View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Calhoun, Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

Theses and Dissertations | Thesis Collection

2011-12

Game theory, probabilistic risk, and randomized strategy: the rulebook revisited with emphasis on Coast Guard Mission Space

Engel, Ryan S.

Monterey, California. Naval Postgraduate School

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

http://www.nps.edu/library

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

GAME THEORY, PROBABILISTIC RISK, AND RANDOMIZED STRATEGY: THE RULEBOOK REVISITED WITH EMPHASIS ON COAST GUARD MISSION SPACE

by

Ryan S. Engel

December 2011

Thesis Co-Advisors:	David L. Alderson Bard K. Mansager
Second Reader:	Joseph DiRenzo

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** December 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Game Theory, Probabilistic Risk, and Randomized Strategy: The Rulebook Revisited with Emphasis on Coast Guard Mission Space		**5. FUNDING NUMBERS**	
6. AUTHOR: Engel, Ryan, S.			
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. IRB Protocol number: N/A			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

The welfare of the United States is highly dependent upon its critical infrastructures and key resources. The Marine Transportation System is critical to the flow of commerce. The United States Coast Guard is charged with facilitating the protection of the Marine Transportation System from acts of terrorism under the Port, Waterways, and Coastal Security Mission. The Coast Guard faces the challenge of providing essential protection strategies with limited resources.

Optimizing limited resources to provide maximum protection from deliberate attacks is a complex problem. In this thesis we explore various analytic techniques that can be used to provide guidance in resource allocation for defense against terrorism. We focus on two techniques, risk-based analysis and game theoretic analysis. We review the fundamental mathematical concepts and philosophical assumptions necessary for these techniques to be applicable.

We review the Coast Guard's role in the protection against potential terrorist attacks. Using a game theory approach, we build a model and present a preliminary analysis on the transportation of commerce along the Pittsburgh Three Rivers area.

14. SUBJECT TERMS: Game theory; probabilistic risk, randomized strategies; Pittsburg Three Rivers project; Coast Guard Ports, Waterways, and Coastal Security risk analysis			**15. NUMBER OF PAGES** 93
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** 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

GAME THEORY, PROBABILISTIC RISK, AND RANDOMIZED STRATEGY: THE RULEBOOK REVISITED WITH EMPHASIS ON COAST GUARD MISSION SPACE

Ryan S. Engel
Lieutenant Commander, United States Coast Guard
B.S., United States Coast Guard Academy, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED MATHEMATICS

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Author: Ryan S. Engel

Approved by: David L. Alderson
Thesis Co-Advisor

Bard K. Mansager
Thesis Co-Advisor

Joseph DiRenzo
Second Reader

Carlos Borges
Chair, Department of Applied Mathematics

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The welfare of the United States is highly dependent upon its critical infrastructures and key resources. The Marine Transportation System is critical to the flow of commerce. The United States Coast Guard is charged with facilitating the protection of the Marine Transportation System from acts of terrorism under the Port, Waterways, and Coastal Security Mission. The Coast Guard faces the challenge of providing essential protection strategies with limited resources.

Optimizing limited resources to provide maximum protection from deliberate attacks is a complex problem. In this thesis we explore various analytic techniques that can be used to provide guidance in resource allocation for defense against terrorism. We focus on two techniques, risk-based analysis and game theoretic analysis. We review the fundamental mathematical concepts and philosophical assumptions necessary for these techniques to be applicable.

We review the Coast Guard's role in the protection against potential terrorist attacks. Using a game theory approach, we build a model and present a preliminary analysis on the transportation of commerce along the Pittsburgh Three Rivers area.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AD	Attacker-Defender
ARDA	Anti-terrorism Risk Based Decision Aid
ASME	American Society of Mechanical Engineers
BTRA	Biological Agent Risk Analysis
C	Consequence
CI/KR	Critical Infrastructure / Key Resources
DAD	Defender-Attacker-Defender
DHS	Department of Homeland Security
FAMS	Federal Air Marshal Service
IWS	Inland Waterway System
MSRAM	Maritime Security Risk Analysis Model
MTS	Marine Transportation System
NIPP	National Infrastructure Protection Plan
NRC	National Research Council
NYPD	New York Police Department
PRA	Probabilistic Risk Analysis
PROTECT	Port Resilience Operational / Tactical Enforcement to Combat Terrorism
PWCS	Ports, Waterways, and Coastal Security
RAMCAP	Risk Analysis and Management for Critical Asset Protections
RIN	Risk Index Number
T	Threat
TVC	Threat-Vulnerability-Consequence
USCG	United States Coast Guard
V	Vulnerability

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To my beautiful and supportive wife, thank you for adapting your life to help me meet my goals and aspirations. You have picked me up and inspired me through it all.

To my son Gus and daughter Molly, you have brought me much joy and many laughs. Your running to the doorway when I get home is always the highlight of my day.

To my parents, your guidance and unending support continue to influence my life thirty five years down the road. Thank you for everything.

Professor David Alderson, I thank you for your tireless efforts and academic insights as my thesis advisor. I have learned a great deal from you and will always be grateful for the time you have spent with me.

Bard Mansager, you are the reason that a door was opened for me to attend the Naval Postgraduate School. Thank you for help and guidance in not only my thesis but throughout my education at NPS.

I thank the entire Applied Mathematics faculty. I have enjoyed your classes tremendously. To Carlos Borges, you are a terrific leader and instructor. Your efforts have bolstered morale throughout the department and inspired the officer-student corps.

To Coast Guard LANT-7, I have learned a tremendous amount about the world of Coast Guard operations research through your office. Dr. DiRenzo, thank you for your support, hospitality, and wisdom. Ben, you are a role model for all officers and especially for those who wish to make significant contributions in ops research. Dr. Jackson, thank you for all the data processing, imaging, and networking you did to help facilitate the Pittsburgh project.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND BACKGROUND

A. UNITED STATES COAST GUARD

1. Brief History

The United States Coast Guard (USCG) has a rich history and significant role in defending our nation's security and prosperity. Through our nation's history, the Coast Guard has continued to modernize and adapt to serve the country's changing needs. In 1790 the Cutter Revenue Service was established to collect taxes from a newly formed nation and help other mariners in distress on the water. In 1915 the Cutter Revenue Service merged with the Life Saving Service, officially forming the United States Coast Guard. In 1939, the U.S. Lighthouse Service was brought under USCG purview, and then in 1942, the Bureau of Maritime Investigations and Navigation was added to the Coast Guard's list of responsibilities. In 1967, the Coast Guard was moved from the Department of Treasury to the Department of Transportation (USCG, 2011b). Following the terrorist attacks against the United States on September 11, 2001, the Coast Guard, already a leader in maritime security, was moved to the Department of Homeland Security (DHS) to assist with anti-terrorism and infrastructure protection missions.

Today, the Coast Guard is a maritime, military, multi-mission service unique among the military branches for having a maritime law enforcement mission (with jurisdiction in both domestic and international waters) and a federal regulatory agency mission in its mission set. It operates under the Department of Homeland Security during peacetime, and can be transferred to the Department of Defense, under the Navy, during time of war (USCG, 2011b).

2. Broad View Mission Scope

The Coast Guard is unique in its capacities and authorities to conduct missions in homeland defense, emergency response, maritime stewardship, and law enforcement. The Coast Guard's enduring roles are maritime safety, maritime security, and maritime stewardship. To carry out those roles the Coast Guard has eleven statutory missions as defined in 6 U.S.C. § 468.

These missions include:

- Search and Rescue (SAR),
- Marine Environmental Protection (MEP),
- Maritime Safety (MARSAFE),
- Alien Migrant Interdiction Operations (AMIO),
- Counter Drug (CD) / Counter Narco-Terrorism (CNT),
- Other Law Enforcement (OLE),
- Aids to Navigation (ATON),
- Defense Readiness (DEFRED),
- Living Marine Resources (LMR)
- Polar Icebreaking Operations, and
- Ports, Waterways, and Coastal Security (PWCS).

Of the missions listed above, we focus in this thesis on the protection of infrastructure under Ports, Waterways, and Coastal Security (PWCS). Since joining DHS, the Coast Guard has made PWCS a primary mission alongside the longstanding Search and Rescue one.

> PWCS is the protection of the U.S. Maritime Domain and the U.S. Marine Transportation System (MTS) and those who live, work or recreate near them; the prevention and disruption of terrorist attacks, sabotage, espionage, or subversive acts; and response to and recovery from those that do occur. Conducting PWCS deters terrorists from using or exploiting the MTS as a means for attacks on U.S. territory, population centers, vessels, critical infrastructure, and key resources. PWCS includes the employment of awareness activities; counterterrorism, antiterrorism, preparedness and response operations; and the establishment and oversight of a maritime security regime. PWCS also includes the national defense role of protecting military out-load operations. (USCG, 2011c)

3. Challenges to the PWCS Mission

a. Non-deliberate Hazards

There are many non-deliberate maritime hazards such as those caused by nature, human error, or mechanical failure. Examples of non-deliberate hazards include hurricane damage to a port, a navigational error that causes a ship to run aground, or a draw bridge that fails to open and requires repair or replacement. The uncertainty of future events is typically addressed by focusing on prevention and response capacities in accordance to the frequency, location, and consequences of past events. Because historical data is typically available for these hazards, it is possible to characterize the frequency of these events in terms of probabilities.

b. Deliberate Threats

PWCS must also contend with deliberate acts committed against a person, group, system, or institution with the intent of causing harm. The United States has significantly less historical data available for these types of threats, making them harder to predict. Within the Coast Guard's mission space, deliberate attacks are essentially acts of terrorism and/or crime; the USCG handles these through their roles in homeland security and law enforcement.

4. Limited Resources for Operations

Despite its wide scope of responsibilities, the Coast Guard remains a relatively small organization. The Coast Guard currently consists of only approximately 42,000 active duty members (USCG, 2011b), comparable to the New York City Police Department (NYPD) with 34,000 uniformed officers (NYPD, 2011). The NYPD's area of responsibility includes a 6,720 square mile grid (NYPD, 2011). The Coast Guard's responsibility spreads over 950,000 miles of coastline to include 260,000 square miles of open-ocean, as well as numerous international and joint force operations (Coast Guard, 2011a). The Coast Guard's motto has always been to do more with less. However, as mission type and complexity continue to increase, USCG is reaching its limits with funding and personnel. These limitations prevent USCG from being able to conduct all its

missions with 100% effectiveness. Therefore, USCG must make judicious decisions to allocate limited resources to most effectively and efficiently conduct operations. To best manage and optimize limited resources, the Coast Guard must analyze each mission independently while maintaining balance across the whole system.

Failure to allocate resources judiciously could create gaps within the United States maritime infrastructure defense. Exposed gaps have the potential to become prime targets for terrorists and may result in loss of life and/or devastating economic ramifications. The Coast Guard must find a way to make the best choices to ensure mission success.

B. INFRASTRUCTURE DEFENSE

The National Infrastructure Protection Plan (NIPP) is a guiding framework for protecting the United States Critical Infrastructure and Key Resources (CI/KR). "The overarching goal of the NIPP is to build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our nation's CI/KR and to strengthen national preparedness, timely response, and rapid recovery of CI/KR in the event of an attack, natural disaster, or other emergency" (NIPP, 2009).

The NIPP defines critical infrastructure as "the assets, systems, and networks whether physical or virtual, so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or a combination thereof" (NIPP, 2009). There are currently 18 CI/KRs designated in the NIPP (e.g., Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities). The NIPP includes all hazards and consists of two prongs. The first objective is to mitigate vulnerabilities by increasing resilience of structural and operational systems and improving medical preparedness. The second objective is to reduce consequences by increasing recovery and response actions in the wake of an attack, whether it is natural or deliberate.

The cornerstone of the NIPP is its risk management. Risk assessment is an important means of prioritizing mitigation efforts, and NIPP risk management enables

risk-informed decisions to protect CI/KR. "This framework is applicable to threats such as natural disasters, manmade safety hazards, and terrorism, although different information and methodologies may be used to understand each" (NIPP, 2009). In general, NIPP addresses *risk* as a function of *Threat (T), Vulnerability (V), and Consequences (C):*

$$Risk = f(T, V, C).$$

We will refer to models of this type as "TVC" models. The USCG, as an agency of DHS, operates under the guidance of NIPP. Accordingly, the Coast Guard uses a TVC model called Maritime Security Risk Analysis Model (MSRAM) as a decision tool for many of its missions to include PWCS (USCG, 2010). We review TVC models, including MSRAM, in Chapter II.

The application of risk-based techniques to the study of infrastructure defense as applied to the PWCS mission would seem to follow naturally from the use of risk to study non-deliberate hazards. Risk-based techniques model the potential for loss from the perspective of a single decision-maker. *Risk assessment* is the process of quantifying the potential loss, while *risk management* is about taking action to mitigate those potential losses. A fundamental question is if and how the potential losses change with mitigation efforts.

From 2000 to 2010 there has been considerable debate as to how best to account for uncertainty in the defense of CI/KR. Risk-based techniques work for non-deliberate hazards, such as industrial safety programs, finance, insurance, and engineering. However, the National Research Council (NRC) has criticized the use of risk-based techniques, and TVC models in particular, when assessing the potential consequences due to terrorism (NRC 2008, NRC 2010). At the heart of this criticism is a recognized need to model the decisions of both the attacker and the defender. *Game theory* has been proposed as an alternate technique for modeling these adversarial interactions, with specific application to *randomized patrolling* and *system interdiction.* We discuss these models in Chapter III.

C. CONTRIBUTIONS OF THESIS

The objective of this thesis is to explore the problem space of PWCS and infrastructure defense, look at examples of the different methods currently being applied, and review the assumptions necessary to make these methods applicable. We analyze the pros and cons of risk-based and game theoretic techniques. We focus on the role and responsibilities of the United States Coast Guard as a major decision maker in protecting CI/KR within the ports, waterways, and coastal areas of the United States.

Optimizing limited resources to provide maximum protection from deliberate attacks can be highly complex. In the way mariners require a navigation chart to safely plot a course to the desired destination, decision makers also need guidance in sorting through the many alternatives and constraints to meet their objectives optimally. Quantitative analysis can help provide key insight, but using quantitative analysis correctly can be tricky. Complicated mathematical models may distance the decision maker from actual input factors and the true meaning of the results produced. Ultimately, understanding when and how to use different models will lead to improved decision making and not merely the perception of better decision making.

