adversary identified as causes of inaccuracy in MSRAM.

A further suggestion by a terrorism expert to improve this maritime terrorism risk assessment was "to make it more dynamic: get numerical estimates once a year, but collect data for future expectations…This would show steady, increasing or decreasing risk" throughout the course of the year.

The expert went on to state:

> The 15 existing scenarios are very good, but the problem is that once you define those scenarios, you leave gaps, and adversaries will try and exploit [using] attacks not accounted for in the models. [While the existing model allows COTPs to add scenarios to MSRAM], there needs to be an update mechanism for the model to update/add/delete scenarios, whether this originates with Coast Guard headquarters, COTPs, or intelligence sources.
>
> This would enable a COTP to account for changing conditions and terrorist threat shifts. The idea is that if one COTP proposes a new scenario, then this scenario should be reviewed and potentially used by other COTPs.

Concerning the PWCS Outcome Measure, a Coast Guard officer stated "This could be improved by better linkage between ONS activities and maritime terrorism risk reduction." This sentiment was expressed by several of the interviewees. This exercise should start with a validation of a complete list of activities that reduce maritime terrorism risk, and then create a strong linkage between this list, ONS activities, MSRAM, and the LROI model to address the causes of inaccuracy identified above.

Another officer indicated, "The Coast Guard needs to improve our assessment of intelligence cueing for the LROI model. Current model assumes two percent intelligence cueing on attempted terrorist attacks. The Coast Guard also needs to improve capacity estimation/assessment" to more accurately model individual activity effectiveness. Assessment of intelligence cueing and capacity assessment were judged the most significant drivers of the model so these should be the highest priority for improvement.

Another recommendation to improve assessment of Coast Guard reduction of maritime terrorism risk is to "convene independent Coast Guard groups who would assess LOA effectiveness, and then compare and/or combine the results of these groups." The same respondent also suggested that:

> …participation by industry and security professionals in groups assessing LOA effectiveness would potentially improve assessment of Coast Guard reduction of maritime terrorism risk. However, there are very few industry and security professionals who are familiar with Coast Guard capabilities to reduce maritime terrorism risk.

This aligns with the concern raised by another interviewee who cited the "lack of outside SMEs in the process used to assess effectiveness in activities that reduce maritime terrorism risk."

One of the causes of inaccuracy identified above was the bias that originates with Coast Guard personnel who "think we're doing better than we're actually doing." This is a case of wishful thinking bias, and will be addressed in Chapter V on expert judgment.

As indicated in response to the previous question, one cause of variance between an accurate PWCS Outcome Measure and the current measure is the LROI model use of high-level activities to assess maritime homeland security mission effectiveness, and the need to disaggregate high level activities into individual components. For example, instead of assessing the effectiveness of the LROI activity "Specialized Use of Force" nationwide, better results would be gained by breaking down "Specialized Use of Force" by COTP zone and then into individual components, such as the number of fully mission capable small boats with qualified crews, and then assessing the effectiveness of those components.

A terrorism expert indicated, “Dynamic assessment of Coast Guard performance in the same manner would improve that assessment in the same manner as [for MSRAM].” This would entail collecting estimates for levels of effectiveness of Coast Guard activities to reduce maritime terrorism “once a year, but collect data for future expectations” to indicate whether SMEs estimated effectiveness would increase, decrease, or maintain existing levels.

He added that:

> The [LROI] Model links specific Coast Guard activities into Lines of Assurance, and then applies those Lines of Assurance against specific scenarios. The issue and danger with the gaps above is that the Coast Guard will not take specific action to assess and address scenarios that are not defined, and this opens up vulnerabilities in the maritime port security system.

The capability to update scenarios already exists in MSRAM and should be added to the LROI model.

5. Risk Modeling

The Coast Guard uses two models to arrive at the PWCS Outcome Measure: the Maritime Security Risk Analysis Model (MSRAM) and the Combating Maritime Terrorism model, which as previously indicated, is called the LROI model.

Most of those interviewed expressed their agreement that additional modeling would improve the PWCS Outcome Measure. One respondent stated, “Micromodeling of each scenario would improve Coast Guard assessment of maritime terrorism risk. Highest risk scenarios should be micromodeled first. Examples of micromodeling include the response calculator and blast calculator already in MSRAM.” These additions to the model allow calculation of response effectiveness and consequences of various sized explosives during the target assessment process and were cited as pertinent examples of improvements that will lead to better risk assessment and, subsequently, better performance assessment of Coast Guard activities designed to reduce maritime terrorism risk.

One Coast Guard officer suggested that "Threat shifting could potentially be incorporated into MSRAM through target attractiveness" to expand upon the vulnerability calculation which is used to account for threat shifting now.

Another Coast Guard officer indicated, "The Coast Guard needs to use independent modeling/calculation of capacity for performance assessment." This would allow more accurate characterization of Coast Guard PWCS capacity based on available platforms and personnel to improve performance assessment of maritime homeland security mission effectiveness.

Finally, in reference to modeling, one expert indicated, "This could be good or bad, depending on whether the model is good or bad, and whether the data put into the model are good or bad."

6. Expert Judgment

All interviewees agreed that expert judgment is critical to both assessment of maritime terrorism risk and assessment of effectiveness in reducing that risk. A terrorism expert stated, "The Coast Guard must use expert judgment to assess maritime terrorism risk. Need to elicit the opinions of the right experts and use them in appropriate ways to assess threat, vulnerability and consequence."

The Coast Guard acquires information on maritime homeland security mission effectiveness for the LROI model by gathering input from Coast Guard SMEs. Several of those interviewed recommended collecting information on estimated effectiveness of Coast Guard maritime homeland security activities from personnel outside the Coast Guard with maritime expertise, including Navy SEAL team members and other subject matter experts in the area of tactics and their use in protecting against maritime threats, tugboat operators, harbor pilots, and others who spend a large amount of time in marine environments. These experts could potentially form a Red Cell similar to U.S. Navy

SEAL Team Six, which tested the security of U.S. Navy bases. The proposed Red Cell would evaluate Coast Guard maritime terrorism risk reduction activities from the perspective of the terrorist mindset. One terrorism expert said:

> Coast Guard assessment of mission effectiveness could be improved through the use of outside experts with similar expertise to the Coast Guard experts. These could, and should include fishermen, America's Cup sailors and others. This should include people who have experience evading maritime security efforts from organizations like the Coast Guard, including convicted smugglers and members of Greenpeace and the Sea Shepherds. There is a need to have heterogeneity in the experts who are consulted.

Sources should include government, industry, academia, and the underworld. Examples cited the American Association of Port Authorities and other organizations, along with people who have experience evading maritime security efforts, such as "reformed" or incarcerated terrorists or smugglers. The need for heterogeneity in experts was emphasized as a variety of viewpoints on Coast Guard mission effectiveness should reduce bias in the results.

A Coast Guard officer indicated that "Current Coast Guard guidance requires the input of [those outside the Coast Guard] on Area Maritime Security Committees on the annual MSRAM data collection process." Another Coast Guard officer stated, "Area Maritime Security Committee (AMSC) input has improved assessment of risk, especially vulnerability since facility and vessel operators know their facilities and vessels best, and threat since local personnel are in the best position to know about those who may want to attack their facility or vessel."

One interviewee said, "In addition to AMSC input, it would benefit the Coast Guard to get outside terrorism experts to conduct a headquarters level review of calculated risk levels within each port to validate local findings," while another proposed, "Input by subject matter experts in the area of tactics and their use in protecting against maritime threats would improve Coast Guard performance assessment." This was restated by an additional interviewee: "Getting a 'reformed' terrorist to assess CG operations would be the best way to improve the assessment of Coast Guard actions to reduce maritime terrorism risk. Another way to do this would be to have a Red Cell assess Coast Guard operations."

An additional issue was raised: "The Coast Guard needs to use expert judgment on the quantification of economic consequences (primary and secondary) of attacks on Maritime Critical Infrastructure/Key Resources (MCI/KR) targets."

A Coast Guard officer stated the Coast Guard could benefit from expert judgment through the following: "Risk experts could conduct a normative review of the Coast Guard process for assessment of maritime terrorism risk and Coast Guard performance assessment."

Finally, a terrorism expert expressed the concern that "Using previous years' SME estimates of effectiveness as a starting point may save time, but the Coast Guard should consider not using these" because this practice introduces anchoring bias into the PWCS outcome measure.

7. Expert Judgment Aggregation

The Coast Guard currently aggregates expert judgment through consensus of unstructured groups for both MSRAM input and to collect data for the PWCS Outcome Measure. A Coast Guard officer familiar with both MSRAM and the LROI model stated:

> We now build consensus between those that are consulted on the assessment of maritime terrorism risk. The use of more sophisticated Expert Judgment Aggregation would improve that assessment. We also build consensus on the assessment of Coast Guard impact on maritime terrorism risk, and the use of more sophisticated Expert Judgment Aggregation would also improve that assessment.

Another Coast Guard officer argued that Coast Guard efforts should not be focused on expert judgment aggregation: "The Coast Guard currently aggregates expert judgment through consensus. At this point it is more important to clearly define maritime terrorism scenarios and activities to thwart those scenarios than it is to use expert judgment aggregation to assess maritime terrorism risk."

Concerning the PWCS Outcome Measure, a Coast Guard officer indicated:

> The current Coast Guard technique is to get the right group of Coast Guard SMEs together to assess Coast Guard capability to reduce maritime terrorism risk through a consensus process. All SMEs have blind spots in their judgments. This consensus process ensures group results are better than individual judgments, since SMEs with different areas of expertise participate: aviators provide information on aircraft capabilities, cuttermen provide information on cutter capabilities, and operations ashore personnel provide information on boat capabilities. There is not really a group of overall experts that could independently assess/rate interdependencies between the activities in each LOA.

No single person possesses the depth of knowledge brought together by a diverse group of Coast Guard experts in the assessment of interdependent activities that are executed in the prevention of maritime terrorism. Another Coast Guard officer concurred with this opinion when he stated:

> Consensus of [the] proper group of Coast Guard SMEs [would be] actually better than aggregation of individual judgments," and "Consensus of group of outside experts obtained separately from CG SMEs, and then considered in conjunction with Coast Guard SME results would be the best way to improve Coast Guard performance assessment.

One terrorism expert stated, "Linear Averaging is best unless there is a specific reason to not use it. If bias exists, the hope is that responses from separate experts will cancel out the bias." He went on to state that:

> Another issue with SME probability estimations is that they tend to underestimate low probability events and overestimate high probability events. This and other issues can be reduced by SME calibration, multiple rounds of elicitation, Delphi studies, and SMEs showing each other and analysts the justification for their responses.

He emphasized the need:

> …to ensure different elicitees don't understand the question in different ways. Everyone might agree 'X' is the most likely outcome, but there is a need to have consistent questions to ensure SMEs are responding with consistent answers. One way to deal with this is to ask the same question in multiple ways.

- Is the chance of dying of cancer 80 percent?
- Is the chance of not dying of cancer 20 percent?

> If an SME is asked to estimate the probability of the occurrence of a particular event in the next 10 years, and provides an estimate of 40%, and then is later asked to estimate the probability of the occurrence of the same particular event in the next 20 years, any answer other than 80% would be inconsistent. The best way to deal with inconsistent results is to drop data from SMEs that provide inconsistent responses. Another way to deal with this issue is to assign less weight to inconsistent elicitees.

The same terrorism expert went on to say, "Anonymous elicitation is one way to avoid groupthink. This can be achieved by placing SMEs in different rooms to remove the personal dynamic. Otherwise, the most forceful member will drive the group to his own answers." However, individual elicitation would remove the synergy gained through combining personnel with expertise in different areas of Coast Guard and antiterrorist operations. This conflict and potential resolution is examined in Chapter V.

8. Event Trees

Each of those interviewed indicated expanded use of event trees provided the potential to improve the PWCS Outcome Measure. A terrorism expert indicated:

> Event trees can be useful if we are unsure about the threat process or about the response/prevention process. They are helpful to ensure we don't leave out important pathways that could lead to maritime terrorism. Event trees could be useful to show potential combinations if there are a number of different attack scenarios, targets, and Coast Guard activities that could be used to prevent or respond to those scenarios.

Another expert said event trees:

> …might cause people to think less about point defense and more about general security procedures; throughout an entire port or waterway instead of just at one facility. This might push people to think about actions that could be taken earlier, as they are more effective across more branches of the tree, especially intelligence.

A Coast Guard officer agreed with the expanded use of event trees when he said:

> This could improve our assessment of maritime terrorism risk by accounting for threat shifting. An example would be terrorist use of a diversion (natural or man-made) which would result in Coast Guard resources being shifted to the area of the primary event. Terrorists could then attack another area that may normally be covered by those resources. This is why it is important for facilities and vessels to have security plans and the resources to execute them (private security staffs, etc.).

The current LROI model uses "modified event trees" which are really event chains. While the national threat algorithm in the LROI model accounts for threat shifting by assigning a higher frequency of attack to certain targets than others; this phenomenon could be more accurately portrayed with event trees.

