2008-06

Development of a decision support tool to inform resource allocation for critical infrastructure protection in Homeland Security

Al Mannai, Waleed I.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DISSERTATION

DEVELOPMENT OF A DECISION SUPPORT TOOL TO INFORM RESOURCE ALLOCATION FOR CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY

by

Waleed I. Al Mannai

June 2008

Dissertation Supervisor: Ted Lewis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2008	**3. REPORT TYPE AND DATES COVERED** Dissertation	
4. TITLE AND SUBTITLE: Development of a Decision Support Tool to Inform Resource Allocation for Critical Infrastructure Protection in Homeland Security		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Waleed I. Al Mannai			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Analysis of risk in critical infrastructure is one of the major problems facing Homeland Security today. Defining risk and applying it to systems, as opposed to individual assets, is a relatively new idea in Homeland Security policy. Thus, there is a need for a decision support tool to inform decision makers in Homeland Security of resource allocation strategies to harden assets that reduce overall network risk. Model Based Risk Assessment (MBRA) is a quantitative method designed to (1) identify the most critical assets of the network in such a way as to reduce expected loss over the entire network, (2) quantify allocation strategies that strategic planners and risk managers can apply across multi-sector systems, and (3) compute vulnerability and total risk reduction of the network.

We formalized the definition of network risk in terms of the connectivity of the network as an extension to the accepted risk equation R=f(T,V,C). We use node degree as a heuristic for criticality of an asset to the overall function of the network. We then modeled the relationship between budget and vulnerability reduction and show how an exponential reduction model compares to a linear or random model. Using the stated definition of network risk, all models rank order assets exactly the same but they reduce risk differently. Lastly, we introduce a two-party model that combines both the defender's and attacker's points of view using a game theory approach. We show the results of this model and compare them to a similar model we refer to as the "arms race model" where we allow both attacker and defender to know each other's budget. Results show that the techniques developed here are useful in conducting a systematic and repeatable analysis of an infrastructure network of assets for risk and then informing resource allocations that serve to reduce risk on the entire network, not just the selected assets.

14. SUBJECT TERMS Vulnerability of Infrastructure Analysis and Risk Assessment, Allocation Distribution, Risk Problems, Critical Infrastructure Protection, Defender-Attack Model, Defender-Only Model, Independent-objective and Joint-objective Functions			**15. NUMBER OF PAGES** 101
			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

DEVELOPMENT OF A DECISION SUPPORT TOOL TO INFORM RESOURCE ALLOCATION FOR CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY

Waleed I. Al Mannai
Lieutenant Colonel, Royal Bahraini Air Force
B.S., Aeronautical Engineering, Northrop University, 1987
M.S., Aeronautical Engineering, Naval Postgraduate School, 1993

Submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY IN MODELING, VIRTUAL ENVIRONMENTS AND SIMULATION

from the

NAVAL POSTGRADUATE SCHOOL
June 2008

Author: _____
Waleed I. Al Mannai

Approved by:

_____	_____
Dr. Ted Lewis Professor of Computer Science Dissertation Supervisor	Dr. Rudolph Darken Professor of Computer Science Dissertation Committee Chair
_____	_____
Dr. Christian Darken Associate Professor of Computer Science	Dr. Jeff Crowson Professor of Educational Research DLIFLC ESD – Research and Analysis
_____	_____
Dr. Tom Mackin Professor of Mechanical Engineering California Polytechnic State University San Luis Obispo, California	Dr. James Wirtz Dean of the School for International Graduate Studies

Approved by: _____
Dr. Mathias Kolsch, Chair, MOVES Academic Committee

Approved by: _____
Dr. Douglas Moses, Associate Provost for Academic Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Analysis of risk in critical infrastructure is one of the major problems facing Homeland Security today. Defining risk and applying it to systems, as opposed to individual assets, is a relatively new idea in Homeland Security policy. Thus, there is a need for a decision support tool to inform decision makers in Homeland Security of resource allocation strategies to harden assets that reduce overall network risk. Model Based Risk Assessment (MBRA) is a quantitative method designed to (1) identify the most critical assets of the network in such a way as to reduce expected loss over the entire network, (2) quantify allocation strategies that strategic planners and risk managers can apply across multi-sector systems, and (3) compute vulnerability and total risk reduction of the network.

We formalized the definition of network risk in terms of the connectivity of the network as an extension to the accepted risk equation R=f(T,V,C). We use node degree as a heuristic for criticality of an asset to the overall function of the network. We then modeled the relationship between budget and vulnerability reduction and show how an exponential reduction model compares to a linear or random model. Using the stated definition of network risk, all models rank order assets exactly the same but they reduce risk differently. Lastly, we introduce a two-party model that combines both the defender's and attacker's points of view using a game theory approach. We show the results of this model and compare them to a similar model we refer to as the "arms race model" where we allow both attacker and defender to know each other's budget. Results show that the techniques developed here are useful in conducting a systematic and repeatable analysis of an infrastructure network of assets for risk and then informing resource allocations that serve to reduce risk on the entire network, not just the selected assets.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This research would not have been possible without the support of many people. I would like to express my deepest thanks to my superiors at Bahrain Defense Force HQ:

H.H. Shaikh Salman Bin Hamad Al Khalifa

The Crown Prince and Deputy Supreme Commander of BDF

H.E. Genaral Shaikh Khalifa Bin Ahmed Al Khalifa

The Commander in Chief of BDF

H.E. Major General Shaikh Daij Bin Salman Al Khalifa

Chief of Staff of BDF

For their encouragement and support during my PhD study at this great institution for the second time to complete my graduate studies.

I would like to express my deepest gratitude to my supervisor, Dr. Ted Lewis, and committee chair, Dr. Rudy Darken for their encouragement, guidance, and support throughout my PhD research at the Naval Postgraduate School.

Special gratitude go to the distinguished members who served on my supervisory committee, Dr. Tom Mackin, Dr. Chris Darken, Dr. Jeff Crowson, and Dr. James Wirtz without whose knowledge and assistance this study would not have been successful.

Another thanks and love go to my wife, and children, Zain and Isa, for their support, patience, and never complained about the long working hours and busy weekends. Moreover, the same thanks go to my parents; I could not achieve that without all of them.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Critical infrastructures are often vast networks of connected assets that serve to provide continuous services to the nation. Their "criticality" is based on the often severe economic impact that the nation might face if those infrastructures (or parts thereof) were disabled or lost. The problem is that these networks of assets are often so large that we cannot afford to protect every mile of pipeline, every mile of power cable, every energy production facility, etc. We need to be able to identify which assets might be more critical than other assets based on some systematic, quantitative, repeatable approach that yields results that decision makers can act upon. Many of the approaches in use today are asset level techniques that evaluate the criticality of assets largely independent of the infrastructure system they are within. We assume that the connected nature of many infrastructures is important and that this should be used in identifying critical assets and informing resource allocation strategies.

This dissertation is about developing a new network-based approach and an associated tool for identifying critical assets within critical infrastructures and informing decision makers of defensible resource allocation options that might best harden and reduce risk from terrorist attacks over the entire infrastructure network. The approach relies on the assumption that *adjacency* in a network graph is important in identifying criticality. The more highly connected an asset is, the more critical it is likely to be.

In order to achieve the goal of this research, a number of issues must be resolved. Among these are:

1. We must decide how to define and model risk in a network of nodes and links. Homeland Security decision makers have been instructed to base their funding strategies on risk reduction. Since it is the whole infrastructure network that we are trying to protect, having a model of network risk is essential.

2. We must model the relationship between budget and vulnerability-reduction in a network. Risk reduction is a means of reducing vulnerability while taking consequence into consideration. If a Homeland Security decision maker is going to efficiently reduce risk, then he must "buy down" vulnerability in a cost effective manner. Relating budget to vulnerability reduction is a key element of this procedure.

3. Since it is probably true that one allocation strategy will not adequately answer all questions a Homeland Security decision maker might have in order to develop a funding strategy, we need to introduce multiple allocation strategies with a corresponding objective comparison of their utility and effectiveness.

4. Lastly, it would be useful if we could extend this work to introduce a two-party model whereby we can identify an effective funding strategy that attempts to reduce risk and then determine what the subsequent best strategy would be for an adversary to allocate his resources to increase risk.

B. LEXICON

There are a number of key terms and definitions that we must clarify as they are used throughout this dissertation. Some of these are concepts and others are specific variables we will use in the mathematical models described here.

Critical infrastructures are "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." – The USA Patriot Act. (2001)

Another definition of critical infrastructures is stated in the PDD[1] 63, (1998) as "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."

[1] Presidential Decision Directive.

The list of "sectors" varies depending on which government document is referenced but the key sectors that will be discussed in this dissertation are: energy (power), water, telecommunications, and transportation. Other sectors include agriculture (food), public health, emergency services, defense industrial base, banking and finance, chemicals and hazardous materials, and postal and shipping.

A network is a collection of assets that can be modeled as a set of nodes (also called *vertices* in graph theory) that are connected by links (also called *edges* in graph theory) and represented mathematically as G(V,E). (Horowitz & Sahni, 1978) We represent a network G(V,E) with two types of information:

1. Network structure is determined by how the nodes are connected to each other by links. (See Figure 1). The number of links connected to node i (which is the same as the number of nodes directly adjacent to node i) defines the node's degree g_i. The set of degrees g over an entire network defines its degree sequence. The degree sequence distribution is a histogram of the degree sequence summing over the entire network and is used to identify concentrations of connectivity. Barabasi (2002) defines these high degree nodes as the hubs of a network. In the approach presented here, we assume that the higher the degree, the more critical the node is to the operation of the infrastructure network.
2. Nodes and links represent assets in an infrastructure network. In the example in Figure 1, if this were a water sector analysis, the nodes might represent reservoirs and pumps while the links might represent water pipes or aqueducts.

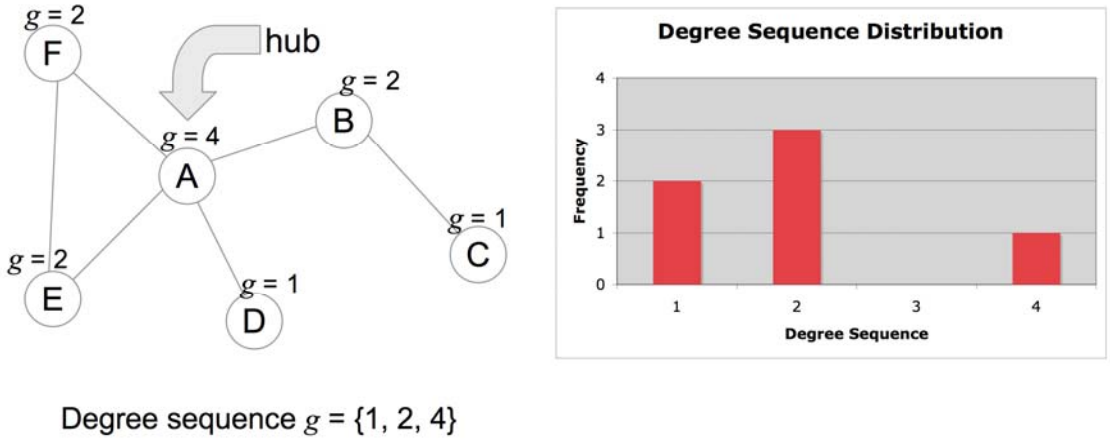

Figure 1 An example network

Threat, t, is the probability that an attack will be attempted. In the Homeland Security context, for a purposeful adversary, this estimate would be based on intelligence values. For natural events, it would be based on event probabilities from weather prediction, geological surveys, etc. For this dissertation, we assume threat to be 100% (or 1.0) thus making all events equally likely to occur, but not equally likely to succeed or to cause damage.

Vulnerability, v, is the probability that an asset fails given a particular type of attack. We define v(C) as the vulnerability function in terms of the defender's investment allocation, C; v(A) as the vulnerability function in terms of the adversary's investment allocation, A; and v(A,C) as the combined vulnerability in terms of both the adversary's and the defender's allocations.

Consequence, or damage, d, is the cost of damage associated with a successful attack, expressed in terms of casualties, loss of productivity, loss of capital equipment, etc. In this dissertation we will use asset replacement cost value in dollars. However, any of these or any combination of these are suitable for use as a consequence value. The only requirement is that the damage value definition for a specific analysis be consistent throughout. For example, if lives lost is monetized and added to damage value for a bridge, it must be added for all assets in the network. We assume that damaging any node also affects the links connected to it which is another reason why degree *g* is used to weight the value of each node.

Risk "In the context of homeland security, the NIPP framework assesses risk as a function of consequence, vulnerability, and threat: R = f(C,V,T)." (NIPP, 2006). As noted previously, in this dissertation we use the following notation:

- Consequence C is represented by the variable *d* (for "damage")
- Vulnerability V is represented by lower case *v*
- Threat T is represented by lower case *t*

We apply the risk definition as it is stated in the National Infrastructure Protection Plan (2006) by including degree sequence *g* in the risk formula. The risk equation becomes a function of degree sequence, consequence, vulnerability, and threat,

$$R = f(g,d,v,t).$$

The total risk of *n* nodes and *m* links is:

$$R = \sum_{i=1}^{n+m} t_i \; v_i \; g_i \; d_i$$

where $g_i = 1.0$ if the asset is a link (because links do not have a degree) and is equal to the degree if the asset is a node.

Attributes of nodes and links in a network include:

Consequence cost, d_i, is the expected damage or loss to an asset (node or link) if successfully attacked. It is typically estimated in dollars.

Cost to eliminate vulnerability, EC_i, is the cost to eliminate a vulnerability to its elimination fraction EF_i. It is typically estimated in dollars. This is also referred to as the Elimination Cost.

Elimination fraction, EF_i, is the vulnerability assumed by the defender for an investment of EC_i. If the vulnerability *v* of an asset is estimated at 100%, for example, and its associated elimination fraction EF is 10%, then the cost to reduce the 100% initial *v* all the way down to its minimum 10% EF is the elimination cost (EC). (See Figure 2)

Cost to increase vulnerability, AC_i, is the opposite of EC_i from the attacker's perspective to (attacker fraction) AF_i. It is estimated in dollars.

Attacker fraction, AF_i, is the vulnerability assumed by the attacker for an investment of AC_i. It can be thought of as the opposite of EF_i. The cost for the adversary to raise risk to AF_i is AC_i. (See Figure 2)

Total defensive resource, B, is the limited budget of the defender to protect and harden assets in the network. It is estimated in dollars.

Total adversary resource, B', is the limited budget of the adversary to attack assets in the network. It is estimated in dollars.

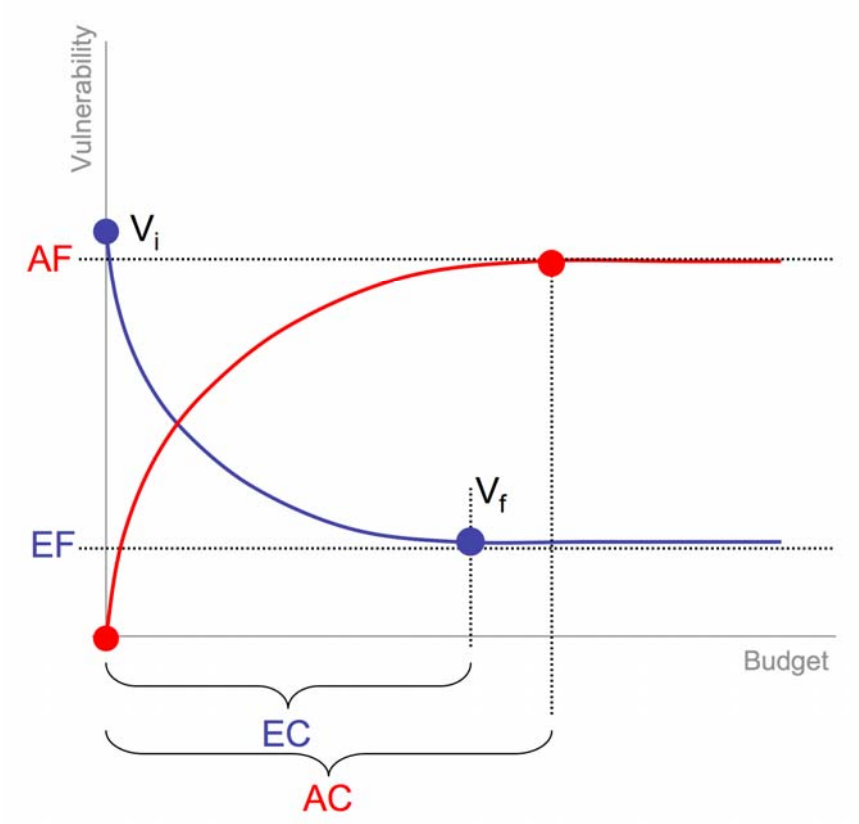

Figure 2 The key variables that relate vulnerability to budget

Allocation to harden (or partially harden) asset i, C_i, is the defender allocated cost to protect or harden asset i in a network where $0 \leq C_i \leq EC_i$. It is expressed in dollars and is computed by the model.

Allocation to attack asset i, A_i, is the allocated adversary cost to attack asset i in the network where $0 \leq A_i \leq AC_i$. It is expressed in dollars and is computed by the model.

Asset risk, r_i, is the risk of an asset and it is determined in terms of degree, vulnerability, and consequence, and is expressed by the formula $r_i = t_i\ g_i\ v_i\ d_i$ where we assume $t_i = 1.0$. This allows us to consider all events as equally likely to occur. If we had intelligence data or other information that could influence threat values, then t_i would not be equal to 1.0. In this dissertation, we will commonly omit t from the risk equation for this reason. Since links do not have a degree, we set g = 1 for links

only. Therefore, asset risk for a link would be expressed as $r_i = t_i\, v_i\, d_i$ with $t_i = 1.0$. This is identical to the DHS[2] definition except that we include degree. Asset risk is expressed in dollars and is computed by the model.

Total network risk, R, is determined as the sum of asset risk over the entire network. It is expressed in dollars and is computed by the model. Since we are using replacement cost as the damage or consequence value in this dissertation, network risk is the total expected replacement cost of components due to an attack or attacks. We cannot draw conclusions as to the specific functioning of the network since the model does not capture the flow of materials. Using this definition, the technique will focus on the components of a network that are most critical to its performance and consequently must be replaced or repaired if rendered inoperable. Currently accepted asset-level definitions for risk compute aggregated risk over a set of assets as the sum of the individual risk values. We extend this here by similarly summing the asset risk values but weighted by the degree as a heuristic for network criticality.

Network normalized risk, R_{norm}, is the total network risk (sum of all individual asset risks) divided by the sum of all potential consequences and is expressed as,

$$R_{norm} = \frac{\sum_{i=1}^{n} g_i\, v_i\, d_i + \sum_{i=1}^{m} v_i\, d_i}{\sum_{i=1}^{n} g_i\, d_i + \sum_{i=1}^{m} d_i}, \text{ where } t_i = 1.0.$$

Network normalized risk is computed by the model.

Criticality. Barabasi (2003) defines criticality as the nodes with highest degree. However, Barabasi did not consider the value of the nodes and links. Lewis (2007) defines criticality as the high-degree and high-value nodes and links because he *does* include node and link values. Brown (2006) defines criticality as the value of protecting or hardening a given asset or a group of assets.

[2] Department of Homeland Security.

We define criticality as a measure of an asset that describes the relative negative impact on the overall network if that asset were disabled or removed from the network. The more important an asset is to the efficient functioning of the network, the higher its criticality. We assume that this is strongly influenced by degree sequence. We therefore use degree sequence *g* as a heuristic for criticality. The higher a node's degree, the more likely it is to be critical. We express this mathematically in this dissertation.

C. CONTRIBUTION

The National Infrastructure Protection Plan states as its goal to "Build a safer, more secure, and more resilient America by enhancing protection of the Nation's critical infrastructures and key resources to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency." (NIPP, 2006)

However, we simply do not have the financial resources to protect everything we might identify as critical in an infrastructure or key resource. Therefore, developing a systematic method of (1) identifying which assets in an infrastructure might be more critical than others and then (2) informing a resource allocation strategy for the protection of our infrastructure systems is paramount to successfully meeting the goal of the NIPP.

Methods already exist that address this problem. The methods that have been approved by DHS for use by state, local, and federal organizations are what we refer to as asset level tools. They rely on lists of assets that can be ranked by criticality, where criticality is based on their respective value, visibility, expected threat, etc. What they do not do is account for the network characteristics of assets in an infrastructure. This dissertation will address this shortcoming and enable the CIP analyst to:

- Model risk in an arbitrary network and provide a solid definition of network risk that directly applies to critical infrastructure systems not just to isolated assets.
- Find an optimal allocation of resources for both defender and attacker, assuming the defender wants to minimize network risk and the attacker to maximize it.

- Employ a quantitative method in the field of critical infrastructure protection for modeling risk assessment of an entire system represented as a network.
- Provide the risk-assessment analyst and policy maker with supportable systematic answers as to how much funds are needed to protect the most critical components of the infrastructure against plausible threats.
- Help policy makers identify critical assets, assess their vulnerabilities, and make rational and optimal decisions as to how to allocate a limited budget to protect the critical infrastructure, based on mathematical techniques and expert opinion in a careful and educated manner.

