Spring 2012

Risk Quadruplet: Integrating Assessments of Threat, Vulnerability, Consequence, and Perception for Homeland Security and Homeland Defense

Kara Norman Hill
Old Dominion University

Recommended Citation
Hill, Kara N.. "Risk Quadruplet: Integrating Assessments of Threat, Vulnerability, Consequence, and Perception for Homeland Security and Homeland Defense" (2012). Doctor of Philosophy (PhD), dissertation, Engineering Management, Old Dominion University, DOI: 10.25777/t546-1573
https://digitalcommons.odu.edu/emse_etds/74

RISK QUADRUPLET: INTEGRATING ASSESSMENTS OF THREAT, VULNERABILITY, CONSEQUENCE, AND PERCEPTION FOR HOMELAND SECURITY AND HOMELAND DEFENSE

by

Kara Norman Hill
B.S. May 2002, Virginia Commonwealth University
M.S. December 2006, The George Washington University

A Dissertation submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

ENGINEERING MANAGEMENT

OLD DOMINION UNIVERSITY
April 2012

Approved by:

Adrian Gheorghe (Director)

Ariel Pinto (Member)

Charles Keating (Member)

Barry Ezell (Member)

ABSTRACT

RISK QUADRUPLET: INTEGRATING ASSESSMENTS OF THREAT, VULNERABILITY, CONSEQUENCE, AND PERCEPTION FOR HOMELAND SECURITY AND HOMELAND DEFENSE

Kara Norman Hill
Old Dominion University, 2012
Director: Adrian Gheorghe

"Where there is much to risk, there is much to consider."

– Platen

Risk for homeland security and homeland defense is often considered to be a function of threat, vulnerability, and consequence. But what is that function? And are we defining and measuring these terms consistently? Threat, vulnerability, and consequence assessments are conducted, often separately, and data from one assessment could be drastically different from that of another due to inconsistent definitions of terms and measurements, differing data collection methods, or varying data sources. It has also long been a challenge to integrate these three disparate assessments to establish an overall picture of risk to a given asset. Further, many agencies conduct these assessments and there is little to no sharing of data, methodologies, or results vertically (between federal, state, and local decision-makers) or horizontally (across the many different sectors), which results in duplication of efforts and conflicting risk assessment results.

Obviously, risk is a function of our perceptions and those perceptions can influence our understanding of threat, vulnerability, and consequence. Some assessments rely on perceptions (elicited from subject matter experts) in order to qualify or quantify threat,

vulnerability, and consequence. Others exclude perception altogether, relying on objective data, if available. Rather than fault the subjectivity of our perceptions, or muddle objective assessments with personal opinions, it makes sense to embrace our perceptions, but segregate them as a unique component of risk.

A *risk quadruplet* is proposed to systematically collect and integrate assessments of threat, vulnerability, consequence, and perception, such that each dimension can be explored uniquely, and such that all four components can be aggregated into an overall risk assessment in a consistent, transparent, traceable, and reproducible manner. The risk quadruplet draws from the fields of homeland security, homeland defense, systems engineering, and even psychology to develop a model of risk that integrates all four assessments using multicriteria decision analysis. The model has undergone preliminary validation and has proven to be a viable solution for ranking assets based on the four proposed components of risk.

This dissertation is dedicated to my husband…

ACKNOWLEDGMENTS

"Only those who will risk going too far can possibly find out how far one can go."
– T.S. Eliot

There are several people who supported me throughout this adventure, and I cannot possibly thank them enough. First, I must thank my doctoral advisor, Dr. Adrian Gheorghe, for his guidance and patience. In 2007, he made it possible for me to begin this degree remotely while living in the Washington, DC area. Since then, he has kept me focused on my dissertation throughout a move to Norfolk, VA, a new and demanding career, my engagement and marriage, and most recently, my pregnancy and the birth of my first child.

I would also like to thank my committee members, Dr. Ariel Pinto and Dr. Charles Keating, for their support throughout my academic career and dissertation research. While Dr. Gheorghe shared my interest in critical infrastructure, Dr. Pinto kindled my curiosity in risk analysis and Dr. Keating offered structure and systematic thinking, which I desperately needed to progress in my research. Next, I would like to thank Dr. Barry Ezell, my external committee member, for his enthusiasm and encouragement. He made what was perhaps the most crucial contribution to this research when he introduced me to risk perception. He is also responsible for the following blunt, but sage advice, "The goal is to graduate."

I will never be able to sufficiently thank my husband, James Hill. He met me only months before I enrolled at Old Dominion University as a doctoral student, and despite this, he still married me! Since then he has stood by me, even when others, myself included, did not always understand the significance of such an undertaking. Somehow he managed to complete his own degree, start a challenging career as a middle school teacher, and with what little spare time remained, he took on countless household responsibilities in order to allow me time for my research. As we begin our next chapter as parents to our amazing daughter, Mackenzy Paige Hill, I am certain our daily lives will be no less demanding, but I am now confident that we can handle anything together.

Lastly, I wish to thank my family who instilled in me a love of learning, a sense of patriotism, a desire to serve, and a strong work ethic. I was a stubborn child (and I have been known to be a stubborn adult, as well), so I am sure my parents and sister spent the majority of the past five years empathizing not with me, but with my advisor and committee. But it is because they know me so well that they were able to love me throughout this challenge and that love sustained me more than they may ever know.

Thank you all so much!

LIST OF ABBREVIATIONS AND ACRONYMS

AHP	Analytic Hierarchy Process
ANP	Analytic Network Process
CI	Critical Infrastructure
CIIA	Critical Infrastructure Information Act
CIKR	Critical Infrastructure and Key Resources
CIKRKA	Critical Infrastructure, Key Resources, and Key Assets
CIP	Critical Infrastructure Protection
CMDTINST	Commandant Instructions
CRS	Congressional Research Service
CSIS	Center for Strategic and International Studies
DC	District of Columbia
DHS	Department of Homeland Security
DOI	Department of the Interior
EIA	Energy Information Administration
EO	Executive Order
EPA	Environmental Protection Agency
EPR&R	Emergency Preparedness, Response, and Recovery
ER	Evidential Reasoning
FEMA	Federal Emergency Management Agency
FY	Fiscal Year
GIS	Geographic Information Systems
HIPAA	Health Insurance Portability and Accountability Act

HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSA	Homeland Security Act
HSAS	Homeland Security Advisory System
HSPD	Homeland Security Presidential Directive
IDS	Intelligent Decision System
IDT	Infrastructure Data Taxonomy
INFORMS	Institute for Operations Research and the Management Sciences
IRB	Institutional Review Board
KA	Key Assets
KR	Key Resources
MAUT	Multi Attribute Utility Theory
MCDA	Multi Criteria Decision Analysis
M&S	Modeling and Simulation
NCDC	National Climatic Data Center
NDRF	National Disaster Recovery Framework
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NOAA	National Oceanic and Atmospheric Administration
NPG	National Preparedness Guidelines
NPS	National Preparedness System
NRC	National Research Council
NRF	National Response Framework

NSHS	National Strategy for Homeland Security
NSPPCIKA	National Strategy of the Physical Protection of Critical Infrastructure and Key Assets
NTAS	National Terrorism Advisory System
OECD	Organisation for Economic Co-operation and Development
PDD	Presidential Decision Directive
PPD	Presidential Policy Directive
PRA	Probabilistic Risk Assessment
QRA	Quantitative Risk Assessment
RA	Risk Acceptability
RD	Risk from Disease
RMF	Risk Management Framework
RPI	Responsible Primary Investigator
RR	Risk Rewards
RRAP	Regional Resiliency Assessment Program
SCADA	Supervisory Control and Data Acquisition
SNRA	Strategic National Risk Assessment
US	United States
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
VA	Virginia
VV&A	Verification, Validation, and Accreditation
WEF	World Economic Forum

TABLE OF CONTENTS

LIST OF TABLES

Table Page

Page

LIST OF FIGURES

Figure Page

Page

Page

Page

LIST OF EQUATIONS

CHAPTER 1

INTRODUCTION

"Suppose a person of the fourth dimension, condescending to visit you, were to say, 'Whenever you open your eyes, you see a plane (which is of two dimensions) and you ***infer*** *a solid (which is of three); but in reality you also see (though you do not recognize) a fourth dimension, which is not color nor brightness nor anything of the kind, but a true dimension, although I cannot point out to you its direction, nor can you possibly measure it.' What would you say to such a visitor? Would not you have him locked up? Well, that is my fate; and it is as natural for us Flatlanders to lock up a Square for preaching the third dimension, as it is for you Spacelanders to lock up a Cube for preaching the fourth. Alas, how strong a family likeness runs through blind and persecuting humanity in all dimensions! Points, Lines, Squares, Cubes, Extra-Cubes — we are all liable to the same errors, all alike the slaves of our respective dimensional prejudices..."*
– Edwin A. Abbott, Flatland

Risk, in most contexts, is a two dimensional function of probability and consequences. Risk, in the field of homeland security and homeland defense, however, is often considered to be a function in three dimensions: threat, vulnerability, and consequence. And still we find those three dimensions lacking. This function is not clearly defined and even if we knew the function, we do not define and measure these terms consistently. These threat, vulnerability, and consequence assessments are conducted separately; in addition, the measurements are inconsistently defined, the data collection methods vary, and the data sources differ. Further, many different agencies conduct these risk assessments and there is little to no sharing of the data, methodologies, or results vertically (between federal, state, and local decision-makers) or horizontally (across the many different sectors). This results in duplication of efforts and conflicting risk assessment results.

In addition to these issues, it is also a challenge to integrate these three disparate assessments to establish an overall picture of risk to a given asset. There are many different types of risk assessments performed on assets and those different assessments explore risk from different perspectives. Is the asset a critical power plant, essential to electricity generation? Is it a large dam, critical to the water supply? Is it a major road, critical to transportation? Or is it a major tourist attraction, critical to national morale? Or, like the Hoover Dam, is it all of these things? Which risk assessment is *right*? How can all of these risk assessments be integrated? Are certain risk assessments more important than others?

Obviously, risk is a function of our perceptions and those perceptions can influence our understanding of threat, vulnerability, and consequence. Furthermore, our perceptions may not always agree with the results of our risk assessments. While some assessments rely solely on perceptions in order to qualify or quantify threat, vulnerability, and consequence, other assessments seek to exclude perception altogether from the assessment process, relying on objective data. Rather than fault the subjectivity of our perceptions, or muddle our objective assessments with personal opinions, it makes more sense to embrace our perceptions, but to segregate them as their own unique component of risk. A risk quadruplet is proposed to systematically collect and integrate assessments of threat, vulnerability, consequence, and perception, such that each dimension can be explored uniquely, and such that all four components can be aggregated into an overall risk assessment in a systematic, transparent, traceable, and reproducible manner.

Although it has been argued that risk to our nation can be assessed and quantified objectively through some application of the homeland security *risk triplet* (threat, vulnerability, and consequence), this risk assessment approach does not account for the type of entity, be it Critical Infrastructure (CI), Key Resource (KR), or Key Asset (KA). The type of asset being assessed intuitively impacts our perceptions and our perceptions may even contradict our quantitative risk assessments. Literature reviews reveal that there is confusion about the definitions of CIKRKA.

Many talk about risk as a function of threat, vulnerability, and consequence (*National Infrastructure Protection Plan,* 2009; H. H. Willis, 2007). Multiple risk assessments which seek to assess threat, vulnerability, and consequence to a specific asset or facility could vary widely. Risk assessments could be based on risk data or perceptions. The data from one assessment could be drastically different from the data of another assessment; one assessment could incorporate factors such as whether the risk was voluntary or involuntary, while another might attempt to calculate risk using traditional risk equations (Turner, 1994).