C. SUMMARY

Those interviewed during this research offered a number of suggestions to improve both MSRAM and the LROI model. Those acquainted with both models indicated that MSRAM results were likely more accurate than LROI model results used to calculate the PWCS Outcome Measure. Although there was some concern expressed about the accuracy of the current PWCS Outcome Measure, the majority of interviewees felt the measure in its current form provides a reasonable representation of the level of Coast Guard reduction in terrorism-related maritime risk in the United States.

1. Potential Improvements to MSRAM Include:

a. Target List Update

Up-to-date target lists of maritime critical infrastructure/key resources and vessels within each COTP Zone to ensure that all targets of interest from a security standpoint are included. This list is already updated annually, but it requires input from Coast Guard and AMSC personnel in each port along with a thorough review by district, area, and headquarters personnel.

b. Threat Updates

Up-to-date assessments of terrorist intent, capability, and presence to conduct direct attacks, exploit vessels for those attacks or transfer terrorists or WMD through the maritime domain so that the threat characterization used in MSRAM is as accurate as possible.

c. Vulnerability Updates

Up-to-date vulnerability assessments: while many components of maritime critical infrastructure/key resources have undergone vulnerability assessments, these require periodic revisions. This should include results of MTSA spot checks to provide information collected in person on target vulnerability.

d. Consequence Updates

Up-to-date consequence assessments: this would require the input of engineering and financial experts to assess direct economic impact, as well as economic experts to provide information on secondary economic impacts. This should also include results of MTSA spot checks to provide information collected in person on potential consequences of an attack on a particular target.

e. Dynamic Risk Component Adjustment

All three components of risk should get more than an annual adjustment even if formal assessments are not made during the course of the year, dynamic estimates as to whether threat, vulnerability, or consequence will go up, down, or remain steady in the coming year would improve risk assessment. The Coast Guard Strategic and Performance Plan for Combating Maritime Terrorism (CMT 2.0) requires periodic MSRAM updates to create an operational risk profile for each COTP zone.

f. MSRAM Training and Job Aids/Video Training Modules

Continued MSRAM training program and updated job aids to ensure that Coast Guard field personnel are using MSRAM correctly and to minimize differences between local assessments and requirements imposed by review at districts, areas, and headquarters.

g. Scenario Creation

The ability to create additional scenarios. While this ability already exists within MSRAM, an enhancement would be the capability to gain swift review of new scenarios with the intention of passing these scenarios to other COTPs, whether they originate with sector personnel, or district, area, and headquarters staffs. This is to avoid the issue of leaving gaps between existing scenarios: adversaries will try to exploit attacks not accounted for in any of the scenarios.

2. Potential Improvements to the PWCS Outcome Measure Include

a. Intelligence Cueing Assessment

More accurate assessment of successful intelligence cueing through consultation with the Coast Guard Intelligence Coordination Center and other Coast Guard intelligence experts to ensure the intelligence cueing levels used in the LROI model reflect the best, most up to date estimates available.

b. Improved Capacity Modeling

Improved activity effectiveness assessment through better modeling of Coast Guard capacity to prevent, protect against, respond to and recover from terrorism. This can be accomplished through disaggregation of assessments of activity effectiveness within the LROI model into individual components. Several schemes were suggested to break down these individual components. The Coast Guard already collects information in the Coast Guard Business Intelligence system using the six facets of readiness (people equipment, supplies, training, information, and infrastructure), so that may be a potential structure to put this idea into place. The MSRAM team may be available to provide insight into and assistance with improving activity effectiveness assessments using Coast Guard and outside experts.

c. Activity Alignment

Alignment between ONS activities, MSRAM, and the LROI model.

d. Scenario Creation

The ability to create additional scenarios in the LROI model. As previously stated, this is to avoid the issue of leaving gaps between existing scenarios: adversaries will try to exploit attacks not accounted for in any of the scenarios.

e. Outside Experts

Inclusion of outside experts in the assessment of Coast Guard effectiveness in reducing terrorism-related maritime risk, which will be covered in greater detail in Chapter V.

f. Bias Reduction

Improved expert judgment through bias reduction, which will also be addressed in Chapter V.

g. Improved Expert Judgment Aggregation

Improved expert judgment aggregation, addressed in Chapter V.

h. Dynamic Effectiveness Adjustment

Dynamic assessment of Coast Guard effectiveness in reducing terrorism-related maritime risk: collect estimates once each year, but acquire information for expected effectiveness levels in the coming year. While the collection of estimates of effectiveness for various times throughout the course of the year could help arrive at a more accurate PWCS Outcome Measure for various times throughout the year, at this point the results are only used to generate an annual measure that is reported both within and outside the Coast Guard for accountability and to support future year funding requests. As a result, this potential change to the PWCS Outcome Measure is not recommended.

i. Event Trees

The use of event trees to more accurately represent potential terrorist actions. As indicated earlier in this chapter, the LROI model uses modified event chains to represent the events leading up to and after a terrorist event. The use of event trees has the potential to more accurately represent potential terrorist actions, but development of these event trees is beyond the scope of this research.

THIS PAGE INTENTIONALLY LEFT BLANK

V. EXPERT JUDGMENT

A. BACKGROUND

Due to the paucity of data on maritime terrorist attacks and prevention of such attacks, the Coast Guard depends on expert judgment to assess both the risk of maritime terrorism and the effectiveness of Coast Guard efforts to reduce that risk. The first section of this chapter examines existing requirements to incorporate input from outside the Coast Guard into the assessment of maritime terrorism risk with special emphasis on the Maritime Transportation Security Act of 2002 and Area Maritime Security Committees. It continues with recommendations for specific actions to increase outside input on the assessment of maritime terrorism risk. The second section of this chapter examines how heuristics and biases affect expert judgment in the assessment of annual reduction in Terrorism-Related Maritime Risk and ways to improve the assessment of subjective probability through bias reduction. The chapter concludes with an examination of expert judgment aggregation.

B. EXPERT JUDGMENT IN THE ASSESSMENT OF TERRORISM-RELATED MARITIME RISK

Expert judgment input from Area Maritime Security Committees in each Coast Guard sector has great potential to improve local, regional, and national risk assessments. This expert judgment, in turn, will provide additional information that can be used to assess Coast Guard impact on the reduction of terrorism related maritime risk. However, there is a need to acknowledge the effect of heuristics and biases, as well as a need to take steps to reduce these effects. This section examines requirements concerning outside input and systems in place to collect that input. The next section contains three recommended methods for gaining this outside input.

1. Requirements and Systems to Collect Outside Input on Terrorism-Related Maritime Risk

The governing law and regulations concerning Area Maritime Security Committees are the Maritime Transportation Safety Act of 2002 (MTSA) and Navigation and Navigable Waters regulations at 33 CFR 103. These direct the Captain of the Port to establish an Area Maritime Security Committee (AMSC, or committee) made up of experienced port stakeholders. This committee must then ensure completion of an Area Maritime Security Assessment, which may be completed by the Captain of the Port, the committee, a Coast Guard Port Security Assessment team, or by another third party approved by the committee. While Coast Guard guidance requires consultation with the committee during preparation of the Area Maritime Security Assessment, this does not occur uniformly throughout the nation.

In addition to creating Area Maritime Security Committees, the MTSA and Coast Guard regulations require each AMSC to "serve as a link for communicating threats and changes in MARSEC Levels, and disseminating appropriate security information to port stakeholders."[69] Since this can contain Sensitive but Unclassified or Sensitive Security Information, the Coast Guard needed to create a secure communication environment available to all AMSC members. In order to provide fast, easy, yet secure information access to port stakeholders, the Coast Guard developed Homeport, a secure internet portal that fulfills the requirements above. The system underwent design and vulnerability testing in 2004 and was beta tested by several Coast Guard COTPs starting in November of that year. Homeport was deployed service-wide in October of 2005 after alterations prompted by field unit input and completion of Coast Guard policy and guidance on its use. To ensure sensitive information remains secure while simultaneously providing open access to useful public information, Homeport is divided into secure and non-secure areas. Access to the secure Homeport web portal is only open to owners, operators, and security officers of vessels or facilities that are required to submit security plans under

[69] U.S. Coast Guard, "Electronic Code of Federal Regulations," *Title 33: Navigation and Navigable Waters*, (Washington, D.C., Government Publication Office, 2002) Government Printing Office, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title33/33cfr103_main_02.tpl (accessed August 20, 2008).

MTSA, Area Maritime Security Committee members, Coast Guard personnel working with the AMSC, and members of national-level port security related committees.

An important aspect of Homeport is its alert and warning system, which allows swift, secure notification of registered Homeport users with automatic notification of receipt to message originators. This allows Coast Guard COTPs to quickly transmit MARSEC level changes and other port security information with automatic receipt tracking and retransmission via alternate means if required. Upon registration, users provide email address (primary means of notification), SMS phone number for text messages, 24 hour phone number (which will receive text to voice conversion of the information), and fax number. Homeport also gives users access to view vessel and facility security plans and MARSEC levels. Finally, Homeport contains a suite of collaboration features which allow users to "work together on projects, set meetings, generate tasking, and exchange information about topics of interest within a secure or non-secure environment."[70]

2. Recommendations to Improve Maritime Terrorism Risk Assessment

As stated above, there are already requirements in place to solicit and incorporate input from Area Maritime Security Committees into Coast Guard Area Maritime Security Assessments. This does not occur uniformly throughout the service. The following section contains three recommendations to improve maritime terrorism risk assessment by making it easier to gain outside input on these assessments so that Coast Guard Captains of the Port can use this information while populating the MSRAM database. The first method to gain outside input is the use of volunteer Coast Guard Auxiliarists to assist with data collection, which has already been accomplished in Sector Northern New England and could easily be replicated in other sectors. The second is expansion of the Homeport secure web portal to provide Coast Guard Captains of the Port and their staffs the ability to send and receive web based surveys to collect input from port stakeholders in conjunction with ongoing communications over the same network. The third is the

[70] Mark Hammond and Karrie Trebbe, "Homeport," *Proceedings of the Marine Safety & Security Council* 63, no. 1 (Spring 2006): 23-25.

implementation of virtual maritime fusion centers as proposed by Detective Candice Wright of the Long Beach Police Department in a recent Naval Postgraduate School thesis.[71] This would link FBI InfraGard, FBI Joint Terrorism Task Force, the Coast Guard Area Maritime Security Committee (through Homeport), and other port stakeholders via a cyber backbone to create a common operating picture and enhance collaborative efforts. This section is followed with an examination of costs, benefits, and pitfalls associated with increased outside input to the Area Maritime Security Assessment process.

a. Coast Guard Auxiliary Role

One potential way to gain the benefits of Area Maritime Security Committee member input on port security risk assessments, while minimizing Coast Guard costs and the time and energy that stakeholders must put forth to provide that input, is to task Coast Guard Auxiliarists to meet with and collect the information at convenient locations and times, instead of requiring attendance at meetings or workshops to accomplish the same task. Coast Guard Auxiliarists are volunteer personnel who serve the country because of their dedication to service and their desire to assist the service in the execution of its duties. Through their work and volunteer experience, Auxiliarists are familiar with the maritime environment and the many public and private organizations that work together to operate ports in a cost effective, safe, and secure manner. Coast Guard Sector Northern New England has already benefited from Coast Guard Auxiliary assistance on Area Maritime Security Assessments in Maine, New Hampshire, Vermont, and New York. In a recent article on MSRAM, Kevin Cady states, "Auxiliarists performed vital data entry and acted as liaison between the Coast Guard and port stakeholders such as local, county and state EMA directors during the information gathering process."[72] Implementation of this Coast Guard Auxiliary program in areas

[71] Candice L. Wright, "Bridging the Gap in Port Security; Network Centric Theory Applied To Public/Private Collaboration" (master's thesis, Naval Postgraduate School, 2007).