D. SIGNIFICANCE

This research will contribute to the approaches senior officials in the Department of Defense, Department of Homeland Security, and their allied international counterparts may use to discover weaknesses in infrastructure networks, identify vulnerabilities and risk, and decide how best to allocate limited resources to minimize overall risk. Officials may use these tools to:

- Quantify "vulnerability" and "risk" so the same definitions apply to all sectors (NIPP, 2006).
- Analyze single and combination events (i.e., multiple-threat attacks).
- Identify what is truly critical in a critical infrastructure.
- Quantify the allocation of resources to reduce vulnerability and risk based on a systematic methodology.
- Provide a rational approach to protecting, increasing the security of, and reducing the risk to critical infrastructure nationwide.
- Provide the policy-maker with a supportable systematic strategy as to how much resources are needed to protect the most critical components of the infrastructure.
- Define a quantitative, repeatable method that is in agreement with current DHS guidelines.

E. DISSERTATION OVERVIEW

This dissertation is organized as follows.

Chapter II: Literature Review surveys the literature of critical infrastructure protection (CIP), comparing different tools used in Homeland Security, discussing various definitions of risk, comparing recent concepts of resource allocation used to distribute resources, and presenting the existing game-theoretical defender-attacker models used in the CIP.

Chapter III: MBRA Tool describes the decision tool and its menus.

Chapter IV: One-Sided Risk Model defines network risk and introduces two investment cost models linear and nonlinear that are used in MBRA tool. We illustrate the approaches taken to achieve vulnerability-reduction, identify critical assets, and minimize network risk from defender's perspective.

Chapter V: Two-Person Game introduces investment cost model to model network by using a joint (combined) function, and introduces allocation strategies used in MBRA tool from defender and attacker perspectives.

Chapter VI: Results, conclusions and future work presents results from comparing two different tools CARVER and MBRA. It summarizes the contribution made by this dissertation and considers possible expansions.

II. LITERATURE REVIEW

United States Secretary of Homeland Security Michael Chertoff discussed risk management in the Wall Street Journal on 14 February 2006 entitled "There is no perfect security," which encourages the use of risk management principles to homeland security.

> This process of assessing risk and setting priorities should be familiar to those in the private sector. Companies use risk management to make tough decisions and weigh the costs and benefits of a particular set of investments in money and effort against an array of potential outcomes. For our department, risk management starts with weighing threats, vulnerabilities and consequences of a potential terrorist attack or catastrophic event, then conducting a rigorous, information-driven analysis both to set priorities for resources and to give focus and strategic direction to our policies and programs.
>
> In short, we drive homeland-security investments by looking to facts and analysis, not politics. We acknowledge, however, that while most people support risk management in theory, enthusiasm tends to diminish once it is applied in practice. This is because risk management, by its very nature, involves a trade-off. In a free and open society, we simply cannot protect every person against every risk at every moment in every place. There is no perfect security. If we tried to attain total security the cost would be exorbitant – in financial terms and in lost freedom and prosperity. Balancing risk necessarily means applying resources against the highest risks – and not against all risk. As in any trade-off, some will gain resources and others will not." (WSJ, 2006)

If a risk assessment methodology is to be driven by facts and analysis rather than politics, then it needs to be defensible. This implies that the results are repeatable and as objective as possible. Trade-offs are made between assets – but these assets may or may not be linked via a network infrastructure. Therefore, considering the network is key.

The literature review in this chapter will include three main areas:

1. An overview of tools supporting risk analysis in Homeland Security. We will focus mainly on practitioner level tools in use by the Department of Homeland Security and their related organizations. Other tools exist or are in development which are not discussed here. Since the technique

developed in this dissertation was based on a methodology approved by DHS, we compare our results only to other approved DHS methodologies and tools.

2. Definitions of risk and how they are related to networks in critical infrastructure protection (CIP), and
3. Resource allocation techniques that use game-theory approaches for max-min problem of two players (terrorist and defender).

A. TOOLS AND TECHNIQUES FOR RISK ANALYSIS IN HOMELAND SECURITY

This section will give a brief description of the tools that are used by practitioners to support risk analysis in the U.S. Department of Homeland Security and related agencies and organizations. Each tool has its respective strengths and weaknesses. We will describe each method or tool and end with a summary.

1. RAMCAP – (Risk Analysis Methodology for Critical Asset Protection)

RAMCAP is a tool designed to analyze and manage the risk of assets associated with terrorist attacks in critical infrastructure. RAMCAP is comprised of seven steps in analyzing risk: (1) Asset characterization and screening. (2) Threat characterization – based on current intelligence. (3) Consequence analysis – measured in financial costs, fatalities and injuries and provided by DHS based on a spectrum of threats. (4) Vulnerability analysis – the determination of the likelihood for a successful attack using a specific threat on a particular asset. (5) Threat assessment – provided by DHS based on intelligence assessments of adversary capabilities and intent. (6) Risk assessment – a systematic and comprehensive evaluation of the terrorist attack scenario for a given asset. (7) Risk management – the process of understanding risk and deciding upon and implementing action to achieve an acceptable level of risk at an acceptable cost.

RAMCAP is a general asset level tool. It is not specific to any one sector. It takes lists of assets, prioritizes them based on heuristics of value, threat, and consequence, and then presents its output as asset level risk. It is up to the analyst to decide how to “buy

down" risk based on the results of the analysis. RAMCAP is not capable of determining how limited resources can be distributed among all assets to reduce risk nor is it modeling risk of a group of assets forming a network. (RAMCAP)

2. CARVER – (Critical Accessibility Recoverability Vulnerability Espyability Redundancy)

CARVER is an asset level tool designed by the National Infrastructure Institute to identify the most critical infrastructure assets and systems in the United States. It prioritizes assets across sectors and ranks them according to their criticality by aggregating the highest scores obtained in each of six categories: criticality, accessibility, recoverability, vulnerability, espyability (notoriety), and redundancy. CARVER uses tables supplied by the developer for weighting the different elements. The tables and the algorithms are proprietary and are the basis of the ranking. CARVER relies on panels of subject matter experts who provide estimates on the six attributes for each asset using a ten-point scale to rank vulnerabilities. Two teams of experts will commonly arrive at different evaluations of the same asset because their respective inputs to the model will not be identical. Because CARVER relies on subjective inputs, it lacks rigorous standards for measuring and reporting risk.

CARVER is a general purpose tool that is designed to cover all sectors and to some extent the interrelationships between sectors. CARVER does not consider the fault probability or funds necessary to protect assets nor does it directly consider the networked aspects of a sector. It considers cross-sector attributes by asking the analyst to directly state which sectors the asset might affect. (CARVER)

3. MSRAM – (Maritime Security Risk Assessment Methodology)

MSRAM is an asset level tool designed to analyze terrorism risk and is used by the U.S. Coast Guard. The assessment of risk is based on scenarios that combine types of targets and terrorist attack modes. MSRAM uses the risk formula defined by the DHS that depends on three elements; threat, vulnerability, and consequence.

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

The threat attack probability depends on the terrorists' intent and capability to deliver an attack on specific target and it is provided by the DHS. Vulnerability assessment based on factors such as attack difficulty, the ability of USCG to interdict an attack, and the ability of the target to withstand the attack. The consequence is defined as the negative impact of a successful attack and it is measured in terms of injuries/deaths, economic impact, environment impact, national security impacts, and symbolic impacts. (Downs, 2007)

MSRAM is an asset risk-management tool that assesses risk based on scenarios. The tool uses a scale system to compute risk similar to other qualitative tools. It identifies and prioritizes assets according to their risks. MSRAM does not consider the amount of resource allocations needed to protect the assets from terrorist attacks.

4. TRAM – (Transit Risk Assessment Tool)

TRAM is an asset level tool developed by the U.S. Department of Homeland Security (DHS), Office of State and Local Government Coordination and Preparedness (SLGCP), Office for Domestic Preparedness (ODP) specifically for the transportation sector. TRAM is the underlying framework for MSRAM. Consequently, they share many of the same strengths and weaknesses. The main objectives of the tool are "to compare relative risks of acts of terrorism against critical assets owned and/or operated by transit agencies and to identify and prioritize enhancements in security, emergency response and recovery that the agencies can implement to reduce those risks". TRAM is composed of seven attributes to assess risk: (1) Criticality assessment, (2) threat assessment, (3) vulnerability assessment, (4) response and recovery capabilities assessment, (5) impact assessment, (6) risk assessment, and (7) needs assessment. The overall risk is determined as the product of the threat, vulnerability, and consequence ratings. The method uses a rating scale from zero to ten. The tool will identify critical assets based on rating scores obtained by best expert judgments to assess overall risk.

TRAM is threat specific. It links assets to their respective threats via scenarios. It then identifies countermeasures that would mitigate some part of the risk for that asset. It is particularly good at being specific about countermeasures appropriate for a given threat for an asset but since it is not a network model, it is not able to accurately model the network aspects of an infrastructure network. (TRAM)

5. Model –Based Risk Assessment (MBRA)

We will provide only a very brief summary of MBRA here as it is fully described in the next chapter. MBRA (Lewis, 2006) was developed as a technique based on network science that would be a practitioner level tool that facilitates the modeling of infrastructure networks for the purpose of assessing risk and informing resource allocation strategies that reduce risk over the system. It is a *systems* level approach, not an asset level approach. It was intended to be relatively easy to use and should produce results that were repeatable (meaning that two analysts performing the same analysis would get approximately the same result), "aggregable" (meaning that two "adjoining" analyses could be joined into one analysis that yields correct results), and quantitative (meaning that it was intended to avoid "ratings" that could be viewed as the opinion of a subject matter expert). The technique uses network models to identify critical assets in a network and then uses fault tree analysis to refine resource allocation strategies.

6. Summary

In Table 1, we compare some key attributes of the tools surveyed here. Generality refers to the tool's ability to assess infrastructure in any of the sectors, not just one or two specific ones. Network model refers to the tool's ability to consider the network attributes of a sector. Risk calculation refers to whether or not the tool calculates risk using the approved DHS risk equation. Resource allocation refers to whether or not the tool is able to directly inform the allocation of resources (mainly funding) to the assets in question to buy down risk, or alternatively, if it indirectly informs resource allocation by ordering criticality. Repeatable refers to whether or not two analysts using the same descriptive data will come up with the same result.

Table 1 Comparison of DHS tools

	RAMCAP	CARVER	MSRAM	TRAM	MBRA
Generality	All sectors	All sectors	Ports	Transportation	All sectors
Network model	Asset level	Asset level	Asset level	Asset level	Network
Risk calculation	No	No	Yes	Yes	Yes
Resource allocation	No	No	No, asset level	No, asset level	Yes, network level
Repeatable	No	No	No	No	Yes

The primary criticism of existing practitioner tools for critical infrastructure assessment is that they rely heavily of subjective inputs thus limiting the repeatability of the results and they also neglect the network characteristics of many infrastructure sectors. What is desirable is a tool that (1) uses network science theory to help identify which assets in a network are the most critical and then (2) directly informs the resource allocation process to efficiently "buy down" network risk in the sector.

B. DEFINITIONS OF RISK IN CIP

It might be assumed that the concept of risk is fairly well understood and that definitions for risk have been developed, agreed upon, and are in use in critical infrastructure assessment today. After all, the Secretary of Homeland Security says we are going to use a risk based approach for investment in critical infrastructures. Unfortunately, only recently has a definition of risk begun to emerge. Many definitions of risk have been proffered as practitioners have defined terms to meet their particular needs. This section presents commonly used definitions and their relationship to the definition recently adopted by the Department of Homeland Security which is also the definition used in this dissertation. Most risk definitions, (NIPP, 2006), (Roper, 1999), (RAM, 2000), (FEMA, 2007), (Willis, 2005), (Mackin, 2005), (Wilcox, 2005), (Moteff, 2005), are expressed as a function of three variables threat, vulnerability, and consequence with minor changes in notations in assessing risk of a single asset.

$$R = f(C,V,T)$$

where,

C = Consequence

V = Vulnerability

T = Threat

In the United States, the White House encourages using risk management strategies to protect infrastructure against terrorist attacks as defined in HSPD[3]-7 (2003).

> (19) In accordance with guidance provided by the Secretary, Sector-Specific Agencies shall:
>
> > (a) collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;
> >
> > (b) conduct or facilitate vulnerability assessments of the sector; and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

The U.S. Department of Homeland Security states the definition of risk in (NIPP, 2006) as

> In the context of homeland security, the NIPP framework assesses risk as a function of consequence, vulnerability, and threat.

The U.S. Government Accountability Office states the risk formula as

> In our framework, risk assessment is a function of threat, vulnerability, and consequence. The product of these elements is used to develop scenarios and help inform actions that are best suited to prevent an attack or mitigate vulnerabilities to a terrorist attack, in conjunction with the risk-based evaluation of alternatives undertaken while considering cost and other factors. (GAO-06-91, 2005)

[3] Homeland Security Presidential Directive.

Risk can be determined quantitatively by multiplying the estimated adverse impact of a successful threat/attack scenario by the probabilities associated with threat and vulnerability. We define impact as consequence, measured in loss of lives, financial loss, or some other quantity, and then define risk as expected loss due to a successful attack on an asset.

Expected loss = (Consequence) x (Probability of an attack) x
(Conditional probability that attack is successful)

We define probability of attack as *threat*, and probability that an attack succeeds as *vulnerability*. Thus, the total expected replacement cost of components due to an attack or attacks is obtained by multiplying threat, vulnerability, and consequence:

Risk = Total expected replacement cost = Threat x Vulnerability x Consequence

This is the definition adopted by DHS. The objective of critical infrastructure risk assessment is to decrease risk by reducing threat, vulnerability, and/or consequence. For example, risk can be reduced by diminishing the threat to the asset (e.g., by eliminating or intercepting the adversary before he strikes); reducing vulnerabilities, (e.g., hardening or shielding the asset to withstand the attack; and softening the impact or consequence of an attack (e.g., by building backup systems or isolating facilities from dense populations).

According to Roper (1999), risk is the potential for damage or loss of an asset, and risk assessment is the evaluation of threats to and vulnerabilities of an asset for the purpose of rendering an opinion as to its probable loss or damage and the potential impact of such. The aim of risk assessment is to guide preventive action (Roper, 1999). He proposed a formula for risk as a function of three variables: impact, threats, and vulnerabilities.

Roper's qualitative risk management process consists of a five-part assessment: first of the asset, then threats, vulnerability, risk, and countermeasures. Roper's process does not consider resource allocation or the attacker's point of view, yet the definition of risk used is remarkably similar to that eventually adopted by DHS.

Sandia National Laboratories defines risk in their risk-assessment methodology (RAM, 2000) for physical security by the formula:

$$Risk = P_A*(1 - P_E)*C$$

where

P_A is the likelihood of adversary attack,

P_E is security system effectiveness,

$1-P_E$ is adversary success, and

C is consequence of loss to the attack.

If we consider P_A to be threat, $(1-P_E)$ to be vulnerability, and C to be consequence, the definition is the same. Lewis (2006) takes a similar approach when he introduces the concept of availability which is defined as the complement of vulnerability (1-*v*). Sandia refers to this as "security system effectiveness".

The Federal Emergency Management Agency (FEMA, 2007) defines risk "as the potential for a loss or damage to an asset to occur. It takes into account the value of an asset, the threats or hazards that potentially impact the asset, and the vulnerability of the asset to the threat or hazard." (FEMA 426, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, pages 1-35 to 1-44). The risk assessment is determined and applied to individual assets using the DHS risk formula. This is again very similar to the accepted DHS definition, not surprising given that FEMA is a part of DHS. Yet other similar definitions exist.

Another definition of terrorism risk is provided by RAND, the center for terrorism risk management policy (Willis, 2005, 2007) as a function of threat, vulnerability, and consequences.

RAMCAP is designed to analyze risks associated with adversary attacks. RAMCAP defines risk by the same DHS formula. (Mackin, 2005)

According to Wilcox (2001), risk is the potential of loss from exposure to a hazard and is represented as the product of occurrence likelihood and accident impact. Wilcox's definition ignores vulnerability, but includes consequence in the form of impact.

A very different definition of risk, found in the Moteff Report for Congress (Moteff, 2005), ranks risk along a qualitative scale, e.g., high, medium, and low depending on different qualitative measures of threat and vulnerability. The problem with conclusions drawn by means of these definitions is that they are not repeatable – experts will likely disagree as their standards for high, medium, and low diverge. This definition therefore is of little value to the analyst.

None of these definitions in and of itself can identify the most critical components of an infrastructure system. Rather, the risk definition models risk of individual assets so that we can compare them on an equal basis. If the DHS definition of risk captured everything that was important to know to identify critical assets in an infrastructure, then any of the rank ordering techniques would be suitable. However, we claim that the definition of risk is important, but inadequate for assessing criticality. Connectedness matters, therefore we need to consider the network characteristics of an infrastructure in order to decide what is critical. Without this, we leave the problem of identifying critical assets to the analyst's judgment, which is often indefensible, and rarely repeatable.

Lewis (2006) borrowed the concept of modeling critical infrastructure systems as vast networks from Barabasi (2002, 2003) and other pioneers of network science. The main idea was that critical infrastructure systems, seemingly random networks of assets, are actually structured. In the terminology of network science, critical infrastructure systems were more likely to be scale-free or small world networks than random networks. This is key, because it allows the defender to identify the most critical nodes and links of a system which should be protected, even at the expense of other nodes and links. The strategy is to use this hidden structure to help identify criticality.

In fact, Albert and Barabasi showed that the most-highly connected nodes of a network could be the "Achille's heel" or vulnerable point of a system modeled as a network (Albert, 2000). If we construct a *degree-sequence distribution* as a histogram showing the percentage of nodes of degree d versus d, we can see the types of structure Barabasi describes. Barabasi renewed scientific interest in networks with heavily skewed degree distributions, in which there are many nodes of low degree, but only a few of high degree (the "hubs"). Barabasi (2002, 2003) defines a *scale-free network* as a network that obeys the *power law*, which describes the degree-sequence distribution of a scale-free network. For the purposes of this dissertation, we are more concerned with networks of scale-free properties than we are networks that strictly conform to the power law. Simply stated, scale-free networks have large hubs which we assume to have significant importance to the overall function of the network.

Lewis combined network theory with probabilistic risk analysis to model infrastructure as a network, and risk as an melding of the DHS risk definition and Barabasi's concept of vulnerability influenced by degree sequence (Barabasi, 2003). The model proposed by Lewis reverts to the Barabasi model when all nodes and links are of equal value. However, when the value of nodes and links vary, the model yields a measure of risk that applies to any arbitrary network with heterogeneous values. It does not assume that nodes with high degree are the most critical. Nodes of lesser degree can be more critical if their value is very high. But criticality is highly influenced by degree. The extension of Barabasi's model to arbitrary networks with arbitrary node/link consequences and vulnerability-reduction costs was a very important step towards a unifying theory of critical infrastructure protection based on risk reduction. However, Lewis did not formalize his model or solve it for linear and non-linear cost functions.

The next step in the evolution of critical infrastructure risk assessment required a definition of risk that extended to networks, not just the individual assets within the network. Lewis's definition of criticality needed a corresponding definition of network risk. The barbell model proposed by Lewis (2006, 2007) defined network risk as the sum of barbell risks, where a barbell is a sub-network, as shown in Figure 3. A barbell

consists of two nodes (A and B) and a link (L) that joins them. Lewis obtained network risk by summing the risk of each barbell over the entire network. Hence, network risk is defined in Lewis (2006) as the sum over *n* nodes and *m* links:

$$R = \sum_{i=1}^{n+m} g_i \, d_i - \sum_{i=1}^{n+m} g_i \, a_i \, d_i = \sum_{i=1}^{n+m} (1 - a_i) g_i \, d_i$$

$$= \sum_{i=1}^{n+m} v_i \, g_i \, d_i$$

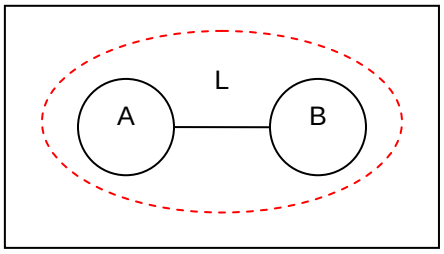

Figure 3 A barbell sub-network

In this section, we have reviewed several different ways to define risk, but most of these definitions agree that risk is the product of threat, vulnerability, and damage. This is the definition that DHS has adopted. We use quantitative techniques to compute the value of risk, so that we can develop allocation strategies for resources to reduce risk in a quantitative manner.

C. RESOURCE ALLOCATIONS AND TWO-PERSON GAMES

Key elements of this dissertation research include the ability to relate resource allocation to vulnerability and also to include a two-person game where we can look at what an intelligent adversary might do as a result of a specific allocation. This section will present an overview of the literature related to these issues.

1. Resource Allocation Strategies and Methods

Lewis (2006) generalized the Albert-Barabasi (2000) result by introducing consequences; each node and link is assigned a damage value in addition to degree. However, Lewis assumed a linear relationship between allocation and reduction of

vulnerability, which is simple but unrealistic. In addition, Lewis offers a heuristic solution to his model and does not provide a closed-form solution to the minimum risk allocation problem we solve in this research.

This research extends Lewis's linear cost model and gives closed-form solutions to the problem of allocating a fixed budget to nodes and links such that risk is minimized. Lewis defined network risk as the sum of all barbell risks in the network:

$$R = \sum_{i}^{n+m} g_i \, v_i \, d_i$$

where

g_i = degree of node if asset i is a node, and is 1 if asset i is a link.

v_i = probability of failure, if attacked.

d_i = damage/consequence if asset i fails.