There is also confusion about the definitions of threat, vulnerability, and consequence, let alone how to assess those nebulous concepts. The many different definitions of these concepts can drastically affect risk calculations. Threat could be viewed as a single scenario, or the likelihood of that scenario. Vulnerability could be seen as a probability, or it could be viewed as a state of the system, from which conditional probabilities of threat might be derived. And there are many types of consequences (economic, environmental, or in some cases loss of life) which must all be assessed in order to give the best possible overall risk picture. Most of this confusion arises from our inherent perceptions. There is, inevitably, an element of subjectivity to any risk assessment, and that subjectivity is currently missing from the risk assessment approach. It only makes sense to integrate our threat, vulnerability, and consequence assessments with our perceptions into an overall, improved, risk assessment approach, thus defining a new risk paradigm. A risk quadruplet is proposed in this dissertation that incorporates threat, vulnerability, consequence, and perception (Figure 1.1).

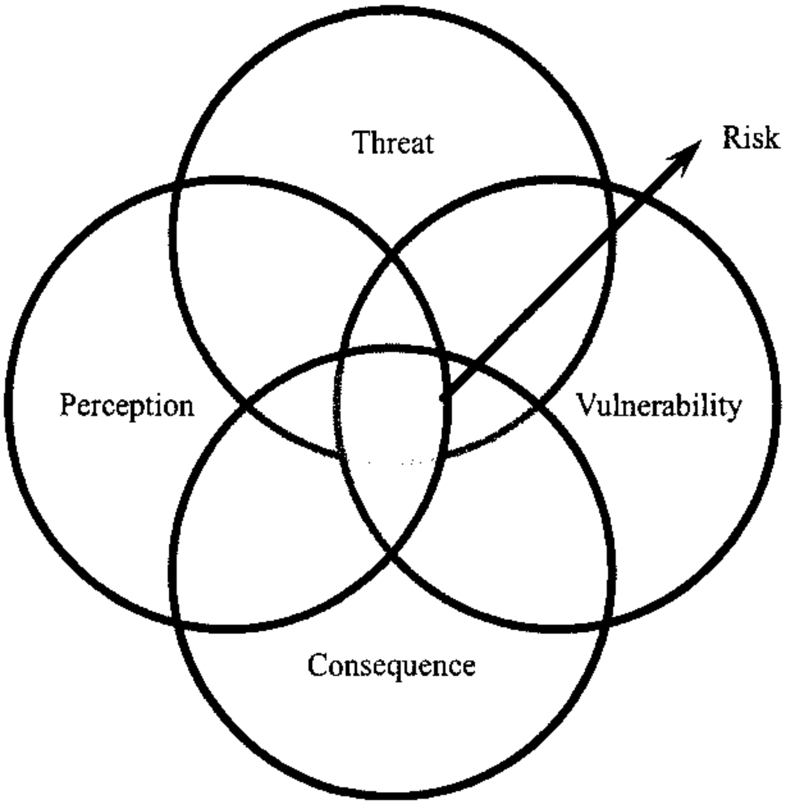


Figure 1.1. Proposed Risk Quadruplet ©

1.1 Research Definitions

Many of the following definitions will be discussed in further detail in the Literature Review (5.4APPENDIX C). However, below is a list of terms and their intended meanings when used throughout this research. Some of these definitions are pulled straight from the literature. Others are modified from definitions provided in official, government documents, such as the Department of Homeland Security (DHS) Risk Lexicon. All of these definitions, as they are presented here, reflect the intents and purposes of this research.

- *Critical Infrastructure:* government and private systems essential to the operation of our nation in any or all aspects of the lives of its citizens (health, safety, economy, etc.), such as utilities, facilities, pipelines, etc.

- *Key Resources:* public or private resources essential to the operation of our nation's government and economy, such as fuel or goods.
- *Key Assets:* those buildings, geographic regions, monuments, or icons, whose destruction would cause a crushing blow to our nation's ego, morale, and identity, but which are not essential to the operation of our nation, such as the Washington Monument or the Statue of Liberty.
- *Asset:* assets are the collective, generalized term used to represent the combination of all critical infrastructure, key resources, and key assets.
- *Risk Scenario:* natural or man-made occurrence, hazard, individual, entity, or action that has or indicates the potential to damage an asset.
- *Threat:* the threat of a risk scenario to an asset. The threat of an intentional risk scenario is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary. For other risk scenarios, threat is generally estimated as the likelihood that the risk scenario will manifest; however, threat can also be estimated qualitatively as perceived likelihood.
- *Vulnerability:* ability of an asset to endure a risk scenario despite physical features, operational attributes, characteristics of design, location, security posture, operation, or any combination thereof that renders an asset open to exploitation or susceptible to a given risk scenario. Vulnerability can be estimated qualitatively, or quantitatively, as the likelihood of a successful risk scenario given the risk scenario is identified, which implies that vulnerability is also related to resilience.

- *Consequence:* effect of a successful risk scenario on an asset. Consequence is commonly assessed along four factors: human, economic, mission, and psychological, but may also include other factors such as impact on the environment; consequence can be measured quantitatively if data exists, but can also be measured qualitatively either along a set of scales or along a single integrated consequence scale for which all consequence factors are considered as a whole.
- *Risk Perception:* subjective judgment about the severity of a risk scenario to an asset; may be driven by sense, emotion, or personal experience; generally measured qualitatively; referred to merely as perception throughout this research.
- *Risk:* potential for an unwanted outcome resulting from a risk scenario, as determined by the threat, vulnerability, consequence, and perception of that risk scenario to an asset. Risk is often measured and used to compare different future situations, as well as to rank assets for the purposes of risk mitigation and budgeting for emergency preparedness, response, and recovery.
- *Systems:* comprised of interrelated or interdependent objects. Systems exhibit holistic properties not necessarily evident at the level of individual objects or subsystems; seek to achieve some final goal or state, and in order to reach this goal they transform inputs into outputs; tend to devolve into entropy without regulation and are typically organized in a hierarchical system of nested subsystems where the subsystems are specialized with different functions within the system. Systems either diverge, in which case it has many ways of

achieving a single goal, or converge, where, from an initial state, it could achieve many different goals (Skyttner, 2005).

- *System of Systems:* possess the same definition as systems, but on a larger scale. For a hierarchy of systems, in which systems are components or subsystems of other systems; component systems each have a purpose of their own and would continue to operate even if separated from the overall system. Each component system is managed individually, rather than being managed within the context of the entire system of systems. System of systems often exhibit characteristics of complexity and widespread geographic distribution. The combination of several interdependent CI showing the characteristics of a single system, but lack an overarching management entity (Gheorghe, Masera, & Voeller, 2008; Maier, 1998; Skyttner, 2005).

1.2 Research Purpose

The risk quadruplet consists of three phases (Figure 1.2). The first phase is the perception assessment. The second phase consists of threat, vulnerability, and consequence assessments. The final phase is the assessment integration phase, where the assessments of threat, vulnerability, consequence, and perception are all assimilated. These phases will be discussed in greater detail in CHAPTER 3.

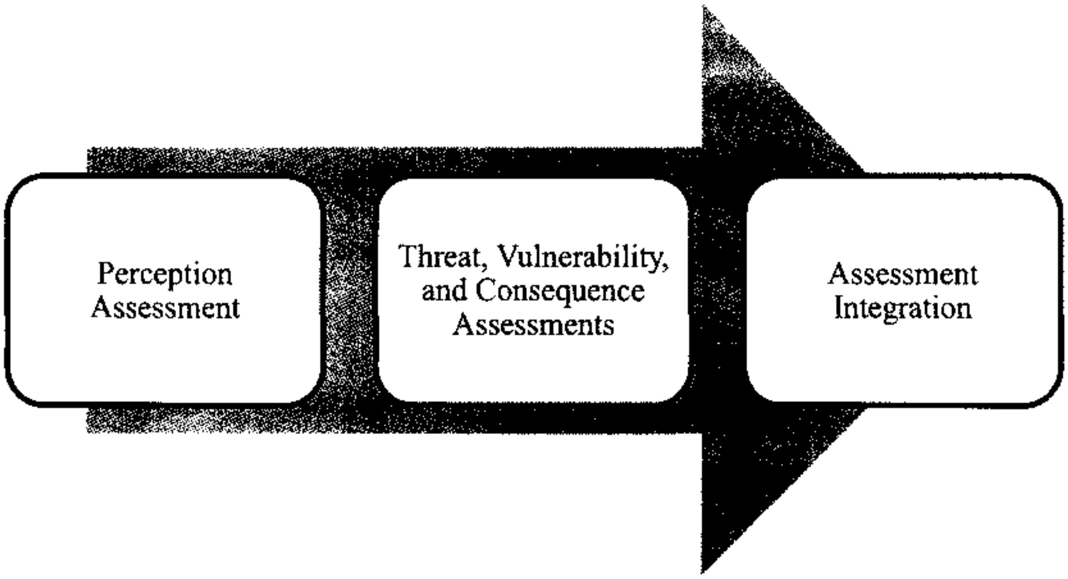


Figure 1.2. Risk Quadruplet Phases ©

The purpose of this research, as shown in Figure 1.3, is three-fold. First, it is necessary to determine how to assess the perceptions of CIKRKA given a risk scenario. We are less concerned with the perception data, itself, or even with which method is considered the best way to collect perception data; rather, we are concerned with integrating perception data, once collected, with threat, vulnerability, and consequence data. It is assumed that data for the threat, vulnerability, consequence, and even perception could be leveraged from previous assessments, collected as part of the research, or simulated, if necessary, in order to demonstrate the viability of the risk quadruplet methodology.

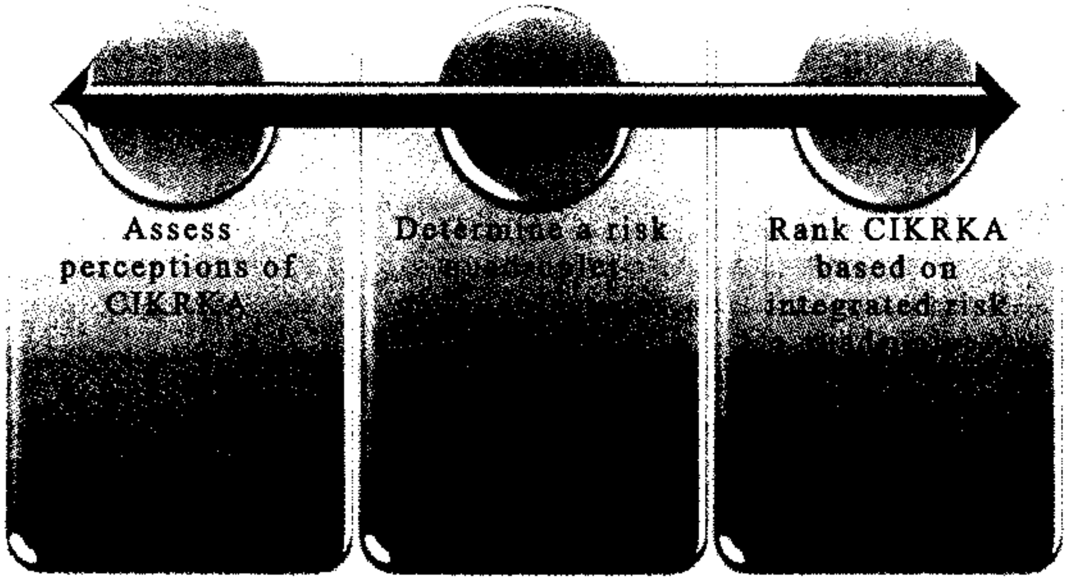

Assess perceptions of CIKRKA
Determine a risk quadruplet
Rank CIKRKA based on integrated risk

Figure 1.3. Research Purpose

Next, an integrated risk quadruplet assessment methodology must be researched. The belief is that the currently accepted homeland security risk triplet (threat, vulnerability, and consequence) is inadequate for characterizing risk to CIKRKA and that a risk quadruplet should be explored to incorporate perception into the current risk assessment approach. But exactly how those components of risk are integrated must be decided. The improved risk assessment integration methodology, based on threat, vulnerability, consequence, and perception assessments, will be developed and presented. This methodology will systematically integrate all four assessments in a meaningful, traceable, and reproducible approach.