II. RISKED BASED TECHNIQUES WITH EMPHASIS ON PROBABILISTIC RISK ANALYSIS

A. ABREVIATED HISTORY OF RISK

1. Origin of Risk Analysis

Bernstein (1996, p. 90) observes that risk analysis has its origins in the 1600s when the flow of commerce began to move trans-oceanic. As trade demands increased so did the number of ships making the inherently dangerous voyages across the ocean. Due to the limited technology and emergence of piracy, a significant number of ships did not complete their voyage to deliver goods to their destinations. In London, England, Edward Lloyd created a list of scheduled shipments with prospective intelligence on conditions abroad and at sea. With information available, merchants and ship captains could determine if they wanted to take the risk of voyage. The concept of *insurance* was developed to keep commerce flow moving. Merchants would pay third parties a nominal amount to receive reimbursement for losses of merchandise experienced during the shipment. One-person insurance operators at the time became known as *underwriters*, and in order to ensure that money could be made, the underwriters had to analyze the odds for insuring the risk taker.

Simultaneously, the desire to quantify personal risk came to the forefront of mathematics. These factors led to the development of probability theory. Insurers began using probabilities to conduct risk analysis to make decisions (e.g., Bernstein, 1996, pp. 89–91). Since then, insurance companies have been flourishing, using a disciplined risk analysis approach known today as actuarial science (e.g., Hubbard, 2009, p. 59).

Actuarial science was perhaps the first quantitative risk assessment technique. Taking a closer look, this kind of assessment can be broken down into two elements:

1. Consequences: Magnitude and/or severity
2. Likelihood: Probability of occurrence of each consequence

Because the word “risk” can be used in many contexts, it is difficult to define precisely, and even more challenging to represent mathematically. As defined by DHS,

risk is "the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences" (DHS, 2010).

2. Probabilistic Risk Analysis

Probabilistic Risk Analysis (PRA) evaluates and quantifies risks associated with complex systems. Kaplan and Garrick (1981) introduce the following questions for discussing risk:

1. What can go wrong?
2. How likely is it that it will happen?
3. If it does happen, what are the consequences?

Collectively, the {scenario, likelihood, consequence} answers form a "triplet" that can be used to assess risk. All PRA models use elements of likelihood and consequence, where likelihood is typically derived from the observation of frequency or by subjective evaluation from subject matter experts.

In the 1960s and 1970s, industries began to focus on reducing risk to improve efficiency and safety for workers and the industry (Garrick, 1984). Industries accumulated data on failure rates and hazards which made PRA a natural next step in modeling risk. Rasmussen (1976) concludes that PRA can be an appropriate and useful tool when constructing safeguards in the nuclear power industry; this led to the Nuclear Regulatory Commission implementing a "PRA Procedures Guide" in 1983 (Nuclear Regulatory Commission, 2011). Other safety programs, including one in the airline industry, began using PRA to assess risk (GAIN, 2003). PRA became a popular tool in engineering to help predict system and component failure due to predicted life cycle lengths and random events.

By the mid-1980s, probabilistic risk-based techniques were prevalent in insurance, finance, and engineering.

B. QUANTITATIVE MEASURES OF RISK

To understand the mathematics of PRA, we will look at a single binary model, where we introduce some basic notation that is used in this thesis. Then, we look at some qualitative properties of PRA under multiple scenarios.

1. Risk as Expected Loss

Let *X* be a random variable representing the loss that we incur in an uncertain future. If the future has discrete outcomes, then *X* is a discrete random variable.

The simplest case is where *X* takes on two possible outcomes, a value $C > 0$ or 0, with probabilities:

$$prob\{X = C\} = p \quad \text{and}$$

$$prob\{X = 0\} = 1 - p.$$

The expected value of *X* is therefore:

$$E\{X\} = p \times C \ + (1 - p) \times 0.$$

Because the second term is zero, this is equivalent to:

$$E\{X\} = p \times C.$$

In words, the expected loss is equal to "probability times consequence."

This definition extends naturally to multiple outcomes. Let $i = 1, 2, 3, \dots, N$ index the possible future outcomes. Let p_i represent the probability that outcome *i* occurs, with $\sum_{i=1}^{N} p_i = 1$. In other words, these outcomes are mutually exclusive and exhaustive. Let C_i represent the consequence associated with outcome i. The expected loss is now:

$$E\{X\} = \sum_{i=1}^{N} p_i \times C_i.$$

Again, we can compute the expected loss according to "probability times consequence."

2. Risk Curves

The expected loss across multiple scenarios is consistent with the notion of "triplets" introduced by Kaplan and Garrick (1981). In review, the idea is to characterize the uncertain future in terms of $\{scenario, likelihood, consequence\}$ triplets that collectively answer the questions: What can go wrong? How likely is it to happen? What are the consequences if it does?

Kaplan and Garrick (1981) argue that probabilistic risk is a function of the entire probability distribution and not just a point estimate given by the expected value. They observe, "a single number is not a big enough concept to communicate risk. It takes a whole curve, or actually a family of curves, to communicate the idea of risk." Kaplan & Garrick (1981) propose the use of a *risk curve* to represent the entire probability distribution. More specifically, they define a risk curve by $Prob\{X \geq a\}$ for all values $a \geq 0$. Thus, a risk curve is the complementary cumulative distribution function (CCDF) of the random variable *X*.

We review a simplified example that demonstrates how risk curves can change with scenarios and how a mean value estimate does not reveal the overall risks. Some of the possible non-deliberate hazards the USCG must contend with in waterways and coastal regions include "collisions, allisions, and groundings" (USCG, 2008). Here we focus on *vessel groundings* and *vessel collisions*. Assuming these hazards are non-deliberate each can be caused by human error, environmental conditions, mechanical failure, or a combination thereof. The possible losses from each hazard include life, environmental pollution, waterway closure, and economic impacts.

We start our example by producing a risk curve for vessel groundings. Consider the notional data in Table 1, which provides hypothetical assessments of damages incurred from vessel groundings. Table 2 shows a notional assessment for damages incurred from vessel collisions. Assume that subject matter experts have assessed a probability of occurrence for each possible level of consequence. Then we can produce a

risk curve that shows the losses over a range of scenarios. We plot the complementary cumulative probability for the varying order of consequences. Figure 1 is the risk curve for vessel groundings.

	Consequence ($K)	Probability	CCDF
Vessel Grounding	0	0.05	1
	10	0.05	0.95
	20	0.1	0.9
	30	0.2	0.8
	40	0.3	0.6
	50	0.3	0.3
	Expected loss:	$35.5K	

Table 1. Notional Risk of Vessel Groundings

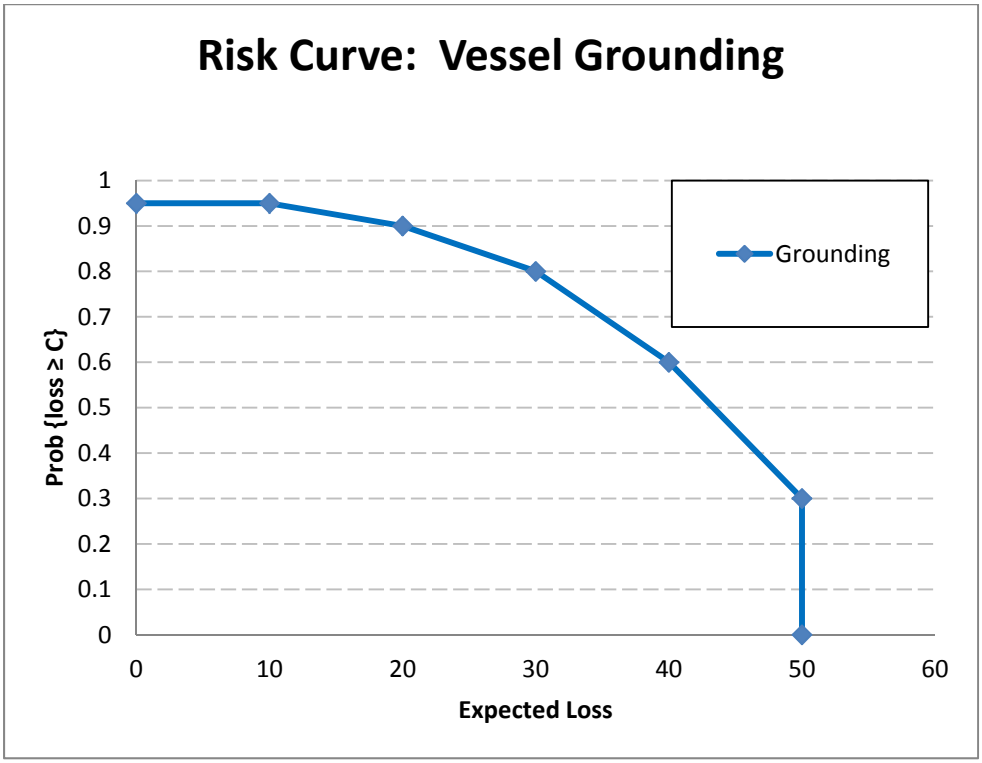

Figure 1. Risk Curve for Vessel Grounding. Each point represents the complementary cumulative probability of expected loss. For example, this curve shows that there is an 80% probability of a loss that is at least $30K.

Figure 2 compares the risk curves of vessel groundings and vessel collisions on one chart, thus showing how the two risk curves vary with scenarios and comparing total expected damage as functions of probability of occurrence.

	Consequence ($K)	Probability	CCDF
Vessel Collision	0	0.235	1
	10	0.035	0.765
	20	0.05	0.73
	30	0.13	0.68
	40	0.1	0.55
	50	0.2	0.45
	65	0.25	0.25
	Expected loss:	$35.5K	

Table 2. Notional Risk of Vessel Collisions

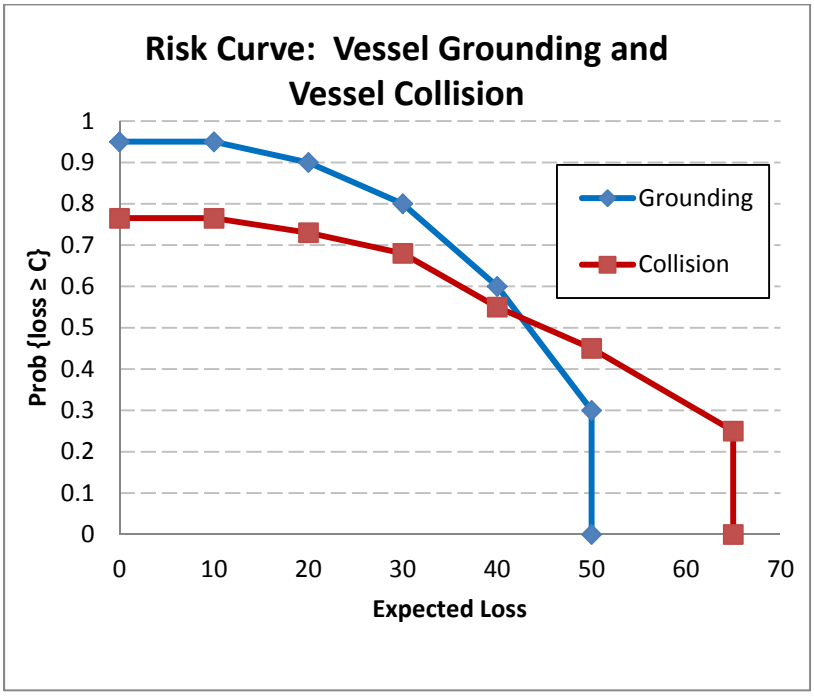

Figure 2. Notional Risk Curves for Groundings and Collisions

Risk is often quantified as a point estimate according to the expected loss as $E\{C\}$. In our nominal example, we face an expected loss of \$35.5K for both vessel groundings and vessel collisions. In expectation, the risks are equal, but the curves in Figure 2 clearly show that the overall risks are not the same. There is a 75% probability of a non-zero loss from vessel collision while there a 95% probability of non-zero loss from a grounding event. Figure 2 also shows that vessel grounding has a probability of 0.71 of exceeding the expected loss while vessel collision has only a 0.62 probability of exceeding the expected loss. We could interpret this to mean a vessel grounding event is a higher risk than a collision event. But, we also observe that a vessel collision event results in greater consequences when an event does occur. Though risk curves present useful information, the use of probabilistic risk does not make it clear how to compare risks.

Risk curves can be viewed across multiple categories and scenarios; a risk curve generalizes to a risk surface with much more information available to the decision maker than a single expected value (Kaplan & Garrick, 1981). These concepts commonly appear in other forms of PRA used in industrial safety and engineering programs.

3. Event Trees

Event trees provide a graphical depiction of random outcomes, and are frequently used in PRA models (e.g., Parnell, 2008). An *event tree* represents a sequence of random variables, called *events*. We represent each event visually using a *node*. Each random-event branching node is followed by the possible random-variable realizations, called *outcomes*, with an arc leading from the branching, predecessor node, to the next, successor-event node. The path from the root to a particular leaf is called a *scenario*. Under the assumption that each event is independent, the probability that a specific path is taken is the probability the scenario occurs, and it is calculated by the product of each condition met along the scenario path. Figure 3 shows a simple example of an event tree using the vessel grounding data from Table 1.

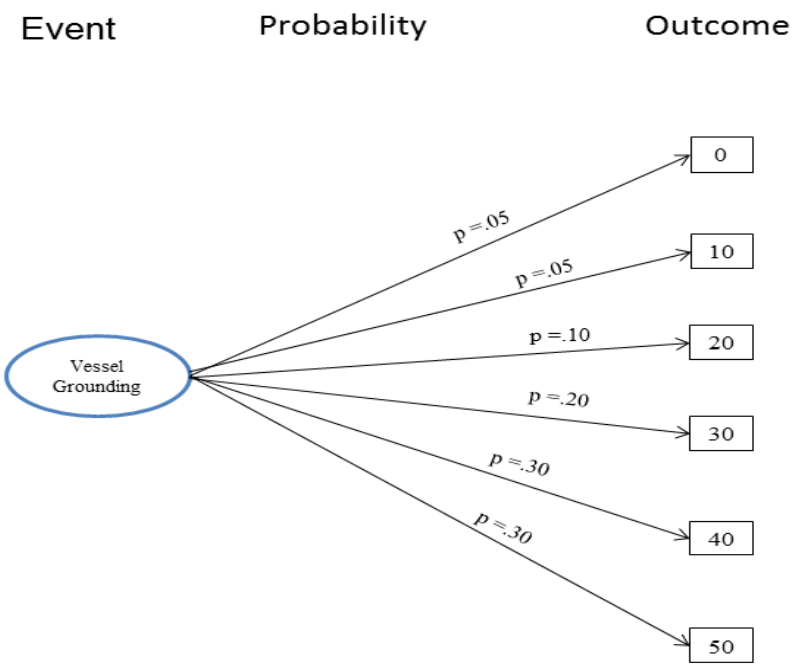

Figure 3. Event Tree for Vessel Grounding

The event tree is a simple form that can show the respective probabilities of different events that can occur. *Decision trees* are formatted in the same way as event trees, but have an additional type of node called a *decision node* where a decision maker can choose which branch to follow. In a decision tree, a decision maker can influence the path from the root node to the leaf node, in order to seek a specific outcome.