In addition, this research extends Lewis's previous results to a non-linear vulnerability-reduction cost function that models the diminishing returns of asset protection where the effectiveness of an allocation drops off exponentially as more resources are allocated to a node or link. This is a more realistic model. It assumes that the policymaker will invest first in the most cost effective countermeasures (in terms of their risk reduction per dollar ratio) working towards the least cost effective countermeasures.

Xie, Tan, and Goh (2000) present a technique for setting priorities and optimal resource allocation using fault-tree analysis (FTA) techniques. They add the number of AND gates leading up to a top event from its basic event. The more AND gates an event has along the path to the top, the less important the basic event. (Xie, 2000). This method of qualitative ranking aims to identify the most significant groups of basic events, rather than provide an exact rank for all basic events. It lacks the capability to model risk and allocate resources.

2. Two-Person Games

Danskin (1967) provides a comprehensive theory of max-min games with many military applications. Several of his applications and solution techniques have modern-day analogs to problems in Homeland Security and Defense.

Owen (1969) considers the case of a two-sided war game in which the attacker is constrained by the number of missiles to maximize the damage of cities, and the defender is constrained by budget limitations to defend the cities with two types of defense: active defense using anti-missile systems and passive defense using shelters. Owen applied his model to minimize fatalities in a nuclear attack. His approach can be modified and applied to assets in a network using the two-sided approach in which the attacker is constrained with a limited budget to maximize the risk of the network, and the defender is constrained by budget constraint to minimize the network risk.

Croucher (1975) considers a two-sided resource allocation game in which both players, attacker and defender, have fixed resources which may be distributed over different targets. Croucher applied the fundamentals of game theory to an example concerning antiballistic missile defense. He examined the problem where a number of targets attacked and defended with the use of missiles. The attacker's total resource consists of a number of ballistic missiles (BM's) to attack k targets, and the defender's resource consists of a number of antiballistic missiles (ABM's) to defend the k targets. He defines a combined probability function in terms of the attacker resource, x, and the defender resource, y, as

$$p(x,y) = \left[1 - e^{-a\,x}\right]\left[e^{-b\,y}\right].$$

The total expected payoff to the attacker is expressed as the product of the combined probability function and target value

$$F(x,y) = \sum_{i=1}^{k} v_i \;\; p(x_i, y_i) = \sum_{i=1}^{k} v_i \left[1 - e^{-b_i\,x_i}\right]\left[e^{-a_i\,y_i}\right]$$

subject to the attacker and defender budget constraints

$$\sum_{i=1}^{k} x_i = X\,, \qquad \sum_{i=1}^{k} y_i = Y$$

where,

a_i, b_i are vulnerability factors

v_i is the values associated with target i

Croucher provided optimal allocation solutions to the problem using Kakutani fixed point theorem (Kakutani, 1941). Where X(y) is the set of points which maximizes F(x, y) for fixed y, and Y(x) is the set of points which minimizes F(x, y) for a fixed x.

Croucher's approach is an important improvement. It involves intensive computations, but it introduces a simple combined probability function, and provides continuous optimal allocations for the attacker and defender. This approach was applied to the allocation of ballistic missiles in the seventies. The approach is still valid now and can be applied to a new type of threat and assets, that is, the threat of terrorist attacks and networked critical infrastructure assets. We rely heavily on Croucher's results in Chapter V.

In related work, Major (2002) models terrorism risk as a two-person, zero-sum game with payoff (expected loss) to the attacker. The attacker has the option to choose the target and assign a resource to it. The defender has to assign resources to all targets simultaneously. The defender wants to minimize, and the attacker to maximize, expected loss.

Major shows how to find an optimal allocation of resources for both attacker and defender using game theory. Major defines expected loss or risk (EL) as a function of both attacker and defender resources, and the value of the asset.

$$EL = \sum_i V_i \, p(V_i, A_i, D_i), \text{ and } \quad p(V_i, A_i, D_i) = \left\{ e^{\frac{-A_i D_i}{\sqrt{V_i}}} \right\} \left\{ \frac{A_i^2}{A_i^2 + V_i} \right\}$$

where,

$p(V_i, A_i, D_i)$ is the probability of a successful attack of target i and it consists of two terms: the probability of a planned attack escaping detection and the probability of successful attack given it is undetected.

V_i the target value

A_i the resource assigned to target i by the attacker

D_i the defender allocation to defend the asset

In Major's model, the assets are ranked according to their values that indicate their criticality. The high value targets will get higher allocations than the low value targets. Moreover, the assets are treated independently with no network model included.

Powers (2005) extended Major's (2002) probability model by allowing simultaneous attacks on multiple assets. Powers introduced a sophisticated attacker-defender model where the defender wants to minimize the attacker's payoff and the attacker maximizes the defender's payoff. He applied a Lagrange multiplier technique to solve the problem. We employ a similar technique to find optimal resource allocation to a network of connected assets, nodes and links.

Powell (2005, 2006) presented a basic game-theory framework for allocating defensive resources against long-term threats. Resources are allocated to harden sites, reduce vulnerabilities, and make the sites less attractive and difficult to attack. Optimally, the defender will allocate resources to minimize the attacker's payoff, and conversely, the attacker will allocate resources to maximize the defender's payoff. Powell's model follows the risk-management approach definition as the product of three elements: threat, vulnerability, and consequence as stated in GAO 2005, 25. Powell's model employs sophisticated math and intensive computations to determine the attacker and defender allocations. We employ a similar risk-management approach to model a network of connected assets rather than individual assets.

Bier (2002) proposed a method for optimal resource allocation for the defense of simple series and parallel systems using game theory to characterize optimal defensive strategies against intentional attack. Bier assumes that the attacker wishes to maximize the probability of success for an attack on the system. Bier defines the probability of success of an attack against a component, as a function of the defensive resources expended to strengthen that component, $P_i(C_i) = a_i\ e^{-bC}{}_i$, where C_i is the defender allocation to defend component i, and a_i and b are constants. The defender wishes to minimize the objective function with or without budgetary constraints. In other words, the defender tries to reduce the probability of successful attack on a component (that is, reduce vulnerability).

Bier (2005) extended her previous work by assuming the attacker will maximize the expected damage of an attack on the system, while the defender will try to reduce expected damage, subject to a budget constraint (in other words, risk reduction). Bier added component values into the objective function. Her model is applied to a system with components connected in either series or parallel and showed how to allocate resources in hardening components using reliability analysis, game theory, and optimization; when combined they can be applied to networks. The model does not determine the allocation of attacker resources to components when the attacker wishes to increase the expected damage of the system.

Brown (2006) introduced attacker–defender (AD) and defender–attacker–defender (DAD) models of network interdiction and applied them to critical infrastructure protection. The AD interdiction model is a bi-level Stackelberg game (Stackelberg, 1952), and DAD is a tri-level game. The models assume transparent information between the attacker and defender. The objective of the defender in these games is to minimize network operating cost, and the objective of the attacker is to maximize this minimum cost.

The approach used in the class of models studied by Brown et al. assumes each network asset is either attacked or not using binary variables to model attacks. These models determine the optimal attack of an infrastructure system given that the defender will operate his system optimally after the attack has occurred. The resulting models are integer linear programs that can be solved with commercially available software.

In this dissertation, we propose an alternate approach whereby network assets succumb to attacks with a certain probability (rather than a binary number), and vulnerability can be "bought down" by making an investment in each node or link of the network. In the new model, partial protection of assets is not only allowed, but assumed, because the defender does not know where an attacker may attack and he has limited funds. In addition, the new model proposes two new vulnerability reduction equations: linear and exponential. Instead of a binary relationship between attacker and defender, the

new model investigates allocation strategies for linear and exponential reduction equations. The vulnerability reduction models are explained in detail in Chapters III and IV.

One can think of the attacker-defender models of Brown et al. as deterministic network models and the new models here as stochastic. Therefore, risk is defined as expected loss. The objective is to reduce risk, not maximize commodity flow. It could be that in many cases, reducing risk means maximizing flow, but in the new model this is not assumed. In particular, if we consider social networks or other networks where there is no obvious commodity flowing through the network, we need this alternate approach that is not flow-based. Since minimization of risk is the objective (rather than maximization of flow), a new definition of network risk must be considered. In this work, network risk is a function of the structure of the network as well as the consequences and costs incurred in protecting its nodes and links. This leads to a formulation of risk that considers network degree sequence, node/link consequence, and vulnerability-reduction models (linear and exponential). The model will be described in detail in Chapter IV.

The new definition of network risk used in this dissertation has its pedigree in probabilistic risk-assessment (PRA) rather than the optimization literature. Since the problem domains are similar, we offer an example optimization approach for comparison purposes. This work combines PRA definitions with network theory to define risk in terms of network structure and component risk. This is in contrast to the network-intervention literature that addresses the flow of a commodity in a network and uses deterministic allocation strategies. Both approaches consider the network characteristics of the infrastructure but clearly, there are cases where one strategy is more suitable than the other.

These models provide the basis for a defender-attacker model that, when combined with network analysis, comprehensively models system-wide risk. We propose a new risk model that incorporates both defender and attacker as proposed by Major (2002), Powell (2005, 2006), and Powers (2005), but in addition, combines network effects as proposed by Al Mannai and Lewis (2007). We refer to our model as a "two-player" model so as not to confuse it with the defender-attacker model previously

described in the optimization literature. The objective of our model is to "buy down" risk by reducing vulnerability partially or fully, depending on the vulnerability reduction equation. This requires a new definition of network risk, and an equation that relates vulnerability to investment.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MODEL-BASED RISK ASSESSMENT (MBRA) TOOL

This chapter will give an overview of the design structure of the Model-Based Risk Assessment (MBRA) tool that we will use throughout this research. The MBRA process was described previously. The purpose of this section is to familiarize the reader with the tool as it relates to the process.

A. MBRA TOOL DESCRIPTION

Lewis (2004) originally created the Model-Based Risk Assessment (MBRA) tool. We modified the tool by adding different algorithms such as the linear and non-linear cost reduction models, resource allocation strategies, and risk assessment that can be applied to analyze various critical infrastructures when modeled as a network composed of nodes and links for single player and two-party models.

The main feature of the MBRA tool is the network model. Not only is the network model important to the algorithms used, but we have found that the network model also adds some level of simplicity for the analyst because the network abstraction is easily comprehensible. The infrastructure looks like what it is. In fact, many analysts use Google™ Maps or other imagery underneath their network models to further clarify the abstraction.

MBRA uses a graphical user interface (GUI) to choose from different menus in order to create a network as nodes and links, enter the values associated with each asset (node and link), run different models, and view the results on the screen monitor. The MBRA tool presents other features such as computing the allocations of each asset for a single player and two-party models based on a limited budget. It computes the risk of each asset and the total risk of the network. In addition, it prioritizes the assets according to their criticality.

B. INTERFACE DESCRIPTION

Figure 4 shows the main window of the MBRA tool with an example of water and power displayed. The MBRA tool consists of:

- Upper panel is composed of:
  - Menus: File, Examples, Consequence, Layout, and Allocation Strategies
  - Network editing buttons: Add Node, Erase Node, Add Link, Erase Link, Edit Defender, and Edit Attacker.
- Display area is composed of:
  - The network created for analysis as nodes that may represent a city, power station, reservoir, refinery, internet switch, etc., and links that may represent roads between two cities, power cables, oil pipelines, fiber-optic cables connecting internet switches, etc.
  - The chart located at the lower left corner of the display represent the degree sequence distribution (histogram) used for identifying the hidden structure of the network. It also computes the best fit to a power law although this is not used directly in this research.
- Bottom panel is composed of:
  - Input fields: Attacker Budget, and Defender Budget.
  - Control buttons: Allocation on, Max Flow On, Depercolate, Propagate ON, Kirchhoff, Reset, and Next Page.

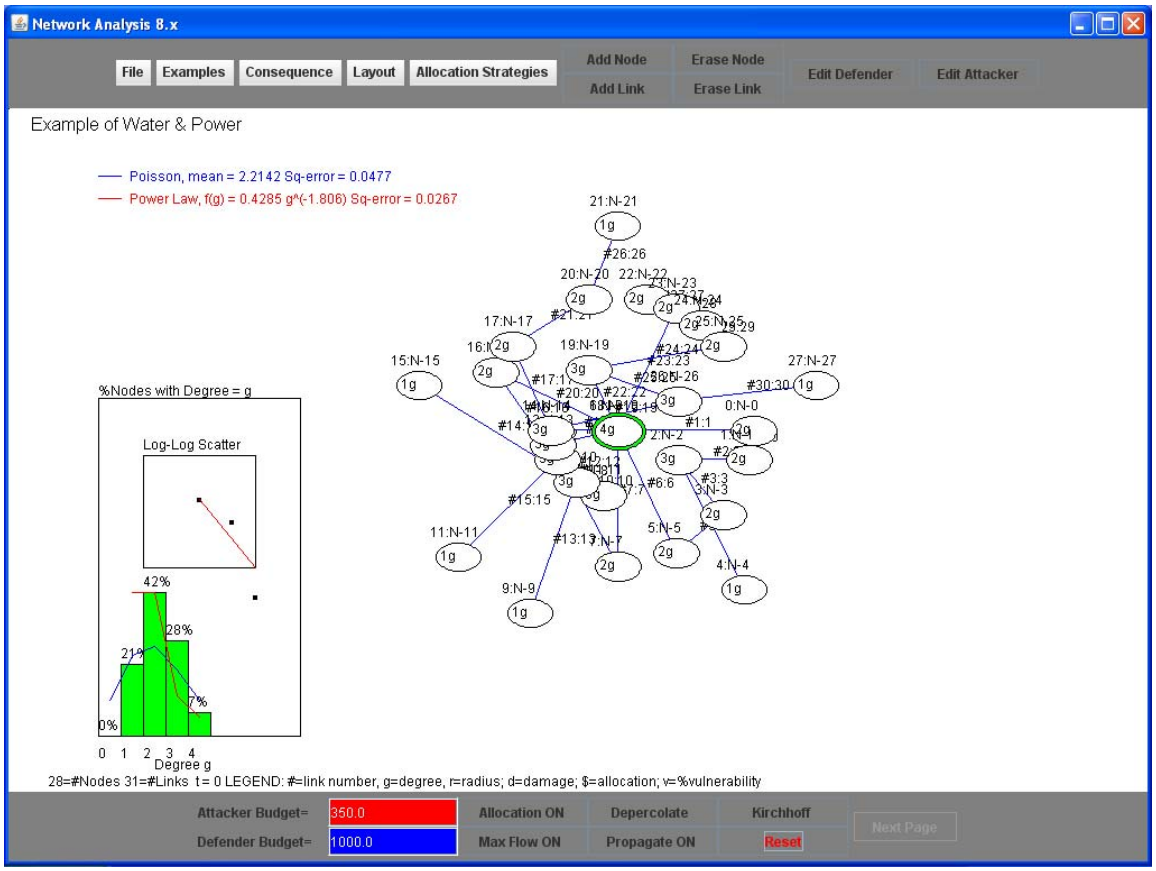

Figure 4 The main MBRA window

The allocation strategies menu in Figure 5 includes all the combinations developed for this dissertation. The three allocation strategies are random, linear, and exponential. We also include an "arms race" model that will be described in detail in the next chapter. Any of these can be matched with any other in a two-party model. To perform a single party analysis, we set the attacker budget to $0. Giving the attacker no resources effectively eliminates it from the analysis.

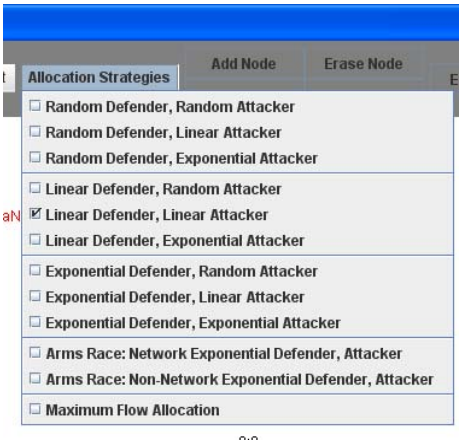

Figure 5 Allocation strategies menu

The analyst has to specify what the consequence value is on which the allocation will be based (see Figure 6). There are many to choose from. The tool allows for number of casualties, repair time, psychological cost, capital loss, economic loss, or any other kind of loss. The technique is not specific to any type of consequence value but it is critical that the analyst be consistent in choosing and providing values for consequence across the entire network. If economic loss is chosen as the consequence value, then an economic loss value must be included with every asset that is to be considered in the analysis. If this is not provided consistently, then the assets will not be assessed on an even basis and the result may be skewed.

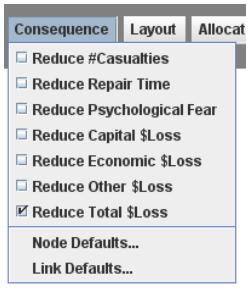

Figure 6 Consequence menu

Many of the networks analyzed are very large. As such, the tool provides a way to reorganize the nodes in a way that helps the analyst see what the results are. The main layouts we typically use are “Around Hubs” where node with high degree are bought to

the center, and “Around $Allocation” where nodes with the highest computed allocation are brought to the center. Layout does not affect the computation in any way (see Figure 7).

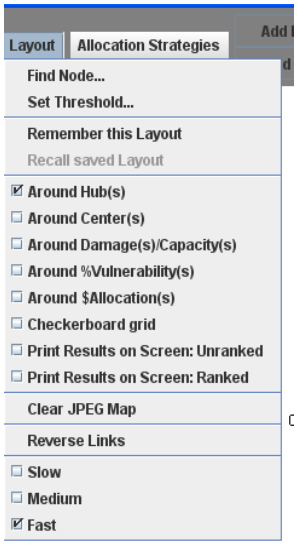

Figure 7 Layout menu

The last two dialogues in Figure 8 and Figure 9 look very similar and they are, except that one is for the defender’s consequence and cost data while the other is for the attacker. In each, we specify which consequence category we wish to provide data. Then we add its associated elimination cost and elimination fraction (see LEXICON for definitions of these). Note that multiple consequences can accept input simultaneously but the tool calculates on only one at a time. If the analyst wishes to aggregate multiple consequence variables, then they can be combined and placed under “Other loss”. Then “Other loss” can be selected form the main “Consequence” menu as the basis for this analysis.

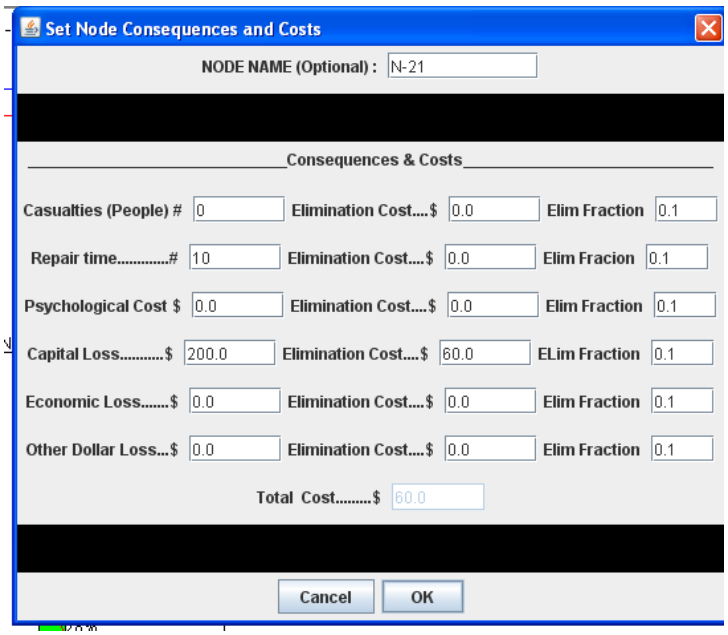

Figure 8 Input Defender consequence and cost data

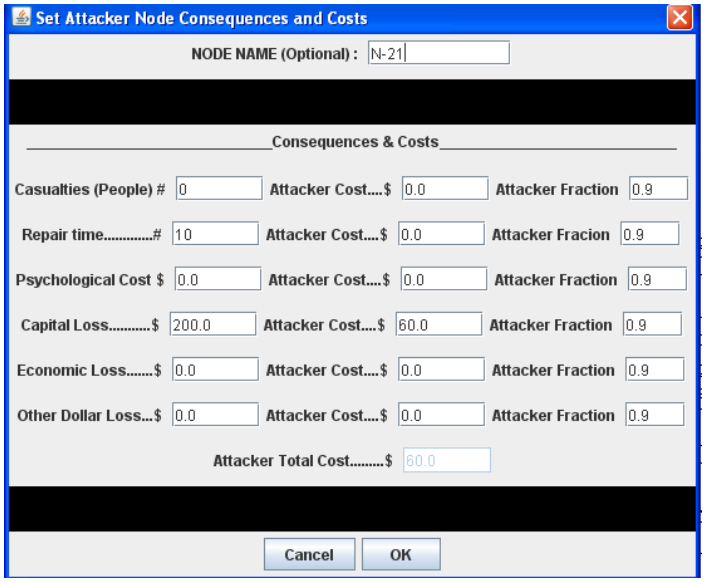

Figure 9 Input attacker consequence and cost data

Lastly, we include a summary dialogue that lists all assets (nodes and links) with all associated data (see Figure 10). This includes all input data and computed data. After an analysis is run, this panel can be opened to view all the results in ranked/unranked ordered in tabular form.