The end result will be a ranking of CIKRKA, based on the risk quadruplet methodology. This will allow for a more comprehensive ranking of these disparate entities along multiple risk scales. This ranking system will improve resource allocation for risk mitigation efforts in support of homeland security and homeland defense missions. Figure

1.4 gives a mind map of the different areas covered by this research. It depicts how these seemingly disparate fields are related when exploring risk to CIKRKA. It also reiterates the goal of the research, which is to ultimately integrate threat, vulnerability, consequence, and perception assessments of CIKRKA using systems engineering techniques such as risk analysis and Multi Criteria Decision Analysis (MCDA).

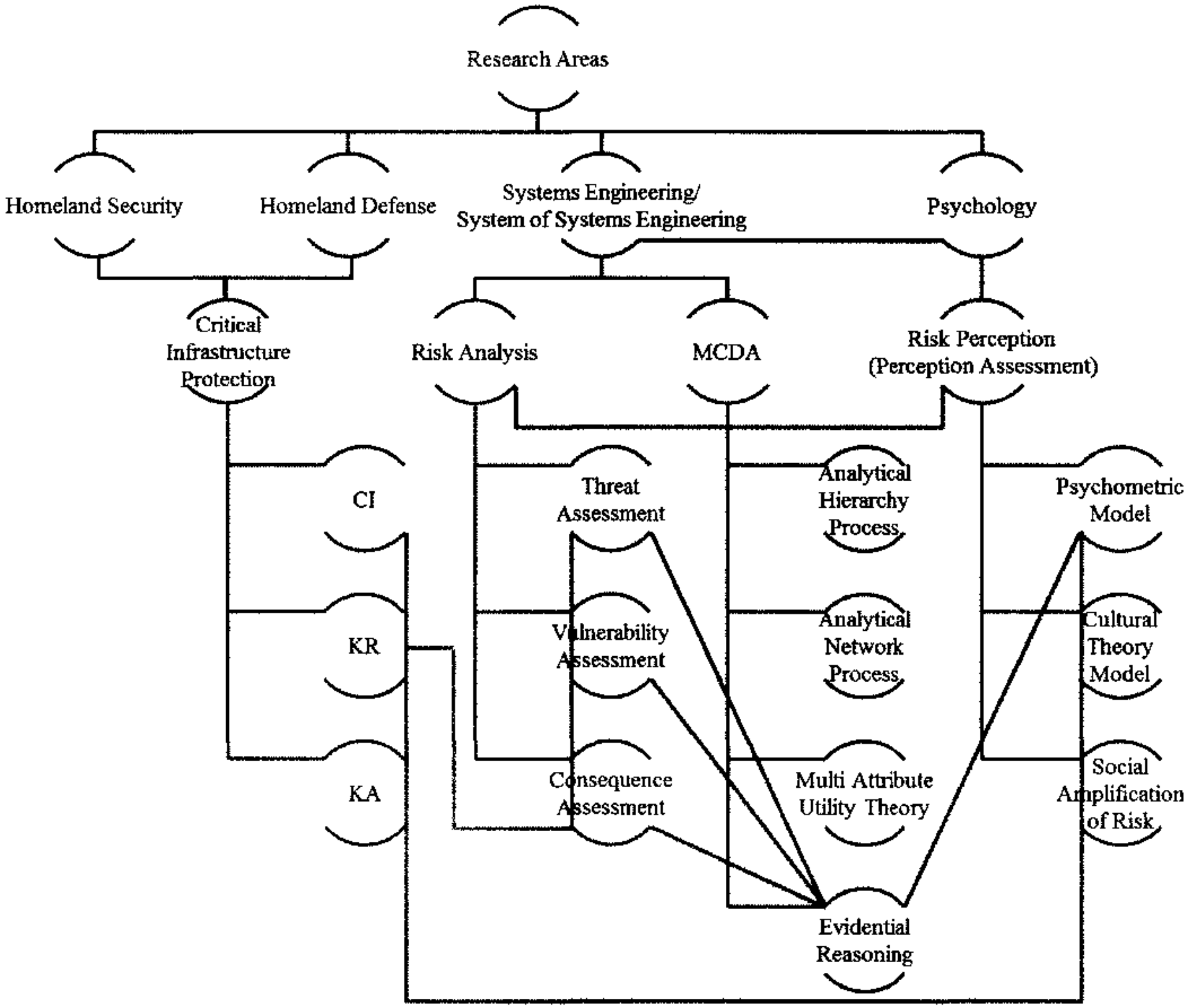
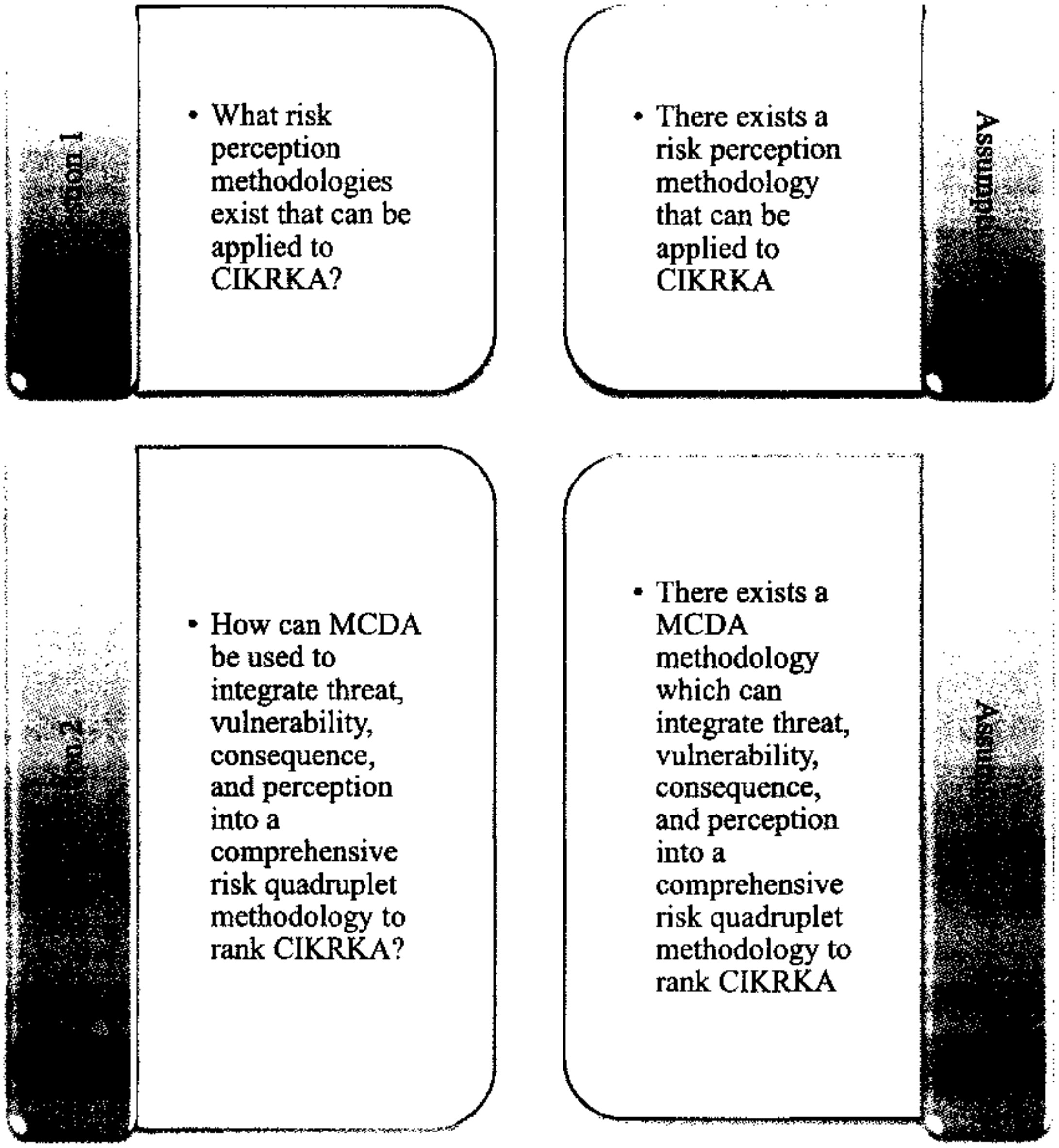


Figure 1.4. Mind Map of Research Areas

1.3 Research Questions and Assumptions

The research will seek to address the two questions presented in Figure 1.5. These questions, and their associated assumptions, are the culmination of an intensive Literature Review (5.4APPENDIX C), which highlighted a number of issues and questions that require resolution in the field of risk analysis for homeland security and homeland defense. There remains confusion about the definitions of CIKRKA. Definitions of threat, vulnerability, and consequence are also inconsistent and do not offer reliable modes of measurement. Perceptions are included haphazardly, often jumbled with threat, vulnerability, and consequence assessments, if they are included at all, which is why the homeland security risk triplet is inadequate. Risk calculation methods can be mathematically misleading and while risk assessments seek objectivity instead of embracing subjectivity, perceptions may contradict risk assessment results. Lastly, the current methodology for integrating threat, vulnerability, and consequence is undefined, leaving analysts to assimilate the results of these disparate assessments indiscriminately, making it impossible to compare assets against each other on the same risk scale.



- What risk perception methodologies exist that can be applied to CIKRKA?

- There exists a risk perception methodology that can be applied to CIKRKA

- How can MCDA be used to integrate threat, vulnerability, consequence, and perception into a comprehensive risk quadruplet methodology to rank CIKRKA?

- There exists a MCDA methodology which can integrate threat, vulnerability, consequence, and perception into a comprehensive risk quadruplet methodology to rank CIKRKA

Figure 1.5. Research Questions and Assumptions

Question 1

What perception methodologies exist that can be applied to CIKRKA? Can a perception model be applied to CIKRKA, and if so, how? Do we only seek perceptions from homeland defense and homeland security experts? Do we include risk experts? Do we include regular citizens since the consequences of threats to CIKRKA could affect them? Can we apply the model to each category separately, using a blocked experimental design?

Does the type of entity at risk (CI, KR, or KA) have an effect on perception? Perception models, such as the Social Amplification of Risk Framework, the Cultural Theory Model, and the Psychometric Model will be explored.

We must assume that a perception methodology exists which can be applied to CIKRKA. Then, assuming that methodology exists and can be exploited to obtain perception data, we would need to integrate that data with data from threat, vulnerability, and consequence assessments. We will explore a number of MCDA approaches to integrate the four components of risk proposed by the risk quadruplet.

Question 2

How can MCDA be used to integrate threat, vulnerability, consequence, and perception into a comprehensive risk quadruplet methodology to rank CIKRKA? Could perception be incorporated into a new risk quadruplet for an improved, overall risk assessment methodology, and if so, how? What is the best way to integrate the results of threat, vulnerability, consequence, and perception assessments? MCDA models, such as Analytic Hierarchy Process (AHP), Analytic Network Process (ANP), Multi Attribute Utility Theory (MAUT), or Evidential Reasoning (ER) will be explored.

What is the output of such a risk assessment approach? An overall risk score, a ranked list of CIKRKA, or both? Could this be applied to items other than CIKRKA? For example, could this approach be used to rank regions or sectors? Could regions or sectors be added as additional criteria in the MCDA model? Or would this methodology only give us a single value for each CI, KR, or KA, in which case how do we integrate those resulting scores across dependent and interdependent CIKRKA. We must assume that the application of this risk quadruplet, which will employ MCDA to integrate threat, vulnerability, consequence, and perception assessments, and would result in a ranked list of CIKRKA which could be used to better inform decision makers about the risks to multiple assets.

1.4 Research Significance

There are two main contributions proposed for this research (Figure 1.6). First, this research will present an MCDA model for integrating assessments of threat, vulnerability, consequence, and perception, incorporating them all into a risk quadruplet assessment approach. Second, this research will produce a methodology for deploying the risk quadruplet model, to include a means for collecting perception data for CIKRKA, and then integrating it with threat, vulnerability, and consequence data.