[72] Kevin Cady, "The Area Maritime Security Committee & the CG Auxiliary," *Safety Lines*, (February 2008): 2.

outside New England will allow Captains of the Port to comply with existing requirements to gain Area Maritime Security Committee input without using scarce Coast Guard active duty personnel resources.

b. Homeport Secure Web Portal Surveys

Coast Guard COTPs conduct Area Maritime Security Assessments on an annual basis, which is the minimum frequency port stakeholders should provide their input on the security risk in the port, and specifically, related to their vessel, facility, or area of responsibility. The latest version of MSRAM allows daily updating of the threat, vulnerability, and consequence level to reflect changing local conditions. This allows the COTP to make tactical decisions on day to day resource allocation to optimize the efficacy of Coast Guard personnel and platforms. In order to collect information from stakeholders more than once a year, COTPs need to make the input process as simple as possible. This could potentially be accomplished through periodic web based surveys through the Homeport secure portal for stakeholders to confirm that security conditions under their cognizance are substantially the same as previous input, with an option to update vulnerability or consequence information. COTPs could also request these updates when sending out communications on port security threats and changes in MARSEC levels via Homeport.

c. Virtual Maritime Fusion Center

As previously indicated, Long Beach Police Detective, Candice Wright, reviewed four existing public/private programs in a recent Naval Postgraduate School thesis. These included FBI InfraGard, FBI Critical Infrastructure JTTF, Coast Guard Area Maritime Security Committees, and Coast Guard Homeport. While acknowledging that these programs provide valuable opportunities for information exchange between the wide variety of personnel involved with security in the Los Angeles/Long Beach Port Complex, she concludes that "they do not fill the gap required to effectively implement port security."[73] Detective Wright initiated creation of a public/private virtual maritime

[73] Wright, "Bridging the Gap In Port Security," 46.

fusion center to link existing systems over a cyber backbone and apply network centric warfare theory to transform port security vulnerabilities into strengths through information sharing and increased maritime domain awareness. Unfortunately, this system is no longer operational. Alteration of Homeport to emulate the ease of use of the Los Angeles/Long Beach public/private virtual maritime fusion center would improve the potential for increased stakeholder input on MSRAM data collection and result in better assessment of maritime security risks.

d. Costs and Benefits

The previous section outlines three recommendations to get outside input from Area Maritime Security Committee members to more accurately assess maritime terrorism risk in U.S. ports. The underlying issue is that acquiring this input is not easy, nor is it cheap. The 2003 cost estimate for implementation of the Area Maritime Security regulations contained in 33 CFR 103 was $477 million.[74] While this is a high cost, the cost of not incorporating AMSC input into port security assessments and then into the Area Maritime Security Plan could be significantly higher in the event of even one single successful terrorist attack. The inclusion of AMSC input into port security risk assessments will impact all committee members who take the time to provide that input. Negative impacts could potentially include loss of time focused toward the completion of the daily business of running their port. However, positive impacts include stronger relationships between all port security partners, leading to not only increased maritime security, but also smoother day-to-day port operations. Interaction with these personnel in a non-emergency environment will ensure relationships are formed and solidified before they are put to the test in a stressful environment. It should also lead to the creation of more useful port security exercises, as the Coast Guard personnel who collect this information are also involved in port security exercise design, execution, and evaluation. Finally, and most importantly, more accurate maritime risk assessment in each port

[74] U.S. Coast Guard, “Area Maritime Security Interim Rule,” *Federal Register* 68, no. 126, (Washington, D.C.: National Archives and Records Administration, no. 39287, 2003).

should lead to more rational allocation of DHS and Coast Guard funding, personnel, surface and aviation platform resources to address the hazards of Terrorism-Related Maritime Risk.

e. Potential Pitfalls

One possible result of this request for increased input from Area Maritime Security Committee members on Terrorism-Related Maritime Risk in their port could be pushback, as port partners are busy people who may not be inclined to spend the time to provide information on their assessment of the level of Terrorism-Related Maritime Risk, unless they are convinced of the positive impacts of relationship building and smoother port operations during both non-emergency and especially emergency conditions. If this measure does not show a Reduction in Terrorism-Related Maritime Risk each year, there could be negative ramifications, as the Coast Guard expends a significant amount of funding in its quest to reduce the level of Terrorism-Related Maritime Risk; the 2008 PWCS Program funding level was $1.794 million.[75] Finally, those tasked with processing and analyzing information from entities providing input on the MSRAM data collection process need to bear in mind that there is a strong connection between MSRAM risk ranking and successful port security grant applications, as there certainly should be. However, there may be a tendency to overstate the vulnerability or consequences associated with maritime terrorism on the part of port stakeholders which could potentially increase the port security grant amounts. As long as MSRAM benchmark guidance is followed throughout the process, and deviations from suggested values for vulnerability or consequences are thoroughly evaluated and documented, this should not cause major concerns.

3. Summary

Three recommendations have been examined to gain outside input on Coast Guard assessment of maritime terrorism risk in order to improve that assessment. Coast Guard resource constraints prevent significant additional expenditures to gain this input.

[75] U.S. Office of Management and Budget, *Program Assessment*.

The recommendation for volunteer Coast Guard Auxiliarists to assist with collection of this input is an extremely low-cost way to comply with existing requirements while improving both the risk assessment and relationships between the Coast Guard and its port partners. Homeport is an existing secure web portal that allows Coast Guard Captains of the Port and their staffs to communicate swiftly and easily with port security partners. The proposal to implement periodic web based surveys through the Homeport secure portal will require approval and programming, but is a relatively simple addition to the existing system. The Port of Los Angeles/Long Beach Virtual Maritime Fusion Center initiative had the potential to provide even more positive interaction between the Coast Guard and other port partners than Homeport, but is no longer in existence. The potential benefits of modifying Homeport to gain the advantages provided by the pilot virtual maritime fusion center in the Port of Los Angeles/Long Beach deserve strong consideration. However, this additional interaction will entail the expenditure of time and energy on programming and convincing port partners of the utility of using Homeport to increase information sharing and maritime domain awareness.

C. EXPERT JUDGMENT IN THE ASSESSMENT OF ANNUAL REDUCTION IN TERRORISM-RELATED MARITIME RISK

In order to assess annual reduction in terrorism-related maritime risk to arrive at the PWCS outcome measure, the Coast Guard gathers in-house subject matter experts (SMEs) to assess service capability to prevent maritime terrorism. As previously indicated, the Coast Guard depends on expert judgment to assess maritime terrorism risk and the effectiveness of Coast Guard efforts to reduce that risk, since "the theories of mathematical probability or of statistical inference cannot deliver the probabilities sought."[76] Instead, the Coast Guard elicits expert opinions on the subjective probability of various events. In addition to considering the impact of outside experts on this measure, this chapter will examine issues that may affect the assessment of Coast Guard actions taken to reduce the risk of terrorism-related maritime terrorism. This assessment

[76] Maya Bar-Hillel, "Subjective Probability Judgments," in *International Encyclopedia of the Social and Behavioral Sciences*, vol. 22, ed. Neil J. Smelser and Paul B. Baltes, 15427 (Amsterdam, Netherlands: Elsevier Science Ltd, 2001).

is affected by systematic error, which is represented as bias and addressed in the first part of this section. The assessment is also affected by random error and is addressed in the last section of this chapter through expert judgment aggregation. It is possible to improve the accuracy and precision of the Coast Guard PWCS Outcome Measure by reducing the systematic and random error in expert judgment used in the calculation of that measure.

1. Heuristics and Biases

This section will review heuristics and cognitive biases and then will examine motivational biases. After describing these biases, the next section will list bias reduction techniques that may be applicable to improving expert judgment in the quest for a more accurate assessment of the PWCS Outcome Measure.

a. Heuristics and Cognitive Biases

Due to the limited capacity of the human mind to process and remember information, Tversky and Kahneman indicate that people rely on heuristics to simplify difficult problems such as the estimation of the probability of uncertain events.[77] Gird Gigerenzer defines heuristic as “the cognitive process that generates a decision.”[78] Otherwise stated, heuristics are mental rules used to make complex decisions or judgments with incomplete data. They are often useful but can be the source of systematic errors or biases. Cognitive bias occurs “when the expert does not follow objective rules or standards,”[79] including logical, mathematical, or statistical standards. Awareness of these heuristics and the biases they cause can improve estimation of the probability of uncertain events.[80] Therefore, making experts aware of biases and implementing actions to reduce bias should improve both the assessment of maritime terrorism risk and the assessment of Coast Guard effectiveness in addressing that risk.

[77] Amos Tversky and Daniel Kahneman, “Judgment under Uncertainty: Heuristics and Biases,” *Science* 185, no. 4157 (September 27, 1974): 1124.

[78] Francesco Parisi and Vernon L. Smith, *The Law and Economics of Irrational Behavior* (Palo Alto, CA: Stanford University Press, 2005), 41.

[79] Mary A. Meyer and Jane M. Booker, *Eliciting and Analyzing Expert Judgment: A Practical Guide* (Philadelphia, PA: Society for Industrial and Applied Mathematics, 2001), 40.

[80] Ibid., 48.

The following section will review and define two common heuristics and several biases, shown in Table 5. Meyer and Booker indicate that the most common cognitive bias in their work is the inconsistency bias,[81] which is the first to be addressed in this section. This is followed by an examination of the availability heuristic and associated biases, and then the anchoring and adjustment heuristic with its associated biases.

Table 5. Heuristics and Cognitive Biases

Heuristics and Cognitive Biases		
Heuristic	**Bias**	**Description**
--------------	Inconsistency Bias	Variability in an expert's response over time resulting in contradictions with previous answers.
Availability	Retrievability Bias	Assignment of higher probabilities to events experts can easily retrieve from memories.
Availability	Search Set Effectiveness Bias	Assignment of higher probabilities to events for which one can easily search.
Availability	Imaginability	Assignment of higher probabilities to events which are easy to imagine.
Anchoring and Adjustment	Insufficient Adjustment	Tendency to assign probabilities based too heavily on initial estimates or source data.
Anchoring and Adjustment	Overconfidence / Underestimation of Uncertainty	Tendency to assign overly narrow confidence intervals leading to overconfidence in estimated probabilities.

(1) Inconsistency Bias. This is a manifestation of the mind's limited capacity to process and hold information that is examined in detail by George Miller in his paper "The Magical Number Seven, Plus or Minus Two."[82] Because of this limitation, experts can make initial assumptions that are later contradicted in the elicitation process, leading to inconsistent results. Meyer and Booker indicate that this is the most common cognitive bias and trace one of the sources of inconsistency bias to memory issues, including faulty memory retrieval. In addition, inconsistency can be caused by fatigue or confusion.[83] Any of the factors outlined can cause experts to shift their assessments over the course of an elicitation session.

[81] Meyer and Booker, *Eliciting and Analyzing Expert Judgment,*136.

[82] George A. Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information," *Psychological Review* 63, no. 2 (1956): 81-97.

[83] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 137.

(2) Availability. The availability heuristic causes people to assign higher probabilities to events which they can more easily bring to mind. While it may be easier to recall certain events due to their higher frequency, there is no guarantee that availability is correlated with actual event probabilities.[84] This heuristic has the potential to lead to several biases, including retrievability bias, search set effectiveness bias, and imaginability bias.

Retrievability bias causes one to assign higher probabilities to events one can easily retrieve from memories. Familiarity is one cause of this bias, as it is easier to recall familiar memories. Another source of retrievability bias is salience; memories with high impact are more retrievable, which causes a person to assign higher probability to emotionally charged events. Recency is a further source of this bias, in that recent events are more easily imagined than those which have occurred in the distant past.[85]

Search set effectiveness bias leads us to assign higher probabilities to events for which one has better defined search sets.[86] This may lead experts to assign higher probabilities to the occurrence of previous maritime terrorism events for which search sets are available, such as the delivery of waterborne improvised explosive devices, and reduced probabilities for occurrence of innovative maritime terrorism events for which no clearly defined search sets yet exist.

Imaginability bias can lead to the improper assessment of risk. Excessively high risk will be assigned to events for which it is easy to imagine modes of failure, whereas excessively low risk may be assigned if sufficient consideration is not given to all possible dangers.[87]

(3) Anchoring and Adjustment. This is the heuristic used to make estimates starting with an initial estimate or calculation and then adjusting to arrive at the

[84] Tversky and Kahneman, “Judgment under Uncertainty,” 1127.

[85] Rose McDermott, *Political Psychology in International Relations* (Ann Arbor: The University Of Michigan Press, 2004), 65.

[86] Tversky and Kahneman, “Judgment under Uncertainty,” 1127.

[87] Ibid., 1128.

final estimate. Use of this heuristic limits the distance between initial and final estimate of a subjective probability and leads to the cognitive biases of insufficient adjustment[88] and overconfidence.

Insufficient adjustment manifests itself when SMEs use whatever data they have available to make an initial estimate and then keep successive estimates too close to the initial value. Research has shown that the final subjective probability an expert provides depends heavily on the initial estimate, whether that initial estimate is provided in advance or is formulated by the expert because of the bias of insufficient adjustment.[89] As an example, when SMEs estimate the effectiveness of Coast Guard efforts toward reducing maritime terrorism risk, providing with experts information of prior year estimates of Coast Guard effectiveness of various terrorism prevention activities will speed the expert elicitation process but will result in probability estimates that are unduly affected by those prior year estimates. Meyer and Booker indicate that because of the limited capacity of the mind to remember and process information, experts make initial judgments based on first impressions and only make minor sequential adjustments upon receipt of additional information, even when that additional information should cause major changes in the initial judgment or even contradict the initial judgment.[90]

Overconfidence, or underestimation of uncertainty, demonstrates the tendency to overestimate knowledge and the tendency to underestimate uncertainty of any given situation. Slovic and others indicate that most people are overconfident about their estimates of subjective probabilities.[91] When overconfident estimators attempt to estimate values with a given confidence interval, they are correct less often than expected. When under-confident estimators attempt to estimate values with a given

[88] Nicholas Eply and Thomas Gilovich, "Putting Adjustment Back in the Anchoring and Adjustment Heruistic," in *Heuristics and Biases: The Psychology of Intuitive Judgment* (Cambridge : Cambridge University Press , 2002), 139.