C. RISK MANAGEMENT

DHS defines risk management as the "process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost" (DHS, 2010). The primary goal of risk management is to reduce or eliminate risk through mitigation measures intended to avoid or reduce expected loss (DHS, 2010). Hubbard (2009) discusses many different ways to manage risk; we focus on probabilistic risk analysis modeling. Techniques like PRA are useful for managing risk by producing quantifiable risk values, enabling a decision maker to manage risks by comparing risk values.

1. Priority Ranking of Risks

One method for managing risks is to quantify all known risks according to their expected loss, and then order them in a prioritized list. To construct a prioritized risk ranking of different events, decision makers must assess the events using a common form of measure, such as money. To fully assess and compare risks, intangible costs are translated into quantified values. The cost of a human life and psychological effects from a significant event are two examples of costs that are subject to interpretation. With a common mode of measure, all scenarios and missions can be compared relative to each other.

Given a priority ranking, the decision maker may choose to apply resources to mitigate the highest ranked risk first and then work down the prioritized list depending on resource availability (Cox, 2009, p. 357).

2. Risk Scoring Techniques

A common approach to risk management is to use *risk scores*. A risk score is a discrete numerical value that has been converted from a continuous probability of an associated risk (Hubbard, 2009, pp. 118–122). Risk scores allow decision makers to quickly review and manage the risks in a format that is understood by the organization (Hubbard, 2009, p. 120). Risks from multiple scenarios and missions are set to the same scale and mode of measure as specified by the scoring format being used. As priority ranking produces relative comparison, risk scoring techniques are used to provide absolute comparisons.

One idea of risk scores is to convert probability and consequence numbers to ordinal scales. For example, risks may be converted from expected loss value to a scale that ranks it from one to five. A risk matrix is a common form to display risks on an ordinal scale (Cox, 2008a). With risks presented in a simplified numerical format, the decision maker can manage risks by directly comparing ordinal numbers. The decision maker may set a threshold number that is a “go” or “no go” for the risk being assessed. Another technique frequently used is to define ranges of risk scores (e.g., risk score

ranges may be defined as green=0–10, yellow=11–15, and red=16–20). The decision maker will take certain action depending on what range the risk score falls into.

The USCG uses PRA to form Risk Index Numbers (RIN) (USCG, 2010). The RIN for the USCG is a basic unit of risk that represents an expected loss of $1 million dollars over the course of a year (USCG, 2010, p. 9). RINs are used as a common risk currency between all missions with measurable consequences. In this way, for example, the USCG can compare risks of drug trafficking to those of terrorism and focus their resources accordingly. Operational assets in the USCG utilize color-coded risk score cards called Green-Amber-Red (GAR) to assess risks before conducting a specific mission. RINs are used for long term planning while GAR assessments are used for daily mission planning.

3. Cost Effectiveness of Risk Management

Risk-based approaches can track cost effectiveness for risk mitigation efforts (Dillon, Liebe, & Bestafka, 2009). Conducting repeated assessments shows the changes in risk scores, which can be compared to the costs of the mitigating actions applied since previous assessments. "MSRAM assessments are conducted annually and provide important components of the USCG's biennial National Maritime Strategic Risk Assessment (NMSRA)" (USCG, 2008b). The USCG uses the MSRAM tool to determine RINs to measure cost effectiveness of policies and mitigating actions implemented the previous year by reviewing the change in RINs (GAO, 2011).

4. Pitfalls in Risk Scoring

Risk scoring presents numerous challenges to accuracy and in some cases can lead to the mismanagement of risks (Hubbard, 2009, pgs 122–123). Risk values that are derived by subject matter experts vice those obtained through historical data will be affected by (Hubbard, 2009, pp. 95–123):

(1) Risk preferences. Is the subject matter expert risk neutral, risk adverse, or risk preferred?

(2) Failure of experience. Assessments made by human opinion will be swayed by personal experience leading to unconscious heuristics and subject preferences.

(3) Failure of interpretation. Undefined subjectivity leads to varying interpretation between subject matter experts. Lack of precise language leads to varying transformations from verbal assessments (i.e., strong possibility) to quantifiable value assessments (i.e., probability of 0.7) .

(4) Emotional attachment to a cause.

(5) Overconfidence or lack of confidence.

(6) Tendency to assign extreme score values to those risks being evaluated last.

Outside this human element, transforming risk values to a specified risk scoring format presents numerous mathematical deficiencies (Hubbard, 2009, p. 122). Conversions of risk values to an ordinal scale causes range value compression, by requiring rounding off to get whole numbers within the desired scale. Components within a discrete risk score can have distinct risk priorities before conversion and then be equal when analyzed on a discrete ordinal scale. For example, assume risk values are converted to a risk score of 1 to 5. One scenario evaluates to 2.9 and another scenario evaluates to 3.3, but to fit in the risk score format, both conditions are converted to 3, losing fidelity of assessments.

Any mathematical function applied to risk scores increases the level of inaccuracy and leads to increasingly arbitrary values (Hubbard, 2009, p. 124). Risk score values that have been compressed no longer have the same arithmetic properties. If adding risk scores together, the risk value conversion must be accounted for, else the results are drastically different than the true assessments (Hubbard, 2009, p. 130).

D. TERRORISM RISK

1. History

The terrorist attacks on the United States on September 11, 2001, shifted attention to modeling deliberate attacks by terrorists and prompted the President to form the

Department of Homeland Security. The newly formed DHS began looking at quantifiable methods to assess risk. In the last decade, leaders and analysts have made significant efforts to quantify the risks of terrorism and determine the cost effectiveness of the policies used to combat those risks (Ezell et al., 2010).

Pate-Cornell and Guikema (2002) present the idea that probability of damage from terrorist attacks can be assessed the same way as probability of damage from a non-deliberate hazard. "Given the scarcity of the experience base regarding terrorist attacks in the present context, the emphasis is on the model's reasoning and structure rather than on the numerical values" (Pate-Cornell & Guikema, 2002). For example, under direction from the Coast Guard Maritime Security and Response Manual (MSRO), the USCG conducts annual assessments of risk involving a water-born IED terrorist attack in major U.S. ports. To date, there has never been a terrorist attack in a U.S. port using water-born IEDs. With no historical data available, the USCG solicits opinions from subject matter experts to estimate probabilities of attack. In general, to conduct probabilistic modeling of terrorist attacks where there is very limited historical data, the only option is to analyze the current terrorist threat to estimate the probability of damage.

In 2002 the U.S. Congress asked the American Society of Mechanical Engineers (ASME) to assist the DHS in developing a method to assess and manage the threat of terrorism in the United States (ASME, 2011). In response, the ASME founded the Innovative Technologies Institute (ITI). ITI produced the Risk Analysis and Management for Critical Asset Protection (RAMCAP) to assess the nation's critical infrastructure to determine how to best focus efforts and resources to protect the United States from future terrorist attacks (ASME, 2011). RAMCAP was one of the first analysis models to use TVC to quantify terrorism risk.

In 2006, DHS established the National Infrastructure Protection Plan. The NIPP provides guidance for all DHS entities to analyze terrorism risk using threat, vulnerability, and consequence assessments (NIPP, 2009). With the NIPP as its guidance, the Coast Guard developed an asset-level decision tool called Maritime Security Risk Analysis Model (MSRAM) (USCG, 2010).

In a TVC model, a risk scenario is typically characterized by the probability that a specific target is attacked in a specific way during a specified time period (NIPP, 2009). Due to uncertainties, threat can be represented as a probability (that an attack occurs) as a single point estimate, or with a probability distribution (Willis, 2007). Vulnerability is measured by the probability that an "asset, system, network, or entity is susceptible to disruption, destruction, or exploitation" (DHS 2010). "Consequence is the magnitude and type of damage resulting from successful terrorist attacks" (Willis, 2007). A TVC model assesses an expected loss value. Greater expected losses equate to higher risk values.

2. Mathematical Representation of Terrorism Risk

Recall our previous definition of risk as expected loss: $Risk = \sum_i p_i C_i$.

The common form of terrorism risk as championed in the NIPP is:

$$Risk = f(T, V, C).$$

The TVC model was derived mathematically by using probability theory. One method to determine p_i for terrorism risk is to separate it into two separate probabilities, the probability that an attack occurs, and the conditional probability that an attack causes damage (Willis, 2007). The probability of attack can be based on the attacker's objectives, constraints, capabilities, etc. The probability that an attack causes damage can include assessments of the target's resilience, the means of attack, countermeasures in place, etc. Using Bayes Theorem, terrorism risk can be expressed as (Willis 2007):

$$Risk = Prob\,\{attack\} \times Prob\{damage|attack\} \times E[damage|damaging\ attack].$$

Under the assumption that threat, vulnerability, and consequence are independent, the terrorism risk function can be written:

$$Risk = Prob\,\{attack\} \times Prob\,\{damage\} \times E[damage].$$

By the definitions under the DHS lexicon, terrorism risk can be rewritten as:

$$Risk = Threat \times Vulnerability \times Consequence.$$

3. Currently Used TVC models

RAMCAP is on its third iteration, remaining an overarching model for defense of critical infrastructure from terrorist attacks and all non-deliberate hazards (ASME, 2011). RAMCAP was initially created to assist the DHS in terrorism risk analysis but has been expanded to all hazards to help government and commercial industries to manage all types of risk (ASME, 2011).

MSRAM is designed to analyze terrorism risk specific to the Coast Guard's area of responsibilities. Where RAMCAP was intended to have a broader overarching analysis, MSRAM is intended to be utilized at the operational asset level. USCG operational units complete annual MSRAM assessments at which time field experts input new values for threat, vulnerability, and consequences for all CI/KR within the Coast Guard's operational domain. The USCG uses MSRAM to review current mission responsibilities and prioritize areas of focus (USCG, 2010).

The Antiterrorism Risk Based Decision Aid (ARDA) model was developed to assess investments for protecting U.S. Navy assets, and "determine whether the most effective anti-terrorism alternatives are being used to reduce the risk to the facilities and war-fighting assets" (Dillon, Liebe, & Bestafka, 2009). ARDA introduces value preference trade-offs in the PRA model in the form of a risk utility function (Dillon, Liebe, & Bestafka, 2009). A utility function will place a higher risk value on assets that are more important to the decision maker. Under the ARDA model, specific risk with a probability p and consequence C can be represented as:

$$Risk = p \times u(C).$$

Using a multi-attribute utility analysis, ARDA allows for input into risk preferences. A risk matrix is built with utility of consequences that can be multiplied by the probability of a linear scenario. ARDA looks to integrate a utility function with the Department of Defense more granular approach to assess vulnerability, called Detection-Assess-Warn-Defend-Recover (DAWDR) (Dillon et al., 2009).

E. CRITICISM OF THE TVC MODEL

In the past decade, the TVC models for terrorism analysis have gained considerable momentum. While there are many who have contributed notable refinements to this terrorism risk assessment, there have also been many who have noted significant deficiencies in the concepts of terrorism risk.

The National Academy of Sciences is a non-profit society of distinguished scholars dedicated to improving scientific and engineering research for the general welfare. In 2006, the U.S. Congress asked the National Research Council (NRC) of the National Academies to review DHS's TVC risk analysis used in Biological Terror Risk Analysis (BTRA). NRC reported concerns about "mathematical and statistical mistakes, unnecessarily complicated probability models, and models with fidelity far exceeding existing data" (NRC, 2008).

Following the NRC's 2008 BTRA report, the U.S. Congress asked that the NRC conduct a review of all the activities of DHS related to risk analysis (NRC, 2010). In the 2010 report, the NRC noted "many weaknesses in risk analysis, modeling of intelligent agents, consequence assessment, and presentation of assessment results that make the results problematic even for assessing a single agent threat." In short, the NRC concludes that *Risk = f(TVC)* is adequate for analysis of natural hazards but is not yet validated for analysis of terrorism, and the formula may not be on the "correct trajectory to ensure reliable risk analyses" (NRC, 2010).

The concerns of terrorism risk analysis are essentially philosophical, practical, and mathematical. We review these deficiencies in some detail.

1. Assumption that Terrorists Act Randomly

In his original work on nuclear safety, Rasmussen (1976), states that in order for PRA to be valid, we must assume that failures are basically random in nature. With the assumption of a random attack we can use an appropriate mathematical combination of known attack rates (Rasmussen, 1976). However, Rasmussen also notes that "in the case of deliberate human action, as in imagined diversion scenarios, such an assumption is surely not valid" (Rasmussen, 1976).

Using probabilistic analysis for terrorism implies that an attacker acts as a random variable according to a fixed probability distribution. However, we know that an intelligent adversary can launch an attack when timing and conditions are optimal, thus maximizing expected damage. Modeling an attacker as a random variable produces an estimated mean for vulnerability and consequence. An estimated mean will not reflect an attacker who waits until conditions are optimal, because the "optimal" conditions as viewed by the attacker are often different from the "normal" conditions reflected in the mean (Cox, 2008b).

In TVC models, probabilities assigned to threat scenarios are static in nature. However, attackers can alter their intent as more information becomes available to them. For example, assume there are three conditions that must be met before a terrorist attempts an attack. The attack is assessed by the defender at given probability before the attacker sees any of the conditions met. An attacker's probability of success prior to the conditions being met is 0.2 but after conditions 1 and 2 are met the probability of success is 0.7 and after condition 3 is met the probability of success increases to 0.9. As each condition is met the attacker's intention to conduct the attack increases significantly. Static probabilities do not account for the attacker's learning curve or changing conditions.

Terrorism risk analysis assigns probabilities to attacks without accounting for the decision process of the attacker. Some models, such as MSRAM, update estimates annually, which does not account for what the attacker learns over the course of that time period. If a resource is invested properly to defend an asset, the attacker may no longer intend to attack that asset which changes the probability of attack (Cox, 2008b). If the attacker knows what is being defended then the attacker will not act as a random variable and thus expected loss calculations will be incorrect (Cox, 2008b).

2. Insufficient Methods for Predicting the Attacker

Probabilistic analysis often uses historical data to derive probabilities through regression analysis. In the case of PRA, where historical data is not available, attempting

to solve probabilities through regression will result in over-fitting, producing results that are useless for real world applications (Brown & Cox, 2011).

Cox (2008b) states that trying to assess probabilities for intelligent adversaries who adaptively pursue their goals as information and experience change, can produce mistaken risk estimates. A prioritized risk scheme could be learned by the attacker, influencing the attacker's decisions, which may change the probabilities or may result in a self-fulfilling prediction by the defender (Brown & Cox, 2011).

Threat probabilities derived by the defender can be different from the probabilities the attacker eventually acts upon (Brown & Cox, 2011). Even when defender experts give unbiased probability estimates based on viable intelligence, the attacker's decision tree is conditioned on different information (Brown & Cox, 2011). "Intelligence analysts cannot condition on knowledge that they do not have" (Brown & Cox, 2011). Attack probabilities actually depend on what the attacker knows or believes and not on what the defender knows or believes. The key issue is that we don't know what decision strategy the attacker is using, and the threat and vulnerability probabilistic assessment by the defender could be misleading (Brown & Cox, 2011).