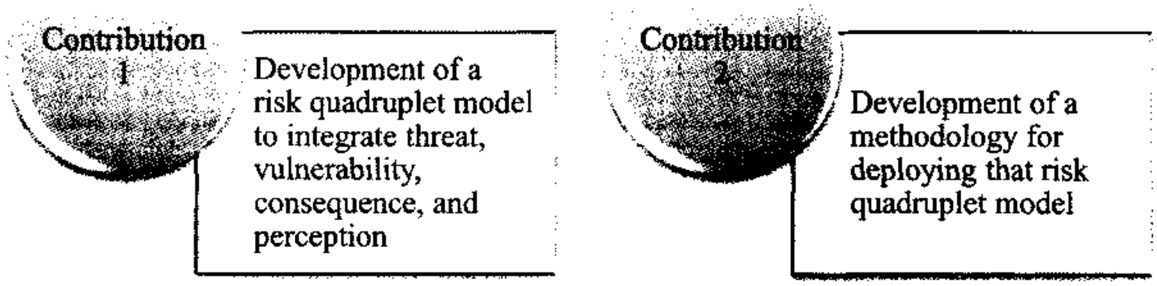

Contribution 1
Development of a risk quadruplet model to integrate threat, vulnerability, consequence, and perception
Contribution 2
Development of a methodology for deploying that risk quadruplet model

Figure 1.6. Research Contributions

1.5 Research Limitations Overview

There are some limitations to this research related to data access or collection, model selections, and technology. A perception assessment model must be selected that will ultimately produce results compatible with the MCDA model selected. Threat, vulnerability, consequence, and perception data will need to be leveraged, collected, or simulated, and again those data must be compatible with the selected MCDA model. And, of course, an MCDA model must be selected from a number of potential options. Finally, the research is at the mercy of the technology available to conduct the assessments, as well as to integrate the assessments during the third phase of the risk quadruplet methodology. All of these limitations are discussed in detail in 5.4APPENDIX B.

In addition to those limitations, there is one additional limitation to be addressed. It would be ideal to validate the risk quadruplet methodology *in vivo* or in the real world, using real data, collected anew, with a full scale model of multiple CIKRKA to compare and rank. However, due to the constraints of scope, cost, and schedule, this type of model verification and validation is beyond the scope of our research. Instead, we intend to explore this model *in vitro*, literally in a petri dish, although in our case, the petri dish is a computer. Given that one of our research contributions is to develop a methodology for deploying the risk quadruplet model, we cannot ignore the in vivo aspect of this research, so we will address data collection methodologies that could be employed in the real world, including surveys and a simplified version of the risk quadruplet model that could be generalized and adapted to more complex problems in the future. Additionally, we will offer a parallel in vitro risk quadruplet methodology viability testing solution (Figure 1.7) that directly corresponds to the in vivo approach. The in vitro approach will rely on simulated data to emulate the real world, a series of risk quadruplet model examples that can be analyzed and compared in order to offer insight into reality, sensitivity analyses, and a preliminary verification and validation of the risk quadruplet model. This will allow us to explore the in vitro risk quadruplet model without risking the exposure of sensitive (in vivo) information that might otherwise jeopardize the very CIKRKA we seek to protect.

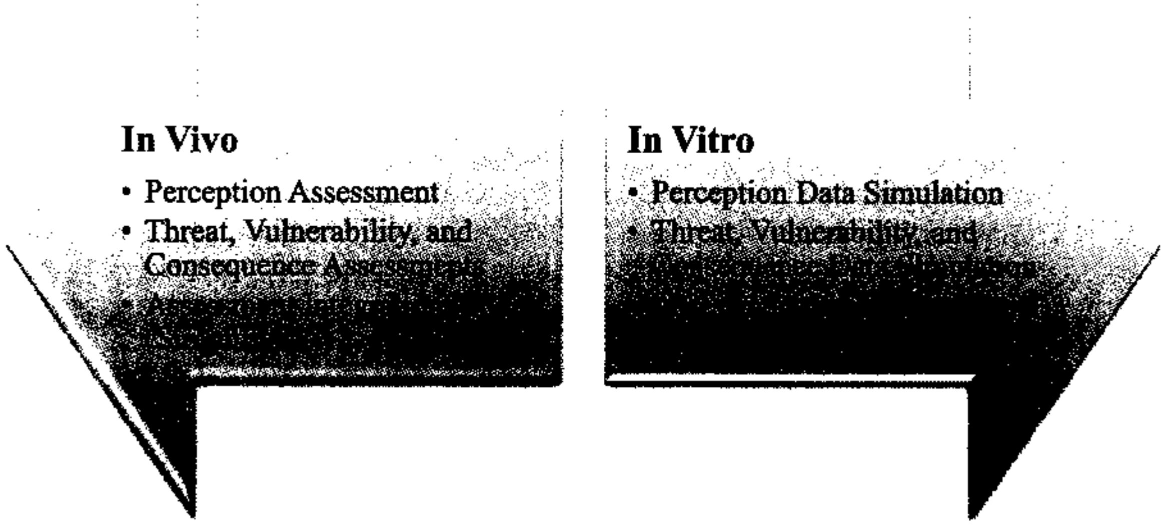

In Vivo
• Perception Assessment
• Threat, Vulnerability, and Consequence Assessment
In Vitro
• Perception Data Simulation
• Threat, Vulnerability, and

Figure 1.7. Risk Quadruplet Viability Testing Options: In Vivo versus In Vitro

The risk quadruplet methodology proposed in CHAPTER 3 (and further described in 5.4APPENDIX D) is the methodology which would be used in vivo. The in vitro solution is also presented in CHAPTER 3 and is crafted to parallel the in vivo methodology. Ideally, future research would verify and validate the risk quadruplet methodology in vivo, based on the lessons learned in vitro. The exploration of research limitations provided in 5.4APPENDIX B is limited to the in vivo application of the model, as the in vitro viability testing does not have the same limitations.

CHAPTER 2

CURRENT STATE ASSESSMENT

"The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning."
– Charles Tremper

We conducted an analysis of four areas of literature related to this research (5.4APPENDIX C). First, we explored national risks, focusing on the evolution of homeland security, the definitions of risk and related terms, and the classification of CIKRKA in the United States (US). Next we explored international risks, specifically an Organisation for Economic Co-operation and Development (OECD) report on risk management for six countries and the annual global risks reports issued by the World Economic Forum (WEF) since 2006. The international perspective also presented a smattering of risk management programs, tools, assessment techniques, as well as visualizations for communicating risk. Delving into Systems Engineering and System of Systems Engineering, we explored whether CIKRKA could be considered systems or system of systems. Finally, we reviewed the risk analysis literature, focusing on risk calculation and risk perception.

We saw problems with risk definitions and calculations when exploring how risk is addressed in a global context. The international community does rely on risk perception for large scale risk assessments, perhaps to a fault, as other threat, vulnerability, and consequence data are likely available. The approach to risk communication is elegant and appears to be more advanced than what we see at the national level. Clear visualizations are used to describe the complex and numerous dimensions associated with risk, which is often described as a function of likelihood and consequence, although sometimes multiple consequence scales were explored (economic versus human loss), and sometimes other risk dimensions were visualized, such as the degree of consensus for the risk or the degree of correlation between risks.

From a national perspective, risk is considered to be a function of threat, vulnerability, and consequence. Numerous government documents exist to describe risk, threat, vulnerability, consequence, perception, and CIKRKA, such as executive orders, presidential decision directives, acts, homeland security presidential directives, as well as national strategies, guidelines, and plans. We analyzed all of these documents, specifically looking at how risk is defined for homeland security. We noted that risk definitions, including threat, vulnerability, consequence, and perception, were inconsistent. Further, the lack of clear definitions complicated the description of risk calculations, making it difficult to know exactly how to go about conducting risk assessments. The definitions of CIKRKA were equally muddled, and the term KA has been abandoned by DHS, although we argue that it should be resurrected as it is a distinct type of asset. Perception was not formally included in the risk assessment process for CIKRKA, even though DHS was criticized for not including diverse perceptions of risk impacts in its approach to risk management.

In reviewing the system and system of systems analysis literature, we acknowledge that a system of systems analysis approach seems both logical and necessary for exploring the dependencies and interdependencies, not only within each CIKR sector, which in and of itself is a system of systems, but also between these CIKR systems, analyzing their vulnerabilities, and planning for their protection as a whole. However, this approach might not be appropriate for KA, which are dependent on CIKR system of systems, but which are not, themselves, typically components of the greater system of systems. In fact, we conclude that further research is necessary to determine whether KA are systems and whether traditional risk assessments as performed on systems should be applied to KA.

After examining the literature for risk analysis, we see that risk is traditionally calculated separately from studies of risk perception. Similar to what we saw in our review of international risks, risk is often calculated as the product of the probability that a risk event will occur (likelihood) and the magnitude of the consequences should the risk event occur. Therefore, the function for risk in homeland security (a triplet of threat, vulnerability, and consequence) is already deviating from the normal approach. Furthermore, an exploration of the calculation used in homeland security reveals some potential mathematical pitfalls. Moving on to risk perception, we note that there have been no attempts to integrate formal perception assessments into the overall risk assessment process. Often, perceptions are incorporated in an ad hoc, haphazard manner, where subject matter expert opinions are elicited for all components of risk (threat, vulnerability, and consequence) or are included alongside quantitative data for threat, vulnerability, and consequence, but the methodology is inconsistent and the parts of the overall risk score attributed to perception versus actual data cannot be extracted. We need a way to systematically incorporate subject matter expertise, or even public opinion, alongside actual data (no matter how limited that data may be). This way, sensitivity analyses can be conducted to determine how much of the overall risk score is being driven by our perceptions, which will aid in the decision-making process, as well as the risk communication process.

All of this research shows a clear gap in the literature that the risk quadruplet will fill. We propose separating perception from threat, vulnerability, and consequence, as its own attribute of risk. We would collect data for threat, vulnerability, and consequence and then integrate that data with data collected from perception assessments. The resulting risk quadruplet will offer a transparent, reproducible, and systematic methodology for integrating perception with threat, vulnerability, and consequence assessment data to improve risk calculation for homeland security, resulting in an overall ranking of CIKRKA.

CHAPTER 3

RESEARCH METHODOLOGY

"People who don't take risks generally make about two big mistakes a year.
People who do take risks generally make about two big mistakes a year."
– Peter F. Drucker

The research methodology consists of a number of steps that relate to the three phases of the risk quadruplet (Figure 1.2), including the selection of the model used to conduct the perception assessment in the first phase, the decision to leverage existing assessment data or conduct new threat, vulnerability, and consequence assessments in the second phase, as well as the selection of the model which will integrate these four assessments in the third, and final, phase. It also covers the research purpose (Figure 1.3), the research questions and assumptions (Figure 1.5), as well as the research contributions (Figure 1.6). It addresses the research limitations, including whether to test the viability of the risk quadruplet in vivo or in vitro (Figure 1.7), and it details the risk quadruplet methodologies for both approaches. Finally, the research methodology addresses the sensitivity analyses along with the preliminary verification and validation of the risk quadruplet model (in vitro). A comprehensive description of the entire risk quadruplet research methodology is given in Figure 3.1.