[89] Tversky and Kahneman, "Judgment under Uncertainty," 1128.

[90] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 40.

[91] Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein, "Perceived Risk: Psychological Factors and Social Implications," *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* 376, no. 1764 (1981): 20.

confidence interval, they are correct more often than expected.[92] Tversky and Kahneman indicate that this bias "is attributable, in part at least, to anchoring"[93] as experts will insufficiently adjust their initial estimates to estimate upper and lower bounds for a given confidence interval. Bar-Hillel argues that a major source of overconfidence stems from the availability heuristic: "what we know is almost by definition more available to us than what we do not know."[94]

b. Motivational Biases

In addition to the cognitive bias view of Tversky and Kahneman, Meyer and Booker take a view from the perspective of motivational bias, which "occurs when an expert consciously or unconsciously makes accommodations to please the interviewer."[95] This can also include shifts in elicited judgments to accommodate the perceived desires of other experts, supervisors, or clients. While the majority of bias found in the PWCS Outcome Measure can be classified as cognitive, there are some aspects of motivational bias that may adversely affect the collection of accurate expert judgment, further defined in Table 6 below. Motivational bias is caused by social pressure which could lead to groupthink. Other motivational biases with the potential to adversely affect the PWCS outcome measure include impression management bias and wishful thinking.

Table 6. Motivational Biases

Motivational Biases	
Bias	**Description**
Groupthink	Premature consensus seeking that may involve internalization, compliance, or both
Impression Management	Tendency of experts to provide answers they think are most desired instead of their true opinions.
Wishful Thinking	Tendency of experts to provide answers for their desired outcome instead of an objective assessment of the most likely outcome.

[92] Douglas W. Hubbard, *How to Measure Anything* (Hoboken, NJ: John Wiley and Sons, Inc., 2007), 54.

[93] Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty," 1129.

[94] Bar-Hillel, "Subjective Probability Judgments," 15250.

[95] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 420.

(1) Groupthink. As indicated above, groupthink is a symptom of social pressure, or what Janis and McCauley call social influence.[96] During expert elicitation tainted by groupthink, experts provide judgments according to their perception of the group desire instead of according to their own beliefs and experience. McCauley proposes the definitions below in his analysis of Janis's book *Groupthink*, and expands the definition of groupthink beyond that put forth by Janis. These definitions are shown in Table 7 below.

During his review of U.S. government policy-making decisions, McCauley finds that group insulation (from outside information), promotional leadership, and group homogeneity all "contribute to both internalization and compliance with a premature consensus"[97] and are therefore good predictors of groupthink.

Table 7. Groupthink Definitions[98]

Groupthink (Janis)	premature consensus seeking
Groupthink (McCauley)	premature consensus seeking that may involve internalization, compliance, or both
Compliance	public without private agreement
Internalization	private acceptance of group consensus
Promotional leadership	Leadership by an authority who early in discussion reveals a favored policy alternative, especially in the absence of methodical procedures for generating and evaluating alternatives

[96] Clark Mccauley, "The Nature of Social Influence in Groupthink: Compliance and Internalization," *Journal of Personality and Social Psychology* 57, no. 2 (August 1989): 250.

[97] Ibid., 258.

[98] Ibid., 250-252.

(2) Impression Management. This is another bias that is caused by social pressure and manifests itself as a desire to please others, whether they are interviewers, clients, employers, other experts, or even society as a whole. This bias causes experts to provide answers that they believe are most the desirable instead of their actual best answer.[99]

(3) Wishful Thinking. Experts who are interested in the outcome of an event exhibit wishful thinking when their desires influence their judgment concerning the outcome of that event, especially if they may benefit from a certain outcome. Often, those who are the most knowledgeable concerning a given topic are those who stand to gain or lose the most, depending on their answer. Meyer and Booker state that "what the subjects think should happen will influence what they think will happen."[100]

2. Improving Subjective Probability Assessment through Bias Reduction

While it is important to inform experts about the various biases that affect their assessment of subjective probability, this is only one of several steps that must be taken to reduce those biases, as most experts are not aware of their use of heuristics and consequent biases. Meyer and Booker propose six steps shown in Table 8 below to reduce bias in the elicitation of expert judgment. This section continues with specific recommendations to reduce the systematic error introduced by the biases previously enumerated.

[99] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 135.

[100] Ibid., 136.

Table 8. Steps to Reduce Bias in the Elicitation of Expert Judgment[101]

1. Anticipate which biases are likely to occur in the planned elicitation. The preceding section outlines those biases that are most likely to occur in the collection of subjective probabilities used to assess Coast Guard effectiveness in reducing the risk of maritime terrorism.
2. Redesign the planned elicitation to make it less prone to the anticipated biases. Plans for eliciting expert judgments should take into account information about likely biases and ideas in the following section to reduce those biases.
3. Make the experts aware of the potential intrusion particular biases and familiarize them with the elicitation procedures. A review of the preceding section with the experts will provide awareness of the biases most likely to affect the elicitation of subjective probabilities for input on the Coast Guard PWCS outcome measure. The desire is that this awareness will result in a reduction of the biases that reduce the accuracy of the measure.
4. Monitor the elicitation for the occurrence of bias. The best way to accomplish this is to include an observer in addition to the interviewer who is familiar with signs of biases that were identified in step 1.
5. Adjust, in real time, to counter the occurrence of bias. The alternatives listed below are focused on techniques to reduce biases that adversely affect the collection of expert judgments.
6. Analyze the data for the occurrence of particular biases. A number of analysis techniques assist with the identification of biased data, including correlation analysis, multivariate analysis, and others.

a. Reducing Inconsistency

As indicated above, fatigue, confusion, and memory issues are all sources of inconsistency. Meyer and Booker suggest two alternatives to reduce inconsistency; the first focuses on adjustments to the elicitation process. Inconsistency reduction during elicitation can be accomplished by ensuring experts do not get overly fatigued by ensuring expert judgment elicitation sessions do not last more than two hours. Memory

[101] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 135.

issues can be at least partially addressed with a thorough review of assumptions and definitions that relate to the judgment before each elicitation. The second alternative is to provide experts information on their previous judgments and allow them to adjust those previous judgments to gain consistency.[102]

b. Reducing Bias Caused by the Availability Heuristic

Retrievability bias, search set effectiveness bias, and imaginability bias all occur because one tends to associate higher probabilities of occurrence with events that are easily available within memories. The solution to reduce these biases is to use brainstorming, free association, or the Crawford Slip Method to maximize consideration of the full spectrum of each expert's recollections.[103] All three of these techniques emphasize suspending censorship while collecting ideas. Free association was developed by Sigmund Freud as a psychoanalytic tool, but it is useful to prompt creativity in that all ideas related in any way to the original concept are recorded for consideration. The Crawford Slip Method is similar to brainstorming in that it is used to quickly collect ideas from a group of people. While brainstorming is conducted verbally, Crawford Slip Method participants write their ideas on a slip of paper. This ensures less aggressive experts get the opportunity to have their ideas presented to the group for consideration, whereas brainstorming tends to favor more outspoken group members.

c. Reducing Anchoring

Meyer and Booker suggest that anchoring can be reduced by ensuring each expert has input from others through group interaction or the Delphi technique, as this will force experts to consider others' viewpoints on the issue. They cite three ideas from Boose and Shaw:

[102] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 179.

[103] Ibid., 180.

(1) ask the experts to describe how other experts might disagree with their responses,

(2) ask the experts to temporarily forget recent events, and

(3) aggregate outcomes with small probabilities into a single, larger class to reduce the perceived joint impact in cases in which probability estimates are elicited.[104]

By going through this process, experts are more likely to shift their judgments away from their original estimates.

d. Reducing Overconfidence and Underestimation of Uncertainty

This bias can be reduced through repetition and feedback. Experts take a calibration test on general information and are directed to specify an upper and lower bound for a given confidence interval. A well-calibrated expert would get nine out of 10 questions correct for a 90 percent confidence interval. Hubbard states that "assessing uncertainty is a skill that can be taught with measurable improvement,"[105] and posits that most experts can markedly improve their calibration by getting feedback on whether they are overconfident or under-confident and repeating the process to further refine their probability calibration.[106]

Arkes offers several principles that can be used to reduce overconfidence. Of these, the primary recommendation is for experts to consider alternatives beyond those initially conceived. The result of imagining alternatives necessitates a more realistic assessment of the probability of each outcome, and reduces overconfidence in the expert's predicted outcome.[107] Hubbard recommends that experts justify the validity of their estimate by formulating two pros (why it is realistic) and two cons (why it might

[104] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 180.

[105] Hubbard, *How to Measure Anything*, 55.

[106] Ibid., 54.

[107] H.R. Arkes, "Overconfidence in Judgmental Forecasting," in *Principles of Forecasting: A Handbook for Researchers and Practitioners,* ed. J. Scott Armstrong, 510 (Norwell, MA: Kluwer Academic, 2001).

be overconfident); this is in line with Arkes' second principle of listing reasons why the expert might be wrong.[108] A pro could be the expert's familiarity with stopping identified drug runners via boardings, which lends credibility to an estimate of ability to stop a suspect terrorist from conducting a waterside attack on a vessel. A con could be a lack of data on a particular maritime terrorism scenario. This aligns with the work of Koriat et al. cited by Lichtenstein, Fischhoff, and Phillips that suggests experts should seek out information that could indicate why their estimates of subjective probabilities might be incorrect to arrive at a more appropriate level of confidence.[109] Arkes' third principle is to consider using a devil's advocate in group interaction. He states that group interaction prompts experts to explain and defend their beliefs, which leads to overconfidence. He suggests using a devil's advocate to force experts to address alternate outcomes that would otherwise not come under consideration.[110]

e. Reducing Groupthink

Meyer and Booker propose two alternatives to reduce groupthink in the elicitation of expert judgment. The first involves directly addressing the causes of groupthink by ensuring all group members are aware that it may occur and impair the collection of expert judgment. Another way to address the cause of groupthink is to reduce the influence of the group leader by waiting until all group members have a chance to express their opinions and then getting the leader's judgments. This would reduce promotional leadership that would lead the group to accept an influential leader's ideas and judgments without sufficient discussion and analysis by the entire group. A further step would be to elicit the leader's opinion apart from the group.[111] In alignment with this concept, Adrian Furnham proposes temporarily removing influential members from the group to avoid undue influence. He also suggests that all group members should

[108] Hubbard, *How to Measure Anything*, 60; Arkes, "Overconfidence in Judgmental Forecasting," 500.

[109] Sarah Lichtenstein, Baruch Fischhoff, and Lawrence D. Phillips, "Calibration of Probabilities: The State of the Art to 1980," *in Judgment under Uncertainty: Heuristics and Biases*, eds. Daniel Kahneman, Paul Slovic, and Amos Tversky, 334 (Cambridge: Cambridge University Press, 1982).

[110] Arkes, "Overconfidence in Judgmental Forecasting," 503.

[111] Meyer and Booker, *Eliciting and Analyzing Expert Judgment: A Practical Guide*, 178.

evaluate group judgments from a critical position, and supports using a devil's advocate to actively contest ideas put forth by the group.[112] A second alternative put forth by Meyer and Booker is to enhance anchoring. This can reduce a group's tendency to quickly reach unwarranted consensus. If experts record their own judgments and supporting thoughts before group discussion, they will tend to anchor on those judgments, so it will be more difficult to slip into groupthink.[113]

Two additional factors that contribute to groupthink are insulation from outside information and group homogeneity. As mentioned in the Chapter IV, current information on maritime homeland security mission effectiveness is gathered from Coast Guard SMEs. While Area Maritime Security Committee member input is requested, this data collection should also include input from Navy SEAL team members and others with expertise in tactics and their use in protecting against maritime threats. Other potential sources are those who have evaded maritime security efforts. This would include "reformed" or incarcerated terrorists or smugglers and members of organizations like Greenpeace and the Sea Shepherds. Additional potential contributors include fishermen, yachtsmen, tugboat operators, harbor pilots, and others with experience working in marine environments. Ensuring the group has ample access to outside information and the formation of heterogeneous groups of experts to assess Coast Guard effectiveness in reducing the risk of maritime terrorism will reduce groupthink and result in a more accurate PWCS outcome measure.

f. Reducing Wishful Thinking

One factor that can reduce wishful thinking includes acquisition of judgments from experts with varied backgrounds, as suggested in Chapter IV and included in the section above, Reducing Groupthink. Inherent in this action is a reduction in the personal connection at least some of the experts have with the outcome of the assessment and a corresponding decrease in wishful thinking. Another factor discussed

[112] Adrian Furnham, *The Psychology of Behaviour at Work* (Hove, UK : Psychology Press, 2005), 555.