The RAMCAP notion of threat is based on intention and capability of an adversary to undertake actions that would be detrimental to an asset or population (ASME, 2011). This calculation may be valid if we know who the adversaries are and we know their intentions. Assuming we know who all the adversaries are, determining the adversaries' capabilities requires a constant game of cat and mouse. Our best efforts may not reveal the adversaries' capacities and intentions entirely. In practice, we don't know who all of our adversaries are. We don't know the information the adversary has against us. The magnitude of uncertainty about the attacker makes probability estimates grossly inaccurate. The following example shows how an attacker's strategy produces different results from the defender's prioritized risk values. Figure 4 is a decision tree that represents three targets that are being assessed for possible attack.

- Let Targets A, B, and C be assets the defender wants to protect and a potential adversary wants to attack.

- Consider two different attackers. Attacker 1 is patient and well trained. Attacker 1 will wait until the optimal moment to complete the tasks and will choose the target with the highest probability of success. Attacker 2 has less experience and desires to cause the maximum amount of damage.
- The probability of a successful attack is equivalent to $T \times V$. The defender completes assessments for each target.
- Assume the defender correctly estimates likelihood of attack for Targets A and B.
- Assume Attacker 1 knows something about Target C that the defender does not know, giving a different assessment of the probability of success for attacking of Target C.

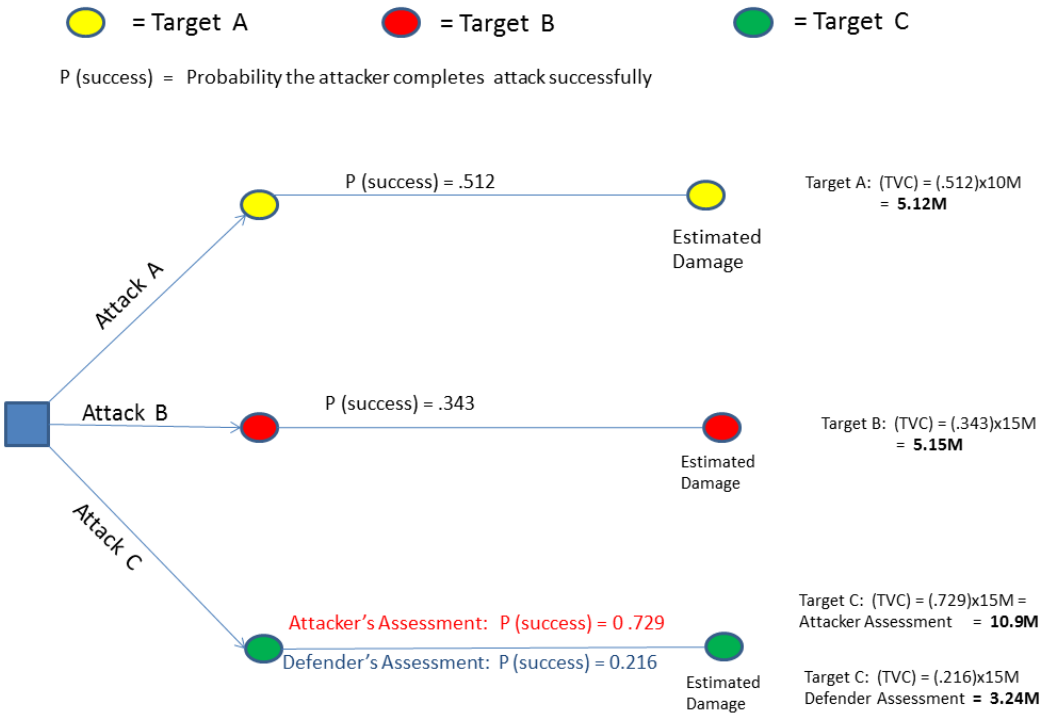

Figure 4. Example Attacker and Defender Prioritization

Even in this simple example, we observe inconsistency in the perspective of these players.

- Defender prioritizes defending targets by risk values from highest to lowest as:

  1. Target B 2. Target A 3. Target C

- Attacker 1 prioritizes Target attacks by best probability of success as:

1. Target C 2. Target A 3. Target B

- Attacker 2 prioritizes Target attacks by maximum damage as:

1. Target B 2. Target C 3. Target A

From this simple example, the assumption that we know the decision process and capabilities of the adversary misleads us in the priority of targets we decide to defend. Under the TVC model, Target B receives the highest risk value. The defender allocates additional patrol assets to Target B. Attacker 1 determines Target C is the softest target and chooses to attack C. Attacker 2 chooses the target with the greatest estimated damage therefore prioritizes Target C above Target A.

3. TVC Models Fail Established Mathematical Principles and Axioms

Cox (2008b) discusses fundamental limitations of the Risk = *f(TVC)* formula: "These limitations include the model's failure to adjust for correlations among its components, non-additivity of risks estimated using the formula, inability to use risk-scoring results to optimally allocate defensive resources, and intrinsic subjectivity and ambiguity of Threat, Vulnerability, and Consequence numbers."

(Cox, 2008b) demonstrates how TVC, such as RAMCAP can reverse the prioritization of risks by attempting to average an upper and lower bound for vulnerability and consequence. The following is an example of this violation (Cox, 2008b):

Target A: (Vulnerability = .25, Consequence = $400M)

Target B: (Vulnerability = 1, Consequence = $60M)

Conditional Risk = V ×C

Target A = ($100M) Target B = $60M

If we know the precise probability for the vulnerability, we see that Target A is a higher risk than Target B. But suppose we have uncertainty about the values of vulnerability and consequence. RAMCAP dictates that we introduce upper and lower bounds then use a uniform distribution to find a mean value. For example,

Target A = ((.25 + .125)/2) × (400+200)/2) = $56.25M

Target B = ((.9+1)/2) × (50+100)/2) = $71.25M

Now Target B is a higher risk than Target A. The two targets' priorities have been reversed due to an attempt to average uncertain vulnerability and consequence values.

Lowder (2010) discusses how TVC as used by the Department of Energy violates probability calculus axioms. Most notably, in order for TVC to be a correct mathematical expression, independence must be established between each probability. The assumption of independence of threat, vulnerability, and consequence indicates that the attacker makes a decision to attack a target without consideration to success or impact. Yet threat is calculated by assessing an adversary's intent and capabilities. Unless the attacker's intentions are explicitly demonstrated through statements or intelligence, we are forced to assess his intentions according to our value system. The defender values targets that are considered vulnerable and/or carry a significant consequence. Innately, these parameters are going to creep into any assessment of threat that is made. This indicates that the threat assessment is conditioned on the defender's vulnerability and consequence values of the asset being defended. The axiom of probability independence is violated, meaning:

$$Risk = Prob\{attack\} \times Prob\{damage\} \times E[damage] \neq T \times V \times C$$

By the assumption of independence, the risk calculation neglects to account for covariance. Cox (2008b) presents the following simple example.

Assume T=0.5, V=0.5, and C=0.5. Assuming independence, then risk as calculated by TVC equals 0.125. If we assume perfectly positively correlated threat values where T=C and T=V, then the expected value of their product is 0.5 not 0.125. Likewise, if threat values are perfectly negatively correlated then T=C and V=1-C, then the expected value of TVC equals 0. Dependencies among the components could produce results ranging from 0 to 0.5, which may be significantly different than the independent calculation of 0.125. TVC models may easily overshoot or undershoot actual values based on correlations not being accounted for (Cox, 2008b).

TVC models can fail when assessing scenarios with low probabilities and high consequences (Dillon et al., 2009). If a consequence is large, any minor change in the probability can greatly change its risk score and its place on a prioritized ranking.

4. TVC Models are Disconnected from Management Actions

Priority ranking from PRA may not support effective resource allocation due to budget constraints (Cox, 2008b). Terrorism risk models are frequently used to develop prioritized actions based on risk scores. To reduce the maximum amount of risk possible, risk managers will try to implement measures to reduce the highest risk scores. Budget constraints may limit the possible mitigation strategies. The limitations could prevent the optimal cost effectiveness for risk reduction.

Cox (2008b) presents the following example:

A defender considers implementing countermeasures to reduce risk. The defender is presented with the following:

- Countermeasure A reduces expected loss by $20 per year, and costs defender $3.
- Countermeasure B reduces expected loss by $25 per year, and costs defender $2.
- Countermeasure C reduces expected loss by $40 per year, and costs defender $4.

Implementation of countermeasures may be limited by budget constraints. We consider budgets of $3, $4, $5, $6, and $9. If the defender has a budget of only $3, then he can afford only B. Given a budget of $4, the defender is better off choosing C. But with a budget of $5 the defender can achieve the best results by picking A and B. Table 3 shows the solutions for all budget considerations to our example problem.

b	A	B	C
$3		1	
$4			1
$5	1	1	
$6		1	1
$9	1	1	1

Table 3. Budget driven countermeasure example (From Cox 2008b). The optimal combination of defensive investments depends on the budget available to invest. A "greedy" investment strategy based on a prioritized list of investments leads to inefficient use of resources.

The budget sensitive countermeasure example presented in Cox (2008b) shows us "that no evaluation of risk-reducing options can allocate resources effectively without considering budget (and other) dependencies" (Cox (2008b). In other words using prioritized ranking or other risk scores to implement countermeasures may lead to inefficient cost effectiveness.

Risk scores used for risk management can give the decision maker an idea of relative importance, but the representational numbers are often arbitrary. For instance, what does it mean to reduce a risk score from 80 to 70? A change in scores may indicate a cause and effect from the decisions made, but it doesn't tell the decision maker anything about what is built into those scores or how to specifically address them. In other words, risk scores can distance the decision maker from understanding the real problem.

F. SUMMARY OF CONCERNS FOR TERRORISM APPLICATIONS

There are many challenges in determining accurate values for risk analysis calculations as discussed in Hubbard (2009). Historical data is generally used to derive and support probability values in other uses of PRA, but there is not sufficient historical data available to derive probabilities for terrorist attacks. Currently available terrorism risk analysis techniques typically require the following assumptions:

(1) The attacker only knows what the defender knows,

(2) Threat, Vulnerability, and Consequence are independent components, and

(3) The attacker's decision process is the same as the defender's decision process.

These assumptions are difficult if not impossible to validate. If the assumptions are inaccurate, then allocating resources based on risk values could lead to poor use of resources.

There are known deficiencies with terrorism risk analysis and TVC models in particular, but what else can be done? Brown et al. (2005), Cox (2008b), NRC (2010) and others suggest the use of game theory models as an alternative. We discuss game theoretical techniques in Chapter III.

THIS PAGE INTENTIONALLY LEFT BLANK

III. GAME THEORY

With proper structuring and careful analysis, game theory can be a powerful tool for solving complex real-world problems. Game theory has many applications, but we narrow our focus to key concepts used to solve security games of infrastructure defense between a defender and an attacker.

A. BACKGROUND OF GAME THEORY

1. Basic Concepts

A *game* is essentially any situation with the following components (Straffin 2006, p. 3):

1. At least two *players*. A player may be an individual or general entity such as a company, nation, or group.
2. Each player has a number of possible *strategies*, each representing a course of action that the player may choose.
3. Strategies chosen by each player determine the *outcome* of the game.
4. Each game outcome has a collection of numerical *payoffs*, one to each player. Payoffs represent the value of the game outcome to the different players.

Some games are influenced by chance and others depend only on the players' actions (Owen 1995, p. 1). The final outcome is determined jointly by the strategies chosen by all of the participating players.

Game theory is a set of concepts aimed at decision making in a competition, conflict, or cooperation. Game theory can be thought of as the study of how players should rationally play games (Straffin 2006, p. 3).

We can model many real-world problems as games and use proven mathematical concepts to determine the optimal strategy for each player. The applications can range from simple parlor games such as poker or chess, to world changing events such as political conflict or war.

In order to apply game theory, we must first determine: (1) what type of game is played, (2) who the players are, and (3) what their respective payoffs are.

a. Payoff Matrices

A game matrix is a common method for representing the payoff structure of the game. The size of the matrix is determined by the number of strategies for each player. One player's strategies make up the rows and the other player's strategies make up the columns. The simplest form of a game involves two players. Player 1 chooses a (row) strategy $i \in \{1,2,3,\ldots.M\}$ and Player 2 chooses (column) strategy $j \in \{1,2,3,\ldots.N\}$. The possible outcomes of the game are then defined by a $M \times N$ size payoff matrix P, whose elements P_{ij} each correspond to a unique combination of strategies by the players.

The payoff matrix in a game is either *zero-sum* or *non-zero-sum*. In zero-sum games, like chess, one player wins the game and the other player loses the game, thus players interests are directly opposed to each other. "A game is zero-sum if and only if, at each terminal vertex, the payoff function is equal to zero. Everything that someone wins must be lost by someone else" (Owen 1995, p.11).

Non-zero-sum games generally mean that the players' payoffs are not directly opposed, therefore concepts such as cooperation, threats, agreements, and betrayal play a role in the outcome.

b. Game Play

One key distinction is whether a game is *sequential,* where players move in turn, or *simultaneous,* where players move at the same time. We can solve sequential games using a "Stackelberg solution" (von Stackelberg, 1948). Simultaneous games can be solved by finding the Nash Equilibrium (Straffin 2006, p. 66).

In general, sequential games are solved by backward induction, using calculus to derive the strategy that produces the optimal outcome. We refer to two sequential players as the leader and the follower. *Stackelberg solutions* optimize the follower's decision variable first then use the results to optimize the leader's decision

variable. For zero-sum games, the leader has a mathematical disadvantage. In contrast, in non-zero-sum games, the leader may have the advantage. If the assumptions and data of a sequential play game are accurate and complete, then the Stackelberg solution will be an equilibrium for the game (Basar & Olsder, 1999).

Simultaneous games can be solved using the "Nash Equilibrium" solution. Each player first looks for a *dominant strategy*, a strategy that always gives him the optimal payoff regardless of any strategy chosen by the other players. If a dominant strategy is not available, the available strategies may produce a *saddle point*. A saddle point is an equilibrium where neither player can achieve a higher payoff when playing an alternative strategy (Owen 1995, p. 12). Saddle points and dominance are considered to be *pure strategies*, where the players have one optimal strategy and always play it. Games that don't have pure strategies have *mixed strategies* (Owen, 1995, p. 13 and 65). Mixed strategies are a set of distinct strategies, where each strategy belonging to the set is played with a given probability (Straffin 2006, p. 13).

In zero-sum games, opposing players desire to keep their strategy secret, however, if the players learn the proportion of strategies that make up the opposing player's mixed strategy, the optimal outcome can still be obtained by playing the strategies in random order (Owen, 1995).