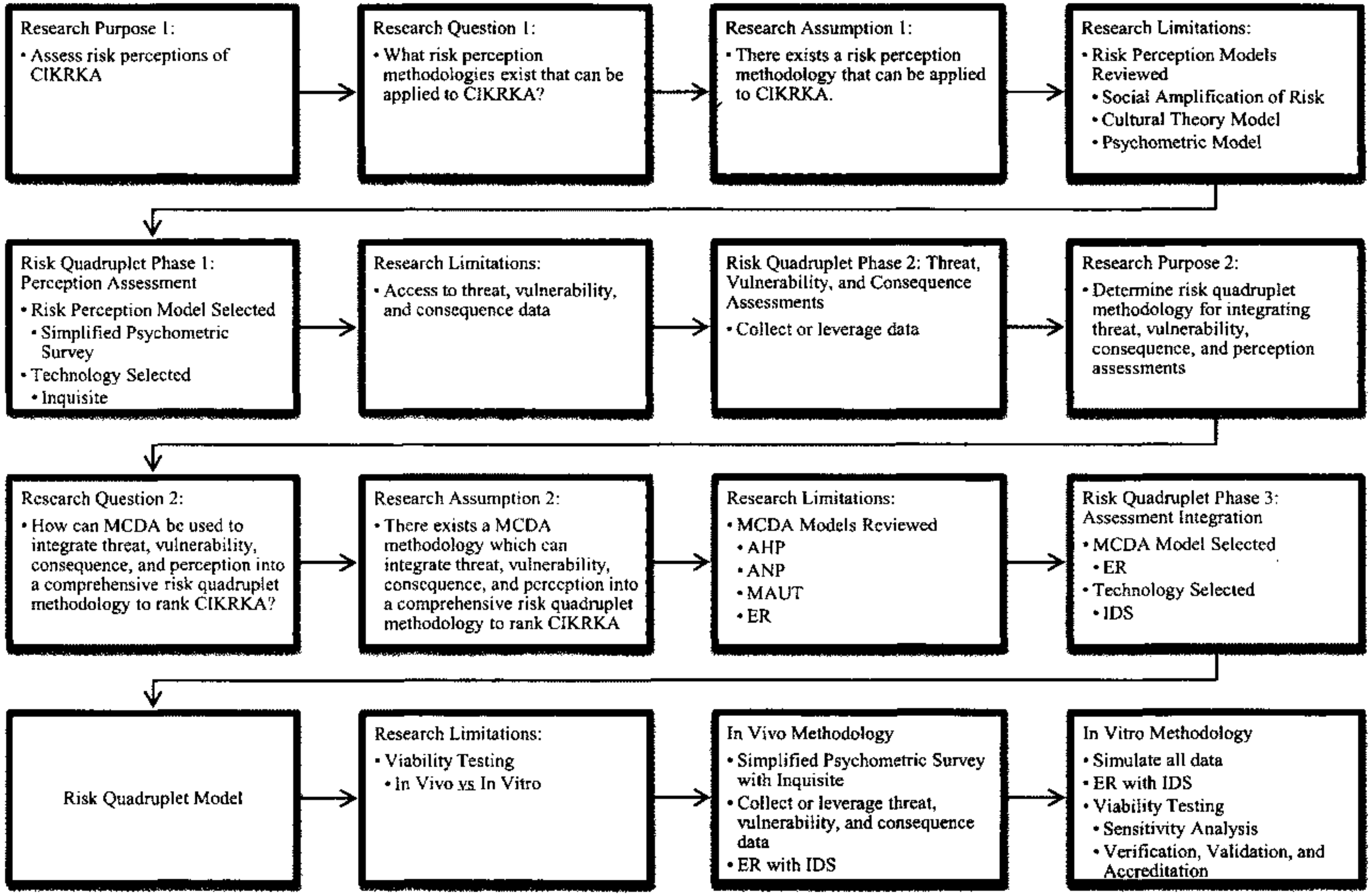

Research Purpose 1:
• Assess risk perceptions of CIKRKA
Research Question 1:
• What risk perception methodologies exist that can be applied to CIKRKA?
Research Assumption 1:
• There exists a risk perception methodology that can be applied to CIKRKA.
Research Limitations:
• Risk Perception Models Reviewed
• Social Amplification of Risk
• Cultural Theory Model
• Psychometric Model
Risk Quadruplet Phase 1: Perception Assessment
• Risk Perception Model Selected
• Simplified Psychometric Survey
• Technology Selected
• Inquisite
Research Limitations:
• Access to threat, vulnerability, and consequence data
Risk Quadruplet Phase 2: Threat, Vulnerability, and Consequence Assessments
• Collect or leverage data
Research Purpose 2:
• Determine risk quadruplet methodology for integrating threat, vulnerability, consequence, and perception assessments
Research Question 2:
• How can MCDA be used to integrate threat, vulnerability, consequence, and perception into a comprehensive risk quadruplet methodology to rank CIKRKA?
Research Assumption 2:
• There exists a MCDA methodology which can integrate threat, vulnerability, consequence, and perception into a comprehensive risk quadruplet methodology to rank CIKRKA
Research Limitations:
• MCDA Models Reviewed
• AHP
• ANP
• MAUT
• ER
Risk Quadruplet Phase 3: Assessment Integration
• MCDA Model Selected
• ER
• Technology Selected
• IDS
Risk Quadruplet Model
Research Limitations:
• Viability Testing
• In Vivo vs In Vitro
In Vivo Methodology
• Simplified Psychometric Survey with Inquisite
• Collect or leverage threat, vulnerability, and consequence data
• ER with IDS
In Vitro Methodology
• Simulate all data
• ER with IDS
• Viability Testing
• Sensitivity Analysis
• Verification, Validation, and Accreditation

Figure 3.1. Research Methodology

The research methodology begins with the first purpose of the research, to assess risk perceptions of CIKRKA. In order to do this, we addressed the first research question, "What risk perception methodologies exist that can be applied to CIKRKA?" and its assumption, that "there exists a risk perception methodology that can be applied to CIKRKA". To address this, we reviewed a number of risk perception models, including the Social Amplification of Risk, the Cultural Theory Model, as well as the Psychometric Model. Details of this review can be found in 5.4APPENDIX B. After reviewing these models, it was decided that the Psychometric Model was best suited to our needs, however, it was recognized that it might need to be adapted as we explored other aspects of the risk quadruplet methodology, such as the model selected for the assessment integration. Thus we had defined the first phase of the risk quadruplet methodology.

The second phase of the risk quadruplet methodology consists of the threat, vulnerability, and consequence assessments. It was assumed that threat, vulnerability, and consequence data could be leveraged from prior assessments, or could be collected in new assessments. Either way, it appeared that the data could easily be fit to the risk quadruplet model. An obvious limitation of the research is acquiring access to this sensitive data. Whether leveraging old assessments or conducting new ones, CIKRKA assets are, by their very definitions, considered important or critical to national operations or morale. Even if permission is granted to collect threat, vulnerability, and consequence data on such assets, that data is likely to be categorized as sensitive information and therefore not publicly available. This is detrimental to research endeavors. Furthermore, conducting multiple assessments, in addition to the perception assessment, would adversely affect the scope and schedule of this research. These research limitations are addressed through alternative risk quadruplet approaches later in the research methodology.

The second purpose of this research is to determine a methodology for integrating threat, vulnerability, consequence, and perception assessments, which directly relates to the third phase of the risk quadruplet (assessment integration). This also directly relates to our second research question and its associated assumption. The second research question is, "how can MCDA be used to integrate threat, vulnerability, consequence, and perception into a comprehensive risk quadruplet methodology to rank CIKRKA?" The second assumption is that "there exists a MCDA methodology which can integrate threat, vulnerability, consequence, and perception into a comprehensive risk quadruplet methodology to rank CIKRKA". We reviewed four MCDA models: AHP, ANP, MAUT, and ER. The best candidate for our purposes was ER. Once we selected the assessment integration model, we realized that the outputs of a traditional Psychometric Model (from the first phase of the risk quadruplet) might not be immediately compatible with our assessment integration model (ER), so we adopted a simplified psychometric survey instead of a full blown Psychometric Model.

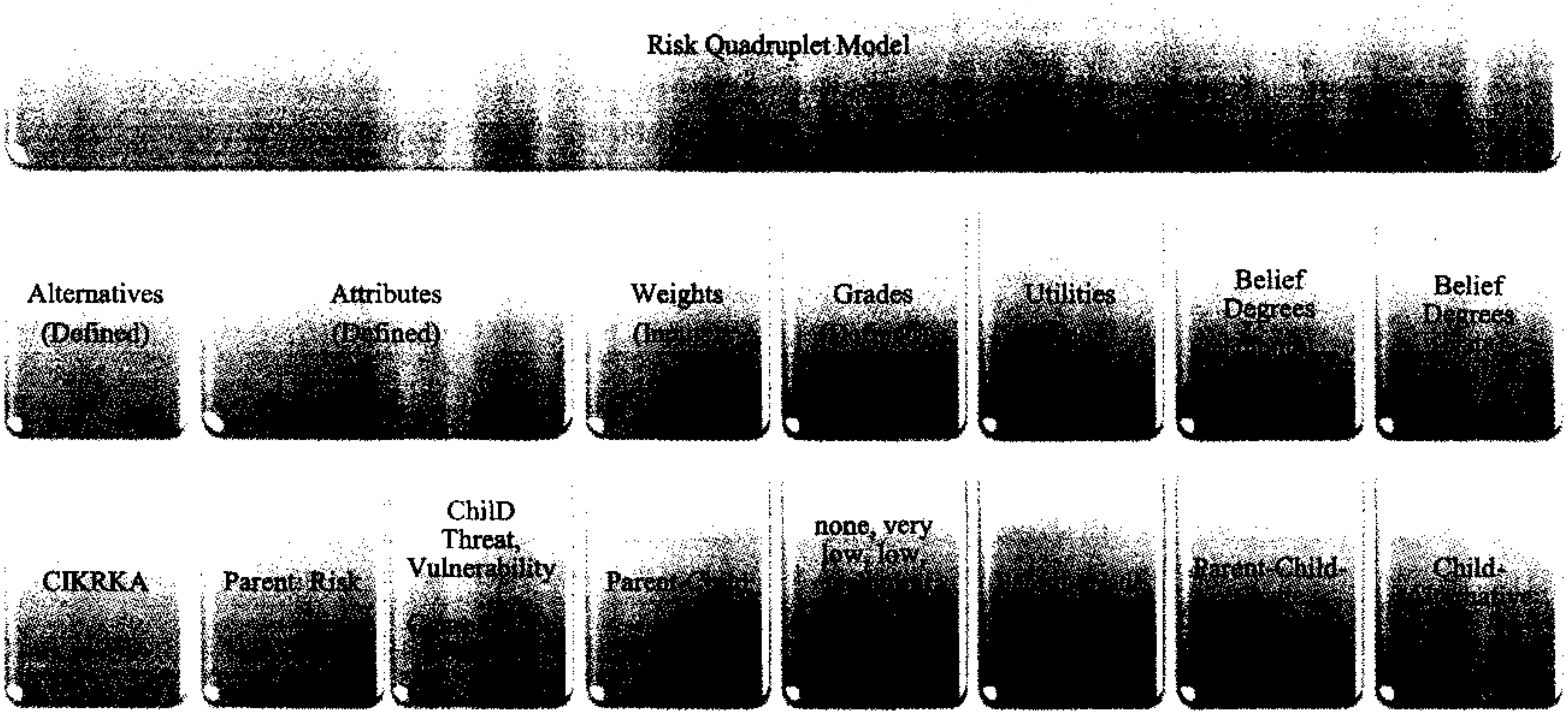


Figure 3.2. Risk Quadruplet Model

The methodology also includes the definition of the risk quadruplet model for our research (Figure 3.2). The risk quadruplet model consists of alternatives, which in our case is a set of CIKRKA assets. Further defining the model, we have a parent attribute denoted as risk (the overall value we are seeking to calculate), as well as child attributes (threat, vulnerability, consequence, and perception), all of which are part of the risk function. We also define grades for the child attributes, as they relate to the alternatives, using a linguistic set (none, very low, low, medium, high, very high). Weights are chosen to relate the child attributes to the parent attribute. Utilities are assigned to relate the grades to the parent attribute. The first set of belief degrees relates grades to the parent and child attributes. In other words, does the linguistic set choice of none for threat, vulnerability, consequence, and perception directly correlate to a linguistic set choice of none for the parent attribute of risk? What about the choice of very low? If so, the belief degrees assigned to relate those relationships would be higher than those relating a grade of none for a child attribute to a grade of high for the parent attribute.

The second set of belief degrees are derived from the assessment data and are used to relate grades to the alternatives within each child attribute. For the perception assessment, the belief degrees are the proportions calculated based on how many respondents selected each of the linguistic set choices. The perception assessment will be discussed later in the research methodology, as will the number and types of respondents providing perception data. For the threat, vulnerability, and consequence assessments, the belief degrees would be translated to the linguistic set if the data was leveraged from historical assessments, or that data could be collected in a new set of assessments using the linguistic set.