[113] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 179.

in Chapter IV that can reduce wishful thinking is the disaggregation of activities being judged for effectiveness. While the current LROI model does disaggregate each Line of Assurance into separate activities, the model uses high level activities to assess maritime homeland security mission effectiveness. Disaggregation of these high level activities into lower level components would decrease wishful thinking and promote better assessment of Coast Guard effectiveness. This would include the breakdown of activities like "Specialized Use of Force" into individual components, such as the number of fully mission capable small boats with qualified crews and then assessing the effectiveness of those components.

3. Expert Judgment Aggregation

This section defines and describes a number of ways to aggregate expert judgment and contains additional information on each method. The first is to hold an unstructured meeting with experts, which is also called a traditional group. The second is to use a structured method, such as the Delphi technique or the Nominal Group technique. Each of these has advantages and disadvantages which will be examined in this section. Finally, expert judgments can be mathematically aggregated into a statistical group without the benefit of using one of the aforementioned methods.

a. Traditional or Unstructured Group

These groups bring together several experts to allow and promote interaction. As indicated in Chapter IV, the interaction between group members' results in better effectiveness estimations of Coast Guard activities undertaken to prevent maritime terrorism as the expertise of each group member is combined in through interaction. Use of the Delphi technique does not allow this face-to-face interaction and, therefore, reduces the opportunity to synergistically merge experts' judgment. In addition, experts in a traditional group possess information about the experience and expertise of other group members and are therefore better able to assess the level of credibility that should be assigned to each expert's opinion. Advantages and disadvantages of the Traditional Group are shown in Table 9.

Table 9. Advantages and Disadvantages of the Traditional Group

Advantages	**Disadvantages**
Takes less time than either the Delphi Technique or Nominal Group Technique	Influential experts dominate group interaction
Large amount of flexibility	Less influential/lower status experts may feel pressure to conform to judgments of influential experts
	Requires travel for face to face meeting of experts

b. Delphi Technique

The Delphi technique was developed by the RAND Corporation as a method for the combination of expert judgments to improve forecasts over traditional group meetings. It capitalizes on the positive aspects of traditional groups of experts by promoting interaction of ideas with input from a number of sources.[114] Since group members in the Delphi remain anonymous, participants have the opportunity to avoid the negative aspects of traditional groups, including social pressure that could lead to groupthink.[115] The first three of four characteristics in the following list differentiate the Delphi from traditional groups; these characteristics are the aforementioned anonymity, iteration, feedback, and statistical aggregation. Experts anonymously complete a questionnaire, and through an iterative process, all participants receive a complete set of feedback in the form of statistically aggregated results and comments. Upon review of this feedback, participants are allowed to change their responses if there is additional information that prompts this change. Once the results converge to an appropriate level (rarely more than two rounds), statistical aggregation is used to complete the process. The Delphi technique takes significantly more time than a traditional group meeting since

[114] Gene Rowe and George Wright, "Expert Opinions in Forecasting: The Role of the Delphi Technique," in *Principles of Forecasting: A Handbook for Researchers and Practitioners*, ed. J. Scott Armstrong, 126 (Boston: Kluwer Academic Publishers, 2001).

[115] Ackerman, "The Future of Jihadists and WMD," 356.

questionnaires must can be prepared, sent out, collected, processed, and sent back out for each round. Advantages and disadvantages of the Delphi technique are shown in Table 10.

Table 10. Advantages and Disadvantages of the Delphi Technique

Advantages	**Disadvantages**
Anonymity prevents influential experts from dominating outcome	Experts may not respond to questions
Anonymity prevents groupthink	
Anonymity allows experts to share information without most forms of social pressure	Impression management may still occur
Allows experts to formulate well thought out judgments	Can be slow: more time consuming than either traditional group or Nominal Group Technique
Does not require travel or face to face meetings of geographically dispersed experts	

c. Nominal Group Technique

The Nominal Group technique was developed by Delbecq and Van de Ven as another structured meeting type that seeks to gain the advantages of the face-to-face interaction that occurs within unstructured groups that is lacking in the Delphi technique while avoiding the disadvantages caused by the social pressure in unstructured groups.[116] When used for the elicitation of expert judgment, the following four steps are used. First, the experts silently record their own judgments. Second, each expert presents their results to the group, without discussion. Third, all experts participate in a facilitated discussion of the results to ensure each group member understand the basis of others' judgments. Finally, experts silently record their own judgments, which are then combined through statistical aggregation. The Nominal Group technique requires significantly less time and preparation than the Delphi technique. However, since experts must record judgments

[116] Andrew H. Van de Ven and Andre L. Delbecq, "The Effectiveness of Nominal, Delphi, and Interacting Group Decision Making Processes," *Academy of Management Journal* 17, no. 4 (December 1974): 606.

individually in writing for the first and fourth steps of the process, Nominal Group technique meetings can take more time than traditional group meetings. Advantages and Disadvantages of the Nominal Group technique are shown in Table 11.

Table 11. Advantages and Disadvantages of the Nominal Group Technique

Advantages	**Disadvantages**
Faster than Delphi Method	More time consuming than traditional group
Facilitation prevents influential experts from dominating outcome	Requires travel for face to face meeting of experts
Allows experts to share information without most forms of social pressure	Less flexibility than traditional group
Allows experts to formulate well thought out judgments	Requires good writing skills

d. Mathematical Aggregation—Statistical Groups

Ravinder considers two aggregation methods: simple averaging and weighted averaging. He states, "Prominent exclusions from this list are the various, often very sophisticated, forms of expert resolution using Bayesian methods. There is no evidence, however, of their practicality, or their superiority over simpler forms of averaging."[117] Meyer and Booker specify that the average referred to by Ravinder includes the mean, median and geometric mean, and that both the median and the geometric mean reduce the effect of extreme values of expert judgments. In addition, they indicate that Kahneman and Tversky show that "when experts provide numerical answers, they really estimate the median value rather than the mean."[118] As a result, when choosing the method of aggregation, serious consideration should be given to using the median to represent the best aggregated value of expert judgment. While they provide extensive information on determining weights through Saaty pair-wise comparison, general linear modeling, and direct estimation, Meyer and Booker conclude that "the best

[117] Handanhal V. Ravinder, "Bias in Aggregations of Subjective Probability and Utility," *Journal of the Operational Research Society* 43, no. 6 (June 1992): 622.

[118] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 316.

recommendation to date on the weight determination problem is to use equal weights…unless some unusual circumstances indicate the use of some different weights”[119]

While Hall, Mouton, and Blake posit that the performance of interacting groups is superior to statistical groups,[120] Larrick and Soll relate that more recent work by Hastie indicates mathematical averaging of individual responses provides results that are as good or better as traditional groups.[121] However, as stated both in this section and Chapter IV, the interaction between experts of varied backgrounds from both inside and outside the Coast Guard is critical to the accurate assessment of Coast Guard capability to address terrorism-related maritime risk. Although the Nominal Group technique requires more time and preparation than a traditional group, the Coast Guard should consider adopting its use to achieve the advantages outlined above. The literature review completed for this research includes information on more technical expert judgment aggregation techniques. However, indications are that the most sensible approach is to use equally weighted averages to aggregate expert judgment as the final step in the Nominal Group technique process.

D. CONCLUSION

This chapter has examined potential improvements to both the assessment of terrorism-related maritime risk, and the assessment of reduction in that risk. Routinely acquiring data on the threats, vulnerabilities and consequences facing port facilities and vessels in the U.S. maritime domain from a heterogeneous information pool will improve the assessment of terrorism-related maritime risk. In addition, acquiring data on the capability of Coast Guard resources to reduce those threats, vulnerabilities, and consequences from a wider set of sources will allow improved assessment of the annual reduction in terrorism-related maritime risk. This chapter has put forth a number of

[119] Meyer and Booker, *Eliciting and Analyzing Expert Judgment*, 29.

[120] Ernest J. Hall, Jane S. Mouton, and Robert R. Blake, “Group Problem Solving Effectiveness Under Conditions of Pooling vs. Interaction,” *Social Psychology* 59, no. 1 (February 1963): 154.

[121] Richard P Larrick and Jack B Soll, “Intuitions About Combining Opinions: Misappreciation of the Averaging Principle,” *Management Science* 52, no. 1 (January 2006): 125.

recommendations to reduce systematic error through minimizing bias common in subjective probability estimations that are used to assess the PWCS outcome measure, and to reduce random error through expert judgment aggregation.

VI. SUMMARY OF RECOMMENDATIONS AND CONCLUSION

A. OVERVIEW OF RESEARCH

This research was guided by two goals. The first goal was to determine if the current measure fairly reflects Coast Guard mission effectiveness in achieving homeland security. The Ports, Waterways, and Coastal Security (PWCS) outcome measure does provide information on risk reduction due to threat, vulnerability, and consequence management by the Coast Guard with respect to 15 maritime terrorism scenarios. As stated in the Office of Management and Budget Program Assessment Rating Tool (PART) assessment of the Coast Guard PWCS program, the PWCS Outcome Measure "scenario-based approach is accepted as a best practice and way ahead among the General Accountability Office, academia, and the private sector."[122] While the current measure provides a good sense of the effectiveness of Coast Guard efforts to reduce the risk of maritime terrorism, there are a number of areas where potential improvements are possible. This finding led to the second goal of the research, which was to provide recommendations to more accurately assess Coast Guard homeland security mission effectiveness.

B. IMPLEMENTION RECOMMENDATIONS

This chapter combines and summarizes recommendations to improve the MSRAM and the LROI models identified in the previous chapters. Since PWCS Outcome Measure calculations performed by the LROI model are based on existing risk information from MSRAM, it is imperative to consider improvements to both models. A complete replacement of the PWCS Outcome Measure is not recommended since there are three years of data available to compare with future results and implementation of the recommendations within the existing models should still significantly improve their precision and accuracy. The following sections of this chapter discuss each recommendation and provide a rough cost estimate for implementation.

[122] U.S. Office of Management and Budget, *Program Assessment*, para 2.7.

Table 12 provides a concise listing of the recommended enhancements to MSRAM and the LROI model, along with an initial cost estimate to implement each recommendation. Thirteen total changes are proposed, and the table indicates the proposed order of implementation. The recommended enhancements are separated into two categories depending on which model is affected, MSRAM or the LROI model.

Table 12. Recommended Enhancements to MSRAM and the LROI Model

Implementation Order	**Recommendation**	**Category / Model**	**Cost Estimate**
1	Improve capacity modeling through Maritime Terrorism Prevention Activity Alignment	MSRAM and LROI Model	$500,000
2	More Accurate Characterization of the Level of Successful Intelligence Cueing	LROI Model	No new costs
3	Create, Share, and Review Additional Maritime Terrorism Scenarios	MSRAM and LROI Model	No new costs
4	Acquire Outside Expert Input for the LROI Model	LROI Model	$30,000
5	Improve Expert Judgment through Bias Reduction and Expert Judgment Aggregation	LROI Model	$20,000
6	Update Terrorist Threat Levels and Predicted Maritime Threat Frequencies	MSRAM	Not Releasable
7	Update Consequence Assessments with new Micromodels in MSRAM	MSRAM	$200,000
8	Expand MSRAM Training and Job Aids/Video Training Modules	MSRAM	$400,000
9	Train Coast Guard Auxiliary to Perform MSRAM Data Acquisition and Processing	MSRAM	$160,000
10	Update Vulnerability Assessments	MSRAM	Contained in #8
11	Update Risk Ownership Matrix	LROI Model	$50,000
12	Modify Homeport to enable Dynamic Risk Assessment	MSRAM	No new costs
13	Update Target Lists using Satellite Photography and Onsite Visits	MSRAM	$150,000

C. IMPLEMENTATION DISCUSSION

Implementation of the recommendations put forth in this research requires a joint effort between the Domestic Port Security Evaluation Division (CG-5142) and Office of Performance Management and Assessment (CG-512). The Domestic Port Security Evaluation Division is responsible for development and maintenance of MSRAM, along with training and review of incoming field data. The Office of Performance Management and Assessment developed the LROI model in conjunction with ABS Consulting, maintains and updates the model and produces annual reports on the PWCS Outcome Measure. Personnel from both these organizations have been extremely supportive of this research, provided valuable information about the current MSRAM and LROI models, offered indispensable insight into potential enhancements to the models, and are enthusiastic about implementing changes. Other important organizations are the Domestic Ports Division (CG-5441), the Operations Systems Management Division (CG-635), and the Office of C4 and Sensors Capabilities (CG-761). These offices at Coast Guard headquarters will be key players in the enhancement of Homeport functionality to increase data collection in the quest to improve the PWCS Outcome Measure.

In an unconstrained resource environment, all of the proposed recommendations would be implemented to improve the PWCS Outcome Measure to the maximum extent possible. The following section lists the proposed order of implementation for the recommendations. In the event that there is insufficient current year funding to implement all of the recommended enhancements, this thesis could potentially serve as background material and justification for one or more resource proposals to enable future execution of these recommendations.