Some games are played only once and therefore called *single-play games*, while other games are played again and again. Knowing if the game is a *repeated game* can affect the optimal strategy for a player.

2. Brief Historical Account

Jon von Neumann published the fundamental theorem of two-person zero-sum games in 1928 (Straffin, 2006). Von Neumann and Oskar Morgenstern began pioneering other game theory concepts, eventually publishing "Theory of Games Economic Behavior" in 1944 (Straffin, 2006). Heirnrich Feiherr von Stackelberg, a German economist, made important game theory contributions in the 1930s and 1940s by modeling leader and follower games, which eventually were termed as *sequential* games (von Stackelberg, 1948). Stackelberg recognized that the leader must account for the

follower's optimal strategy in response to the leader's actions. Stackelberg's game theory concepts have been used in business and economics over the past 50 years, and recently, in the study of security games.

John Nash, an American mathematician and economist, made significant contributions to the study of game theory during the second half of the twentieth century. Most notably, Nash determined that all games have at least one *equilibrium,* a point in the game where if all players make rational choices, no player can do better by choosing an action that does not belong to the equilibrium. In other words, there is at least one stable solution to any game, given that it is set up correctly and assuming all players act rationally.

B. SECURITY PROBLEMS AS GAMES

1. Basic Setup

In security games we have two types of players, *defenders* and *attackers*. We consider two types of security games (1) protection and (2) system interdiction. We distinguish these two types of games by the players' *objectives*. A protection game is a situation where the defender's objective is to protect an asset, system, resource, or other value from possible attacks. A system interdiction game is one in which the defender desires to prevent disruptions to a system of operation.

We present the basic concepts of a security game using the following notional example. Consider a simple zero-sum game between an attacker and defender, where the defender's objectives is to protect two assets from possible attacks.

- Let's consider two infrastructure assets, A and B.
- Let C_A denote the consequence of a 'successful' attack on A. Let C_B denote the consequence of a successful attack on B.
- Assume $C_A > C_B$.
- Assume that an attack on an undefended asset is always successful.
- Assume an attack on a defended asset always fails.

- Assume the defender is limited by resources and can only protect one asset at a time. Likewise, the attacker is limited by resources and can only launch one attack at time.

Figure 5 is the game matrix for our notional protection security game.

		Attacker	
		Attack "A"	Attack "B"
Defender	Defend "A"	0	C_B
	Defend "B"	C_A	0

Figure 5. Basic Security Example

2. Simultaneous vs. Sequential Zero Sum Games

If the game play is sequential as modeled in a Stackelberg game, we observe a clear disadvantage to the leader of the game. For instance, if the defender commits the first move to defend asset A, the attacker can observe the defenders move and launch an attack on asset B. This will result in the defender receiving a payoff of $-C_B$ and the attacker receiving a payoff of $+C_B$. In a similar way, if the attacker commits the first move by attacking asset A, the defender can choose to defend asset A and both players would receive a payoff of zero.

If the game is simultaneous then both players will look for a dominant strategy, saddle point, or optimal mixed strategy. To solve this game, we must determine if the game is a single event (such as an investment in infrastructure by the defender) or a repeated event (such as conducting a daily security patrol).

Assuming this game is a single event and no additional information is available, the defender may choose a conservative strategy that minimizes the possible consequences. In decision theory this strategy is referred to as *minimax*, where the player desires to minimize the maximum possible regret.

$$\min_i \max_j P_{ij}$$

Defend A → $\max(0, C_B) = C_B$

Defend B → max (C_A,0) = C_A

Because the defender values $C_A > C_B$, then the defender will choose to defend asset A, effectively conceding asset B to attack.

3. Mixed Strategy

Assuming this is a repeated game, given the defender plays a pure strategy to defend asset A, the attacker would learn over time to always choose to attack B. In order to prevent a constant loss of asset B, the defender can choose to play a mixed strategy instead of a pure strategy. A repeated protection game can be optimized with a mixed strategy and solved using the Nash Equilibrium. A mixed strategy for the defender would be to defend asset A, a proportion of time equal to $\frac{C_A}{(C_A+C_B)}$ and then defend asset B a proportion of time equal to $\frac{C_B}{(C_A+C_B)}$. Playing a mixed strategy will result in a payoff of $-\frac{C_A C_B}{(C_A+C_B)}$ for the defender. This is a smaller expected loss than playing the pure strategy to always defend A which results in an expected loss of C_B. Consider the following proof:

$$\frac{C_A C_B}{(C_A + C_B)} < C_B$$

$$C_A C_B < C_B(C_A + C_B)$$

$$C_A C_B < C_A C_B + C_B^2$$

$$0 < C_B^2.$$

To avoid predictability, each player will randomize his respective strategy when playing the probabilities given above.

4. Non-Zero Sum Games

In some games, the attackers may not share the same objectives as the defenders and therefore have different payoffs. With different payoffs, the game is no longer zero-sum. Figure 6 shows a notional example of a non-zero-sum game matrix presented in

(Tambe, Shieh, & An, 2011). In each box, the payoffs on the left side of the comma belong to the defender while the payoffs on the right side of the comma belong to the attacker.

		Attacker	
		C	D
Defender	A	2,1	4,0
	B	1,0	3,2

Figure 6. Non-Zero Security Example

For a sequential game play, we observe a stark contrast to the zero-sum game. The leader in a non-zero sum game will have an advantage by going first. In this example, if the defender only considers his own payoffs, then the defender would always choose strategy A because it is a dominant strategy. By choosing strategy A, the defender will receive a payoff of 2 because the attacker prefers strategy C to strategy D in this case. If the defender also considers the attacker's payoffs, then he realizes that by playing strategy B he can do better: the attacker will choose strategy D and the defender will receive a payoff of 3. In a non-zero-sum game there is a first-mover (leader) advantage, but this advantage relies on the assumption that the adversary's payoffs are known.

If the game is simultaneous, then defender and attackers will optimize their payoffs by solving for the Nash Equilibrium. That Nash equilibrium for this problem is:

Defender plays strategy A: 2/3 Defender plays strategy B: 1/3

Attacker play strategy C: 1/2 Attacker plays strategy D: 1/2

Sampling randomly from these mixed strategies assures each player receives the optimal payoff, which for this game is (8/3,2/3). Any player choosing to play something other than the mixed strategy equilibrium will realize a reduced expected payoff in the long term while the other player will realize an increased payoff.

Non-zero-sum games have become popular for representing security conflict because it is generally recognized that terrorists have different objectives than ours (Keeney, 2009). Unfortunately, any advantage in problem realism brought by non-zero-sum payoffs is balanced (and perhaps overwhelmed) by two strong disadvantages. The first disadvantage is the assumption of known adversary payoffs. Modeling the payoffs for an adversary is as difficult as trying to assess intent (see the discussion in Chapter II), and errors in assumed adversary payoffs can lead to poor defense. The second disadvantage is that the theory for solving non-zero-sum games often falls short in the sense that it does not provide clear guidance on how to solve them. Two famous examples are the *prisoner's dilemma* (Straffin, 2006, p. 73) and the *vacation game* (Owen, 1995, p. 163) that even in simple forms are problematic for identifying clear decision guidance.

5. Secrecy

For zero-sum games, each player desires to keep his actions secret from the other player. For sequential games, the follower will lose the advantage if he is unable to determine the leader's move. If the follower cannot see the leader's action, then the game can be played as a simultaneous game. In practice, the leader in a security game will generally attempt to keep actions secret to achieve a higher payoff.

Players often make significant efforts to learn information about the moves or intended moves of the other players. Both players use available means to learn information through intelligence gathering, observation, and modeling. If correct information is learned, a player can achieve a payoff greater than what is achieved through a Nash Equilibrium.

C. RANDOMIZED PATROLLING

Another application of game theory to infrastructure defense is the randomization of security patrols. Consider the situation where a defender conducts security patrols to locate, stop, and/or deter attackers. A predictable security patrol creates a vulnerability to the system being defended. Attackers that observe predictable patrols can determine area of coverage and the time periods of that coverage. Armed with this information, attackers

can accurately determine what gaps exist in the security, and then exploit those gaps. If the defender's actions appear random, the attacker can't determine security gaps with the same high level of certainty.

1. Framework for Randomizing Security Patrols

One way to model security patrols is to use the Stackelberg Equilibrium which assumes the defender will choose an optimal strategy based on the assumption that the attacker will observe this strategy and choose an optimal response (Tambe, Shieh, & An, 2011). Researchers at the University of Southern California (USC) have developed an algorithm named Decomposed Optimal Bayesian Stackelberg Solver (DOBSS) to solve mixed integer linear programs to randomize scheduling, and optimize the time and location of security patrols.

2. Currently Used Randomization Models

The Los Angeles Airport (LAX) security forces face the challenge of patrolling an expansive area with limited number of personnel to stop and deter acts of terrorism. Researchers at the USC developed a game theory model called Assistant for Randomized Monitoring of Routes (ARMOR) to optimize the feasible defender actions by randomizing the security patrol schedules (Tambe, Shieh, & An, 2011).

Intelligent Randomization in Scheduling (IRIS) was also created at USC for the Federal Air Marshal Service (FAMS). There are approximately 29,000 commercial flights each day (Teamcore, 2011). FAMS does not have enough man-power to cover all those flights, so they must prioritize limited resources to provide the best coverage possible. FAMS utilizes the DHS risk based assessment to prioritize flights then uses IRIS to provide the appearance of randomization to the observing attacker.

Similarly, the Coast Guard is trying to solve the same problem with the Ports, Waterways, and Coastal Security (PWCS) mission by developing a scheduling tool called Port Resilience Operational / Tactical Enforcement to Combat Terrorism (PROTECT) (Tambe, Shieh, & An, 2011). PROTECT is being reviewed as a possible solution to scheduling Coast Guard air and sea resources across multiple mission requirements

(Tambe, Shieh, & An, 2011). These models provide a randomized strategy for the defender that is more difficult for a terrorist to predict.

D. SYSTEM INTERDICTION MODELS

Another application of game theory in the context of infrastructure defense has been the study of *system interdiction problems*. Researchers at the Naval Postgraduate School (NPS) have developed a mathematical technique with a wide range of applications that focuses on system *resiliency* given any possible attack or combinations of attacks (Brown et al., 2005). Resiliency is the "ability to resist, absorb, recover from or successfully adapt to adversity or change in conditions" (DHS, 2010).

1. Framework for System Interdiction

In this thesis, a *system* is a collection of individual *components* that work together to achieve a particular *function*, governed by domain-specific physics, protocols, operating rules, etc. The interactions of components are often non-additive and non-intuitive. The *system operator* makes decisions about the activities that take place in a system. These decisions are typically limited by finite resources, component interdependence, or other constraints (i.e., what is feasible). We can evaluate the *system performance* that results from these choices. The *objective* states what the decision maker is trying to get the system to do.

2. System Interdiction Models

Dixon (2011) presents the following progression of system interdiction models for infrastructure defense.

a. Isolated Operations Model

We start by modeling infrastructure in isolation to assess our basic system operation. This model allows us to capture accurate operational details of the system. A system operator is presented with various decisions to run his system. The system operator decision variables are represented by y which belongs to a set of all possible decisions Y, which are limited by the system's constraints. Under normal operations there

is a set of known conditions x_o that the system runs within. Thus, x_o represents a single scenario of normal operating conditions. Without loss of generality, we assume that operators want to run the system at a minimum *cost*. Costs can be measured monetarily or by other key resources such as manpower or other commodity according to a function $f(y, x_0)$. We formulate an "Operator Model" system under normal conditions as:

$$\min_{y \in Y} f(y, x_o).$$

b. Systems with Multiple Scenarios

Many systems experience more than one set of operating conditions. Operators often adjust the decision variable *y* for different scenarios. Simple examples of this type of adjustment are the use of different staff sizes from weekdays to weekends or following different routes during rush hour and at midnight. The mathematics to solve this type of system are the same as our normal operations problem, where for a given scenario $\bar{x}$, we solve:

$$\min_{y \in Y} f(y, \bar{x}).$$

With the operator's model, we can systematically solve for the best activities *y* under each scenario $\bar{x}$ of interest.

c. Systems with Non-Deliberate Hazards

Some systems experience random disruptions. Random disruptions can be accounted for in our set of conditions *x*. We can think of random disruptions as non-deliberate attacks. A simple example of this type of disruption might be a waterway blockage due to hurricane damage or a transportation asset experiencing a mechanical failure. We can represent random changes to our normal conditions as a random variable $\tilde{x}$ and we can simulate values for $\tilde{x}$ by using Monte Carlo techniques and statistical analysis, given data of historical hazards. Here, the operator is represented as the defender and the hazard is represented as the attacker. In the presence of non-deliberate hazards, the operator might choose activities according to:

$$\min_{y \in Y} E_{\tilde{x}}\{ f(y, \tilde{x}\,)\}$$

or some other measure of performance for this uncertain system.

d. Systems with Deliberate Attacks

In the case of an attacker who deliberately attempts to disrupt the system, we have a two-stage, zero-sum game. The deliberate attack is no longer a random variable, but instead becomes a decision variable *x*. The attacker is also limited in resources and capabilities, therefore the decision variable *x* must belong to a feasible set *X*, which represents the constraints on the attacker. The system operator's objective remains to run the system at a minimum cost. The attacker's objective is to cause the maximum disruption to the system. We represent this game as an *attacker-defender* (*AD*) model (Brown et al., 2005) of the following form:

$$\max_{x \in X} \min_{y \in Y} f(y, x).$$

e. Investment to Reduce Attack

If the defender can invest resources that reduce the attacker's capabilities to disrupt the system, the defender is making the first move and the attacker becomes the follower. For any system investment $\bar{w}$ that reduces the attacker's capabilities in the set *X*, the worst-case disruption to the system is again solved by:

$$\max_{x \in X(\bar{w})} \min_{y \in Y} f(y, x, \bar{w})$$

Where $X(\bar{w})$ is the new feasible set of attacks for the attacker given investments $\bar{w}$, and the function *f* also reflects this defensive investment.

f. Defender Attacker Defender (DAD)

In general, the amount of resources the defender can invest to make the system more resilient to attack is also limited. The defender wants to optimize the investment of resources to build system resiliency. Our investment *w* now becomes a decision variable of the defender. We represent investment constraints by saying that *w* is an element of the set *W* of possible resource investments. We assume the attacker acts to

cause maximum disruption. Our system interdiction model is now a *defender-attacker-defender* (*DAD*) problem of the following form (Alderson et al. 2011):

$$\min_{w \in W} \max_{x \in X(w)} \min_{y \in Y} f(y, x, w).$$

E. GAME THEORY AND PORTS, WATERWAYS, AND COASTAL SECURITY (PWCS)

Under the PWCS mission area, the Coast Guard plays the role of the defender when protecting the maritime transportation system and CI/KR. In this situation, the attacker could be either natural hazards and/or deliberate attackers such as terrorists. These two different types of attackers have different payoffs and decision processes. Natural hazards act randomly regardless of the decisions the defender makes. The terrorist is an intelligent adversary who acts deliberately, considers the defender's actions, and uses timing and conditions that will optimize the attack.