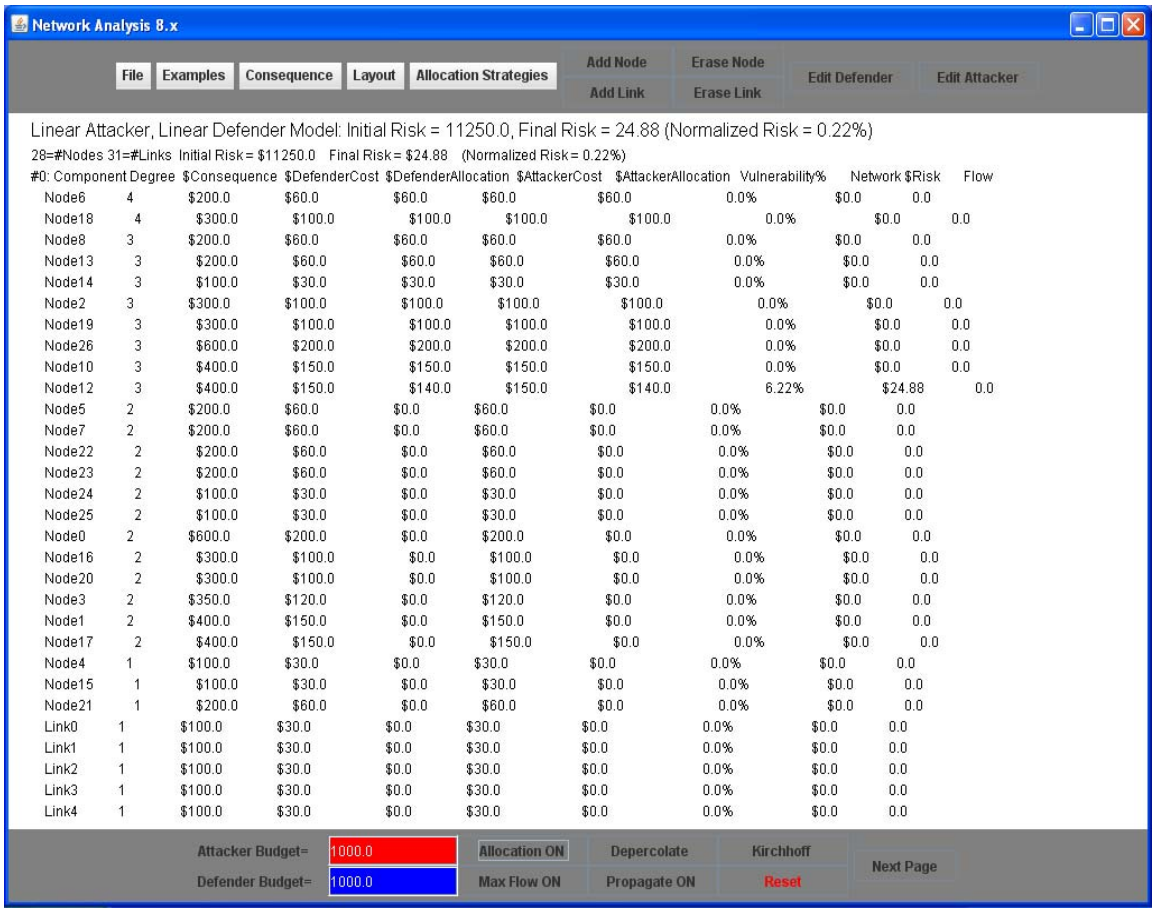

Figure 10 Results in tabular form

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ONE-SIDED NETWORK RISK MODELS

This chapter presents and solves the problem of minimizing total expected replacement cost, or *network risk*, by allocating a limited budget to lowering the vulnerability of individual components in a network. Following Lewis (2006), we apply a "barbell" model to define network risk in an infrastructure system where component adjacencies are considered. We consider two separate functions that relate the amount of a budget a defender allocates to protecting a component to that component's resulting vulnerability: a linear function and an exponential function. In both models, we assume that component vulnerability decreases as a function of the defender's protection allocation to that component.

We establish the structure of an optimal protection allocation in both the linear and exponential vulnerability cases using simple interchange arguments, and, further, we show in both cases that a greedy investment policy provides the optimal reduction in total expected replacement cost.

Our approach is illustrated and applied to a generic network model of a water-and-power system using fictitious data.

A. OPTIMAL DEFENSIVE BUDGET ALLOCATION

Suppose a defender has a total budget, B, to allocate among components in a system in order to protect them, and further suppose that if the defender chooses to allocate an amount, C_i, of the budget to protecting component i that the resulting vulnerability of component i is given by the function $v_i(C_i)$. The question becomes, what portion of B shall be allocated to each asset such that R is minimized? More formally,

$$\textit{Minimize} \quad R = \sum_{i=1}^{n+m} g_i \, d_i \, v_i(C_i) \tag{1}$$

subject to the constraints:

$$\sum_{i=1}^{n+m} C_i \le B \,. \tag{2}$$

$$C_i \ge 0 \qquad \forall i \,. \tag{3}$$

Al Mannai and Lewis (2007) defined vulnerability functions in terms of the availability of an asset *i*; we simply change notation and use vulnerability, the complement of availability, of an asset for our models.

1. Linear Vulnerability Reduction Model

In the linear vulnerability reduction model, we assume a linear relationship between the investment cost of hardening and the vulnerability of the asset. That is, the more we allocate to protect an asset, the less vulnerable it is, as shown in Figure 12. Al Mannai and Lewis (2007) postulate a linear relationship between the "hardening cost" and the availability of the asset. In this document, we simply change notation and use vulnerability, which is the complement of availability. We express the vulnerability function in the linear model as

$$v_i(C_i) = \left(1 - \frac{C_i}{EC_i}\right)$$

$$0 \le v_i(C_i) \le 1.0 \qquad . \tag{4}$$

$$0 \le C_i \le EC_i$$

Note that this function is completely defined by a single parameter, EC_i, which we refer to as the *elimination cost* of component *i*; it represents the cost to reduce the vulnerability of component *i* to zero. (When there is no defensive allocation to protect asset *i*, *i.e.,* $C_i = 0$, its vulnerability is 100%.)

2. Exponential Vulnerability Reduction Model

In the exponential vulnerability reduction model, we represent the vulnerability as a decreasing exponential function of the resource allocation to harden asset *i*, C_i. This function is defined in terms of two parameters, the "elimination" cost, $EC_i>0$, required to reduce component *i* vulnerability to an elimination fraction, $0<EF_i<1$.

As the allocation C_i increases, vulnerability decreases according to the formula

$$v_i(C_i) = e^{-\alpha_i C_i} \qquad , 0 < v_i(C_i) \le 1.0 \tag{5}$$

where

$$\alpha_i = \frac{-\ln(EF_i)}{EC_i} \qquad , 0 < EF_i \le 1.0 . \tag{6}$$

These are the two primary models that we will use throughout the rest of this dissertation that relate investment to vulnerability reduction. We then set the stage to proceed to the next section in determining how to allocate the limited budget to protect assets in the network.

B. OPTIMAL ALLOCATION STRATEGIES AND ALGORITHMS

In this section, we establish optimal allocations for both the linear and exponential vulnerability functions. We show that in each case a greedy algorithm solves the corresponding optimal allocation problem.

1. Linear Vulnerability Function

In the linear case the contribution of component *i* to network risk is:

$$\begin{aligned} R_i &= g_i d_i v_i(C_i) \\ &= g_i d_i - \frac{g_i d_i}{EC_i} C_i . \end{aligned} \tag{7}$$

Theorem 1: If $C_i > 0$ for any *i*, then $C_j = EC_j$ for all j with $\frac{g_j\ d_j}{EC_j} > \frac{g_i\ d_i}{EC_i}$.

Proof: Assume $C_i > 0$, but $C_j < EC_j$ for some j with $\frac{g_j\, d_j}{EC_j} > \frac{g_i\, d_i}{EC_i}$.

Let $\delta = \min(C_i\,, EC_j - C_j) \geq 0$. Now shift δ from C_i to C_j, and the resulting change in overall network risk, Δ, involves only components i and j:

$$\begin{aligned}
\Delta &= \frac{g_i d_i v_i(C_i - \delta)}{EC_i} + \frac{g_j d_j v_j(C_j + \delta)}{EC_j} - \left(\frac{g_i d_i v_i(C_i)}{EC_i} + \frac{g_j d_j v_j(C_j)}{EC_j} \right) \\
&= \frac{g_i d_i v_i(C_i)}{EC_i} + \frac{g_i d_i \delta}{EC_i} + \frac{g_j d_j v_j(C_j)}{EC_j} - \frac{g_j d_j \delta}{EC_j} - \left(\frac{g_i d_i v_i(C_i)}{EC_i} + \frac{g_j d_j v_j(C_j)}{EC_j} \right) \\
&= \frac{g_i d_i \delta}{EC_i} - \frac{g_j d_j \delta}{EC_j} \\
&= \left(\frac{g_i d_i}{EC_i} - \frac{g_j d_j}{EC_j} \right) \delta
\end{aligned}$$

But $\left(\frac{g_i d_i}{EC_i} - \frac{g_j d_j}{EC_j} \right) < 0$, by assumption, and so the original allocation could not have been optimal.

A simple greedy algorithm for the linear case invests as much as possible in the component with the highest ratio, and then invests as much of the remaining budget as possible into the component with the second largest ratio, etc., until no more budget (or no other component) remains.

2. Exponential Vulnerability Function

In the nonlinear case, the contribution of component i to network risk is:

$$R_i = g_i d_i e^{-\alpha_i C_i} \tag{8}$$

Theorem 2: There is a value Φ such that, for all i with $C_i > 0$,

$$\frac{\partial}{\partial C_i}\, g_i\, d_i\, v_i(C_i) = \Phi \quad \text{, (so} \quad -\alpha_i\, g_i\, d_i\, e^{-\alpha_i C_i} = \Phi \text{)}$$

and if $-\alpha_i\, g_i\, d_i > \Phi$ *then* $C_i = 0$

Proof: Assume $C_i, C_j > 0$, but $-\alpha_i\ g_i\ d_i\ e^{-\alpha_i C_i} > -\alpha_j\ g_j\ d_j\ e^{-\alpha_j C_j}$

So $\alpha_i\ g_i\ d_i\ e^{-\alpha_i C_i} - \alpha_j\ g_j\ d_j\ e^{-\alpha_j C_j} < 0$

The parts of the network risk function involving just assets *i* and *j* is:

$$g_i\ d_i\ e^{-\alpha_i C_i} + g_j\ d_j\ e^{-\alpha_j C_j} \tag{9}$$

Now consider shifting an infinitesimal amount δ from the allocation to asset *i* to the allocation to asset *j*

$$\begin{aligned}
\frac{\partial}{\partial \delta} R &= \frac{\partial}{\partial \delta}\left(g_i d_i e^{-\alpha_i (C_i - \delta)} + g_j d_j e^{-\alpha_j (C_j + \delta)}\right) \\
&= \frac{\partial}{\partial \delta}\left(g_i d_i e^{-\alpha_i C_i} e^{\alpha_i \delta} + g_j d_j e^{-\alpha_j C_j} e^{-\alpha_j \delta}\right) \\
&= \alpha_i g_i d_i e^{-\alpha_i C_i} e^{\alpha_i \delta} - \alpha_j g_j d_j e^{-\alpha_j C_j} e^{-\alpha_j \delta} \\
&\le \alpha_i g_i d_i e^{-\alpha_i C_i} - \alpha_j g_j d_j e^{-\alpha_j C_j} \\
&< 0
\end{aligned}$$

where we use the non-negativity of *d* in the second to last step. Therefore, the initial allocation could not have been optimal.

Finally, if $-\alpha_i g_i d_i > \Phi$, then $-\alpha_i g_i d_i e^{-\alpha_i C_i} > \Phi, \forall C_i \ge 0$, so in such a case it will never be optimal to allocate any budget to asset *i*.

C. ONE-SIDED MODEL COMPARISON

This section presents the results of implementing the one-sided network risk model when applied to a generic network model of a water-and-power system. We use fictitious data and hide the names of the assets in the network for security reasons. The input values are not actual values but serve to illustrate the investment cost models.

As an illustration, suppose we compare the two strategies, linear and exponential, of the one-sided network risk model to our fictional water-and-power system comprising

of fifty-nine components - twenty-eight nodes and thirty-one links. Assuming a defender budget of B, and values associated with each asset EC_i, EFi, and d_i, summarized in Appendix, Table 3, we obtain the results shown in Figures 12-17.

We employ the model-based risk analysis (MBRA) software provided by Lewis (2006) and modified by Al Mannai and use the input values of Table 3 to obtain risk reduction. Figure 11 shows partial results of the calculation. The graphical display is annotated with the number and name of each node and link, as well as the degree of each node. The bar chart shown in the lower-left corner is the degree-sequence distribution of nodes and gives an indication of the network's structure although this is not used in this research. Each node and link has an associated elimination cost, EC_i, elimination fraction, EFi, and damage value, d_i, but these values are not shown in Figure 11.

The graphical annotations are

0 : N-0	node number: node identifier (a unique name)
#5: 5	link number: link identifier (a unique name)
2g	degree of a node

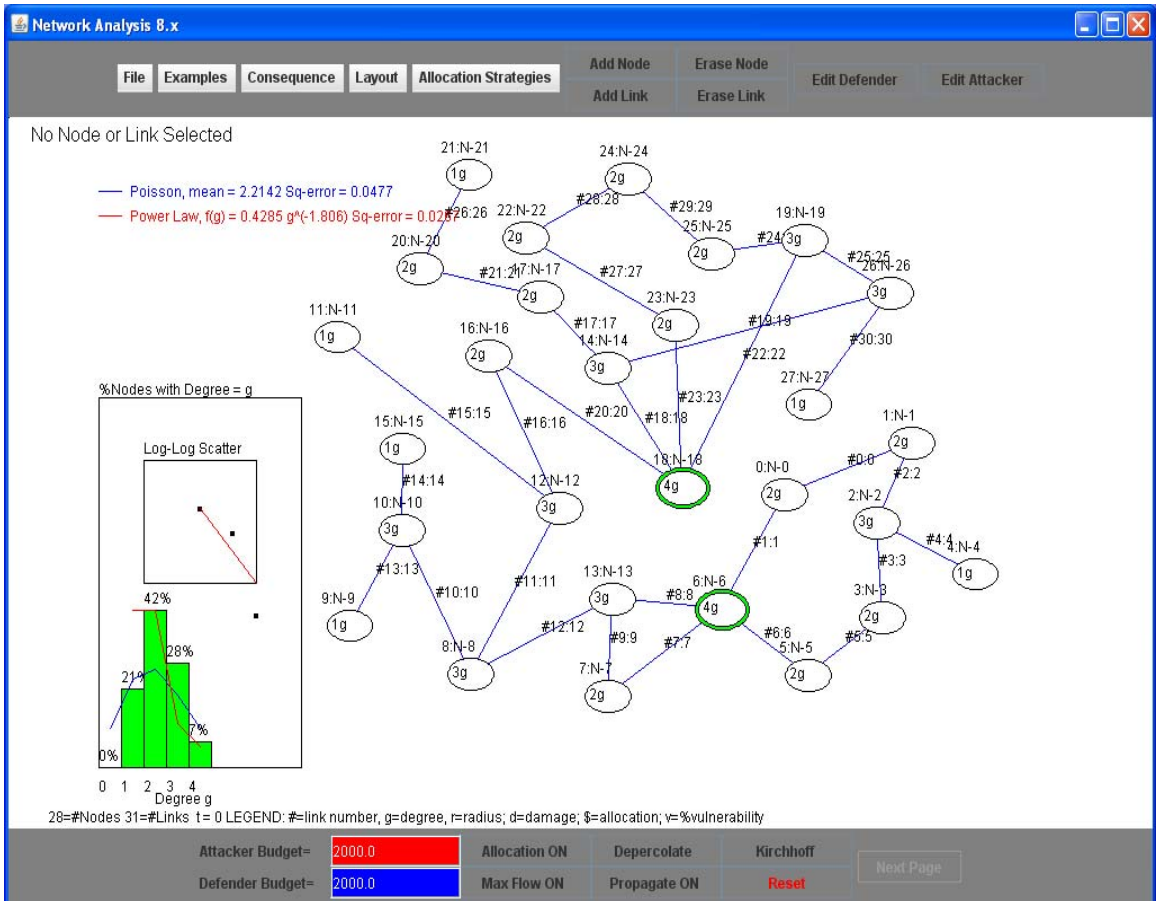

Figure 11 Network-analysis software

Figure 12 shows the comparison of risk-reduction rates of the two cost models, linear and exponential (nonlinear). The increase in investments of resources to harden the assets in the network reduces network risk. The difference in risk reduction between the linear and nonlinear cost models is due to the nature and behavior of the functions used in each model. In the linear cost strategy, the linear decline of risk versus budget shows the linear relationship of allocation cost, C_i, to vulnerability, v_i. In the nonlinear cost model, the exponential function decreases faster than linearly and never reaches 0% vulnerability. In other words, an infinite amount of budget needs to be allocated to achieve minimum vulnerability.

In addition, for a total budget, B =$3700.00, the overall risk of the network is reduced to zero when using linear strategy, i.e., every asset is fully protected in the

network. But when using the nonlinear strategy, overall risk is reduced to only R_{norm} = 8.9%. It would take an infinite budget to reduce risk to zero under the nonlinear strategy due to the exponential function's behavior. Which cost strategy to implement is a question for policymakers to make their decision.

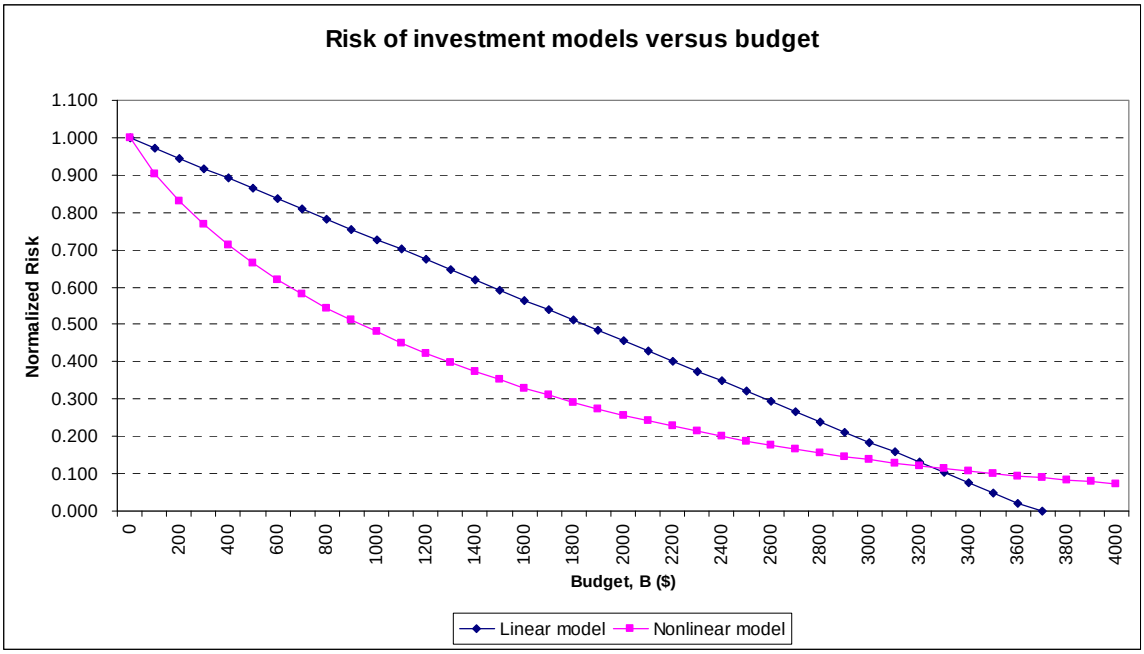

Figure 12 Risk of investment models value budget

While it may seem odd that for the two models, a budget that drives risk to zero in one does not do so in the other. We view this as an inherent artifact of the abstraction the models provide. Even though the linear cost model shows risk approaching zero, we know this is not actually the case. Risk remains even after full investment. It is just that from the analyst's point of view, it is beyond reach so it is ignored. The nonlinear model, however, models this better because it shows that risk cannot be driven to zero even with infinite budget.

The results also show that applying either the linear or exponential (nonlinear) cost strategy leads to ranking of assets in a network according to the product of damage cost, d_i, and node degree, g_i, (where g_i=1 for links), divided by vulnerability-

elimination cost, EC_i. This is shown in Figures 13-16, where both models identify exactly the same nodes and links in rank order from the highest to the lowest but with different allocation costs, C_i, and resulting vulnerabilities, $v_i(C_i)$. For instance, node 6 is the most critical asset and node 11 is the least critical asset in this example.

For example, in Figure 13, we apply the linear cost model to the network example with a budget of B=$1000.00, we find that only nine nodes (6, 18, 8, 13, 14, 2, 19, 10, and 12) are the most critical assets and are receiving allocations where the remaining assets are not getting any funds as shown in Figure 13. These assets are fully funded except node 12, which is partially funded with an allocation C_{12} = $140.00 (or an allocation ratio of C_{12}/ EC_{12} = 0.933 as shown in Figure 13). This is due to the budget being not enough to fully fund this node which leaves the remaining assets unfunded, and consequently, only partial vulnerability reduction on this node, $v_{12}(C_{12})$ = 0.0667 as shown in Figure 14.

A budget allocation of $1000.00 to these assets reduces network risk by 27%, i.e., with a budget of $1000.00 network risk is reduced from 100% to 73% (a reduction of 27%). Increasing the defensive budget from $1000.00 to $3700.00 steadily reduces network risk until it reaches zero (as in Figure 12).