1. Improve Capacity Modeling through Maritime Terrorism Prevention Activity Alignment

One of the most significant drivers of the PWCS Outcome Measure is the level of capacity modeling. Though the initial cost estimate indicates that improvement of capacity modeling through activity alignment will be more costly than other recommended changes, the Coast Guard should strongly consider pursuing this change due to its impact on the PWCS Outcome Measure. In addition, the Coast Guard has initiated a revision to the Combating Maritime Terrorism Strategic and Performance Plan, which will be CMT 3.0. The creation of CMT 3.0 provides the opportunity to bring together subject matter experts from each of the component systems to create a unified activity and scenario list between the Combating Maritime Terrorism Strategic and Performance Plan, Operation Neptune Shield, MSRAM, and the LROI model. This is also an opportunity to clearly state the requirement in the body of CMT 3.0 for daily/operational risk profiles to bring more visibility to this requirement.

The PWCS Outcome Measure is dependent on the estimated effectiveness of Coast Guard platforms and personnel to prevent, protect against, respond to, and recover from terrorist attacks. The LROI model uses effectiveness judgments of subject matter experts for each of the 29 activities conducted to reduce the risk of maritime terrorism, along with a capacity factor for the platform used in the operation. This capacity factor is calculated with information from the Coast Guard Abstract of Operations system (AOPS) and Operation Neptune Shield results (ONS). AOPS records the hourly activities of Coast Guard platforms (aircraft, boat, or cutter) according to which of the 11 Coast Guard missions that platform performs, while ONS results reflect execution of activities in the Operation Neptune Shield Operations Order, including aviation and surface patrols, boardings, escorts, and security zones. Unfortunately, the maritime terrorism prevention activities in MSRAM, the LROI model and Operation Neptune Shield are not closely linked, which makes calculation of the PWCS Outcome Measure problematic. Alignment of the activity libraries in each of these systems and the Combating Maritime Terrorism Strategic and Performance Plan would be an important step toward improved capacity modeling, and would result in better assessment of the impact of Coast Guard activities in the reduction of maritime terrorism risk. The MSRAM team has conducted effectiveness measurement of various Coast Guard adaptive force packages and could provide valuable insight into and assistance with improving activity effectiveness assessments using Coast Guard and outside experts. The estimated cost to conduct facilitated meetings with representatives from each of the affected systems combined with subsequent programming to effect the changes outlined above is $500,000.

2. More Accurate Characterization of the Level of Successful Intelligence Cueing in the LROI Model

Over half of the Lines of Assurance in the LROI model are dependent on intelligence cueing to successfully prevent acts of maritime terrorism. As a result, the assumed level of intelligence cueing has a major impact on the PWCS Outcome Measure, and this recommendation has a high priority for implementation. The LROI model assumes the same level of intelligence cueing for each of the 15 maritime terrorism scenarios. More accurate characterization of the level of successful intelligence cueing will directly lead to improved assessment of Coast Guard homeland security mission effectiveness.

The 2008 Coast Guard Posture Statement indicates, "The Coast Guard Intelligence Coordination Center (ICC) is the National Level Coordinator for collection, analysis, production, and dissemination of Coast Guard intelligence…[and]…partners closely with the Director of National Intelligence and other components of the Intelligence Community to maintain an integrated intelligence regime."[123] Consequently, the ICC is in the best position to provide more detailed information on the expected level of intelligence cueing as they provided input on the current estimate, and are considering providing an updated intelligence cueing assessment for each of the 15 maritime terrorism scenarios. At this point, the assessment would be prepared in-house, so no new costs would be incurred as a result of this work.

3. Create, Share, and Review Additional Maritime Terrorism Scenarios

Since no new costs are associated with the recommendation to create, share, and review additional maritime terrorism scenarios, this can be implemented immediately. As stated in Chapter IV, MSRAM results would be improved by expanding the ability to create and subsequently share additional scenarios amongst local, regional and national users. MSRAM already allows creation of custom scenarios by field units, and these are

[123] U.S. Coast Guard Office of Budget and Programs, *U.S. Coast Guard Posture Statement*, (Washington, D.C.: U.S. Coast Guard Office of Budget and Programs, 2008), 34, U.S. Coast Guard, http://www.uscg.mil/comdt/DOCS/LOW.RES.CG%20FY09%20Posture%20Statement.FINAL.Jan29.pdf (accessed March 8, 2009).

reviewed for potential incorporation into subsequent annual MSRAM software updates. This cycle time could be reduced by promoting interaction between sectors when custom scenarios are created to provide near real time adaptability and usability. These scenarios could be posted on the Homeport MSRAM microsite for use by other sectors and could then be used by other Coast Guard sectors instead of waiting for the next strategic annual MSRAM update. This will reduce the possibility of terrorists using methods that are not accounted for by existing annual MSRAM scenarios. At this point, MSRAM does not include either transfer scenario contained in the LROI model, though plans are in place to add these two scenarios with MSRAM PLUS software in FY 2009. Since the MSRAM microsite already exists and the MSRAM team already has a budget for scenario updates, there is no anticipated additional cost associated with implementing this recommendation.

As indicated above, alignment between activities in MSRAM and the LROI model will significantly enhance the usefulness of MSRAM data for use in the LROI model and will result in more accurate assessment of the PWCS Outcome Measure. An additional important improvement would be the ability to create additional scenarios in the LROI model in alignment with MSRAM scenarios. As stated in Chapter IV, this is to avoid the issue of leaving gaps between existing scenarios: adversaries will try to exploit attacks not accounted for in any of the scenarios. Scenario updates in both MSRAM and the LROI model are highly recommended in conjunction with the revision of the Combating Maritime Terrorism Strategic and Performance Plan, and implemented on a joint basis to achieve and maintain alignment between the models. Once MSRAM contains the transfer scenarios, the model scenarios will be in alignment, so no new costs are contemplated for the LROI model until additional scenarios are proposed.

4. Acquire Outside Expert Input for the LROI Model

The next highest priority recommendation for implementation is the acquisition of outside expert input on the effectiveness of Coast Guard activities to reduce terrorism-related maritime risk. This was pointed out by the Office of Management and Budget in the 2006 PART review as an area in which the Coast Guard could improve the PWCS Outcome Measure, and the estimated implementation cost is relatively low.

As mentioned in Chapter I and discussed at length in Chapters IV and V, the inclusion of outside experts is critical to improve the assessment of Coast Guard effectiveness in reducing terrorism-related maritime risk. Each of those interviewed voiced the opinion that this additional input would provide a more accurate assessment of Coast Guard effectiveness, while Chapter V indicates that the use of heterogeneous groups of experts will result in a more accurate PWCS outcome measure. The cost estimate to acquire input from a group of five outside experts during an annual five-day PWCS performance assessment meeting is $30,000.

5. Improve Expert Judgment through Bias Reduction and Expert Judgment Aggregation

Another recommendation relating to the use of expert judgment that lends itself to implementation in conjunction the previous recommendation is the improvement of expert judgment through bias reduction and expert judgment aggregation. This is another area in which the Coast Guard could improve the PWCS Outcome Measure with a relatively low estimated implementation cost.

Chapter V covered an extensive list of procedures to reduce bias, along with a recommendation for expert judgment aggregation that would be used during the PWCS performance assessment meeting. The first technique to reduce biases in expert judgment elicitation is to ensure the experts are familiar with the biases so that they are aware of the potential detriment to expert judgment. Other areas to address are reducing inconsistency, retrievability bias, search set effectiveness bias, imaginability bias, anchoring, overconfidence, groupthink, and wishful thinking. The use of a facilitator to guide subject matter experts in the use of the Nominal Group Technique allows critical interaction between experts of varied backgrounds from both inside and outside the Coast Guard to gain multiple perspectives while avoiding groupthink. Using the ideas set forth in Chapter V, the facilitator can take actions before and during expert judgment elicitation to attenuate the other biases listed above. Unless there are strong indications to do otherwise, equally weighted averages should be used to aggregate expert judgment in the final step of the Nominal Group technique. The cost estimate for a facilitator to conduct an annual five-day PWCS performance assessment meeting along with travel expenses for Coast Guard SME attendance is $20,000.

6. Update Terrorist Threat Levels and Predicted Maritime Threat Frequencies

Terrorist threat updates are the next priority, including predicted maritime terrorism frequencies. As indicated in Chapter III, the Coast Guard Intelligence Coordination Center (ICC) provides information on the threat level for calculation of existing terrorism-related maritime risk in MSRAM annually, and through the National Maritime Terrorism Threat Assessment (NMTTA) biennially. These include assessments of terrorist intent, capability and presence required to conduct direct attacks, exploitation of vessels for those attacks, or transfer of terrorists or WMD through the maritime domain. The threat updates provided by the Coast Guard ICC affect MSRAM, which in turn affects the LROI model, and leads to the recommendation to implement this change as a relatively high priority.

https://apps.dtic.mil/dtic/tr/fulltext/u2/a527037.pdf (retrieved 20 January 2019)

The predicted maritime terrorism frequency affects every effectiveness calculation in the LROI model, and an update to this frequency could potentially be accomplished as part of future National Maritime Terrorism Threat Assessments. A headquarters planning team used information from ICC combined with additional research to estimate the frequency of the scenarios in the LROI model. Current frequencies are one direct attack/exploitation every year, one transfer of terrorists every 10 years, and one transfer of weapons of mass destruction every 20 years. As stated in Chapter III, while these frequency estimates are aligned with at least one other study, an examination and update of the estimated frequency of direct attack/exploitation, transfer of terrorists, and transfer of WMD is highly recommended.

Continued annual MSRAM threat updates, biennial NMTTA updates, and inclusion of predicted maritime terrorism frequencies will ensure the threat characterization in MSRAM is as accurate as possible. The cost estimate for the NMTTA is not available for publication since there is an active contract for this work that has not yet been awarded.

7. Update Consequence Assessments with New Micromodels in MSRAM

There is a need to periodically update and improve consequence assessments to more accurately characterize those associated with terrorism-related maritime risk. As previously indicated, this will require the input of engineering and financial experts to assess direct economic impact, and economic experts to provide information on secondary economic impacts. The creation of micromodels to capture this input and information to more accurately enumerate the primary and secondary economic consequences associated with an event of maritime terrorism is recommended for consideration because of the success achieved with the response calculator and blast calculator micromodels already used in MSRAM. The cost estimate to create micromodels in MSRAM to more accurately assess the consequences of maritime terrorist attacks is $200,000.

8. Expand MSRAM Training and Job Aids/Video Training Modules

While expanding MSRAM Training and Job Aids/Video Training Modules is important, this item is recommended for later implementation because a MSRAM training program already exists. Nonetheless, an expanded MSRAM training program will ensure that all field personnel using MSRAM are familiar with the program and use it correctly. This will improve data quality in both MSRAM and the LROI model, and thereby improve the PWCS Outcome Measure. Another desired outcome is a reduction in conflicts between local assessments and during the review process by Coast Guard district, area, and headquarters staffs. The cost estimate to expand the MSRAM training program to enable on site training of 250 personnel annually, along with updates of existing job aids and video training modules is approximately $400,000.

9. Train Coast Guard Auxiliary to Perform MSRAM Data Acquisition and Processing

Coast Guard Auxiliary training for the use of MSRAM is the next item recommended for implementation because of the very low cost of achieving the benefit the Coast Guard Auxiliarists can provide. Five of the eight recommendations to improve MSRAM refer to enhanced information collection. An option that has proven successful in this arena is Coast Guard Auxiliary acquisition and processing of data from Area Maritime Security Committee members to assist Captains of the Port with MSRAM data input requirements. The estimated cost to conduct a five day training session with travel and per diem for a total of 100 Coast Guard Auxiliarists on the use of MSRAM would be approximately $160,000, which would provide an average of three trained Coast Guard Auxiliarists at each sector, though larger sectors with more available Auxiliarists would receive more training quotas. This cost does not consider any overhead requirements for additional security clearances.

10. Update Vulnerability Assessments

While beneficial, the recommendation to update vulnerability assessments is relatively late in the implementation sequence since Coast Guard sector personnel already assess attack achievability, system security, and target hardness to complete the vulnerability assessment process in MSRAM, as discussed in Chapter III. These assessments are reviewed by district, area and headquarters personnel along with other MSRAM data. As indicated in Chapter IV, while many components of maritime critical infrastructure/key resources have undergone vulnerability assessments, these require periodic revisions. Vessel and port facility owners should provide updated vulnerability assessment information to the COTP. This will ensure MSRAM reflects the latest, best data available. The benefit will be more accurate risk assessment, and a resultant improvement in the PWCS Outcome Measure accuracy.

The Coast Guard Auxiliary is a prime candidate for this data collection and processing. In addition, the annual MSRAM update should include results of MTSA spot checks to provide information collected in person on target vulnerability. If existing

Coast Guard personnel resources are used to update vulnerability assessments as recommended, then the increased cost to collect and process this additional information should be covered by the Auxiliarist cost cited above.

11. Update Risk Ownership Matrix

The recommendation to update the Coast Guard Risk Ownership matrix is fairly late in the implementation sequence since the existing matrix contains useful though somewhat dated information and the higher priority recommendations address issues that have greater potential for large-scale impact. As with many of the other recommendations, the benefit of implementing this recommendation is an improvement in the accuracy of the PWCS Outcome Measure, which takes into account the level of Coast Guard risk ownership for each maritime terrorism scenario.