Using system interdiction models to analyze the PWCS mission requires an understanding of how a system operates. Our use of mathematical optimization (1) identifies the attacker's strategies that maximize system disruption and (2) identifies the defender's actions that minimize those consequences. In other words, it will determine the worse-case scenario for the defender, pointing the defender in the right direction for applying resources to maintain system operation regardless of what action the attacker takes. We look at a system interdiction model for the PWCS mission in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SYSTEM INTERDICTION MODEL FOR THE TRANSPORT OF COAL IN THE PITTSBURGH THREE RIVERS AREA

A. DEFINING THE PROBLEM

Pittsburgh is one of the major industrial cities of the United States. Commodities can travel in and out of Pittsburgh by highway, rail, and waterway. Pittsburgh is uniquely located at the convergence of the Ohio, the Allegheny, and the Monongahela Rivers, known collectively as the *Three Rivers*. These rivers connect to three of the four largest coal mining states in the U.S.: Kentucky, West Virginia, and Pennsylvania. Currently, Pittsburgh is the second-largest inland port and the 20th largest overall port in the United States (Port of Pittsburgh Commission, 2011). Figure 7 shows Pittsburgh's connection to the inland waterways of United States.

Figure 7. Inland Waterway System (From: Port of Pittsburgh)

There is $9 billion of commerce flow through the Port of Pittsburgh annually. Coal comprises 76% of the total commerce flow through Pittsburgh, making it by far the most influential commodity in that area (Port of Pittsburgh Commission, 2011). Nationally, coal is used to provide power to run approximately half of the U.S. electrical

power grid. Coal can be categorized into two types, lignite and coke. Coke coal is a primary resource for the production of steel. Pittsburgh currently produces 25% of the steel used in the United States. Lignite coal is used to provide power for production in factories and power to the U.S. electrical grid. Given this, coal is a key resource and primary driver of the commerce flow along the *Three Rivers*.

"USCG missions and actions foster economic prosperity and national security by ensuring that the marine transportation system supplying food, energy, raw materials, consumer goods and technology is safe, secure, and reliable" (USCG, 2011d). The Marine Transportation System (MTS) includes all coastal areas and the Inland Waterway System (IWS). Under the Department of Homeland Security, the USCG is also charged with protecting critical infrastructure and key resources from possible terrorist attacks. Specifically, through the PWCS mission, the Coast Guard must ensure the continuous flow of commerce along the MTS. To do this, the USCG must allocate its limited resources to provide optimal protection from potential terrorist attacks. Therefore, the USCG needs to understand the resilience of the system that moves coal through the Port of Pittsburgh along the *Three Rivers*.

B. DEFINING THE SYSTEM

The cost to move a ton of coal one mile by barge is $.005, by railway the cost is $.05, and by truck the cost is $.10 (Port of Pittsburgh Commission, 2011). A typical shipment of coal consists of fifteen jumbo barges carrying 1,750 tons of coal each, yielding 26,250 tons total per shipment. In contrast, one truck and trailer can haul approximately 25 tons. It would take about 1,050 trucks to transport the same quantity of coal as just one barge shipment. One jumbo hopper rail car can carry approximately 110 tons. It would take 216 rail cars to carry the same as amount as one barge shipment of coal. The waterways are therefore the most efficient and economical mode of transportation. Figure 8 shows the relative comparison of coal transport capacities.

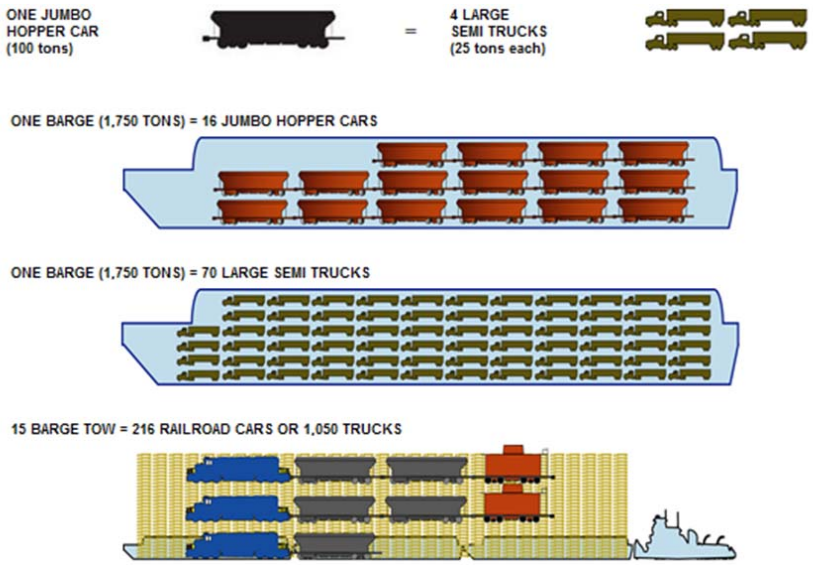

Figure 8. Mode of Transport Comparison (From: Port of Pittsburgh)

Pittsburgh has infrastructure in place to move coal by all three modes of transport, however, under normal operation coal is transported by barge along the waterways. If something were to disrupt the normal flow, contingencies are in place to move coal by rail, but there are constraints of crane offloading capacities and increased costs. Movement by truck is cost prohibitive, so we restrict attention to waterways and railways for our system model.

We build a *network* to model the movement of coal. We identify supply and demand locations, choke points and transfer locations, which we represent by *nodes*. We use *arcs* between nodes to indicate the pathways that coal can follow. We include both waterway arcs and railway arcs to move coal from its supply nodes to the demand nodes.

We scope our network geographically to approximately a 15 mile radius from the Port of Pittsburgh (convergence point of the Three Rivers). The first lock and dam system along each river from the Point of Pittsburgh make up the network boundaries. Figure 9 depicts the geographical area that is assessed in our problem. We use a time period of one week to determine the capacities and costs.

Figure 9. Geographic depiction of model (From: Google Earth)

The objective of the coal transport network problem is to minimize the overall cost, even in the presence of disruptions. To solve this problem, we use a min-cost network flow model.

C. MATHEMATICAL REPRESENTATION

1. Defender Problem (D)

The first step in solving a min-cost network flow problem is to define a network that represents the defender's objective. In our network, the defender's objective is to minimize the cost required to transport the total flow of coal from the supply nodes to the demand nodes. The model is subject to balance of flow constraints and a maximum capacity of flow along each arc.

Let $G = (N, A)$ represent a directed graph, where N is a set of nodes and $A \subseteq N \times N$ is a set of directed arcs. We use a standard format to represent this problem.

Index Sets

$n \in N$	Nodes in the system (alias i, j)	
$(i,j) \in A$	Directed arcs	

Data

C_{ij}	Cost per-unit of operating arc $(i,j) \in A$	[$/ton]
u_{ij}	Capacity of arc $(i,j) \in A$	[tons]
$penalty_n$	Penalty for unmet demand at node n	[$/ton]
l_n	Supply at node n when $l_n > 0$	[tons]
	$(-$ Demand) at node n when $l_n < 0$	[tons]

Decision Variables

y_{ij}	Flow on arc (i,j)	[$/ton]

Elastic Variables

$unmet.demand_n$	Commodity not reaching demand at node n	[tons]
$unmet.supply_n$	Commodity not leaving supply at node n	[tons]

Formulation 1: Defender Model (D)

$$\min_{y} \quad \sum_{(i,j)\in A} C_{ij}y_{ij} + \sum_{j\in N}(penalty_j \times unmet.demand_j) \qquad \text{(D0)}$$

Subject to:

$$\sum_{i:(i,j)\in A} y_{ij} - \sum_{i:(j,i)\in A} y_{ij} = l_j - unmet.demand_j + unmet.supply_j \ \ \forall j \in N \qquad \text{(D1)}$$

$$y_{ij} \leq u_{ij} \qquad \forall (i,j) \in A \qquad \text{(D2)}$$

$$y_{ij} \geq 0 \qquad \forall (i,j) \in A \qquad \text{(D3)}$$

$$unmet.demand_j \geq 0 \qquad \forall\, j \qquad \text{(D4)}$$

$$unmet.supply_j \geq 0 \qquad \forall\, j \qquad \text{(D5)}$$

The objective (D0) calculates the flow cost. The decision variable y_{ij} represents a movement of coal. A penalty cost is added for any demands not met. The balance of flow constraint (D1) assures mathematical feasibility and assigns supply and demands to the nodes. We restrict the flow y_{ij} to the maximum arc capacity u_{ij} in constraint (D2). Equation (D3) is a non-negativity constraint on the decision variable and equations (D4) and (D5) are the non-negativity constraints for the elastic variables.

2. Attacker Defender (AD)

We consider an intelligent attacker with an objective to disrupt the system. We assume that the defender's system will operate optimally when undisrupted. The attacker makes a decision as to which arc to attack to cause a maximum disruption. We assume the attacker is constrained in how many simultaneous attacks can be made.

To model an arc disruption we create a penalty that is an artificial value greater than the cost of any possible path through the network. The penalty ensures that the operator will take a shortfall only when no feasible path exists, but the penalty has no actual meaning in cost to the problem. We represent a penalty for disruption as:

$$q_{ij} = n \times \max_{(i,j)\in A}\{C_{ij}\}.$$

To model the Attacker-Defender problem we include the following data and decision variables.

Data

q_{ij}	Penalty imposed on attacked arc	[$/ton]
num.attacks	Number of allowable attacks	[parameter]

Decision Variable

x_{ij}	Disrupt flow on arc (i,j)	[binary]

Formulation 2: Attacker-Defender Model (AD)

$$\max_{x} \min_{y} \sum_{(i,j)\in A} (C_{ij} + x_{ij}q_{ij})y_{ij} + \sum_{j\in N} (penalty_j \times unmet.demand_j) \qquad (AD0)$$

Subject to:

$$\sum_{i:(i,j)\in A} y_{ij} - \sum_{i:(j,i)\in A} y_{ji} = l_j - unmet.demand_j + unmet.supply_j \quad \forall\, j \in N \quad (AD1)$$

$$y_{ij} \le u_{ij} \qquad \forall (i,j) \in A \qquad (AD2)$$

$$y_{ij} \ge 0 \qquad \forall (i,j) \in A \qquad (AD3)$$

$$\sum_{(i,j)\in A} x_{ij} \le 2(num.attacks) \qquad (AD4)$$

$$x_{ij} = x_{ji} \qquad \forall (i,j) \in A \qquad (AD5)$$

$$x_{ij} \in \{0,1\} \qquad \forall (i,j) \in A \qquad (AD6)$$

By adding the attacker to the defender's problem (D), the formulation (AD) becomes a two-stage optimization problem. Our objective (AD0) introduces an additional penalty induced by the attacker's decision to disrupt arc x_{ij}. Constraint (AD1) is the same balance of flow as in problem (D). Equation (AD2) and (AD3) restricts the defender's flow from zero to the maximum capacity of each arc. We restrict the number of allowable

attacks in equation (AD4). Equation (AD5) indicates that an attack on a directed arc will also disrupt the flow in the opposite direction on the attacked arc. Equation (AD6) constrains the attack to a binary variable, where $x_{ij} = 1$ on an attacked arc and $x_{ij} = 0$ for arcs with no attacks.

The network model consists of 25 nodes and 70 directed arcs. Overall there are two net supply nodes and three net demand nodes. Eight of the nodes represent the railways and 17 nodes make up the waterways. Of the arcs, nine are railway arcs, eight are terminal offload arcs, and eighteen are river arcs. See *Appendix B* for details of nodes, arcs, and data used in this model. We determine the cost of each arc by a function of distance and a ratio of dollars per ton for each mode of transport. The capacities are formed by flow limitations on each arc and by loading limitations at the transfer stations. Figure 10 shows the resulting representation of the coal transport system.

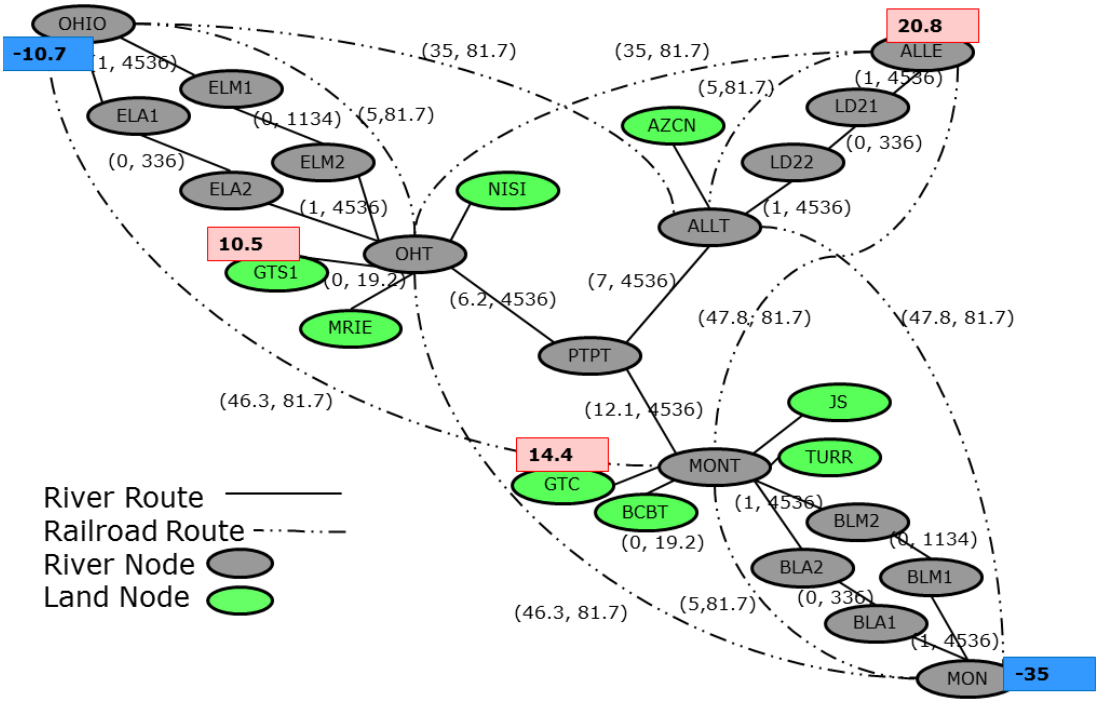

Figure 10. Representation of coal transport system. Arcs are labeled as (Cost, Capacity). Supply nodes are depicted with a negative tonnage (K-tons per week and demand nodes are depicted with positive K-tons per week.