With the methodology defined, the next problem was how to test its viability. One option would have been to test it in vivo, but a number of research limitations made that infeasible. Furthermore, we did not want the first test of this methodology to rely on subject matter experts and their risk perception data, along with real threat, vulnerability, and consequence data (all of which, for obvious reasons, could be sensitive). It is more appropriate to test the risk quadruplet in a safe setting first, in vitro, to ensure that the details of the methodology are validated, that the models selected perform as expected, and that the outcome of the entire risk quadruplet produce the desired results (a ranking of CIKRKA assets from most to least risky, as defined in the third purpose of this research). It was decided that an in vivo methodology would be proposed in detail, as if we intended to deploy the risk quadruplet methodology using real data. However, we would actually test the methodology in vitro, which allowed us the freedom to explore more complex versions of the risk quadruplet model.

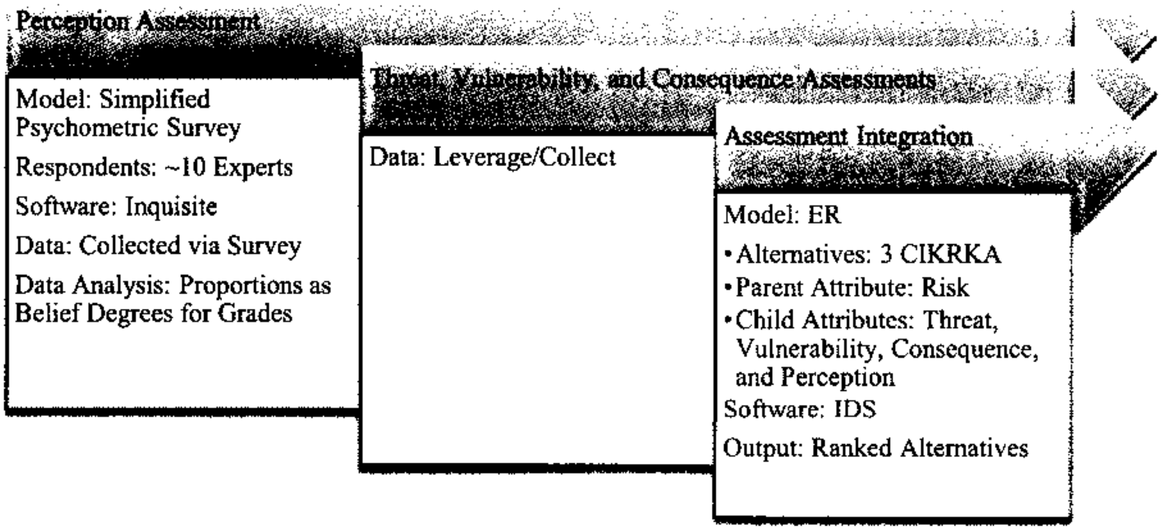

Perception Assessment
Model: Simplified Psychometric Survey
Respondents: ~10 Experts
Software: Inquisite
Data: Collected via Survey
Data Analysis: Proportions as Belief Degrees for Grades
Threat, Vulnerability, and Consequence Assessments
Data: Leverage/Collect
Assessment Integration
Model: ER
•Alternatives: 3 CIKRKA
•Parent Attribute: Risk
•Child Attributes: Threat, Vulnerability, Consequence, and Perception
Software: IDS
Output: Ranked Alternatives

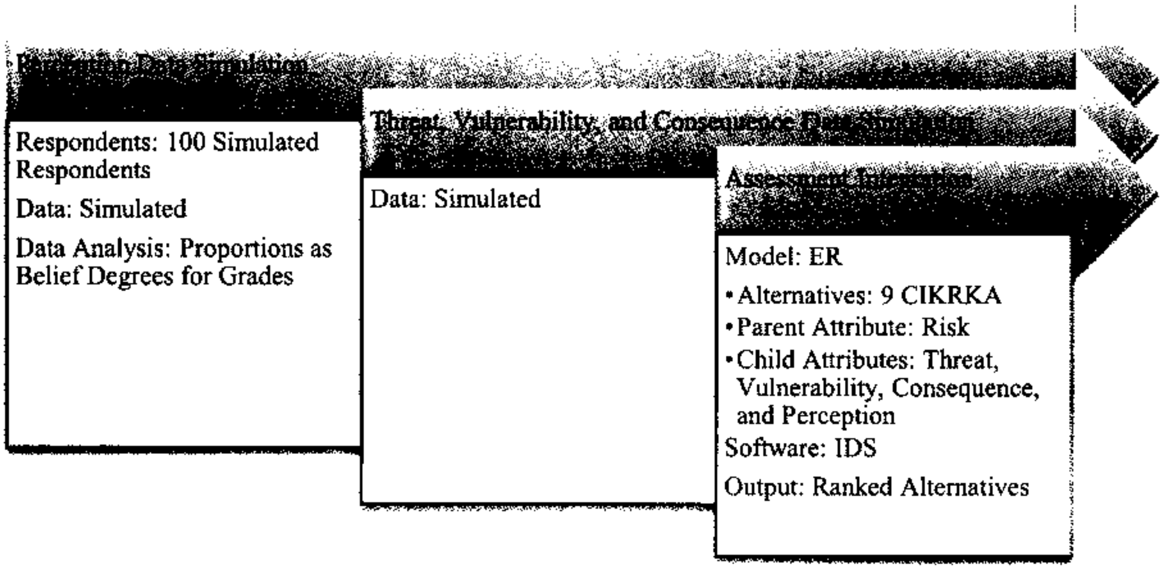
Figure 3.3. Risk Quadruplet Methodology (In Vivo)

The proposed in vivo risk quadruplet methodology (Figure 3.3) consists of the same three phases (assessment of perception; assessments of threat, vulnerability, and consequence; and assessment integration) as previously defined (Figure 1.2). However, we have included additional details on the approach for deploying this methodology. For the first phase, we have already discussed the model selected, a simplified psychometric survey, which we determined would be deployed with a small group of subject matter experts and stakeholders. In order to conduct this survey, we chose Inquisite, a software package capable of deploying surveys online and collecting data. Once we had selected the survey software, we set out to design the questionnaire. This involved a number of steps, such as selecting a region, risk scenario, and a selection of CIKRKA assets to scope the survey. We chose the National Capital Region for our area of focus. We also decided to limit the survey (and thus the overall in vivo model) to three CIKRKA assets, and we chose an example for each of the assets. For the CI we selected The George Washington University Hospital in Washington, DC, for the KR we selected motor gasoline in the state of VA, and for the KA we selected the Lincoln Memorial in Washington, DC. Information on these choices was included in the survey. Additionally, to further scope the survey and model, we selected a single risk scenario, a tornado, for which we provided pertinent data describing likelihood and consequences of that risk scenario in the selected region. We also chose a linguistic set for the survey responses (none, very low, low, medium, high, very high), which would be consistent with the ER model we developed. In order to provide data compatible with our ER model, we knew that we would need to collect the proportion of responses for each of the linguistic set choices for each of the CIKRKA assets, so the final step for this phase of the risk quadruplet model would be to analyze the survey results and determine those proportions.

The proposed in vivo methodology continues with the second phase, where it is assumed that the data for threat, vulnerability, and consequence could be leveraged from previous assessments, or that those assessments could be conducted. The goal of the risk quadruplet is not to determine how to conduct these assessments, as they are already being conducted and many approaches already exist for doing so. Rather, the point of the risk quadruplet is to determine how to integrate these assessments with the perception assessment we proposed for the first phase of the methodology.

Therefore, the final phase of the in vivo risk quadruplet methodology focuses on integrating these assessments. The ER model is defined with the three alternatives (CIKRKA assets) used in the Inquisite survey. The parent attribute and child attributes, weights, utilities, and belief degrees are also defined. And the final belief degrees would be input into the model based on the data collected from the perception, threat, vulnerability, and consequence assessments.

Finally, IDS was the software selected for implementing the ER model, so the alternatives, attributes, weights, utilities, and belief degrees would be input into IDS for analysis. With the choices for all three phases of the research defined, we have developed the in vivo risk quadruplet methodology which combines a simplified psychometric survey to collect perception data, leveraged or collected threat, vulnerability, and consequence data, along with an ER model to integrate all four assessments together.



Perception Data Simulation

Respondents: 100 Simulated Respondents

Data: Simulated

Data Analysis: Proportions as Belief Degrees for Grades

Threat, Vulnerability, and Consequence Data Simulation

Data: Simulated

Assessment Integration

Model: ER

- Alternatives: 9 CIKRKA
- Parent Attribute: Risk
- Child Attributes: Threat, Vulnerability, Consequence, and Perception

Software: IDS

Output: Ranked Alternatives

Figure 3.4. Risk Quadruplet Methodology (In Vitro)

The in vitro risk quadruplet methodology (Figure 3.4) consists of the same three phases as the in vivo risk quadruplet methodology; however, there are some obvious differences. For the first phase of the in vitro approach, we simulated the perception assessment data using 100 simulated respondents. We chose the triangular distribution to simulate this information as we were looking for a range of possible linguistic set choices across multiple respondents. From this data, we were able to determine the number of responses for each of the linguistic set choices for each CIKRKA asset to be used in the assessment integration phase. Rather than rely on leveraging or collecting data for threat, vulnerability, and consequence data in the second phase, we simulated this data, as well. We used the uniform distribution for this data simulation, as we are not seeking to simulate more than one response for each of the linguistic set choices for this data, we just need one choice for each asset as these assessments would only be conducted once in the real world. For example, we would not expect to conduct multiple threat assessments for each CIKRKA asset. Lastly, the assessment integration phase remains fairly similar to the in vivo approach. However, since we are not constrained to the limits of the survey respondents, we increase the number of alternatives to nine hypothetical assets (three CI, three KR, and three KA). The attributes remain the same, as do the grades, weights, utilities, and parent-child belief degrees. The belief degrees relating the alternatives to the child attributes are input based on the simulated data from the first two phases (the proportions calculated from the simulated respondents for the perception data and the simulated data for the threat, vulnerability, and consequence data). The same software, IDS, would be used to analyze the results.

The resulting analysis from both the in vivo methodology, as well as the in vitro viability testing, would provide a ranked output of CIKRKA assets (alternatives) based on their parent attribute scores (risk), which, incidentally, is the third purpose of this research. The first contribution defined for this research was to develop a risk quadruplet model to integrate threat, vulnerability, consequence, and perception assessments, and this model was, indeed, developed, and further tested in vitro. The second contribution of this research was to develop a methodology for deploying the risk quadruplet model, and we have crafted an in vivo methodology which could be used as is, or easily adapted, to deploy the risk quadruplet model. While the methodology was not actually deployed, aspects of the methodology along with the model, itself, were tested successfully in vitro .Sensitivity analyses and preliminary verification and validation of the risk quadruplet model demonstrates the viability of the risk quadruplet methodology.