When applying the nonlinear cost strategy with B=$1000.00, funding is spread over many more nodes and links in the network, as shown in Figure 12. The network risk after allocation of $1000.00 is reduced to 48%. That is, with a budget of $1000.00, we can achieve a risk reduction of 52% to the network. The partial funding of all nodes and links in the network is due to the behavior of the exponential function and the greedy algorithm optimization technique which partially distributes total budget over all assets in the network. This is illustrated in Figure 13 where more assets are partially funded in the nonlinear model than in the linear model.

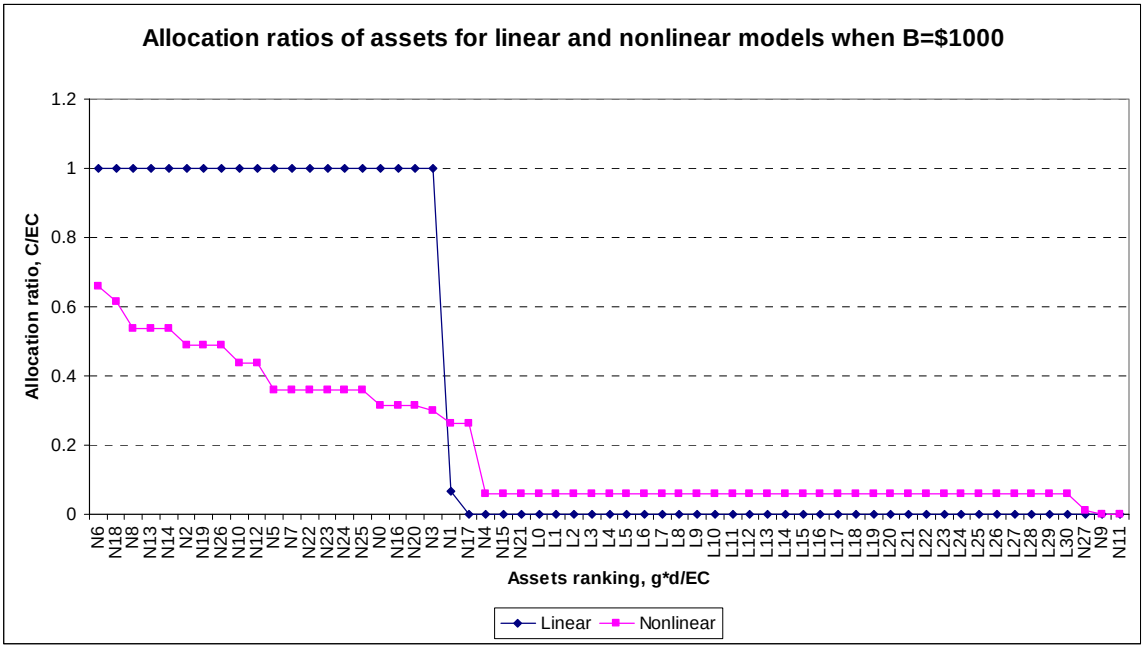

Figure 13 Allocation ratios of assets for linear and nonlinear models when B=$1000

Figure 14 shows asset vulnerability when a total budget of B=$1000 is applied to protect the assets in the network example. The vulnerability is zero for the most critical assets when they are fully funded as shown in Figure 14 by the linear cost model, and is 100% for the non-critical unfunded assets. In the case of the nonlinear cost model, the vulnerability is achieving the minimum value but never reaches zero for the most critical assets and is one for the unfunded assets. This graph is the inverse of Figure 13.

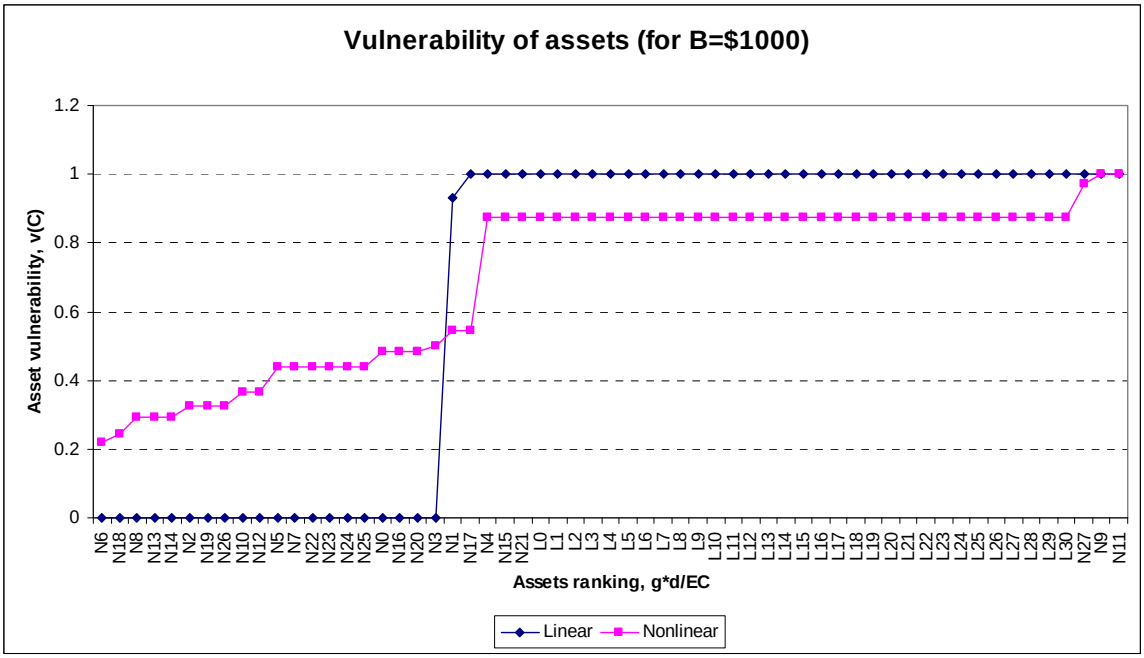

Figure 14 Vulnerability of assets when B=$1000

Suppose the decision maker wants to know how much it will cost to buy down vulnerability and achieve network risk reduction of 50%.

Let us take a close look at Figure 12 where the 50% risk reduction crosses the linear line at a budget B=$1840.00 and crosses the nonlinear curve at a budget of B=$920.00. It would cost the decision maker $1840.00 when using the linear cost model and $920.00 if uses the nonlinear cost model. The next question is how to distribute these budgets to assets and what is the buy down in vulnerabilities.

Figure 15 shows the results when applying a budget of B=$1840.00 to the linear cost model, we find that there are 21 most critical assets that are fully protected and leaving 38 assets unfunded. Note that node 1, N_1, is partially funded with what is left from the total budget, i.e., C_1=$10.00 where EC_1=$150.00. The vulnerability is illustrated in Figure 16 where the fully protected assets achieve zero vulnerability and the unfunded assets are 100% vulnerable. In addition, the total budget B=$1840.00 is distributed to only 21 assets of a network with 59 assets.

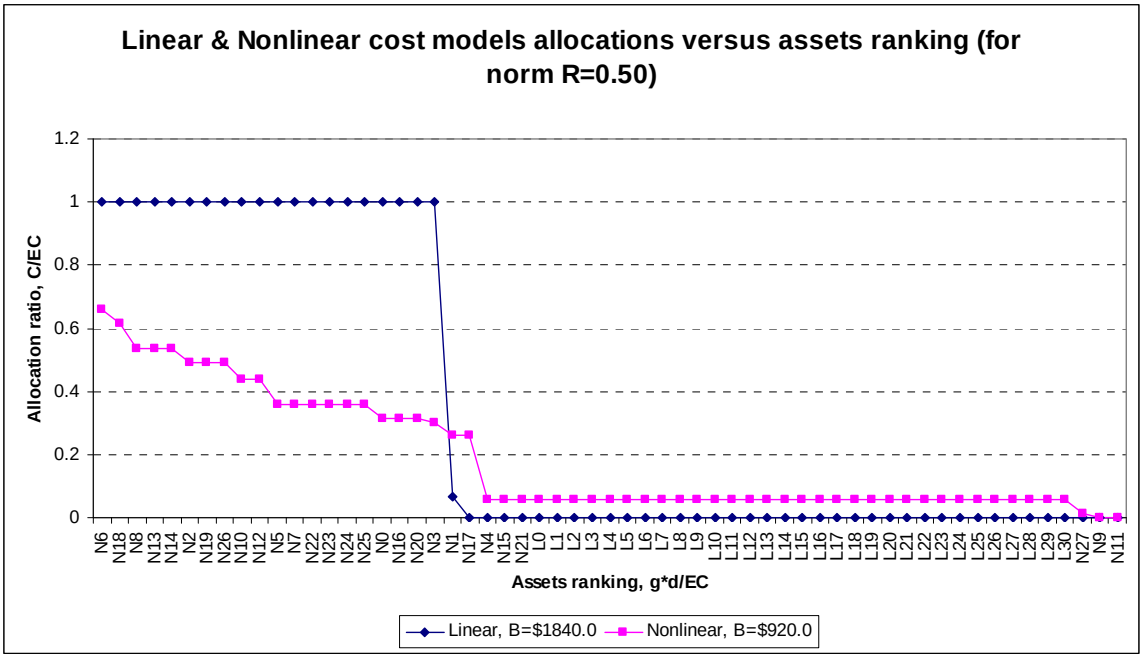

Figure 15 Linear and nonlinear cost models allocations versus assets ranking (for norm R=0.50)

When applying the nonlinear cost model, results reveal that all assets are partially protected. The most critical assets achieve minimum vulnerability but never reach zero. The less-critical assets remain at high vulnerability but they are still less than the ones in the linear model. Note that in the nonlinear model the total budget is distributed all over the assets in the network, i.e., about 57 assets are getting funds as shown in Figure 15.

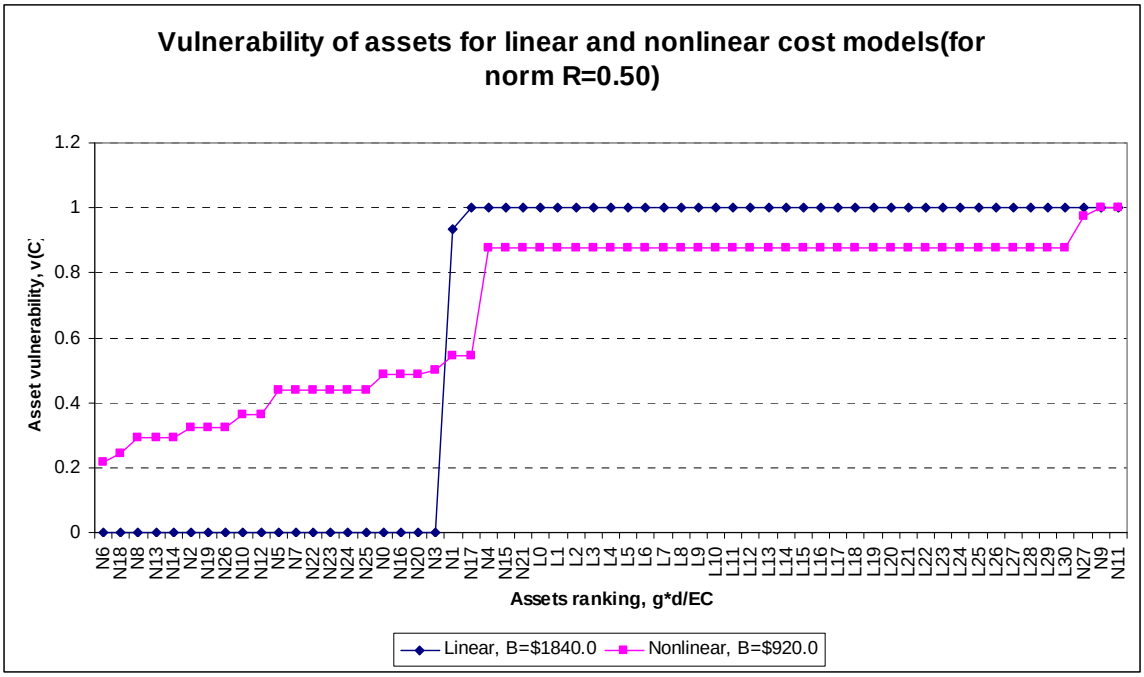

Figure 16 Vulnerability of assets for linear & nonlinear cost models (for norm R=0.50)

Two cost models were introduced in this chapter and the results showed that whether a linear or exponential (nonlinear) cost model is used, a budget will be distributed optimally in rank order according to the product of damage cost, d_i, node degree, g_i, (where g_i=1 for links), divided by vulnerability-elimination cost, EC_i. In addition, both models identify exactly the same assets in ranking order in the network. Furthermore, optimal allocation applies more funding to critical nodes and links than to noncritical. This strategy makes it possible to maximize availability of a critical infrastructure without having to protect everything. However, the linear cost model will distribute the budget to a few assets in full, leaving some assets unfunded. The nonlinear cost model will distribute the budget partially over all the assets in the entire network, leaving some risk in the overall network. Lastly, the nonlinear cost model achieves lower risk than the linear model as shown from the results.

THIS PAGE INTENTIONALLY LEFT BLANK

V. TWO-PERSON GAME FOR NETWORK RISK

This chapter extends the one-sided risk model in the previous chapter by formulating and solving a two-person zero-sum game for network risk. One player, the *defender*, seeks to minimize network risk by allocating resources to reduce the vulnerability of individual components in the network, and the other player, the *attacker*, seeks to maximize network risk by allocating attack resources to increase the vulnerability of individual components in the network.

Thus, an arms race ensues because the defender allocates resources to assets based on perceived attacker allocation and then the attacker adds or reallocates assets to counter the defender's precautionary measures. The term "arms-race" thus captures this "action-reaction" phenomena because it describes an iterative process whereby actors' initiatives are directly linked to the previous or anticipated actions off their competitors. (Hammond, 1993) It is similar to a Stackelberg (1952) competition game where the leader moves first and then the follower moves sequentially. We provide an iterative algorithm for finding the min-max solution to this conundrum.

Recall that our definition of network risk is the total expected replacement cost due to damage to the components in the network, and, applying the "barbell" model of Lewis (2006), it is defined in terms of (node) degree, g_i, component damage, d_i, and component vulnerability, v_i:

$$R = \sum_{i=1}^{n+m} g_i d_i v_i$$

In our two-person model we assume that the vulnerability of each component i is determined by a function $v_i(A_i, C_i)$ of an allocation, A_i, of limited attacker resources towards damaging component i, and an allocation, C_i, of limited defender resources towards protecting component i. This yields the following formula for network risk as a function of A_i and C_i:

$$R(A_i, C_i) \equiv \sum_{i}^{n+m} g_i d_i v_i(A_i, C_i) \tag{10}$$

We seek an equilibrium allocation $\left(A_i^*, C_i^*\right)$ for *R*: specifically, for fixed attack allocation A_i^*, no other defense allocation C_i can reduce the value of $R\left(A_i^*, C_i\right)$, and for fixed C_i^* no other A_i can increase $R\left(A_i, C_i^*\right)$. Therefore, the equilibrium solution minimizes *R* from the defender's point of view and maximizes R from the attacker's view. The attacker represents a terrorist group that wants to attack the defender's infrastructure and cause severe damage to the country. The defender represents the homeland security officials who want to protect and harden critical infrastructures from attack in order to minimize the expected replacement costs in the aftermath of an attack.

A. TWO-PERSON VULNERABILITY FUNCTIONS

In this section, we will represent vulnerability as the product of two exponential functions of attacker and defender resource allocations. We will modify the vulnerability function introduced in the previous chapter to include a term for the attacker's allocation (Al Mannai and Lewis, 2008).

1. Nonlinear Cost Models (Exponential)

We introduced the vulnerability as an exponential function for the defender in the previous chapter as

$$v_i^C(C_i) = e^{-\alpha_i C_i} \qquad 0 < v_i\left(C_i\right) \le 1 \tag{11}$$

where we use the superscript *C* to distinguish from the attacker, and

$$\alpha_i = \frac{-\ln\left(EF_i\right)}{EC_i} \qquad 0 < \left(EF_i\right) \le 1 \tag{12}$$

An asset's vulnerability is an exponentially decreasing function of the amount of funding used to harden an asset: greater spending yields lower vulnerability. Note that vulnerability is 100% when there is no allocation, $C_i = 0$. On the other hand, it takes an infinite allocation to entirely eliminate vulnerability. Parameter α_i is chosen so that

vulnerability decreases to EF_i when $C_i = EC_i$. Therefore, α_i is determined by elimination cost EC_i, and the elimination fraction, EF_i. Parameters EC_i and EF_i are used to calibrate these functions as in Chapter IV.

The same argument is made for the attacker, except vulnerability increases with the amount of funding applied by the attacker: (Al Mannai and Lewis, 2008)

$$v_i^A\left(A_i\right) = 1 - e^{-\gamma_i A_i} \qquad 0 \le v_i\left(A_i\right) < 1 \tag{13}$$

where

$$\gamma_i = \frac{-\ln\left(1 - AF_i\right)}{AC_i} \qquad 0 \le \left(AF_i\right) < 1 \tag{14}$$

We assume that the probability of a successful attack depends on two independent events occurring: the attacker succeeds in executing his attack, and the defender fails to avoid the attack. Therefore, the joint probability of a successful attack is the product of the probabilities of the two required events:

$$v_i\left(A_i, C_i\right) = v_i\left(A_i\right)\, v_i\left(C_i\right) \tag{15}$$

Note that, if there is no defense mounted (i.e., $C_i = 0$), and no attack ($A_i = 0$), the vulnerability of component i is zero. If there is an attack, and the defender has expended no resource $C_i = 0$, vulnerability is simply $v_i(A_i)$.

Substituting equation (15) for $v_i\,(A_i, C_i)$ gives:

$$\begin{aligned} R(A_i, C_i) &= \sum_{i=1}^{n+m} g_i d_i v_i^A(A_i) v_i^C(C_i) \\ &= \sum_{i=1}^{n+m} g_i d_i \left(1 - e^{-\gamma_i A_i}\right)\left(e^{-\alpha_i C_i}\right) \end{aligned} \tag{16}$$

Network risk is identical to PRA risk when $g_i = 1$, which corresponds with a non-network definition. There each asset, node and link, is treated as an independent target. On the other hand, when $g_i \ge 1$, highly connected nodes become more critical than those less connected. In this case, network risk resembles (but is defined differently from) the definition used by Albert and Barabasi.

B. A SIMULTANEOUS GAME FOR NETWORK RISK

Our two-person zero-sum game describes a situation in which the defender has a budget B from which to make defensive allocations C_i, and the attacker has budget B' from which to make attack allocations A_i, and the defender and the attacker are aware of each other's budgets, but make their respective allocations in secret. The resulting two-person, zero-sum game can be stated as:

$$\min_{C_i} \max_{A_i} R(A_i, C_i) \equiv \sum_{i=1}^{n+m} g_i d_i \left(1 - e^{-\gamma_i A_i}\right)\left(e^{-\alpha_i C_i}\right) \tag{17}$$

subject to

$$\begin{aligned} &\sum_{i=1}^{n+m} C_i = B \\ &\sum_{i=1}^{n+m} A_i = B' \\ &C_i, A_i \geq 0 \end{aligned} \tag{18}$$

1. Network Allocation Strategy

The optimal offensive and defensive allocations can be determined to any desired accuracy using fictitious play (Washburn, 2001), which provides a convergent algorithm for solving two-person zero sum games. However, the form of this game is identical to that presented in Croucher (1975), and we can take advantage of that work to develop an algorithm to solve for the optimal allocations in a finite number of steps.

Modifying the results from Croucher to conform to our notation, the solution requires the determination of Lagrange multipliers μ and λ from the following equations:

$$\sum_{\frac{\lambda}{\gamma_i} < g_i d_i \leq \frac{\lambda}{\gamma_i} + \frac{\mu}{\alpha_i}}^{n+m} \left(\frac{1}{\gamma_i}\right) \ln\left(\frac{g_i d_i \gamma_i}{\lambda}\right) + \sum_{g_i d_i > \frac{\lambda}{\gamma_i} + \frac{\mu}{\alpha_i}}^{n+m} \left(\frac{1}{\gamma_i}\right) \ln\left(\frac{\frac{\lambda}{\gamma_i} + \frac{\mu}{\alpha_i}}{\left(\frac{\lambda}{\gamma_i}\right)}\right) = B' \tag{19}$$

and,

$$\sum_{g_i d_i > \frac{\lambda}{\gamma_i} + \frac{\mu}{\alpha_i}}^{n+m} \left(\frac{1}{\alpha_i}\right) \ln\left(\frac{g_i d_i}{\frac{\lambda}{\gamma_i} + \frac{\mu}{\alpha_i}}\right) = B \tag{20}$$

In the special case where $\alpha_i = \gamma_i$ for each component *i*, Croucher points out that there is a very straightforward procedure for determining both μ and λ. Here are the steps for running his algorithm, adapted to our notation:

1. Sort the components so that the values $g_i d_i \alpha_i$ appear in ascending order.
2. For each $i<n+m$, in turn, assume $g_i d_i \alpha_i \le \lambda + \mu < g_{i+1} d_{i+1} \alpha_{i+1}$, and solve equation (20) for the value $\lambda + \mu$. If $g_i d_i \alpha_i \le \lambda + \mu < g_{i+1} d_{i+1} \alpha_{i+1}$, then continue to step (3), otherwise continue searching for the interval containing $\lambda + \mu$.
3. Solve equation (19) for λ, then determine μ
4. Use the values of μ and λ to find the optimal attacker and defender allocations, A_i and C_i, respectively.