D. RESULTS

1. General Results

Under normal operations, the coal supply flows from the Monongahela River and the Ohio River through the river arcs to the demand terminal nodes of GTC and GTS. The remainder of the coal supply continues along the waterway arcs to the net demand node, ALLE, which represents demands of terminals upriver along the Allegheny River. We assume a shortfall penalty q_{ij} for each node that fails to meet the desired demand. The base cost for normal operations is \$452K and there are no shortfalls in demand. Figure 11 shows the results of the system under normal conditions. The highlighted arcs indicate the optimal pathway for coal movement.

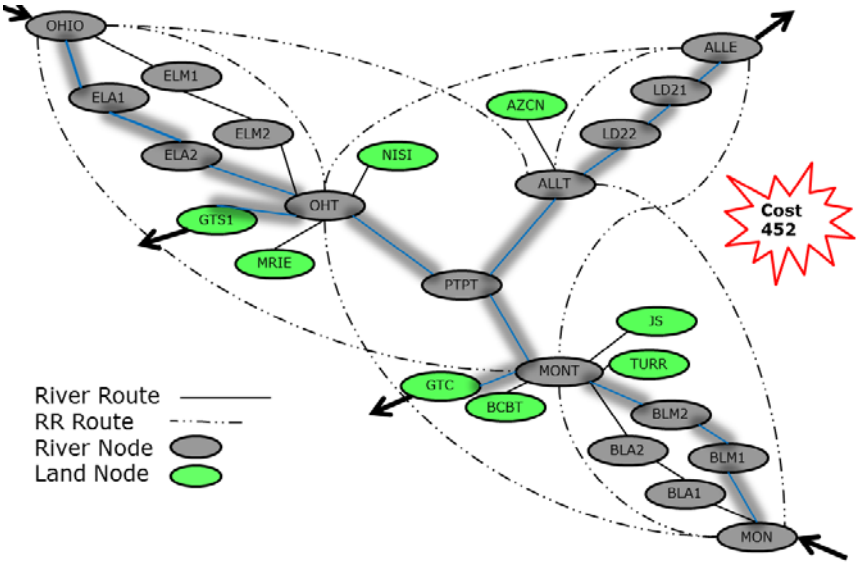

Figure 11. Normal Flow Coal Transport Network

We next introduce disruptions to the system. We begin by limiting the attacker to one attack, then step-by-step increase the number of simultaneous attacks allowed. For any value of num.attacks, we find the most critical arcs being attacked. We find the second most critical arc to attack by removing the most critical arc from the set of feasible attacks.

By allowing the attacker to make a single attack (num.attacks = 1), we observe that the maximum disruption from a single attack occurs at the arc between the Point of

Pittsburgh (PTPT) and the Allegheny Transfer node (ALLT). The loss of this most critical single arc doubles the normal operations cost to a value of $1026K. A disruption on this arc forces the coal supply to ALLE to use railroad arcs to meet demand, as seen in Figure 12. The second worst single arc attack is between the Monongahela River Transfer (MONT) to PTPT. The cost of the second most critical arc is $1022K. Figure 12 shows the resulting costs of the most critical single attacks.

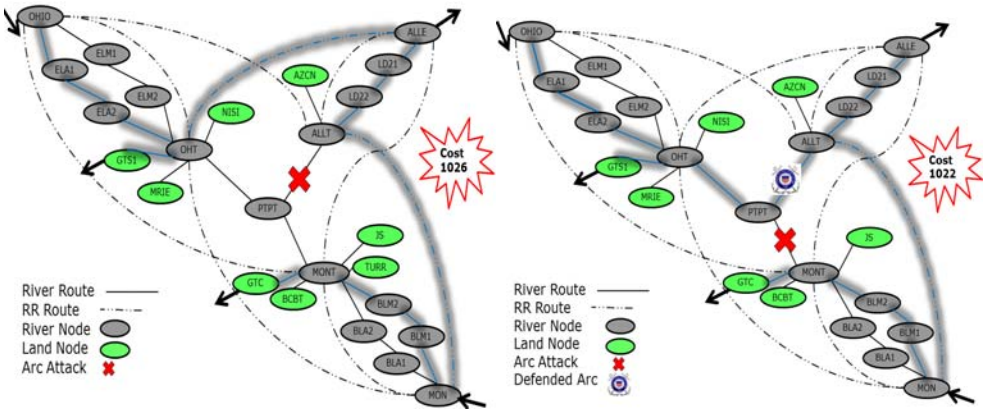

Figure 12. Single-arc attacks. Left: worst single-arc attack. Right: second worst single arc attack.

Figure 13 shows the effects from the nine most significant single-arc attacks. Only the first two result in costs significantly above normal operations.

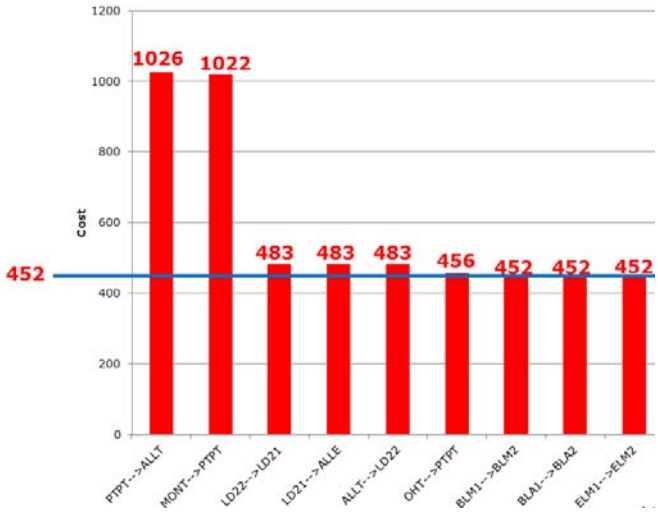

Figure 13. Operating costs resulting from single-arc attacks on system

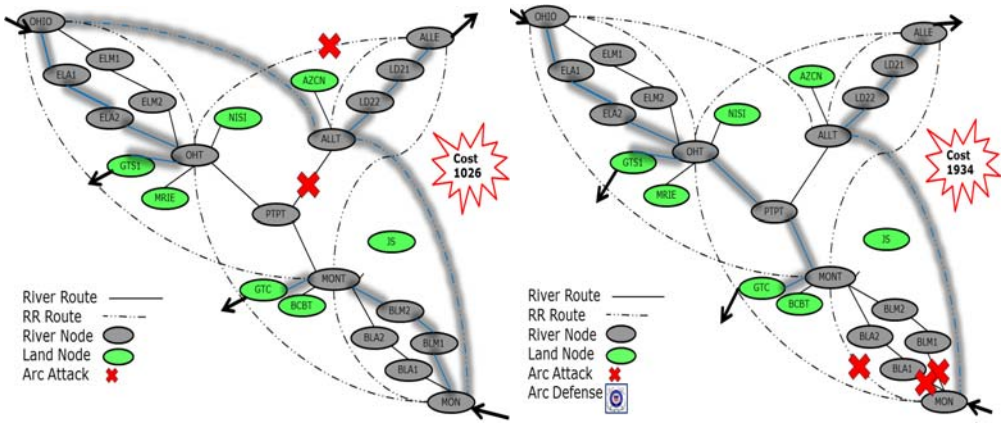

Figure 14. Left: Worst two-arc attack – Right: Worst three-arc attack

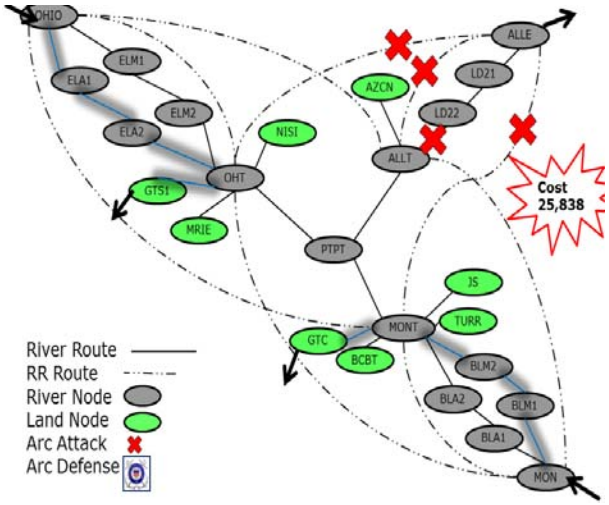

Figure 15. Left: Worst four-arc attack

We next examine the system given the attacker can launch two, three, and four simultaneous disruptions. Figures 14–15 show the results from these most critical attack sets.

When num.attacks =2, the worst case disruption increases the cost to $1026K, the same as a single attack to the most critical arc. This is because the redundancy of the railroad infrastructure in the study area prevents further cost increases from a second arc attack to the system.

When num.attacks = 3, the attacker is capable of shutting off flow through the Braddock Lock and Dam system on the Monongahela River. This forces the flow of coal to travel on longer, and hence more costly, railway routes, resulting in system cost of $1934K.

When num.attacks = 4, the demands are no longer met on the Allegheny River. Because of the penalty imposed for shortfalls, the cost to the system becomes an artificial value of $25,838K, which indicates the problem is infeasible. Note, however, that this four-arc attack interdicts three separate railroad arcs to ALLE in order to create the shortfall. In practice, each of these railroad arcs is really a network of possible rail routes, which have considerable redundancy and would likely be much harder to disrupt. As long as one of these rail routes remains available, then this artificial cost of $25,838K drops to a more realistic $2,337K.

Our system interdiction model for the transportation of coal through the Port of Pittsburgh produces some insightful results. In general we are able to determine the most critical pathways for minimizing the transport of coal. We are able to determine where an adversary can cause the greatest damage. The most notable results from our study show that one attack at a critical location along the waterway could double the cost of total coal movement. Four simultaneous attacks to the system stops demand from being met on the Allegheny River, resulting in a significant economic impact to the system. By protecting the three waterway arcs between ALLT and ALLE, USCG could ensure system feasibility and prevent significant economic impact to the system.

2. Future Study

This preliminary analysis made the following assumptions:

(1) We consider only a single commodity, namely coal, and we assume the flow in and out of the study area is a net supply or demand. We also assume only one type of coal is being transported. There are two distinct types of coal (lignite and coke) which will have distinct supply and demand locations. A more thorough analysis would consider multiple commodities to more accurately track the total flow of each type of coal.

(2) We used a time period of one week for our model. We assume an attack on any one arc in our network would cause a minimum of a seven-day disruption. Modeling this problem for longer durations would introduce diversity in the length of time a specific arc would be removed from the system, depending on the infrastructure and method of attack. For example, we expect that a lock and dam would take longer to repair than a blocked waterway.

(3) It is clear that cost of transporting coal by rail is greater than the cost of transporting by waterway, however, these exact costs could vary from location to location. A more detailed economic analysis of the transport systems may provide additional insight to this problem.

(4) We abstracted the movement of coal by rail to single direct arcs. In practice, there is a separate railroad network for moving coal that could produce different insights into the locations of critical nodes and/or arcs.

(5) The geographic boundaries used for this model included waterways and rail within approximately 15 miles from the Port of Pittsburgh. The waterways were evaluated from the Port of Pittsburgh to the first lock and dam system on each of the three rivers. There are many supply and demand locations on the rivers that are located outside the study area.

Further study for this project should entail analyzing the system under multiple time frames such as a month and a year, and broadening the geographical scope of the network to include other supply and demand locations.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

This thesis explores various analytic techniques for guiding defense of the United States from acts of terrorism, with specific emphasis on the United States Coast Guard's role in this mission. We conclude by summarizing our work and proposing ideas for future study.

A. SUMMARY

Probabilistic Risk Analysis (PRA) techniques originated with the insurance field in the late 1600s. Since that time, risk-based methods and models have been used in a variety of contexts including engineering, organizational safety programs, and recently in defense against terrorism.

Risk is frequently represented in terms of the likelihood that a negative outcome will be realized. Determining the likelihood of an event presents many challenges when applied to real life problems. Sampling historical data from domestic and international incidents can provide insight on frequency of events and lead to more confident probabilities of future events, provided that past events are representative of an uncertain future. When historical data is limited or not available, probability assessments rely on subjective opinions, which can be difficult to validate and can lead to poor assessments of the real problem. In the case of terrorism, historical data is significantly limited.

Terrorism risk is typically quantified by a function of threat, vulnerability, and consequence assessments. The Department of Homeland Security (DHS), the USCG, and others use TVC ($threat \times vulnerability \times consequence$) models to quantify risk. There are significant philosophical, practical, and mathematical concerns with this view of terrorism risk.

Risk-based techniques for terrorism typically model terrorists as random variables. An intelligent adversary can adapt strategy, learn from past events, and use timing and current events to optimize an attack. Therefore, an intelligent adversary does not act randomly; this produces different results than a random attacker.

Terrorism risk quantified by TVC assumes independence of threat, vulnerability, and consequence assessments, or sequential dependence. Threat is commonly determined by the intention and capabilities of an attacker. In practice, we face many possible attackers, some known and some unknown, and this makes it difficult or impossible to assess comprehensively their intentions and capabilities. To quantify a threat value, we must consider a target's vulnerability and consequence values. This logic indicates that threat assessments depend on vulnerability and consequence assessments. TVC calculations can vary considerably from assessments that account for correlation.

Terrorism risk also assumes the attacker only knows what the defender knows and that the attacker's decision process is the same as the defender's. We can see clear examples in Chapter II where these assumptions can be incorrect and lead to mismanagement of risks.

Game theoretic techniques are a suggested alternative to PRA in the defense against an intelligent attacker. If a problem is properly structured and carefully assessed, game theory can be used to solve security games of infrastructure defense between a defender and an attacker. We study the use of game theory for protection and infrastructure defense. We review protection models currently in use by the Federal Air Marshal Service, LAX security forces, and the USCG that optimize the location and time periods that security forces are implemented.

In contrast to PRA techniques, such as TVC models, system interdiction models do not rely on subjective analysis of potential attackers. System interdiction models focus on the analysis of how the system functions and how to make that system more resilient in the presence of potential attacks. For systems with unambiguous measures of performance, system interdiction models provide decision makers with clear guidance for resource allocation, where risk-based models may distance the decision maker from solving the real problem.

We build a system interdiction model to analyze a relevant and current infrastructure defense problem along the western rivers of the Inland Waterway System (IWS). We identify the Port of Pittsburgh as a critical inland port, with coal as a key

resource that is transported along the inland waterways. Our preliminary system interdiction model provides insight on the resilience of the transportation of coal through the Port of Pittsburgh. With further study, the model can provide guidance on resource allocation, such as infrastructure investments, and for the USCG in the Ports, Waterways, and Coastal Security (PWCS) mission.

B. FUTURE WORK

1. Model Refinements

This thesis made several simplifying assumptions in the Three Rivers coal transport problem. We consider only one type of coal and assume flows are driven by net demands, making our model a single commodity minimum cost flow problem. However, the costs and penalties for disruptions may vary with the actual type of coal being transported, and this can greatly impact the overall cost and identification of what is most critical. A natural next step is to build a multi-commodity model that accounts for different coal types and multiple intertwined supply and demand networks.