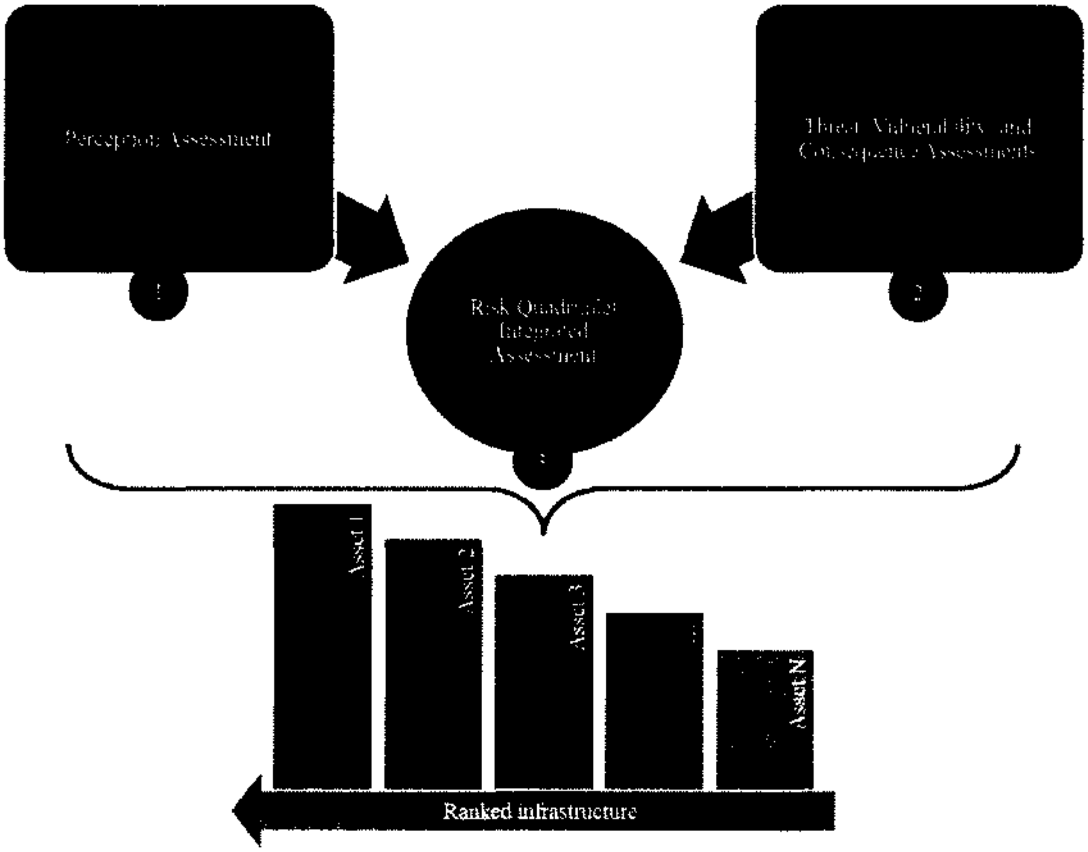

Perception Assessment
Threat, Vulnerability, and Consequence Assessments
1
2
Risk Quadruplet Integrated Assessment
3
Asset 1
Asset 2
Asset 3
...
Asset N
Ranked infrastructure

Figure 3.5. Risk Quadruplet Methodology

The generalized risk quadruplet methodology (whether in vivo or in vitro) is given in Figure 3.5. Further information on the perception and MCDA model selections, as well as the software selections, and research limitations can be found in 5.4APPENDIX B. The details of the in vivo methodology can be found in 5.4APPENDIX D. A text version of the Inquisite survey can be found in 5.4APPENDIX E and an Informed Consent Document, which would be provided to respondents participating in the survey, can be found in

5.4APPENDIX F. The details of the in vitro data simulation can be found in 5.4APPENDIX G. Lastly, the details and results of the in vitro viability testing, along with sensitivity analyses and a preliminary verification and validation of the risk quadruplet model, can be found in CHAPTER 4.

CHAPTER 4

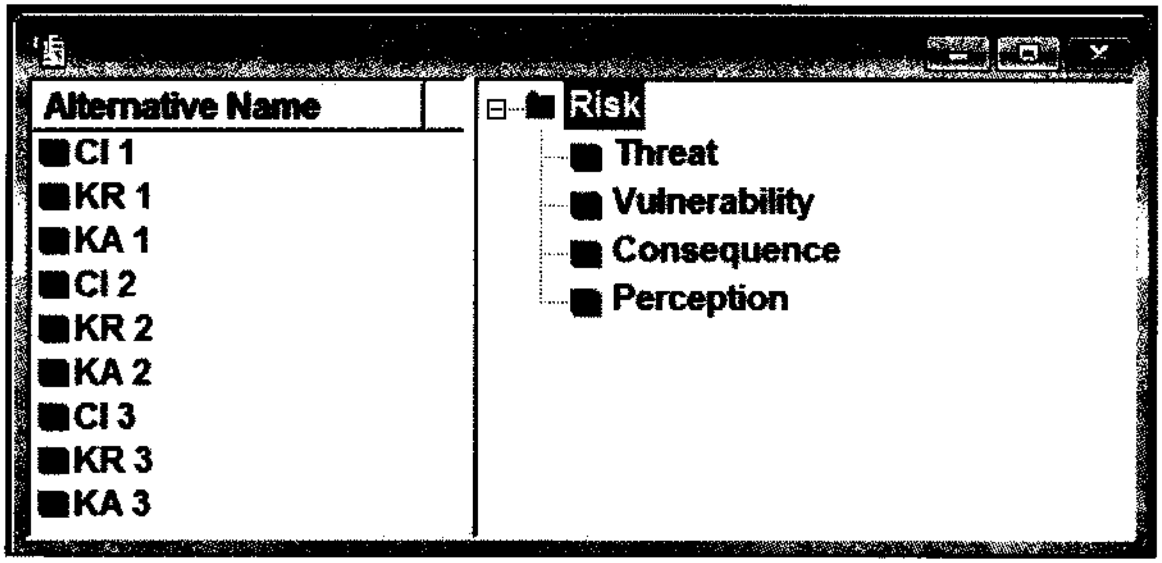
RISK QUADRUPLET VIABILITY TESTING (IN VITRO)

"If we don't succeed, we run the risk of failure."
– Dan Quayle

The goals of this research are to assess perceptions of CIKRKA, determine a methodology for integrating threat, vulnerability, and consequence assessments with a CIKRKA perception assessment, and to ultimately rank those CIKRKA accordingly. The in vitro approach for testing the viability of the risk quadruplet methodology relies on simulated data. However, this research is still informative and allows us to explore how the model behaves prior to an in vivo deployment of the methodology. Even the way in which we simulate the data can be done to mimic our in vivo methodology. For example, the perception data is simulated as if 100 respondents were surveyed, a sample size that would not have been easily achievable during this research. Furthermore, we increase the complexity of the model by introducing additional CIKRKA assets (alternatives), which would have made the in vivo perception data collection much more tedious. Figure 3.4 shows how the risk quadruplet methodology differs only slightly during the in vitro viability testing when compared to Figure 3.3 which shows our in vivo risk quadruplet methodology.

With IDS we are able to build an ER model for the risk quadruplet using a combination of collected perception data and simulated threat, vulnerability, and consequence data. A model was described in IDS, consisting of nine alternatives (CIKRKA), and four child attributes (threat, vulnerability, consequence, and perception) nested under an overall parent attribute (risk). The model also uses weighting (to determine the contribution of the child attributes to the parent attribute), utilities (to determine the relationship between the grades and the child attributes), and two sets of belief degrees (one to relate the grades of child and parent attributes, the other to determine the beliefs held for the grades selected within each child attribute for each alternative).

It is important to note that while this model is relatively simple, it is extensible and could easily handle additional layers of complexity from an increase in the number of alternatives under study, to a more complex description of the parent and child attributes (perhaps breaking the perception attribute into two sub-categories for public versus private risk perception assessments). However, as Albert Einstein is famous for saying, "Everything should be as simple as possible, but not simpler." His opinion is echoed in the world of modeling, as well, when Vamanu claims that "model complexity does not necessarily [...] contribute to model quality," (Vamanu, Gheorghe, Acasandrei, & Vamanu, 2011). The beauty of ER, and the IDS software for implementing ER, is its simple structure, which can be organized into countless combinations of attributes and alternatives making it easy to implement, but capable of handling complex problems without overcomplicating them.



Alternative Name

- CI 1
- KR 1
- KA 1
- CI 2
- KR 2
- KA 2
- CI 3
- KR 3
- KA 3

Risk

- Threat
- Vulnerability
- Consequence
- Perception

Figure 4.1. Risk Quadruplet Model (In Vitro)

An example of how this model appears in IDS is shown in Figure 4.1. In the IDS model display window, users can opt to select **View > Dialog Box View** to see a more visual version of the model (Figure 4.2). Each alternative is shown in yellow and has three boxes for displaying the alternative name at the top, its ranking in the bottom left, and its attribute score in the bottom right (depending on which attribute was selected at the time; in this case the parent attribute of risk was selected). Each attribute is shown in blue and also includes three boxes for displaying the attribute name at the top, its weight in the bottom left, and its average score in the bottom right.

Figure 4.2. Dialog Box View

Each of the attributes (threat, vulnerability, consequence, and perception) were defined in IDS as qualitative, so as to grade them using the same linguistic scale. Future research would be necessary to decide whether to define any of the attributes as quantitative, but ER can integrate both qualitative and quantitative data, and IDS provides that option when defining attributes. For example, if the attribute is defined as quantitative, then the user can also decide whether it is a certain or uncertain attribute. This is useful for defining stochastic quantitative attributes, which could be random variables with some underlying distribution, may be difficult to assess, or could suffer from missing data ("IDS Multicriteria Assessor Quick Guide," 2010).

Utilities for the overall or parent attribute (risk) were assigned to these grades (from our linguistic set of none, very low, low, medium, high, and very high) as shown in Table 4.1. The utilities were chosen arbitrarily, but it may be worth exploring, during future research, how to assess and incorporate the utilities of those providing inputs for the ER model. These values could easily be revised in future iterations of the model. For our purposes, a risk grade of none would be ideal and thus would receive a Utility of 1. The remaining grades were ranked accordingly. Utilities, unlike probabilities, need not sum to 1.

Table 4.1. Grades and Utilities

[illegible]	[illegible]
None	1
Very Low	.9
Low	.7
Medium	.5
High	.3
Very High	.1

To relate parent and child attributes, the following belief degrees were used for each child (threat, vulnerability, consequence, and perception). These values could also be adjusted easily in future iterations of the model. For example, if the child grade of threat is very low, that could relate to a parent grade of none, very low, and low risk with belief degrees of .25, .50, and .25, respectively. However, in the interest of keeping this model simple, belief degrees were assigned using the identity matrix (Table 4.2). These belief degrees that relate the parent and child grades are not the same belief degrees that are selected by respondents during data collection when they chose the grade they deem appropriate for a given combination of alternative and attribute.

Table 4.2. Belief Degrees for Relating Parent and Child Grades

[illegible]	[illegible]	[illegible]	[illegible]	Medium	[illegible]	[illegible]
[illegible]	1	0	0	0	0	0
[illegible]	0	1	0	0	0	0
[illegible]	0	0	1	0	0	0
[illegible]	0	0	0	1	0	0
[illegible]	0	0	0	0	1	0
[illegible]	0	0	0	0	0	1

Weights are then used to relate the child attributes to the parent attribute. This can be done using visual scoring or using a pairwise comparison of attributes. Again, future versions of the model could work with respondents or subject matter experts to complete the pairwise comparison approach provided with the IDS software, which is basically an AHP approach for weighting the child attributes. For the in vitro viability testing, we used the visual scoring approach, selected **normalized** to ensure the weights added to 1, and while the weights initially started as equal (.25, .25, .25, and .25), it was realized that perception might not be considered equally important as the other attributes by stakeholders. Therefore, we will explore a version of the model for which the perception attribute weight was set to be approximately half as important as the other attributes (where the other attributes were weighted equally) as shown in Figure 4.3. Other versions of the model will be explored during the Sensitivity Analysis.

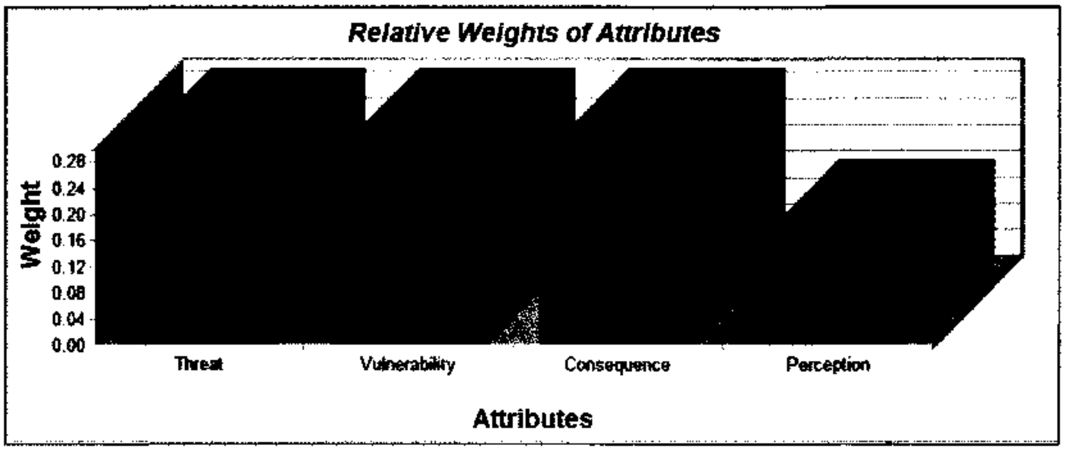


Figure 4.3. Attribute Weights Using Visual Scoring (Low Perception)

The details of the simulations used to create perception, threat, vulnerability, and consequence data are provided in 5.4APPENDIX G. The following perception data set was the result of the perception assessment simulation (Table 4.3). The simulated data for threat, vulnerability, and consequence is provided in Table 4.4. This data was input into IDS using the data input dialog box (Figure D.8).