Chapter III examined the Coast Guard portion of risk ownership for each of the 15 scenarios in the LROI model, arrived at through consultation with Coast Guard personnel who participated in the 2005 risk-based PWCS Outcome Measure effort. Changes in laws, regulations, policies and partnerships since 2005 indicate the need for the Coast Guard portion of risk ownership to be reassessed. The estimated cost to collect current information, update the Risk Ownership matrix and incorporate this information into the LROI model is $50,000.

12. Modify Homeport to Enable Dynamic Risk Assessment

The alteration of Homeport to gain the functionality of Virtual Maritime Fusion Centers is significant in its own right, and Coast Guard support of this initiative on a nationwide basis is highly recommended. While the collection of dynamic risk assessment information is an important step forward, the recommendation to modify Homeport to enable Dynamic Risk Assessment through Homeport Secure Web Surveys and Virtual Maritime Fusion Centers appears later in the implementation sequence because there is a need to improve data collection and analysis before increasing data collection frequency.

In addition to threat, vulnerability and consequence updates recommended in the preceding paragraphs, the Combating Maritime Terrorism Strategic and Performance Plan (CMT 2.0) requires periodic MSRAM updates to create an operational risk profile for each COTP zone throughout the course of the year. These updates would be based on information collected from Area Maritime Security Committee members at AMSC meetings, in person, over the phone, or through Homeport Secure Web Portal Surveys. These surveys would be periodic Web-based surveys sent through the Homeport secure portal for stakeholders to confirm that security conditions under their cognizance are substantially the same as previous input, with an option to update vulnerability or consequence information. Another avenue to acquire dynamic risk assessment information is through a modification to Homeport so it emulates the ease of use seen in the Port of Los Angeles/Long Beach Virtual Maritime Fusion Center. As stated in the previous chapter, this would increase information sharing by linking the FBI InfraGard Program, the FBI Joint Terrorism Task Force, the Coast Guard Area Maritime Security Committee, local law enforcement agencies, and other port stakeholders to create a common operating picture and enhance collaborative efforts. The Homeport development team in the Coast Guard Headquarters Operations Systems Management Division already has a budget for program maintenance, and they are considering implementation of Secure Web Portal Surveys at no additional cost. Before developing the cost estimate to alter Homeport to gain the advantages of a Virtual Maritime Fusion Center for all Coast Guard COTP zones, requirements must be agreed upon by the Coast Guard Headquarters Domestic Ports Division, the Domestic Port Security Evaluation Division, and the Office of C4 and Sensors Capabilities.

13. Update Target Lists using Satellite Photography and Onsite Visits

The recommendation to conduct target list updates appears last in the implementation plan because sector personnel already collect data on an annual basis to update target lists, and this recommendation was to provide an additional check to ensure all appropriate targets are continually included in MSRAM.

Nonetheless, continued emphasis must be maintained on annual target list updates, including the addition of new maritime critical infrastructure/key resources and vessels within each COTP Zone. This will ensure all potential targets subject to maritime terrorism are included in MSRAM. Targets no longer physically present or no longer periodically transiting the zone should be removed from the current MSRAM database but can be kept for historical and auditing purposes. While each sector updates this list annually, analysis of satellite photography and other available information such as required annual onsite visits would serve as a valuable cross check on field level target update information. The estimated cost for this analysis is $150,000.

D. AREAS FOR FURTHER RESEARCH

MSRAM accounts for threat shifting through quantification of characteristics that affect terrorist selection of one target over another. This includes attack achievability, system security, and target hardness, which are components of vulnerability. Components of consequence also affect threat shifting; including the expected number of deaths or injuries, primary and secondary economic impact, environmental impact, national security/national defense impacts, and symbolic impact, quantifying damage to landmarks. All of these characteristics are quantified as part of the MSRAM data acquisition process. Less information is available about dynamic threat shifting that occurs during an attack as a result of security presence at the scene of an intended target as required by Operation Neptune Shield or other factors. Future research into this area has the potential to better inform the Coast Guard, other government agencies, and owners and operators of port facilities and vessels affected by the threat shift process in the maritime domain.

As previously indicated, the LROI model uses modified event chains to represent the events leading up to and after a terrorist event. The development of event trees to represent threat shifting and other terrorist options before and during an attack is an area that may be considered for future research.

The Coast Guard models reviewed in this research are based on the assumption that the threat, vulnerability and consequences assigned in the assessment process match those of terrorists. Another area of valuable future research would be an examination of these assumptions to determine if the Coast Guard is using the same criteria as terrorists to quantify risk in the maritime domain.

E. SUMMARY

As the lead federal agency for maritime homeland security, the Coast Guard is responsible for execution of five mission programs directly related to homeland security: Drug Interdiction; Migrant Interdiction; Ports, Waterways, and Coastal Security; Other Law Enforcement; and Defense Readiness. This research has examined measurement of Coast Guard mission effectiveness through the Ports, Waterways, and Coastal Security outcome measure and made recommendations to improve this measure through enhancements to the Maritime Security Risk Analysis Model and the LROI model on which the outcome measure is based. Implementation of the recommendations contained in this research will lead to more accurate assessment of Coast Guard effectiveness in achieving homeland security, and result in improved allocation of resources in the quest to reduce terrorism-related maritime risk.

APPENDIX

Line of Assurance	Activity	Category	Type	Risk Component
A - Intervene after attack - recovery	25 - Respond to Terrorist Attack	3 - Effective Maritime Security Regime	Independent	Consequence
B - Intervene after attack - response	26 - Recover from Terrorist Attack	3 - Effective Maritime Security Regime	Independent	Consequence
C - Intervene by controlling access	17 - Control Port Access, Activity and Movement	2 - Maritime Security & Response Ops	Dependent	Consequence
D - Intervene by escort	11 - Escort Vessels	2 - Maritime Security & Response Ops	Independent	Vulnerability
E - Intervene by fixed security zone	12 - Enforce Fixed Security Zones	2 - Maritime Security & Response Ops	Independent	Vulnerability
F - Intervene by investigating anomalies	16 - Investigate Anomalies	2 - Maritime Security & Response Ops	Dependent	Vulnerability
H - Intervene by patrolling	7 - Conduct Waterborne, Shoreside, and Aerial Patrols	2 - Maritime Security & Response Ops	Independent	Vulnerability
I - Intervene by random boardings – border and coastal zone	9 - Conduct Random Boardings in the border/coastal zone	2 - Maritime Security & Response Ops	Independent	Vulnerability
J - Intervene by random boardings – international zone	10 - Conduct Random Boardings in the international zone	2 - Maritime Security & Response Ops	Independent	Vulnerability
K - Intervene by security boardings – domestic zone	8 - Conduct Security Boardings	2 - Maritime Security & Response Ops	Independent	Vulnerability
L - Intervene by specialized use of force – border and coastal zone	19 - Specialized Use of Force - Border/Coastal Zone	2 - Maritime Security & Response Ops	Dependent	Vulnerability
M - Intervene by specialized use of force – domestic zone	18 - Specialized Use of Force - Domestic Zone	2 - Maritime Security & Response Ops	Dependent	Vulnerability
N - Intervene by specialized use of force – international zone	20 - Specialized Use of Force - International Zone	2 - Maritime Security & Response Ops	Dependent	Vulnerability
O - Intervene by suspect vessel boardings – border and coastal zone	14 - Conduct suspect vessel boardings in the Border/Coastal Zone	2 - Maritime Security & Response Ops	Dependent	Threat
P - Intervene by suspect vessel boardings – domestic zone	13 - Conduct suspect vessel boardings in the Domestic Zone	2 - Maritime Security & Response Ops	Dependent	Threat

Line of Assurance	Activity	Category	Type	Risk Component
Q - Intervene by suspect vessel boardings – international zone	15 - Conduct suspect vessel boardings in the International Zone	2 - Maritime Security & Response Ops	Dependent	Threat
R - Intervene by use of force – border and coastal zone	22 - End Game Prosecution - Border/Coastal Zone	2 - Maritime Security & Response Ops	Dependent	Vulnerability
S - Intervene by use of force – domestic zone	21 - End Game Prosecution - Domestic Zone	2 - Maritime Security & Response Ops	Dependent	Vulnerability
T - Intervene by use of force – international zone	23 - End Game Prosecution - International Zone	2 - Maritime Security & Response Ops	Dependent	Vulnerability
U - Intervene by owner/operator security	29 - Review, Approve, and Enforce Compliance with Domestic Vessel, Facility and Outer Continental Shelf (OCS) Facility Security Plans	3 - Effective Maritime Security Regime	Independent	Vulnerability
V - Intervene by Port State Control measures	30 - Enforce Foreign Flag Vessel Compliance with International Ship and Port Facility Security (ISPS) Code - Implement and Monitor Port State Control Measures	3 - Effective Maritime Security Regime	Independent	Vulnerability
	3 - USCG Intelligence	1 - Maritime Domain Awareness	Supporting	Threat
	4 - Non-USCG Intelligence	1 - Maritime Domain Awareness	Supporting	Threat
	31 - Execute International Port Security Program	3 - Effective Maritime Security Regime	Supporting	Vulnerability
	32 - Lead Outreach/Partnership Activities	3 - Effective Maritime Security Regime	Supporting	Vulnerability
	33 - Review, Approve, and Exercise Area Maritime Security Plans (AMSPs)	3 - Effective Maritime Security Regime	Supporting	Vulnerability
	34 - Prepare and Exercise National Strategic Plans	3 - Effective Maritime Security Regime	Supporting	Vulnerability
	35 - Execute and Monitor the Special Interest Vessel (SIV) Program	3 - Effective Maritime Security Regime	Supporting	Vulnerability
	24 - Conduct Military Outload (MOL) Security Support	2 - Lead and Conduct Effective Maritime Security and Response Operations	Supporting	Vulnerability

LIST OF REFERENCES

Ackerman, Gary. "Chasing Shadows: Determining the Terrorist Threat." Presented at Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2007. Los Alamos National Laboratory. http://risk.lanl.gov/site2k7/RS2007Presentations.html (accessed January 2008).

———. "The Future of Jihadists and WMD." In *Jihadists and Weapons of Mass Destruction*, edited by Gary Ackerman and Jeremy Tamsett, 356-366. Boca Raton, FL: CRC Press, 2008.

Allen, Thad W. *Fiscal Year 2009 President's Budget*. Statement to the U.S. Senate Committee on Commerce, Science, and Transportation, Sub-committee on Oceans, Atmosphere, Fisheries, and Coast Guard, Washington, D.C., March 6, 2008. U.S. Coast Guard. http://www.uscg.mil/comdt/speeches/docs/CST_FY09_Budget_6_Mar_08.pdf (accessed March 6, 2008).

Arkes, Hal R. "Overconfidence in Judgmental Forecasting." In *Principles of Forecasting: A Handbook for Researchers and Practitioners*, edited by J. Scott Armstrong, 510. Norwell, MA: Kluwer Academic, 2001.

Ayyub, Bilal. *Risk Analysis in Engineering and Economics*. Boca Raton, FL: Taylor and Francis, Inc., 2003.

Bar-Hillel, Maya. "Subjective Probability Judgments." *International Encyclopedia of the Social and Behavioral Sciences*. Amsterdam, Netherlands: Elsevier Science Ltd, 2001, http://www.tower.com/international-encyclopedia-social-behavioral-sciences-neil-j-smelser-hardcover/wapi/100329523 (accessed November 16, 2008).

Bryant, Dennis. "Port Security: A Historical Perspective." Marine Link (March 8, 2004), http://www.marinelink.com/Story/Column:+Port+Security:+A+Historical+Perspective-13883.html (accessed November 28, 2007).

Cady, Kevin. "The Area Maritime Security Committee and the CG Auxiliary." *Safety Lines*. (February 2008): 2.

Casey, William, Wendy Peck, Natalie Webb, and Phil Quast. *Enterprise Excellence: Driving Strategic Results Instead of Metric Mania*. Lakewood, CO, Executive Leadership Group, 2006.

Chalk, Peter. *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States*. Santa Monica, CA: RAND Corporation, 2008. RAND Corporation. http://www.rand.org/pubs/monographs/2008/RAND_MG697.pdf (accessed February 9, 2009).

Cooper, Dave. "How the Coast Guard Attempts to Optimize Mission Execution through Risk Reduction Return on Investment." Presented at Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2007. Los Alamos National Laboratory. http://risk.lanl.gov/site2k7/RS2007Presentations.html (accessed January 27, 2008).

Department of the Navy. *Naval Doctrine Publication 2: Naval Intelligence*. Naval Warfare Development Command. http://www.nwdc.navy.mil/content/Library/Documents/NDPs/ndp2/ndp20007.htm (accessed September 1, 2008).

Downs, Brady. "The Maritime Security Risk Analysis Model." *Proceedings of the Marine Safety & Security Council* 64, no. 1 (Spring 2007): 36, 37.