From Croucher, if $\overset{\circ}{A}_i > 0$ *and* $\overset{\circ}{C}_i > 0$, then the optimal attacker and defender allocations expressed as:

$$\overset{\circ}{A}_i = \left(\frac{1}{\gamma_i}\right) \ln\left(1 + \frac{\mu \gamma_i}{\lambda \alpha_i}\right) \tag{21}$$

$$\overset{\circ}{C}_i = \left(\frac{1}{\alpha_i}\right) \ln\left(\frac{g_i d_i}{\frac{\lambda}{\gamma_i} + \frac{\mu}{\alpha_i}}\right) \tag{22}$$

And if $\overset{\circ}{A}_i > 0$ *and* $\overset{\circ}{C}_i = 0$, then

$$\overset{\circ}{A}_i = \left(\frac{1}{\gamma_i}\right) \ln\left(\frac{g_i d_i \gamma_i}{\lambda}\right) \tag{23}$$

2. Non-Network Allocation Strategy

This strategy ignores network adjacencies and sets $g_i = 1$ in equation (18). In this case, the defender's objective is to minimize network risk while the attacker wants to maximize it. Repeating Croucher (1975) approach for this strategy by setting $g_i=1$ yields new expressions for the defender and attacker allocations, C_i and A_i, respectively.

If $\overset{\circ}{A}_i > 0 \quad and \quad \overset{\circ}{C}_i > 0$, then the optimal attacker and defender allocations expressed as:

$$\overset{\circ}{A}_i = \left(\frac{1}{\gamma_i}\right) \ln\left(1 + \frac{\mu\,\gamma_i}{\lambda\,\alpha_i}\right) \tag{24}$$

$$\overset{\circ}{C}_i = \left(\frac{1}{\alpha_i}\right) \ln\left(\frac{d_i}{\frac{\lambda}{\gamma_i} + \frac{\mu}{\alpha_i}}\right) \tag{25}$$

And if $\overset{\circ}{A}_i > 0 \quad and \quad \overset{\circ}{C}_i = 0$, then

$$\overset{\circ}{A}_i = \left(\frac{1}{\gamma_i}\right) \ln\left(\frac{d_i\,\gamma_i}{\lambda}\right) \tag{26}$$

C. TWO-PERSON RISK MODEL RESULTS

This section presents the results of implementing the two-person network risk model when applied to the same network example used in the previous chapter. We use fictitious data to illustrate the model.

We will present the results for two allocation strategies network and non-network. Let us apply the two-person game risk model to the network example introduced in the previous chapter. Assume a defender's input values of *B*, *EC*, and *EF*, and an attacker's input values of *B′*, *AC*, and *AF*. The input values are tabulated in Appendix, Table 3, and the results presented in Figures 17-24. In each case, we use a heuristic algorithm that is a myopic (i.e., memory less) application of the basic fictitious play algorithm; we pick an allocation for the attacker, then solve for the optimal resulting allocation for the defender,

and iterate until the change in each player's allocation is insignificant. Although we have no proof that this procedure converges, we suspect that it does; in each case we achieved equilibrium solutions for our models using this algorithm.

The results of applying the joint-vulnerability strategies to our generic water-and-power network show that the non-network achieves lower normalized risk than the network for small budgets, and achieves higher risk with large budgets. Recall that the non-network strategy ignores network structure and sets node degree to one, g_i=1.0 as shown in Figure 17. At low budgets, the attacker is more successful using the network model. The attacker experiences diminishing returns because of fewer funds allocated to high-ranking targets.

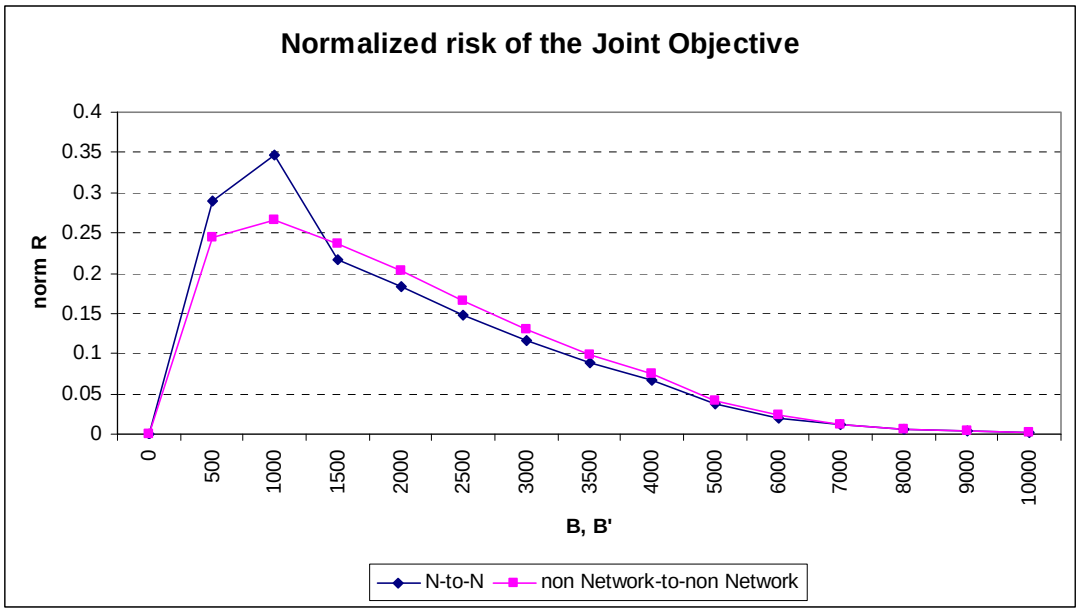

Figure 17 Normalized risk of the joint-objective strategies

Figure 18 reveals the network-to-network variation of defensive budget when the offensive budget is equal to B'=$2000, and when the attacker's budget is varied, the defender's budget is set to B=$2000. Increasing the defender's budget, the normalized risk exponentially decreases. Conversely, an increase in the attacker's budget results in an exponential increase in normalized risk. This satisfies the main objective of this model as the defender wants to minimize risk, and the attacker wants to maximize it. Note that

when both players have similar budgets of B=B'=$2000 the normalized risk is R_{norm}=0.1833 to the attacker. If the defender increases his resources, that is more funds allocated to harden the assets, then normalized risk will decrease and vise versa.

Similar explanation is applied to the results in Figure 19 for the non-network strategy, but when the budgets B=B'=$2000 the normalized risk is R_{norm}=0.2034 to the attacker. This shows that the attacker will achieve high-normalized risk if he plays non-network strategy that ignores node degree.

Figure 20 shows the results of network risk when fixing the defender's budget to different values and varying the attacker's budget. At low defender's budget (for example, B=$2000), the attacker achieves high network risk because the assets are less protected. Moreover, as the defender invests more in hardening the assets the attacker is less successful in causing damages to the assets in the infrastructure.

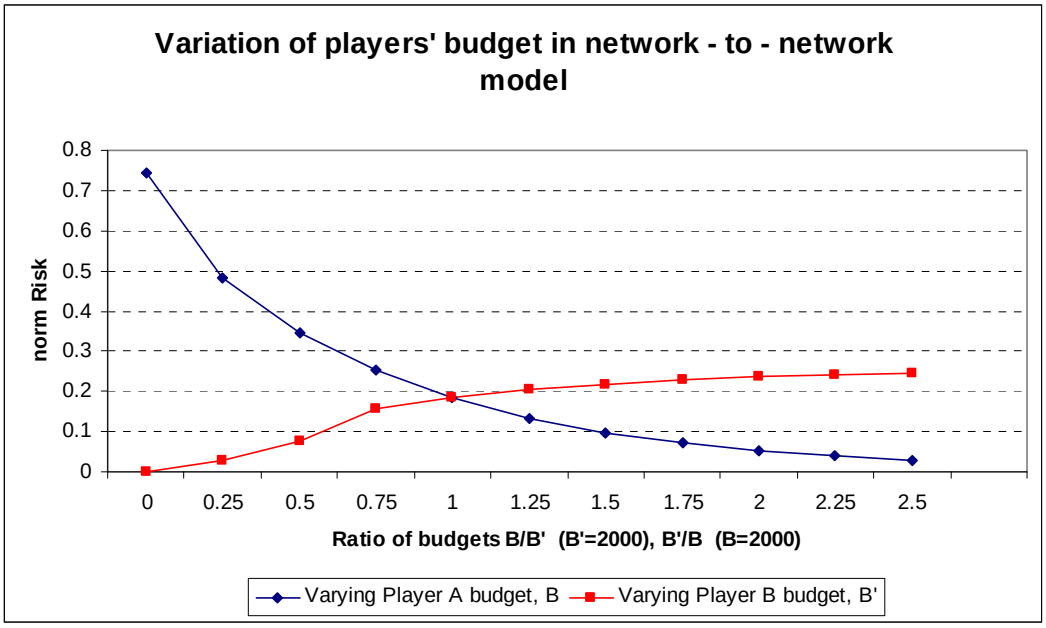

Figure 18 Variation of players' budgets in network-to-network model

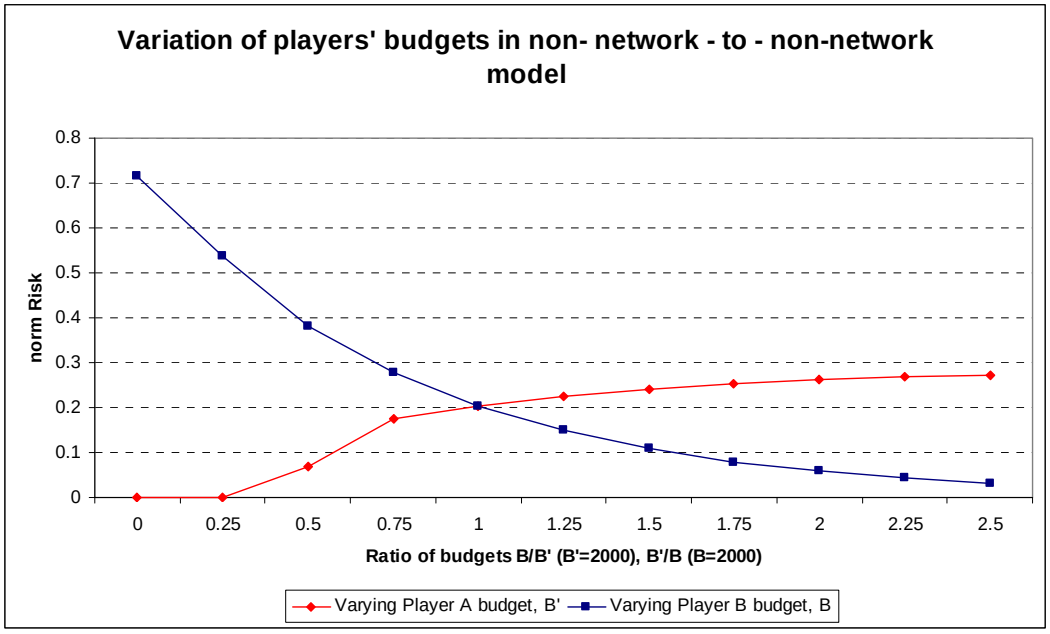

Figure 19 Variation of players' budgets in non-network-to-non network model

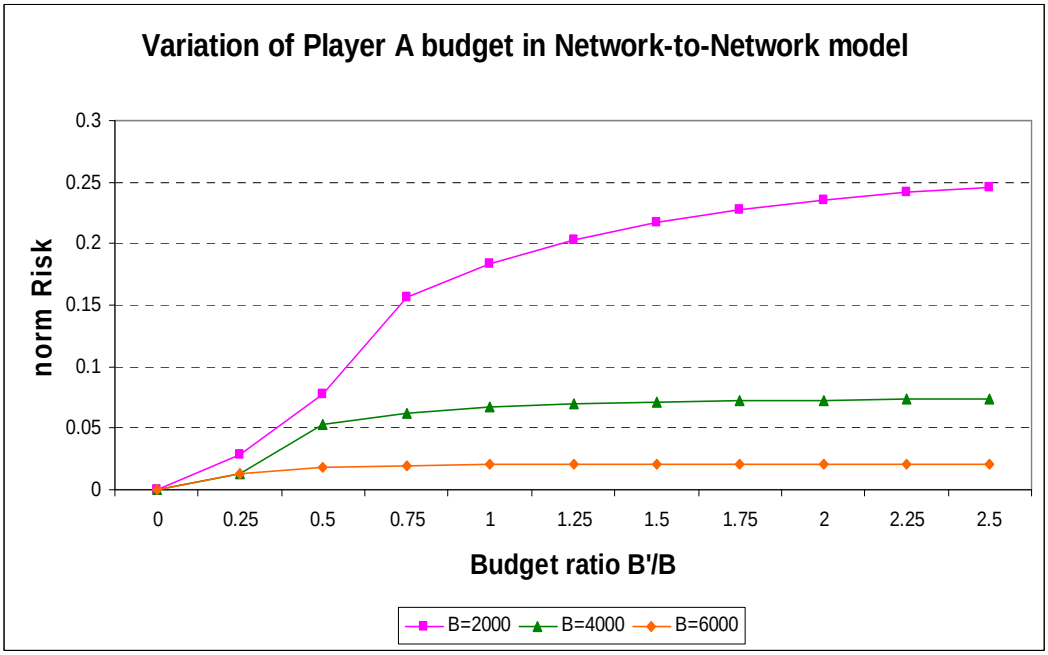

Figure 20 Variation of attacker's budget for various fixed defender's budgets

Figure 21 shows the defender-and-attacker allocation ratios to ranked network assets. The result shows that the defender-allocation ratios form an exponential decay curve, and the attacker-allocation ratios are almost constant value over all the assets.

Moreover, it indicates that the defender allocates his resources towards protecting his most critical assets while the attacker focuses on attacking less-critical assets. The result show that the normalized risk is 0.2274, the total network risk is 2558.3, and the initial network risk is 11250 when B=B'=2000.

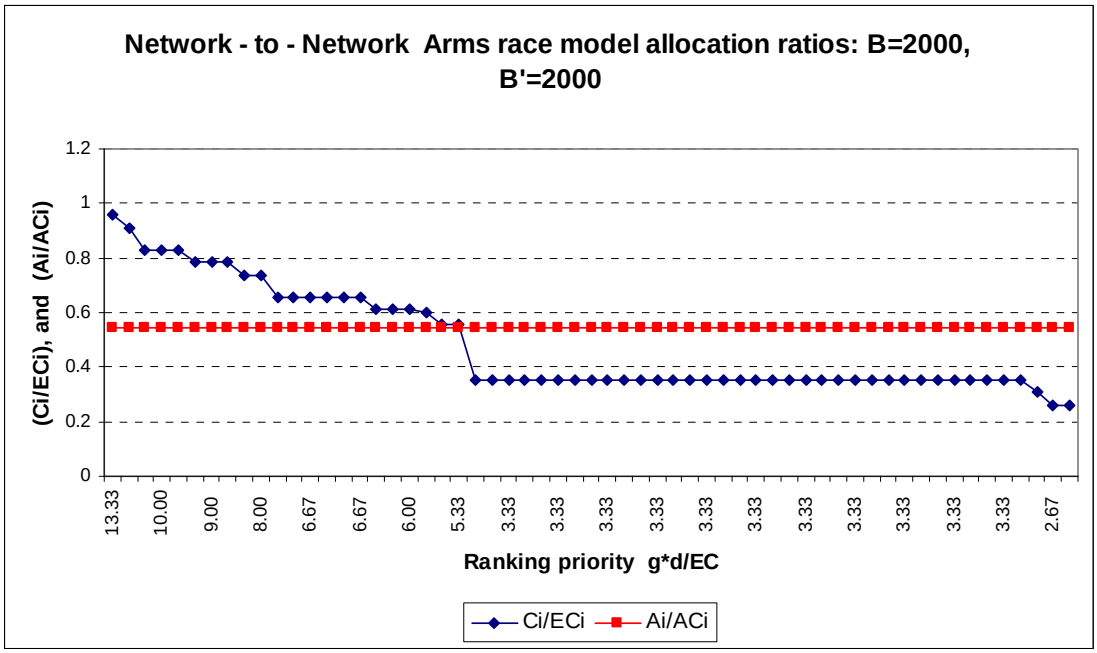

Figure 21 Network arms-race ratio of allocations to assets

Let us look closely at how defender and attacker budgets are distributed optimally among assets in the network. Figure 22 shows the optimal distributions of defensive and offensive resources to assets in the network. The defender invests towards protecting the most critical assets, and the attacker focuses on investing more toward attacking the less-critical assets.

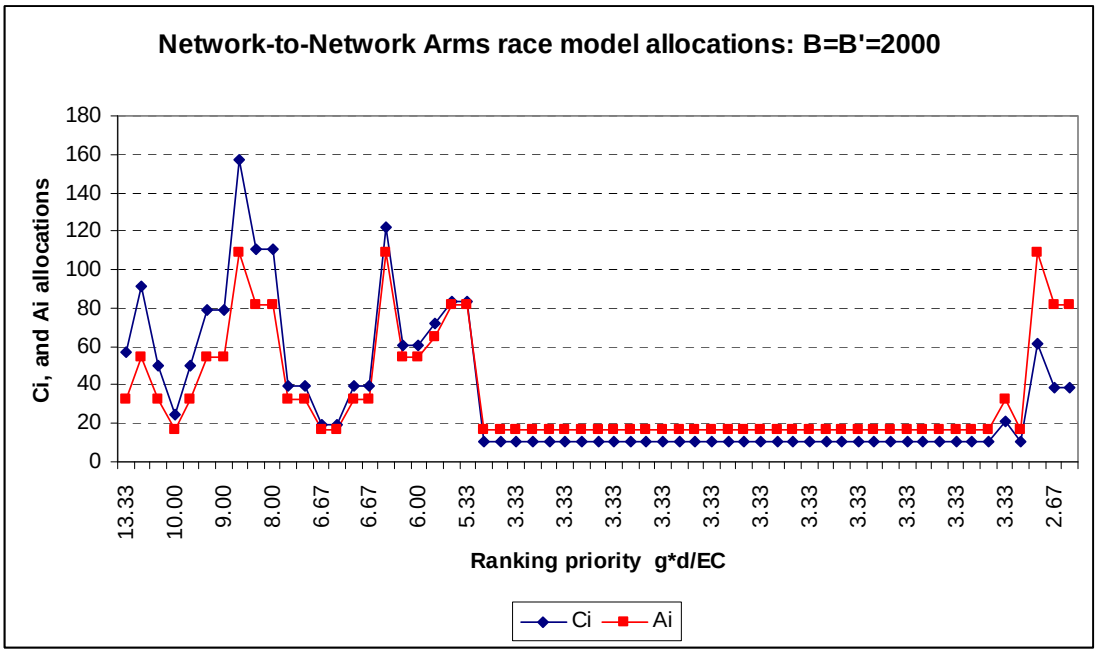

Figure 22 Network arms-race allocations to assets

In the non-network strategy, where the degree sequence is ignored and set to one, g_i=1. Figure 23 indicates that asset rank is ignored, as is obvious from the way allocation ratios are shown. The attacker's allocation ratios are almost equal to all assets, and the defender's are distributed differently among the assets, because the degree sequence is ignored in this strategy and assets are not ranked.

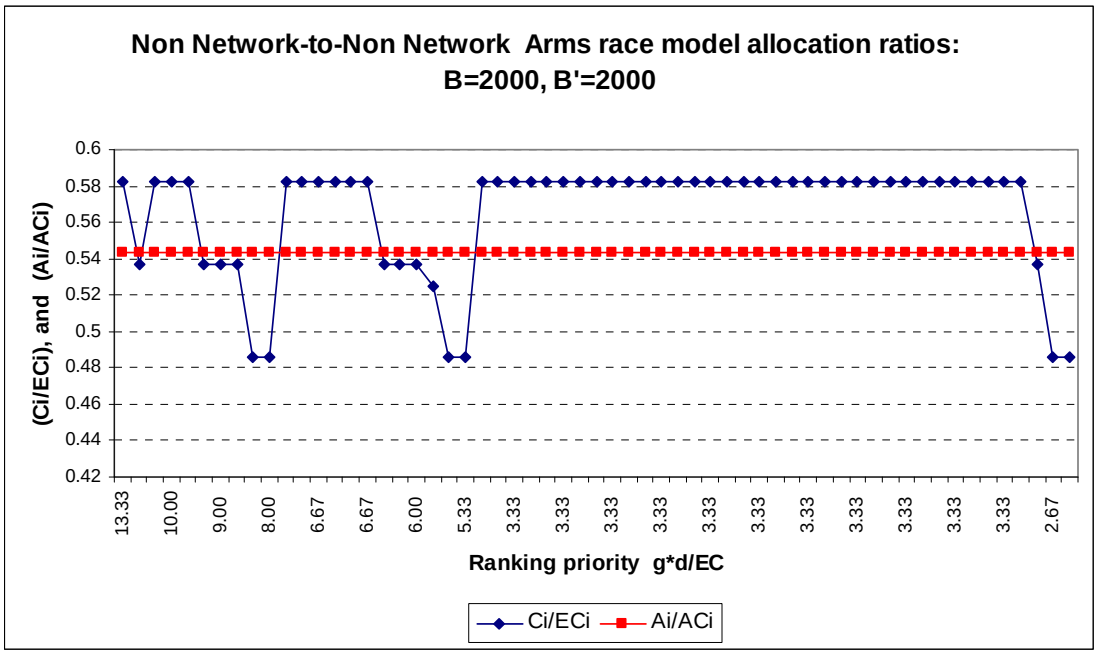

Figure 23 Non-network arms race ratio of allocations to assets

Figure 24 shows the exact allocations to each asset by the defender and the attacker. Note defensive allocations are lower than offensive allocations. The result shows that normalized risk is 0.20344, the total network risk is 2288.75, and the initial network risk is 11250.