We assume simplified transport costs of each mode of transport based on general data obtained from the Port of Pittsburgh Commission. Actual costs can depend on local businesses, current environmental conditions, and other influences. A more detailed economic analysis of transport costs and penalties for unmet demands will help validate the model's results.

Our model uses a time period of one week to capture normal business operations, with the assumption that a notable disruption to the system would last a minimum of one week. To provide more guidance to decision makers, we should model other time periods to include assessments of one month and one year. The study of additional time periods may produce results that are different then the results discussed in Chapter IV.

2. Expanding the Model's Geographic Area of Study

We model the waterways and railways systems between the Emsworth Lock and Dam on the Ohio River, the Braddock Lock and Dam on the Monongahela Rivers, and the Lock and Dam Two on the Allegheny River. This model does not include analysis of

many key supply and demand locations located outside the first set of lock and dam systems on each river. Expanding the geographical scope will account for these other significant influences on the system. The USCG suggests expanding the area of study to include Dashields Lock and Dam on the Ohio River, Lock and Dam Three on the Monongahela River, and Lock and Dam Three on the Allegheny River. The expanded boundaries include additional coal terminals and factories not assessed in the preliminary analysis.

3. Determining the Most Useful Scope of Modeling Inland Waterways

Creating system interdiction models can be labor intensive. Modeling system interdiction requires a thorough understanding of the system and a reasonably accurate assessment of system performance. In contrast, models in general that are built with excessive intricacies and complexities tend to produce results that either mask the actual influences or do not give the decision maker useful guidance.

To use system interdiction modeling for analysis of the entire IWS, the USCG faces a challenging problem of striking the right balance of modeling the system with enough detail to be accurate but without such complexity that the model does not provide useful results. Future study for determining the proper scope of system interdiction modeling of the inland waterways may consider two distinctly different approaches.

One approach may be to assess the entire IWS using a single-commodity minimum cost flow model that focuses only on big picture influences. Various commodities may be grouped together into one super commodity that accounts for all major commerce flow. A model of this type may be useful for longer term organizational strategic planning.

A second approach would be to build multi-commodity minimum cost flow models that are geographically restricted to specified regions such as our Three Rivers coal transport model. A regional model would include more details with results that would be useful to local operators such as Coast Guard Marine Safety Units and Coast Guard Sector commands.

4. The Coast Guard's PWCS Mission

The Coast Guard's PWCS mission entails the protection of the U.S. Maritime Domain and the Marine Transportation System and those who live, work or recreate near them. The Department of Homeland Security has directed the USCG to treat the PWCS as its primary mission alongside Search and Rescue. The USCG has limited resources available. Currently the USCG uses a form of PRA as a decision tool in allocation of resources towards the PWCS mission. This thesis reviews many concerns of risk-based approaches to terrorism analysis and specifically TVC models such as the one the USCG uses.

We recommend that future studies be conducted to help chart a course for the development and validation of decision support tools. In this thesis we discuss the use of game theory and its applications to the Coast Guard's PWCS mission, as an alternative to risk based models. Additional studies of game theory approaches such as system interdiction may provide a "navigational chart" that gives the USCG key insight and guidance in resource allocation.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

Definitions used by the Department of Homeland Security

Adversary: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Consequence: Effect of an event, incident, or occurrence. Measured by human, economic, mission, environmental, and psychological impacts.

Likelihood: Estimate of the potential of an incident or event's occurrence. Used interchangeably with probability.

Probability: Likelihood that is expressed as a number between 0 and 1.

Resilience: Ability to resist, absorb, recover from or successfully adapt to adversity or change in conditions.

Risk: Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and associated consequences.

Scenario: Hypothetical situation comprised of a hazard, an entity impacted by that hazard, and associated conditions including consequences when appropriate.

Threat: Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property. Intentional hazard is generally estimated as the likelihood of an attack that accounts for the intent and capability of the adversary, being attempted by an adversary.

Vulnerability: Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.. Characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

The case study in Chapter IV uses the following node data on page B.1 and arc data on page B.2.

Node Name		Supply / Demand (K-tons/week)
ALLE	Allegheny River	20.8
ALLT	Allegheny River Transfer Station	0
AZCN	Terminal	0
BCBT	Terminal	0
BLA1	Braddock Lock Auxiliary 1	0
BLA2	Braddock Lock Auxiliary 2	0
BLM1	Braddock Lock Main 1	0
BLM2	Braddock Lock Main 2	0
ELA1	Emsworth Lock Auxiliary 1	0
ELA2	Emsworth Lock Auxiliary 2	0
ELM1	Emsworth Lock Main 1	0
ELM2	Emsworth Lock Main 2	0
GTC	Coal Terminal	14.4
GTS1	Coal Terminal	10.5
JS	Terminal	0
LD21	Lock and Dam (2) on Allegheny River 1	0
LD22	Lock and Dam (2) on Allegheny River 2	0
MON	Monongahela River	-35
MONT	Monongahela River Transfer Station	0
MRIE	Terminal	0
NISI	Terminal	0
OHIO	Ohio River	-10.7
OHT	Ohio River Transfer Station	0
PTPT	Point of Pittsburgh	0
TURR	Terminal	0

StartNode	EndNode	Capacity (k-tons/week)	Cost
ALLE	LD21	4536	1
ALLE	MONT	81.7	47.75
ALLE	ALLT	81.7	2.5
ALLE	OHT	81.7	35
ALLT	MON	81.7	47.75
ALLT	PTPT	4536	7
ALLT	AZCN	19.2	1
ALLT	ALLE	81.7	2.5
ALLT	LD22	4536	1
ALLT	OHIO	81.7	35
AZCN	ALLT	81.7	0
BCBT	MONT	0	0
BLA1	BLA2	336	0
BLA1	MON	4536	0
BLA2	MONT	4536	1
BLA2	BLA1	336	0
BLM1	BLM2	1134	0
BLM1	MON	4536	0
BLM2	MONT	4536	1
BLM2	BLM1	1134	0
ELA1	ELA2	336	0
ELA1	OHIO	4536	0
ELA2	OHT	4536	0
ELA2	ELA1	336	0
ELM1	ELM2	1134	0
ELM1	OHIO	4536	0
ELM2	OHT	4536	0
ELM2	ELM1	1134	0
GTC	MONT	19.2	0
GTS1	OHT	19.2	0
JS	MONT	0	0
LD21	LD22	336	0
LD21	ALLE	4536	0
LD22	ALLT	4536	1
LD22	LD21	1134	0
MON	BLM1	4536	0
MON	BLA1	4536	0
MON	OHT	81.7	46.25

StartNode	EndNode	Capacity (k-tons/week)	Cost	
MON	MONT	81.7	2.5	
MONT	JS	0	0	
MONT	GTC	19.2	0	
MONT	BCBT	0	0	
MONT	TURR	0	0	
MONT	PTPT	4536	12.1	
MONT	MON	81.7	2.5	
MONT	BLM2	4536	1	
MONT	BLA2	4536	1	
MONT	ALLE	81.7	47.75	
MONT	OHIO	81.7	46.25	
MRIE	OHT	0	0	
NISI	OHT	0	0	
OHIO	ELM1	4536	0	
OHIO	ELA1	4536	0	
OHIO	MONT	81.7	46.25	
OHIO	OHT	81.7	0	
OHIO	ALLT	81.7	35	THIS
OHT	MON	81.7	46.25	
OHT	ALLE	81.7	35	
OHT	PTPT	4536	6.2	
OHT	NISI	0	0	
OHT	GTS1	19.2	0	
OHT	MRIE	0	0	
OHT	ELM2	4536	0	
OHT	ELA2	4536	0	
OHT	OHIO	81.7	0	
PTPT	MONT	4536	12.1	
PTPT	ALLT	4536	7	
PTPT	OHT	4536	6.2	
TURR	MONT	0	0	

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

ASME Innovative Technologies Institute. (2011). RAMCAP framework 2.0 (2006).and RAMCAP plus (2011). Retrieved from ASME website: http://www.asme-iti.org/RAMCAP

Alderson, D., Brown, G., Carlyle, M., & Wood, K. (2011). Solving defender-attacker-defender models for infrastructure defense. In *Operations Research, Computing, and Homeland Defense,* R.K. Wood and R.F. Dell, editors, INFORMS, Hanover, MD, pp. 28–49.

Basar, T., & Olsder, G. (1999). *Dynamic Non-cooperative game theory.* 2nd ed. Philadelphia: Society of Industrial and Applied Mathematics.

Bedford, T., & Cooke, R. (2001). *Probabilistic Risk Analysis Foundations and Methods*. Cambridge: Cambridge University Press.

Bernstein P. (1996). *Against the gods; the remarkable story of risk*. Hoboken: John Wiley & Sons.

Brown, G., Carlyle, M., Salmeron, J., & Wood, K. (2005). Analyzing the vulnerability of critical infrastructure to attack and planning defenses, in *Tutorials in Operations Research: Emerging Theory, Methods, and Applications.* H. Greenberg and J. Smith, eds., Institute for Operations Research and Management Science, Hanover, MD.

Brown, G. & Cox, A. (2011). How probabilistic risk assessment can mislead terrorism risk analysts. Risk Analysis, vol. 31, no. 2.

Cox, A. (2008a). What's wrong with risk matrices? Risk Analysis, vol. 28, no. 2, 2008.

Cox, A. (2008b). Some limitations of "Risk = Threat × Vulnerability × Consequence" for risk analysis of terrorist attacks. Risk Analysis, vol 28, no. 6.

Cox, A. (2009). *Risk analysis of complex and uncertain systems*. New York: Springer.

Department of Homeland Security (DHS) (2010). Risk steering committee. DHS risk Lexicon.

Dillon, R., Liebe, R., & Bestafka, T. (2009). Risk-based decision making for terrorism applications. Risk Analysis, vol. 29, no. 3.

Dixon, C. (2011). Assessing vulnerabilities in interdependent infrastructures using attacker-defender models. Masters thesis, Naval Postgraduate School, Monterey.

Ezell, B., Bennett, D., Von Winterfeldt, J., Sokolowski, J., & Collins, A. (2010). Probabilistic risk analysis and terrorism risk. Risk Analysis, vol. 30, no. 4.

GAIN (2003). Guide to methods and tools for airline flight safety analysis. 2nd ed. Retrieved from: http://flightsafety.org

Garrick, J. (1984). Recent case studies and advancements in probabilistic risk assessment. Risk Analysis, vol. 4, no. 4.

Government Accounting Office (GAO) (2011). Security risk model meets DHS criteria, but more training could enhance its use for managing programs and operations. Retrieved from: http://www.gao.gov/assets/590/587144.pdf

Hubbard, D. (2009). *The failure of risk management; why it's broken and how to fix it*. Hoboken: John Wiley & Sons.

Kaplan, S., & Garrick, J. (1981). On the quantitative definition of risk. Risk Analysis, vol 1, no. 1.

Keeney, G. (2009). Identifying and structuring objectives of terrorists. Retrieved from: http://create.usc.edu/publications/KeeneyReport.pdf

Lin, K., & Regnier, R. (2011). Topics in Decision and Risk Analysis. Naval Postgraduate School.

Lowder, J. (2010). Why risk = TVC is mathematical non-sense, *Risk Analysis.* Retrieved from: http://www.bloginfosec.om/2010/08/31why-the-%E2%80%9Crisk-threat-x-vulnerability-x-impact%E2%80%9D-formula-is-mathematical-nonsense-part-2/.

National Infrastructure Protection Plan (NIPP) (2009). Retrieved from: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

NRC (2008). Department of Homeland Security bioterrorism risk assessment a call for change. Retrieved from: http://www.nap.edu/catalog/12206.html

NRC (2010). Review of the departments of security approach to risk analysis. Retrieved from: http://www.nap.edu/catalog 12972.html

Nuclear Regulatory Commission (2011). PRA procedures guide: a guide to the performance of probabilistic risk assessments for nuclear power plants. Retrieved fm: http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr2300/vol2/

New York City Police Department (NYPD) (2011). Retrieved from: http://www.nyc.gov/html/nypd/html/faq/faq_police.shtml#1

Owen, G. (1995) *Game theory*. 3rd ed. San Diego: Academic Press.

Parnell, G. (2008) Bioterrorism risk analysis with decision trees. DHS Bioterrorism risk assessment, a Call for Change. 2008. Appendix D.

Pate´-Cornell, M., & Guikema, S. (2002). Probabilistic modeling or terrorist threats: a systems analysis approach to setting priorities among countermeasures. Military Operations Research Society (MORS), Vol. 7.

Port of Pittsburgh Commission (2011). Port of Pittsburgh information. Retrieved from: www.port.pittsburgh.pa.us/home/

Rasmussen, N. 1976. Probabilistic Risk Analysis Its Possible Use in Safeguards Problems. Presented at the Institute for Nuclear Materials Management meeting. Fall. Pp 66–88.

Straffin, P. (2006) Game theory and strategy. Washington D.C.: The Mathematical Association of America.

Tambe, M., Shieh, E., & An, B. (2011). Application of game theory to optimizing CG resource allocation for PWCS deterrence missions. Coast Guard Research and Development Center.

Teamcore (2011). Research on game theory for security. Retrieved from: http://teamcore.usc.edu/project/security/

United States Coast Guard (USCG) (2008). Commandant's Direction 2011. Retrieved from: http://www.uscg.mil/seniorleadership/docs/ccgs-direction-2011.pdf

United States Coast Guard (USCG). (2008b). *Marine Safety Manual*.

United States Coast Guard (USCG) (2010). Joint, CG Atlantic and CG Pacific Area Operational Risk Assessment Model (ORAM).

United States Coast Guard (USCG) (2011a). USCG history. Retrieved from: http://www.uscg.mil/history/

United States Coast Guard (USCG) (2011b). Coast Guard FAQs. Retrieved from: http://www.uscg.mil/seniorleadership/FAQ/FAQ%204.pdf

United States Coast Guard (USCG) (2011c), PWCS. Retrieved from: http://www.uscg.mil/hq/cg5/cg532/pwcs.asp

United States Coast Guard (USCG) (2011d), FY2008 USCG performance report. Retrieved from: http://www.uscg.mil/history/allen/docs/USCGFY08PerformanceReportFinal.pdf

von Stackelberg, H. (1948). Foundations of theoretical economics. Berne: Springer.

Willis, H. (2007). Guiding resource allocations based on terrorism risk, Risk Analysis, vol. 27, no. 3.

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. Commander
   Atlantic Command
   U.S. Coast Guard
   Federal Building

4. Commander
   Eighth Coast Guard District
   Hale Boggs Federal Building

5. Sector Ohio Valley
   Louisville, KY