Eply, Nicholas and Thomas Gilovich. "Putting Adjustment Back in the Anchoring and Adjustment Heuristic." In *Heuristics and Biases: The Psychology of Intuitive Judgment*, edited by Thomas Gilovich, Dale Griffin, and Daniel Kahneman, 139. Cambridge: Cambridge University Press, 2002.

Falaschetti, Dino and Bryan Roberts. "Threat Shifting: A Key Issue in Terrorism Risk Analysis." Presented at Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2006. Los Alamos National Laboratory. http://risk.lanl.gov/site2k6/archives/pgm2006.html (accessed January 27, 2008).

Furnham, Adrian. *The Psychology of Behaviour at Work*. Hove, UK: Psychology Press, 2005.

Guikema, Seth. "A Critical Assessment of Game Theory in Terrorist Risk Assessment." Presented at Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2006. Los Alamos National Laboratory. http://risk.lanl.gov/site2k6/archives/pgm2006.html (accessed January 2008).

Hall, Ernest J., Jane S. Mouton, and Robert R. Blake. "Group Problem Solving Effectiveness under Conditions of Pooling vs. Interaction." *Social Psychology* 59, no. 1 (1963): 147-157.

Hammond, Mark and Karrie Trebbe. "Homeport." *Proceedings of the Marine Safety & Security Council* 63, no. 1 (Spring 2006): 23-25.

Harrald, John R., Hugh W. Stephens, and Johann Rene van Dorp. “A Framework for Sustainable Port Security.” *Journal of Homeland Security and Emergency Management* 1, no. 2 (2004). Berkeley Electronic Press. http://www.bepress.com/jhsem/vol1/iss2/12/ (accessed January 27, 2008).

Hubbard, Douglas W. *How to Measure Anything*. Hoboken, NJ: John Wiley and Sons, Inc., 2007.

Kaplan, Stanley and B. John. Garrick. “On the Quantitative Definition of Risk.” *Risk Analysis* 1, no. 1 (1981): 11-28.

Larrick, Richard P and Jack B Soll. “Intuitions about Combining Opinions: Misappreciation of the Averaging Principle.” *Management Science* 52, no. 1 (2006): 111-128.

Lichtenstein, Sarah, Baruch Fischhoff, and Lawrence D. Phillips, “Calibration of Probabilities: The State of the Art to 1980.” In *Heuristics and Biases: Judgment under Uncertainty*, edited by Thomas Gilovich, Dale Griffin, and Daniel Kahneman, 334. Cambridge: Cambridge University Press, 1982.

Macesker, Bert, Joseph J. Myers, Vernon H. Guthrie, David A. Walker, and Stephen G. Schoolcraft. “Quick-reference Guide to Risk-based Decision Making (RBDM): A Step-by-step Example of the RBDM Process in the Field.” Air University. http://www.au.af.mil/au/awc/awcgate/uscg/risk-qrg.pdf (accessed October 25, 2008).

McCauley, Clark. “The Nature of Social Influence in Groupthink: Compliance and Internalization.” *Journal of Personality and Social Psychology* 57, no. 2 (1989): 250-260.

McDermott, Rose. *Political Psychology in International Relations*. Ann Arbor: University of Michigan Press, 2004.

Meyer, Mary A. and Jane M. Booker. *Eliciting and Analyzing Expert Judgment: A Practical Guide*. Philadelphia, PA: Society for Industrial and Applied Mathematics, 2001.

Miller, George A. “The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information.” *Psychological Review* 63, no. 2 (1956): 81-97.

Moran, James. “Maritime Security Risk Assessment Process.” Presented at Los Alamos National Laboratory Risk Symposium, Santa FE, NM, 2007. Los Alamos National Laboratory. http://risk.lanl.gov/site2k7/RS2007Presentations.html (accessed January 27, 2008).

Mowrer, Matthew. “2008 Risk Change and Margin of Error.xls.” Internal document. Washington, D.C.: U.S. Coast Guard Headquarters Office of Performance Management and Assessment, 2008.

Myers, Joseph. “Risk-Based Decision Making.” *Proceedings of the Marine Safety & Security Council* 64, no. 1 (2007): 6-9.

Parisi, Francesco and Vernon L. Smith. *The Law and Economics of Irrational Behavior*. Palo Alto, CA: Stanford University Press, 2005, http://books.google.com/books?id=pbP2NQokNnIC (accessed November 16, 2008).

Predd, J. B., S.R. Kulkarni, H.V. Poor, Daniel Osherson. “Scalable Algorithms for Aggregating Disparate Forecasts of Probability” Presented at Proceedings of the Ninth International Conference on Information Fusion, Florence, Italy, 2006.

Rabkin, Norman J. *Strengthening the Use of Risk Management Principles in Homeland Security*. Statement to U.S. House of Representative Committee on Homeland Security. Washington, D.C.: U.S. Government Accountability Office, GAO-08-904T, 2008. Committee on Homeland Security. http://homeland.house.gov/SiteDocuments/20080625151226-90211.pdf (January 27, 2008).

Ravinder, Handanhal V. “Bias in Aggregations of Subjective Probability and Utility.” *Journal of the Operational Research Society* 43, no. 6 (1992): 621-627.

Risk Management Solutions. *Managing Terrorism Risk*. Newark, CA: Risk Management Solutions, 2003. Risk Management Solutions. http://www.rms.com/publications/terrorism_risk_modeling.pdf (accessed January 28, 2008).

Ross, Robert. Risk and Decision-Making in Homeland Security. Unpublished paper, Department of Homeland Security, Washington, D.C., 2006.

Rowe, Gene and George Wright. “Expert Opinions in Forecasting: The Role of the Delphi Technique.” In *Principles of Forecasting: A Handbook for Researchers and Practitioners*, edited by J. Scott Armstrong, 126. Boston: Kluwer Academic Publishers, 2001.

Salerno, Brian M. *Combating Maritime Terrorism Strategic and Performance Plan*. Washington, D.C.: United States Coast Guard, 2008.

———. “Navigation and Vessel Inspection Circular No. 9-02” Washington, D.C.: U.S. Coast Guard, 2008. Assistant Commandant for Marine Safety, Security, and Stewardship, http://www.uscg.mil/hq/cg5/NVIC/pdf/2002/NVIC_09_02_Change_3.pdf (accessed July 8, 2008).

Scheina, Robert. “The U.S. Coast Guard at War: A History.” U.S. Coast Guard. http://www.uscg.mil/History/articles/h_CGatwar.asp (accessed November 11, 2007).

Slovic, Paul, Baruch Fischhoff, and Sarah Lichtenstein. “Perceived Risk: Psychological Factors and Social Implications.” *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* 376, no. 1764 (1981): 20.

Tastle, William J. and Mark J. Wierman. “Determining Risk Assessment Using the Weighted Ordinal Agreement Measure.” *Journal of Homeland Security* (June 2007). Homeland Security Institute. http://www.homelandsecurity.org/newjournal/Articles/displayArticle2.asp?article=157 (accessed January 2008).

Tversky, Amos and Daniel Kahneman. “Judgment under Uncertainty: Heuristics and Biases.” *Science* 185, no. 4157 (September 1974): 1124-1131.

U. S. Coast Guard. *Abstract of Operations*. Washington, D.C.: U.S. Coast Guard, 2007.

———. “Area Maritime Security Interim Rule.” *Federal Register* 68, no. 126. Washington, D.C.: National Archives and Records Administration, no. 39287, 2003.

———. “Electronic Code of Federal Regulations.” *Title 33: Navigation and Navigable Waters*. Washington, D.C., Government Publication Office, 2002. Government Printing Office, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title33/33cfr103_main_02.tpl (accessed August 20, 2008).

———. *Maritime Security Risk Analysis Model (MSRAM) Training and Software Manual*. Washington, D.C.: United States Coast Guard, 2008.

U.S. Coast Guard Headquarters Human Factors Division. “Operational Risk Management.” *Commandant Instruction 3500.3*. Washington, D.C.: U.S. Coast Guard, 2000. U.S. Coast Guard. http://www.uscg.mil/directives/ci/3000-3999/CI_3500_3.pdf (accessed October 25, 2008).

U.S. Coast Guard Headquarters Office of Performance Management and Assessment. "USCG Combating Maritime Terrorism Strategic Planning Process Overview." Washington, D.C.: Coast Guard Headquarters Office of Performance Management and Assessment, 2007).

U.S. Coast Guard Headquarters Office of Plans and Policy. *Combating Maritime Terrorism – Definitions*. Washington, D.C.: Coast Guard Headquarters Office of Plans and Policy, 2006.

U.S. Coast Guard Headquarters Office of Office of Performance Management and Assessment. "LROI Model" Washington, D.C.: U.S. Coast Guard Headquarters Office of Policy and Planning Integration, 2008.

U.S. Coast Guard Headquarters Port Safety and Security Division. *USCG Port Security Risk Assessment Tool* (Version 2) Users' Manual. Washington, D.C.: U.S. Coast Guard, 2002.

U.S. Coast Guard Office of Budget and Programs. *U.S. Coast Guard Posture Statement*. Washington, D.C.: U.S. Coast Guard Office of Budget and Programs, 2008, http://www.uscg.mil/comdt/DOCS/LOW.RES.CG%20FY09%20Posture%20Statement.FINAL.Jan29.pdf (accessed March 8, 2009).

U.S. Office of Management and Budget. *Program Assessment on the Coast Guard Ports, Waterways and Coastal Security, Assessment Year 2006*. Washington, D.C.: Office of Management and Budget, 2006. White House. http://www.whitehouse.gov/omb/expectmore/detail/10003635.2006.html (accessed December 9, 2007).

Unwin, Stephen D. "Adaptability of Conventional Risk-Based Decision Methods to Homeland Defense." Los Alamos National Laboratory Risk Symposium, Santa Fe, NM, 2006. Los Alamos National Laboratory. http://risk.lanl.gov/site2k6/archives/pgm2006.html (accessed January 27, 2008).

Van de Ven, Andrew H. and Andre L. Delbecq. "The Effectiveness of Nominal, Delphi, and Interacting Group Decision Making Processes." *Academy of Management Journal* 17, no. 4 (December 1974): 606.

Von Winterfeldt, Detlof and Heather Rosoff. "Using Project Risk Analysis to Counter Terrorism." Presented at USC Symposium on Terrorism Risk Analysis, Los Angeles, CA, 2005. University of Southern California. http://www.usc.edu/dept/create/assets/002/51845.pdf (accessed January 28, 2008).

Willis, Henry. *Guiding Resource Allocations Based on Terrorism Risk*. Santa Monica, CA: RAND, 2006. RAND Corporation. http://www.rand.org/pubs/working_papers/2006/RAND_WR371.pdf (accessed January 28, 2008).

Willis, Henry H., Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby. *Estimating Terrorism Risk*. Santa Monica, CA: RAND Corporation, 2005. RAND Corporation. http://www.rand.org/pubs/monographs/MG388/ (accessed January 28, 2008).

Willis, Henry, Tom LaTourrette, Terrence K. Kelly, Scot Hickey, and Samuel Neil. *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*, (Santa Monica, CA: RAND Corporation, MG-388-R TR-386-DHS, 2007. RAND Corporation. http://www.rand.org/pubs/technical_reports/2007/RAND_TR386.sum.pdf (accessed January 28, 2008).

Woo, Gordon. “The Evolution of Terrorism Risk Modeling.” *Journal of Reinsurance* 10, no. 3 (2003): 1.

———. “Quantifying Insurance Terrorism Risk.” Working paper. National Bureau of Economic Research, Cambridge, MA, 2002. Risk Management Solutions. http://www.rms.com/newspress/quantifying_insurance_terrorism_risk.pdf (accessed January 28, 2008).

———. “Terrorism Risk.” In *Wiley Handbook of Science and Technology for Homeland Security*, edited by John G. Voeller, 2. London: John Wiley and Sons, Inc., 2007.

———. *Understanding Terrorism Risk*. Newark, CA: Risk Management Solutions, 2002. Risk Management Solutions. http://www.rms.com/Publications/UnderstandTerRisk_Woo_RiskReport04.pdf (accessed January 28, 2008).

Wright, Candice J. “Bridging the Gap in Port Security; Network Centric Theory Applied to Public/Private Collaboration.” Master's thesis, Naval Postgraduate School, 2007.

Wrightson, Margaret. *Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*. Washington, D.C.: U.S. Government Accountability Office, 2005. U.S. Government Accountability Office. http://www.gao.gov/new.items/d0691.pdf (accessed October 25, 2008).

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. Robert Josefek
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California

4. Admiral Manson Brown
   Fourteenth Coast Guard District
   Honolulu, Hawaii

5. Admiral Brian Salerno
   U.S. Coast Guard
   Washington, D.C.

6. Dana Goward
   U.S. Coast Guard
   Washington, D.C.

7. Brady Downs
   U.S. Coast Guard
   Washington, D.C.

8. Dave Cooper
   U.S. Coast Guard
   Washington, D.C.