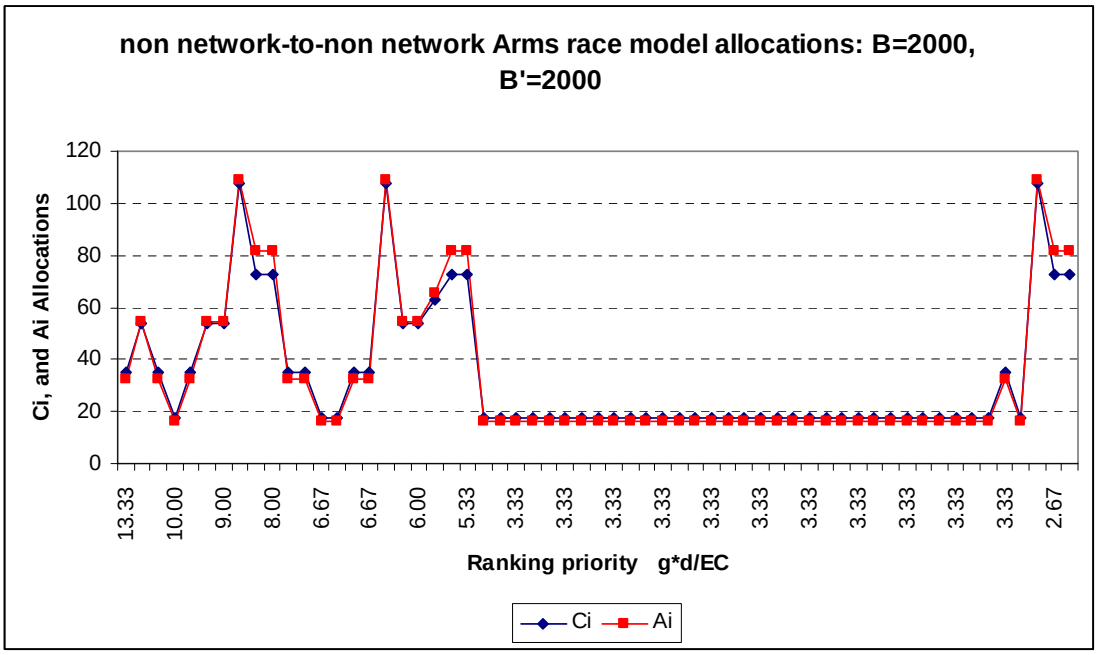

Figure 24 Non-network arms race allocations to assets

Comparing the network arms race strategy with non-network indicates that minimum risk is achieved by the non-network strategy. This is understandable because of the degree-sequence ignorance of the non-network strategy. Moreover, the attacker is less successful using the network strategy at high budgets, and more successful at low budgets.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. COMPARATIVE RESULTS, CONCLUSIONS, AND FUTURE WORK

This chapter comprises three sections -- the results of comparing two decision tools, CARVER and MBRA, used by DHS, concluding thoughts on this dissertation research, its contribution to the critical infrastructure protection literature, and its extension to the MBRA technique, and plans and ideas for future work in this area.

A. COMPARISON OF TOOLS

In this section, we compare two tools, CARVER developed by the National Infrastructure Institute and MBRA originally developed by Lewis (2006) and modified by Al Mannai in this research. We use the fictitious San Luis Rey (SLR) water supply network for the comparison as shown in Figure 25. The San Luis Rey water supply network comprises 35 assets, 17 nodes and 18 links. The input values associated with each asset are tabulated in Table 3 for MBRA and in Table 4 for CARVER. Each tool requires a different set of input values, but we made these values similar without loss of the assets' identity.

CARVER is a tool designed to prioritize assets and rank them according to their scores obtained from the six categories. On the other hand, MBRA is a tool deigned to prioritize assets according to their criticality, quantify the allocation of resources to reduce vulnerabilities and risk for one-player and two-players. The common attribute that both techniques have is the ranking of assets by criticality. We will use this as the basis for our comparison.

Suppose we are given a budget of B=$1000 and we want to protect the San Luis Rey water supply network from terrorist attacks. What are the most critical assets in the network and how can we distribute the limited resources to reduce vulnerability and risk?

Figure 25 shows the structure connectivity of the San Luis Rey network in MBRA. The input values associated with each node and link are entered using the set node/link consequences and costs menus as shown in Chapter II, Figure 8.

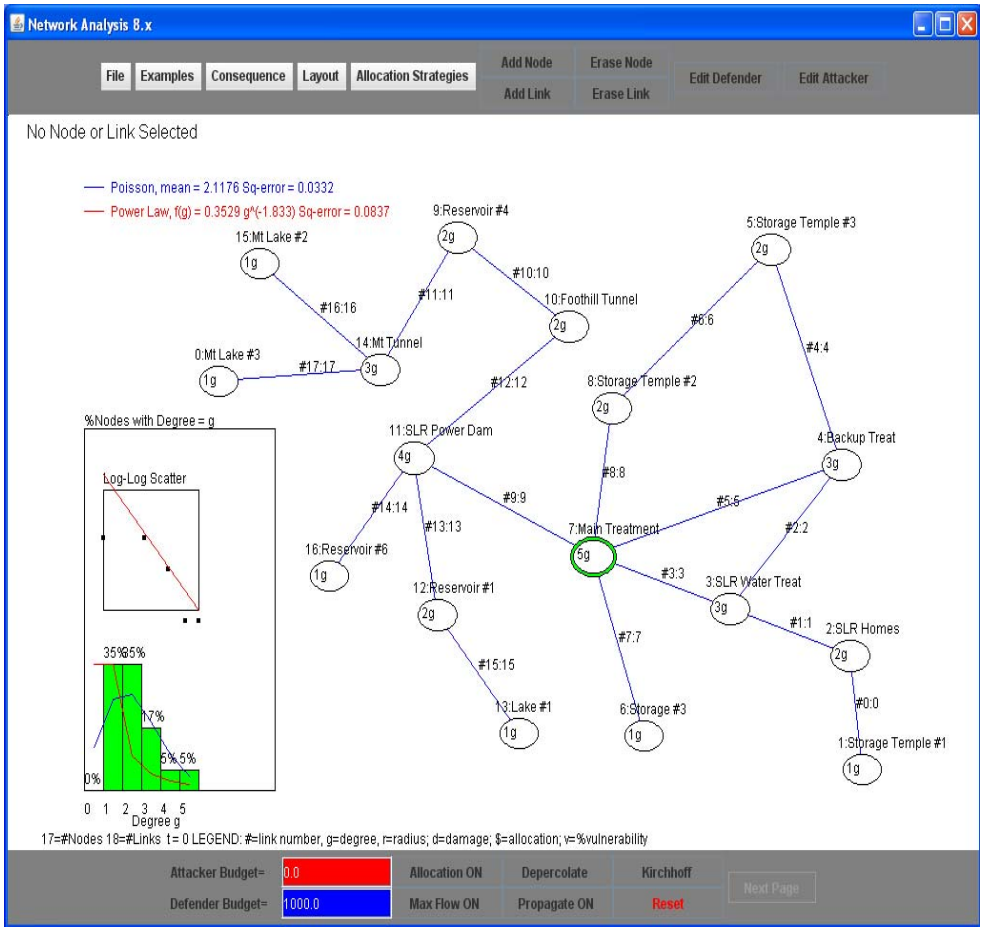

Figure 25 San Luis Rey network using MBRA

Figure 26 shows the display of CARVER with its six attributes: criticality, accessibility, recoverability, vulnerability, espyability, and redundancy. Each attribute has menu items for the operator to choose for each asset. The operator has to select the value or round it off to match the value from the drop down menu. For example, the economic loss for N_{03} (water treatment) is estimated to be \$400M; in this case we have to round off the value to the nearest value displayed from the drop down menu. That is, we have to choose either \$250M or \$500M, so we select \$500M since this asset is costly.

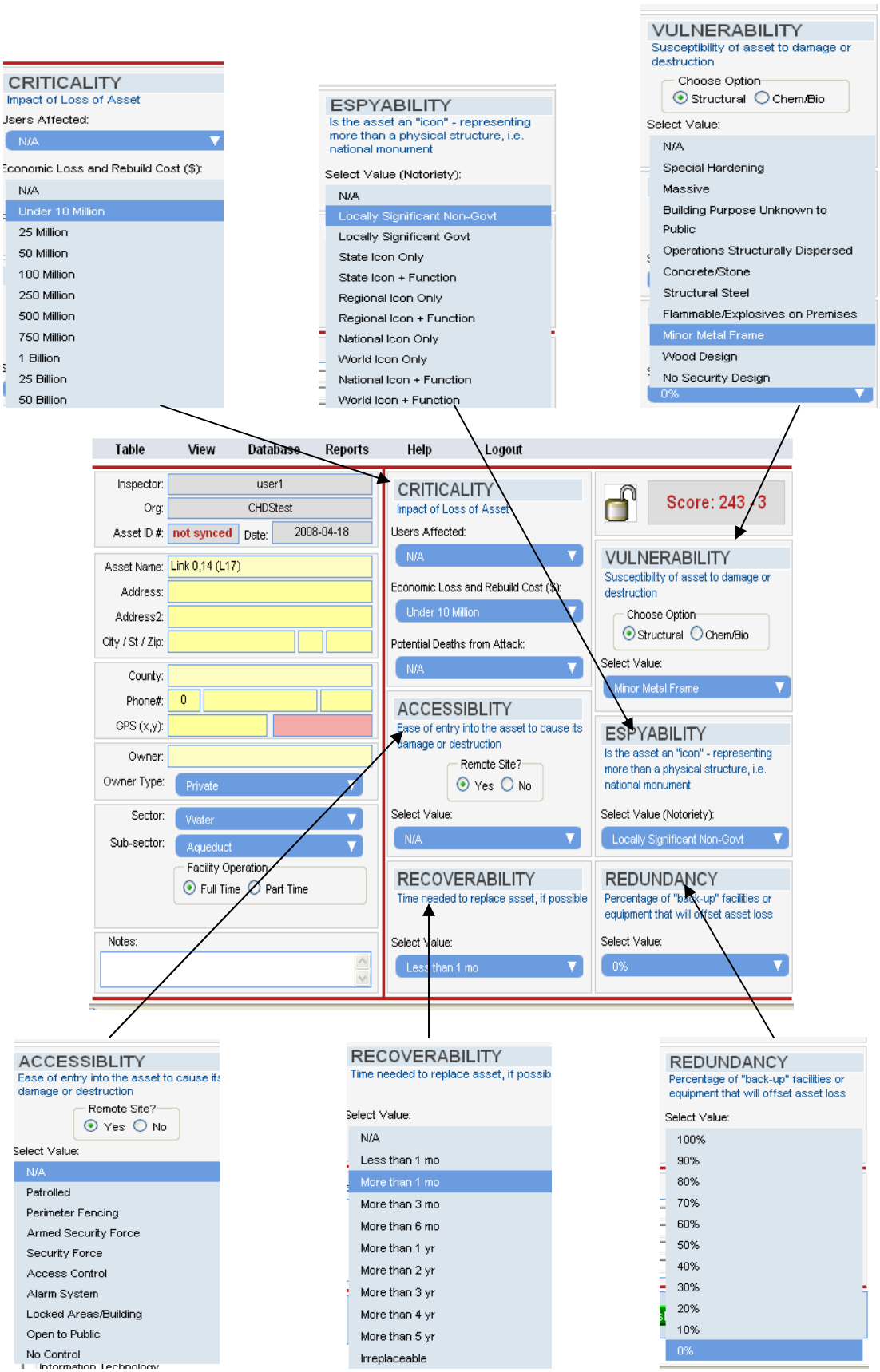

Figure 26 CARVER display

For this comparison we will apply the one-sided risk model in MBRA as described in this dissertation with a budget B=$1000 for both linear and nonlinear cost models. The results show that both the linear and nonlinear models achieve exactly the same ranking order of assets according to formula g*d/EC. This is consistent with the results reported previously. The network risk is reduced to 0.431 (43%) in the linear cost model, and to 0.224 (22.4%) for the nonlinear cost model. The resource allocation is distributed in full to assets leaving some assets unfunded in the linear model, and partially distribution over all assets in the network in the nonlinear model as shown in Figure 27.

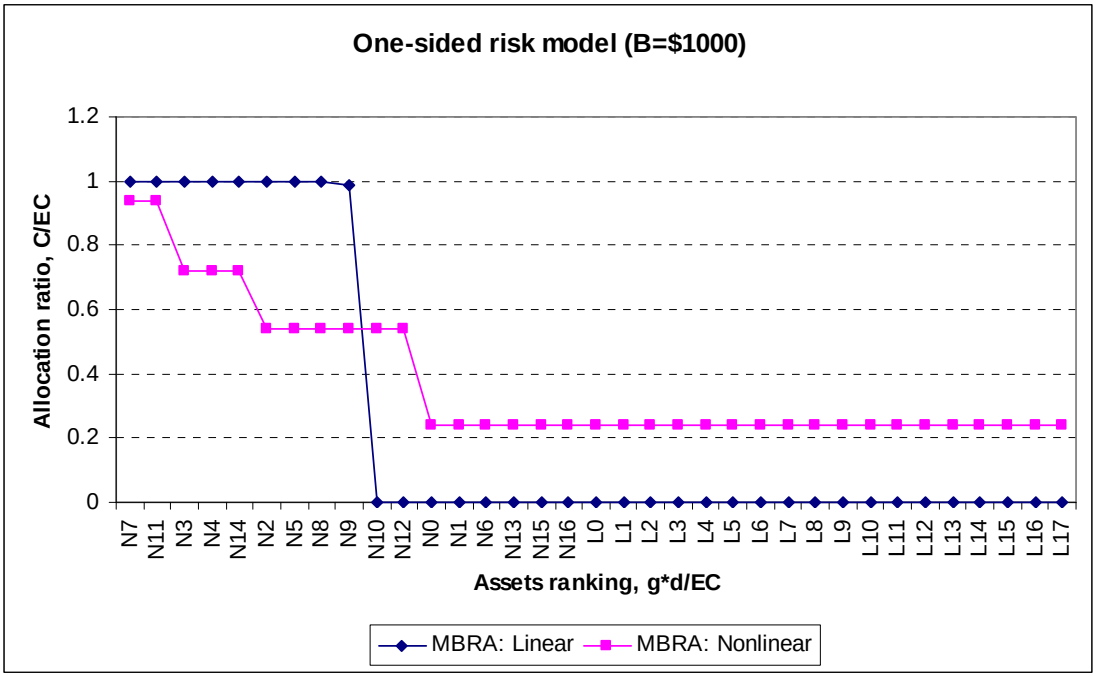

Figure 27 One-sided risk model allocation distribution

Figure 28 shows the assets ranking according to their criticality when applying MBRA. The results show exactly the same assets in ranking order for the linear and nonlinear cost models. The three most critical assets are N7, N11, and N3, that represent main treatment, power dam, and water treatment, respectively. However, notice the relative differences between the highest ranked assets in both graphs. For CARVER the

values are tightly clustered suggesting that they are sensitive to small changes. If an analyst rated a certain asset slightly differently, the overall ordering would likely change. This is not the case in MBRA where groups of assets cluster but their relative differences are significant.

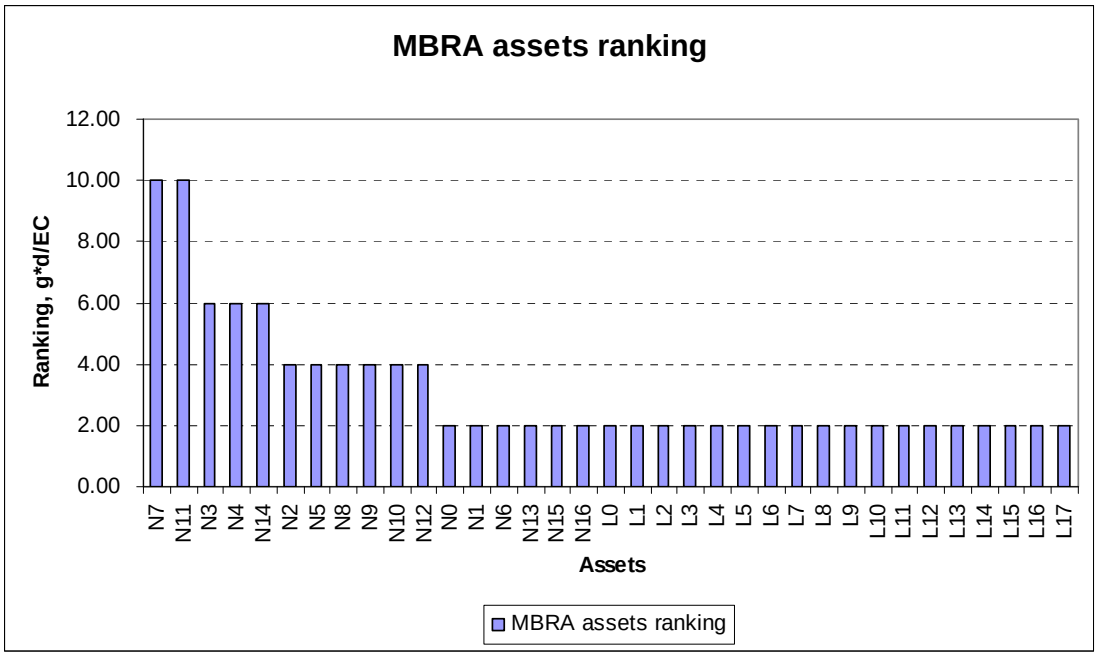

Figure 28 MBRA assets ranking

MBRA gives the operator the flexibility to change the values associated with each asset, run the tool for different budgets, and view the results on the display screen. In addition, the operator has the option to select any of the other strategies from the one-sided or two-party risk models to determine the best network risk reduction.

The results from applying CARVER show slightly different ranking order of assets from MBRA as shown in Figure 29. The three most critical assets are N_2, N_7, and N_{11} that represent SLR homes, main treatment, and power dam, respectively. In reality, losing homes or any end consumer does not affect the operation of the network as much as losing the main treatment or power dam would. CARVER has the capability to rank the first hundred top assets according to their scores obtained from the six categories

shown in Table 5. It is not capable of allocating resources to assets nor can it assess network risk. It is up to the decision maker to decide how much to invest in protecting these critical assets.

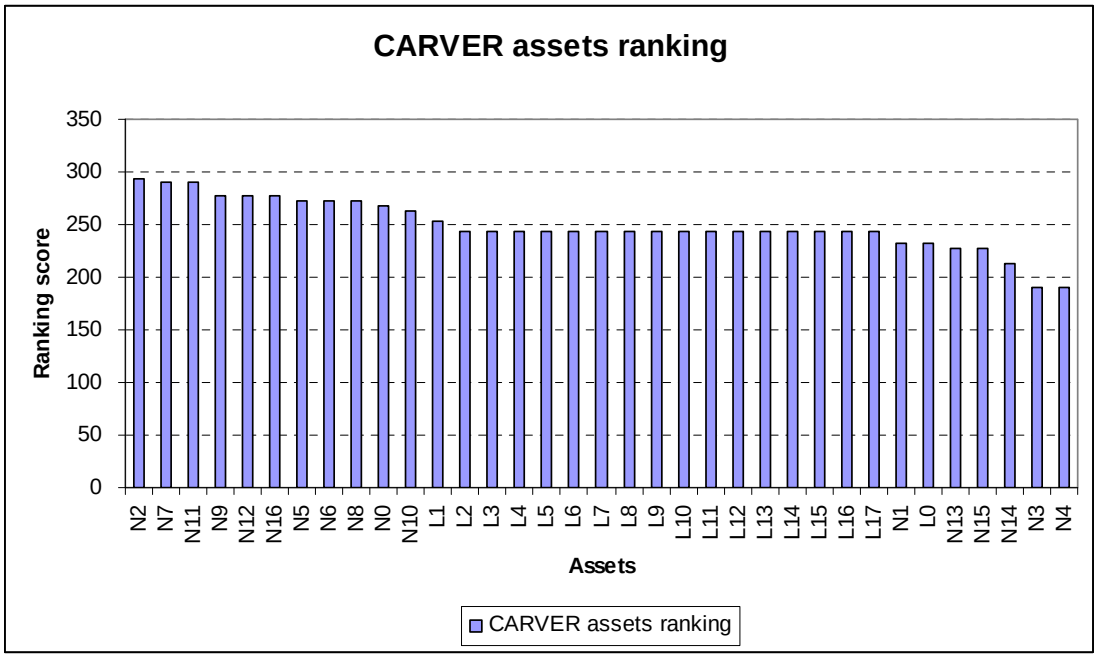

Figure 29 CARVER assets ranking

B. CONCLUSIONS

This research addressed several problems in the field of critical infrastructure protection and assessment. We formalized the definition of network risk in terms of degree sequence, vulnerability, and consequences, $R = \sum_{i=1}^{n+m} g_i \, v_i \, d_i$, that can be applied to any infrastructure. We consider this definition the basis for network risk assessment throughout this research. We have modeled the relationship between budget and network vulnerability. A one-sided risk model that represents a defensive point of view with two cost strategies - linear and nonlinear – was introduced. The results show that no matter the cost model used, the budget will be distributed optimally by rank according to the

product of damage cost, d_i, times degree, g_i, (where g_i=1 for links), divided by the defender's vulnerability-elimination cost, EC_i. Closed-form solutions are achieved for both strategies using greedy algorithm to determine the optimal allocations.

The results show that vulnerability decreases linearly or exponentially with an increase in the defender's budget. However, the linear cost strategy will distribute the budget to a few assets in full while leaving some assets unfunded. The nonlinear cost strategy will distribute the budget partially over all, or most of, the assets in a network, leaving some risk in the overall network.

Finally, this research extends the one-sided model and introduces a two-person game risk model that combines two players' defensive and offensive points of view. A defender wants to minimize network risk, and an attacker wants to maximize risk.

A joint-vulnerability function is introduced that combines the attacker and defender vulnerability. Two strategies are introduced network and non-network. The results confirm the defender and attacker's min-max objectives. In other words, as the defender's budget increases, network risk decreases exponentially to the minimum; and as the attacker's budget increases, network risk increases. The non-network arms-race strategy achieves minimum network risk for small budgets because it ignores degree sequence. The attacker is more successful when using the network strategy at low budgets because fewer funds allocated to high-ranking targets.

C. FUTURE WORK

Having laid the foundation for the MBRA tool, we note many opportunities to extend this research. An essential part of this research was the use of degree sequence as a heuristic for criticality. We assumed, based on the findings of the network science literature, that nodes with higher degree tend to be more important to the network than less connected nodes. However, degree sequence isn't the only heuristic that could be used. For other types of networks - social networks, for example - in which product or material does not flow through the network, it may be more suitable to quantify

"influence" or some other more suitable attribute of a social network. How the MBRA technique extends to these types of networks has not been well explored to date.

Another direction is to measure the effectiveness of combining the different strategies with each other to find which mixed strategy works best for the defender to minimize network risk. We focused mainly on homogeneous combinations here but it would be of interest to investigate heterogeneous combinations as well.

While the nonlinear model is certainly a closer fit to the realities of "buying down" risk, it is still an abstraction. One area where the TRAM technique excels is in directly relating specific countermeasures to specific threats as they apply to specific assets. In this way, a decision maker could not only decide to fund a certain asset at a specific amount but he would know exactly what it paid for and how much risk reduction was gained. The weakness of this technique is that it is a brute force method that relies on much more data than MBRA or even CARVER require and consequently, results need refreshing more often. It could be that MBRA is a strong complement to these types of techniques but again, this should be explored further.

We have thought about a more accurate model of the network than just the connectivity attributes. It would be useful to model the physical nature of certain sectors in an effort to be more accurate (in addition to degree sequence) in determining what impact the loss of an asset might have. Furthermore, this would allow us even greater insight into the nature of cascading networks. This would be an extremely important enhancement to the current state of the art, but as each sector functions very differently, this is no small undertaking.

Other issues of concern include the usability of the tool and training materials to assist in learning how to model networks and perform analyses using MBRA. We also envision a national database of asset data that would lessen the fluctuation in data and results year to year. DHS requires that these analyses be done with some frequency yet many of the personnel change from one analysis to the next. Cataloging and allowing comparison from region to region would be very useful in minimizing the effects of "gaming" the resource allocation system.

APPENDIX

Table 2 Input values for the one-sided & two-party risk models*

B = 2000 **k = 59**
B' = 2000

			Defender			*Attacker*			
Asset	**d**	**g**	**EF**	**EC**	**alpha**	**AF**	**AC**	**gamma**	**g*d/EC**
N11	400	1	0.1	150	0.01535	0.9	150	0.01535	2.67
N9	400	1	0.1	150	0.01535	0.9	150	0.01535	2.67
N27	600	1	0.1	200	0.01151	0.9	200	0.01151	3.00
L0	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L1	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L10	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L11	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L12	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L13	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L14	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L15	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L16	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L17	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L18	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L19	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L2	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L20	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L21	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L22	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L23	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L24	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L25	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L26	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L27	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L28	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L29	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L3	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L30	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L4	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L5	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L6	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L7	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L8	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
L9	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
N15	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33

B = 2000 **k = 59**
B' = 2000

			Defender			*Attacker*			
Asset	**d**	**g**	**EF**	**EC**	**alpha**	**AF**	**AC**	**gamma**	**g*d/EC**
N21	200	1	0.1	60	0.03838	0.9	60	0.03838	3.33
N4	100	1	0.1	30	0.07675	0.9	30	0.07675	3.33
N17	400	2	0.1	150	0.01535	0.9	150	0.01535	5.33
N1	400	2	0.1	150	0.01535	0.9	150	0.01535	5.33
N3	350	2	0.1	120	0.01919	0.9	120	0.01919	5.83
N0	600	2	0.1	200	0.01151	0.9	200	0.01151	6.00
N16	300	2	0.1	100	0.02303	0.9	100	0.02303	6.00
N20	300	2	0.1	100	0.02303	0.9	100	0.02303	6.00
N22	200	2	0.1	60	0.03838	0.9	60	0.03838	6.67
N23	200	2	0.1	60	0.03838	0.9	60	0.03838	6.67
N24	100	2	0.1	30	0.07675	0.9	30	0.07675	6.67
N25	100	2	0.1	30	0.07675	0.9	30	0.07675	6.67
N5	200	2	0.1	60	0.03838	0.9	60	0.03838	6.67
N7	200	2	0.1	60	0.03838	0.9	60	0.03838	6.67
N10	400	3	0.1	150	0.01535	0.9	150	0.01535	8.00
N12	400	3	0.1	150	0.01535	0.9	150	0.01535	8.00
N19	300	3	0.1	100	0.02303	0.9	100	0.02303	9.00
N2	300	3	0.1	100	0.02303	0.9	100	0.02303	9.00
N26	600	3	0.1	200	0.01151	0.9	200	0.01151	9.00
N13	200	3	0.1	60	0.03838	0.9	60	0.03838	10.00
N14	100	3	0.1	30	0.07675	0.9	30	0.07675	10.00
N8	200	3	0.1	60	0.03838	0.9	60	0.03838	10.00
N18	300	4	0.1	100	0.02303	0.9	100	0.02303	12.00
N6	200	4	0.1	60	0.03838	0.9	60	0.03838	13.33

- These are not actual values, but serve to illustrate the model

Table 3 Input values of San Luis Rey water supply network in MBRA

Asset	Name	d	g	EF	EC
N0	Mt. Lake	300	1	0.1	150
N1	Storage Temple #1	1	1	0.1	0.5
N2	SLR Homes	100	2	0.1	50
N3	SLR Water Treatment	400	3	0.1	200
N4	Backup Treatment	400	3	0.1	200
N5	Storage Temple #3	1	2	0.1	0.5
N6	Storage #3	1	1	0.1	0.5
N7	Main Treatment	400	5	0.1	200
N8	Storage Temple #2	1	2	0.1	0.5
N9	Reservoir #4	300	2	0.1	150
N10	Foothill Tunnel	1	2	0.1	0.5
N11	SLR Power Dam	500	4	0.1	200
N12	Reservoir #1	300	2	0.1	150
N13	Lake #1	300	1	0.1	150
N14	Mt. Tunnel	1	3	0.1	0.5
N15	Mt. Lake #2	300	1	0.1	150
N16	Reservoir #6	300	1	0.1	150
L0	1,2	0.5		0.1	0.25
L1	2,3	0.5		0.1	0.25
L2	3,4	0.5		0.1	0.25
L3	3,7	0.5		0.1	0.25
L4	4,5	0.5		0.1	0.25
L5	4,7	0.5		0.1	0.25
L6	5,8	0.5		0.1	0.25
L7	6,7	0.5		0.1	0.25
L8	7,8	0.5		0.1	0.25
L9	7,11	0.5		0.1	0.25
L10	9,10	0.5		0.1	0.25
L11	14,9	0.5		0.1	0.25
L12	10,11	0.5		0.1	0.25
L13	11,12	0.5		0.1	0.25
L14	16,11	0.5		0.1	0.25
L15	13,12	0.5		0.1	0.25
L16	15,14	0.5		0.1	0.25
L17	0,14	0.5		0.1	0.25

Table 4 Input values San Luis Rey water supply network in CARVER

Asset	Connectivity	Type	Sector	People Affected	Estimated Deaths	Repair Time	Economic Loss	Existing Security	Icon Status
N00	1	Mt. Lake	Water	NA	NA	6 months	250M	Fencing	Locally significant
N01	1	storage temple #1	Water	NA	NA	6 months	under 10M	Open to public	Locally significant
N02	2	SLR homes	Water	NA	NA	6 months	100M	Open to public	Locally significant
N03	3	Water treatment	Water	NA	NA	1 year	500M	Fencing	Locally significant
N04	3	backup treatment	Water	NA	NA	1 year	500M	Fencing	Locally significant
N05	2	storage temple #3	Water	NA	NA	6 months	under 10M	Fencing	Locally significant
N06	1	storage #3	Water	NA	NA	6 months	under 10M	Fencing	Locally significant
N07	5	main treatment	Water	NA	NA	1 year	500M	Fencing	Locally significant
N08	2	storage temple #2	Water	NA	NA	6 months	under 10M	Fencing	Locally significant
N09	2	reservoir #4	Water	NA	NA	6 months	250M	Fencing	Locally significant
N10	2	foothill tunnel	Water	NA	NA	6 months	under 10M	Fencing	Locally significant
N11	4	power dam	Water	NA	NA	1 year	500M	Fencing	Locally significant
N12	2	reservoir #1	Water	NA	NA	6 months	250M	Fencing	Locally significant
N13	1	lake #1	Water	NA	NA	6 months	250M	Fencing	Locally significant
N14	3	Mt. tunnel	Water	NA	NA	6 months	under 10M	Fencing	Locally significant
N15	1	Mt. lake #2	Water	NA	NA	6 months	250M	Fencing	Locally significant
N16	1	reservoir #6	Water	NA	NA	6 months	250M	Fencing	Locally significant
L00	N01,N02	Link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L01	N02,N03	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L02	N03,N04	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L03	N03,N07	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L04	N04,N05	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L05	N04,N07	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L06	N05,N08	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L07	N06,N07	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L08	N07,N08	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L09	N07,N11	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L10	N09,N10	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L11	N14,N09	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L12	N10,N11	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L13	N11,N12	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L14	N16,N11	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L15	N13,N12	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L16	N15,N14	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant
L17	N00,N14	link	Water	NA	NA	< 1 month	under 10M	Open to public	Locally significant

Table 5 CARVER's top 100 ranked assets

Top 100 Ranked Assets

April 19, 2008

Asset ID	Asset Name	Sector	Score	Criticality	Accessibility	Recoverability	Vulnerability	Espyability	Redundancy	Interdependancy
	SLR Homes (N2)	WATER	293	40	0	40	100	100	100	3
	SLR powerdam (N11)	WATER	290	60	30	40	50	100	100	3
	Main treatment (N7)	WATER	290	60	30	40	50	100	100	3
	Reservoir#6 (N16)	WATER	277	50	30	30	50	100	100	3
	Reservoir #4 (N9)	WATER	277	50	30	30	50	100	100	3
	Reservoir (N12)	WATER	277	50	30	30	50	100	100	3
	Storage #3 (N6)	WATER	273	10	30	30	60	100	100	3
	Storage temple #2 (N8)	WATER	273	10	30	30	60	100	100	3
	Storage temple # 3 (N5)	WATER	273	10	30	30	60	100	100	3
	Mt. Lake (N0)	WATER	267	50	30	30	50	100	100	3
	Foothill tunnel (N18)	WATER	263	10	30	30	50	100	100	3
	Link 2,3 (L1)	WATER	253	10	0	20	60	100	100	3
	Link 13,12 (L15)	WATER	243	10	0	10	80	100	100	3
	Link 16,11 (L14)	WATER	243	10	0	10	80	100	100	3
	Link 11,12 (L13)	WATER	243	10	0	10	80	100	100	3
	Link 15,14 (L16)	WATER	243	10	0	10	80	100	100	3
	Link 0,16 (L17)	WATER	243	10	0	10	80	100	100	3
	Link 10,11 (L12)	WATER	243	10	0	10	80	100	100	3
	Link 3,7 (L3)	WATER	243	10	0	10	80	100	100	3
	Link 4,5 (L4)	WATER	243	10	0	10	80	100	100	3
	Link 4,7 (L5)	WATER	243	10	0	10	80	100	100	3
	Link 5,6 (L6)	WATER	243	10	0	10	80	100	100	3
	Link 6,7 (L7)	WATER	243	10	0	10	80	100	100	3
	Link 7,8 (L8)	WATER	243	10	0	10	80	100	100	3
	Link 7,11 (L9)	WATER	243	10	0	10	80	100	100	3
	Link 9,10 (L10)	WATER	243	10	0	10	80	100	100	3
	Link 14,9 (L11)	WATER	243	10	0	10	80	100	100	3
	Link 3,4 (L2)	WATER	243	10	0	10	80	100	100	3
	Storage Temple #1 (N1)	WATER	233	10	0	30	60	100	100	3
	Link 1,2 (L0)	WATER	233	10	0	20	80	100	100	1
	Lake #1 (N13)	WATER	227	50	30	30	0	100	100	3
	Mt. Lake #2 (N15)	WATER	227	50	30	30	0	100	100	3
	Mt. Tunnel (N14)	WATER	213	10	30	30	0	100	100	3
	Backup treatment (N4)	WATER	190	60	30	40	50	0	0	3
	Water treatment (N3)	WATER	190	60	30	40	50	0	0	3
	Total Score of All35 Assets		8707	820	450	760	2230	340	3380	103

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Albert, R., Jeong, H., and Barabasi, A. (2000). "The Internet's Achilles' Heel: Error and Attack Tolerance of Complex Networks." *Nature*, 406: 378-382.

Al Mannai, W. and Lewis, T. (2007, August). "Minimizing Network Risk with Application to Critical Infrastructure Protection." *Journal of Information Warfare*, 6 (2): 52-68.

Al Mannai, W. and Lewis, T. (2008). (in press). "A General Defender-Attacker Risk Model for Networks." *Journal of Risk Finance*.

Barabasi, Albert-Laszlo. (2002). *Linked: The New Science of Networks*. Cambridge, MA: Perseus Publishing.

Barabasi, Albert-Laszlo. (2003). "Scale-Free Networks." *Scientific American*, May 2003, 288(5):60-69.

Bier, V., Abhichandani, V. (2002). "Optimal Allocation of Resources for Defense of Simple Series and Parallel Systems from Determined Adversaries." *Proceedings of the Engineering Foundation Conference on Risk-Based Decision making in Water Resources*. Santa Barbara, CA: American Society of Civil Engineers.

Bier, V., Nagaraj, A., and Abhichandani, V. (2005). "Protection of Simple Series and Parallel Systems with Components of Different Values." *Reliability Engineering and System Safety*, Vol. 87, 315-323.

Brown, G., Carlyle, M., Salmeron, J., and Wood, K. (2006, November-December). "Defending Critical Infrastructure." *Interfaces*, Vol. 36, No. 6, 530-544.

CARVER. (2006). "Criticality Accessibility Recoverability Vulnerability Espyability Redundancy, (CARVER)." *National Infrastructure Institute, Center for Infrastructure Expertise*. http://www.ni2cie.org/CARVER2.asp (last accessed March 2008).

Croucher, J. (1975, March). Application of the Fundamental Theorem of Games to an Example Concerning Antiballistic Missile Defense. *Naval Research Logistics Quarterly*, Vol. 22, No. 1, NAVSO P-1278, 19.

Danskin, J. (1967). *The Theory of Max-Min.* Springer-Verlag Inc., New York.

Down, B. (2007, August). "Balancing Resources to Risk." *Presentation to SCOTS/ NCHRP 20-59*. Irvine, CA.

FEMA 426. (2007). "Building Design for Homeland Security: Unit V Risk Assessment/Risk Management." *Federal Emergency Management Agency Reference Manual*. http://www.fema.gov/library/viewRecord.do?id=1559 (last accessed March 2008).

GAO. (2005). "Risk Management." *Government Accountability Office*, GAO-06-91. Washington, DC. www.gao.gov/cgi-bin/getrpt (last accessed March 2008).

Hammond, G. (1993). *Plowshares into Swords*. Columbia, South Carolina: University of South Carolina Press.

Horowitz, E. and Sahni, S. (1978). *Fundamentals of Computer Algorithms*. Computer Science Press, Inc.

HSPD 7. (2003, December 13). "Homeland Security Presidential Directive/(HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection." *The White House,* Washington, DC.

Kakutani, S. (1941). "A Generalization of Brouwer's Fixed Point Theorem." *Duke Math J*. 8, 457-459.

Lewis, Ted. (2004). "Vulnerability Analysis in Critical Infrastructure Protection." *Journal of Information Warfare*, Vol. 3, Issue 2, June 2004.

Lewis, T. (2006). *Critical Infrastructure Protection in Homeland Security: Defending A Networked Nation*. New Jersey: John Wiley & Sons.

Lewis, T. Darken, R., and Mackin, T. (2007). (in press). "Managing Risk in critical Infrastructures using Network modeling." *IEEE Spectrum*.

Mackin, T. (2005). "Risk Analysis Methodology for Critical Assets Protection (RAMCAP)." *Department of Mechanical Engineering, University of Illinois*. Illinois.

Major, J. (2002, Fall). Advanced Techniques for Modeling Terrorism Risk. *Journal of Risk Finance*. Vol. 4, Issue 1.

Moteff, J. (2005, February 4). "Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences." Report for Congress RL32561, *The Library of Congress*.

NIPP. (2006). *The National Infrastructure Protection Plan*. The U.S. Department of Homeland Security.

Owen, G. (1969). "Minimization of Fatalities in a Nuclear Attack Model." *Operations Research*, 17, 489-505.

PDD 63. (1998, May 22). *Protecting America's Critical Infrastructures: Presidential Decision Directive 63*. The White House, Office of the Press Secretary, Annapolis, MD.

Powell, R. (2005). Defending Against Terrorist Attacks with Limited Resources. *Department of Political Science. University of California Berkeley*. Berkeley, CA.

Powell, R. (2006). "Defending Strategic Terrorists Over the Long Run: A Basic Approach to Resource Allocation." *Institute of Governmental Studies (University of California, Berkeley)*, paper WP2006-34. Berkeley, CA.

Powers, M. R. and Shen, Z. (2005). "Colonel Blotto in the War on Terror: Implications for Event Frequency." *Fox School Working Paper*. Temple University.

RAM. (2000). "Risk Assessment Methodology for Physical Security (RAM)." *Sandia Corporation, Sandia National Laboratories*. http://www.sandia.gov/ram/references.htm (last accessed March 2008).

RAMCAP. (2005). "Risk Analysis and Management for Critical Asset Protection." *ASME Innovative Technologies Institute*. http://en.wikipedia.org/wiki/User:RAMCAP; http://files.asme.org/ASMEITI/RAMCAP/12604.pdf; http://www.asme-iti.org/RAMCAP/RAMCAP_FAQs.cfm (last accessed February 2008).

Roper, Carl A. (1999). *Risk Management for Security Professionals*. Butterworth Heinemann.

Stackelberg, H. (1952). *The Theory of the Market Economy*, (translated from German). William Hodge & Co., London, UK.

TRAM. (2008). *Transit Risk Assessment Tool*. The U.S. Department of Homeland Security. Version 2.0.

USA Partriot Act. (2001, October 26). *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*. The White House, Washington, DC.

Xie, M., Tan, K., and Goh, K. (2000). "Optimum prioritization and resource allocation based on fault tree analysis." *International Journal of Quality & Reliability Management*, Vol. 17, No. 2, 189-199.

Washburn, A. (2001). A New Kind of Fictitious Play. *Naval Research Logistics*, Vol. 48, Issue 4, 270-280. John Wiley & Sons, Inc.

Washburn, A. (2002). *Search and Detection*. 4th Edition. INFORMS. Institute for Operations Research and the Management Sciences. Linthicum, MD.

Wilcox, R., Ayyub, B., Burrows, M., and Ghosh, S. (2001, July 1). "Risk-based Technology Methodology for the Safety Assessment of Marine Compressed Natural Gas Fuel Systems." *Marine Technology*, Vol. 38, No. 3, 193-207 (15).

Willis, H., Morral, A., Kelly, T., and Medby, J. (2005). "Estimating Terrorism Risk." *RAND Center for Terrorism Risk Management Policy*. www.rand.org (last accessed December 2007).

Willis, H. (2007). "Guiding Resource Allocations Based on Terrorism Risk." *Risk Analysis*, Vol. 27, No. 3.

WSJ. (2006, February 14). "There is No Perfect Security by Michael Chertoff." *The Wall Street Journal Online*. www.WSJ.com, (last accessed February 2008).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Waleed I. Al Mannai
   Manama, Kingdom of Bahrain

4. Prof Dr. Stefan Pickl
   Fakultat fur Informatik
   Universitat der Bundeswehr Munchen
   Institut fur Angewandte Systemwissenschafen und Wirtschaftsinformatik
   Neubiberg, Germany

5. Robert Powell
   Robson Professor
   Travers Department of Political Science
   UC Berkeley
   Berkeley, California

6. Vickie Bovell
   Department of Homeland Security
   Infrastructure Information Collection Division
   Washington, DC

7. Dr. Thomas J. Mackin
   Professor and Chair
   Mechanical Engineering Department
   California Polytechnic State University
   San Luis Obispo, California

8. Ash Chatterjee
   Branch Chief, Risk Assessment & Analysis
   Mass Transit Security/TSNM
   Transportation Security Administration Hq
   Arlington, Virginia