Table 4.3. Perception Grades and Belief Degrees

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	0.01	0.04	0.10	0.10	0.05	0.05	0.01	0.06	0.29
[redacted]	0.06	0.20	0.33	0.41	0.35	0.06	0.14	0.37	0.28
[redacted]	0.20	0.38	0.31	0.20	0.25	0.21	0.20	0.25	0.20
[redacted]	0.32	0.25	0.18	0.13	0.21	0.27	0.40	0.19	0.17
[redacted]	0.37	0.11	0.07	0.14	0.14	0.38	0.24	0.11	0.05
[redacted]	0.04	0.02	0.01	0.02	0.00	0.03	0.01	0.02	0.01

Table 4.4. Threat, Vulnerability, and Consequence Grades and Belief Degrees

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	0.22	0.08	0.29	0.27	0.23	0.07	0.29	0.13	0.12
[redacted]	0.33	0.12	0.26	0.15	0.26	0.01	0.10	0.15	0.04
[redacted]	0.06	0.24	0.09	0.01	0.09	0.22	0.15	0.25	0.23
[redacted]	0.11	0.20	0.22	0.17	0.23	0.12	0.25	0.21	0.23
[redacted]	0.20	0.22	0.13	0.20	0.00	0.53	0.21	0.23	0.22
[redacted]	0.08	0.14	0.01	0.20	0.19	0.05	0.00	0.03	0.16
[redacted]	0.08	0.05	0.25	0.30	0.15	0.25	0.13	0.19	0.04
[redacted]	0.34	0.21	0.14	0.03	0.17	0.25	0.02	0.25	0.25
[redacted]	0.33	0.22	0.10	0.08	0.04	0.01	0.32	0.21	0.05
[redacted]	0.16	0.06	0.22	0.10	0.30	0.08	0.28	0.01	0.19
[redacted]	0.05	0.16	0.19	0.21	0.15	0.14	0.21	0.02	0.23
[redacted]	0.04	0.30	0.10	0.28	0.19	0.27	0.04	0.32	0.24
[redacted]	0.13	0.28	0.22	0.11	0.20	0.26	0.03	0.23	0.33
[redacted]	0.15	0.05	0.28	0.20	0.08	0.26	0.32	0.19	0.15
[redacted]	0.14	0.15	0.08	0.02	0.18	0.11	0.09	0.00	0.14
[redacted]	0.30	0.15	0.15	0.29	0.16	0.18	0.00	0.34	0.24
[redacted]	0.12	0.09	0.10	0.30	0.21	0.15	0.33	0.20	0.06
[redacted]	0.16	0.28	0.17	0.08	0.17	0.04	0.23	0.04	0.08

Using the simulated data for threat, vulnerability, consequence, and perception, the IDS model can now rank the nine alternatives (CIKRKA) based on the attributes, grades, and associated utilities, belief degrees, and weights. The user can select **Report > Graph**

Ranking within IDS to obtain the overall ranking of alternatives on risk, the parent attribute (Figure 4.4). The user can also select **Report > Visual Comparison** to see further breakdowns of the nine alternatives across the four attributes (Figure 4.10). Figure 4.5 shows a comparison of the nine CIKRKA alternatives based on their respective overall risk scores. But Figure 4.8 shows this comparison broken down by the attributes of risk (threat, vulnerability, consequence, and perception).

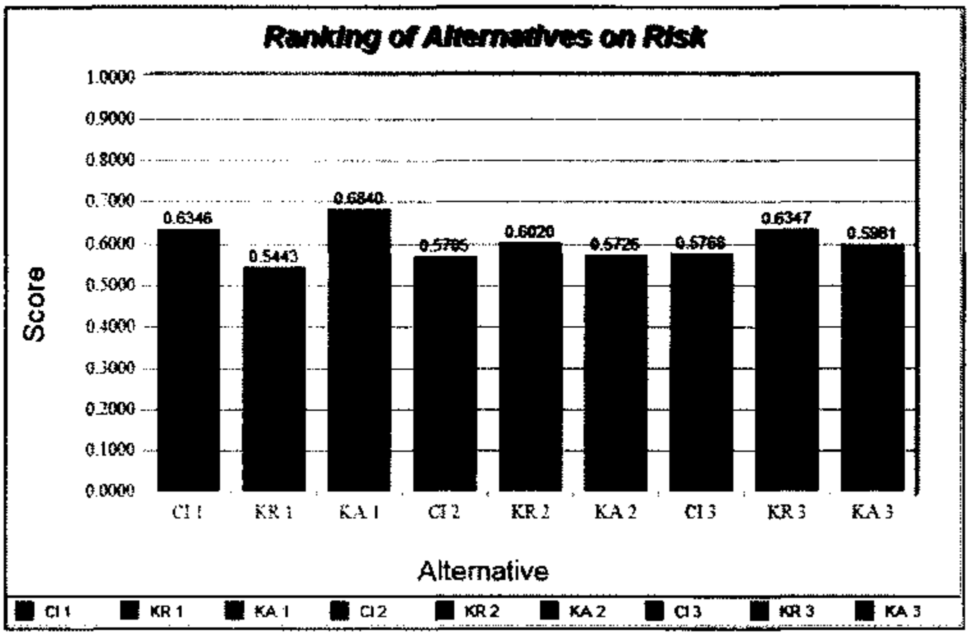


Figure 4.4. Ranking of Alternatives on Risk Attribute (Low Perception)

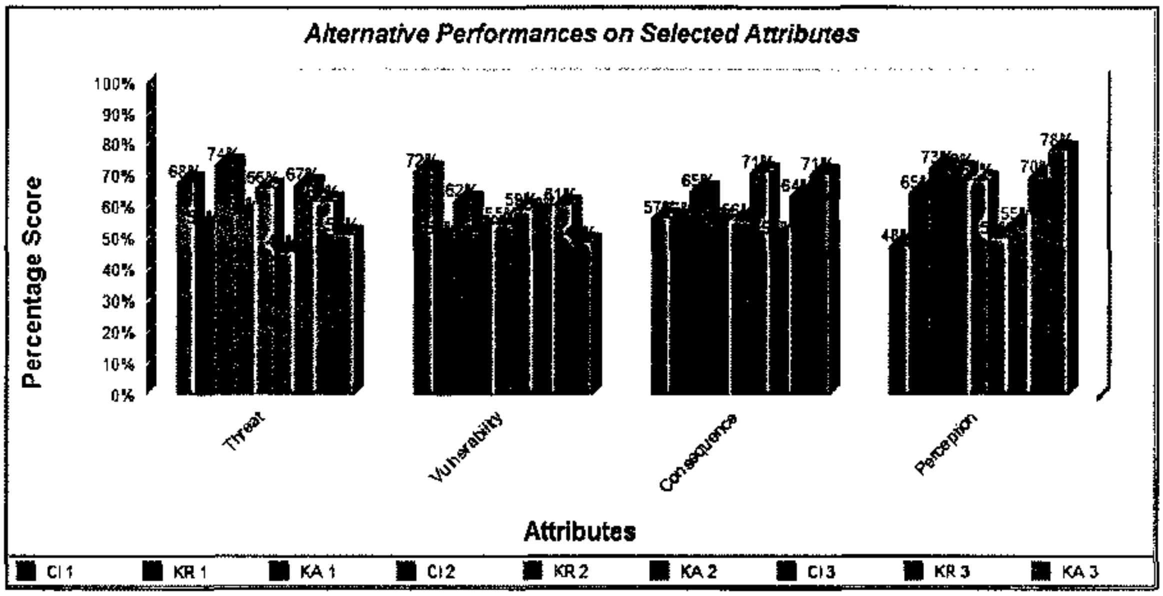


Figure 4.5. Alternative Performances Across Child Attributes (Low Perception)

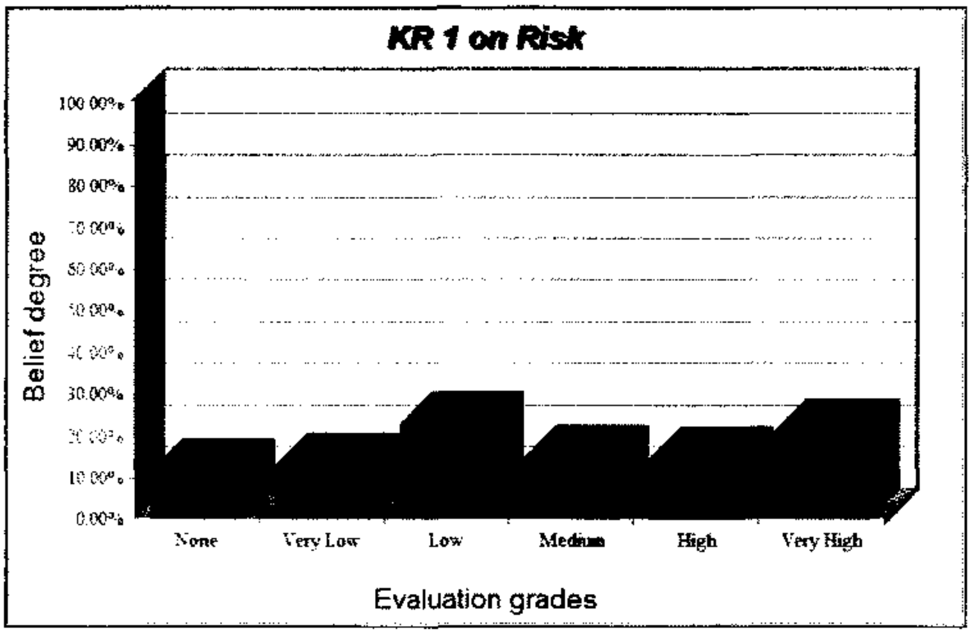


Figure 4.6. KR 1 Grades for Risk Attribute (Low Perception)

Figure 4.6 can be obtained by highlighting the alternative of interest, then selecting **Report > Graph Belief Degree > Att at Alt,** where the last selection means, "Attribute at Alternative", so whichever combination of attribute and alternative are highlighted at the time this report is run, that is the combination that will be used to create the chart. This charts show the breakdown of grades for KR 1 (with the lowest overall risk in the model for which perception was weighted lower than the other attributes) at the parent attribute level (risk). This gives an overall distribution of the calculated grades and belief degrees for risk, based on the grades and belief degrees for the child attributes (threat, vulnerability, consequence, and perception). Similar charts can also be created to explore the belief degrees input by respondents on the individual child attributes.

Another interesting chart that is available in IDS is the radar plot. By plotting the values of all of the child attributes, alongside the parent attribute, it is easy to see which of the child attributes might be driving the overall risk score. In IDS, users can select **Report > Visual Comparison**, then select the **Tool Bar** button to obtain a menu of options. One of the options is an icon displaying the type of chart selected, and by clicking on it, users see a drop-down list of chart types, including the radar plot. The default view of this chart is three-dimensional, however, clicking the icon that looks like a set of three-dimensional glasses will recalibrate the view to two dimensions. Because we are exploring nine alternatives, it may be difficult to compare them all on the same radar plot. However, by highlighting alternatives and using the **Select One**, **Select Group**, **Select All**, **Deselect**, and **Draw** buttons we are able to explore alternatives individually (Figure 4.7). We can see, for example, that consequence shows some influence on KA 1, while perception affects KR 2 for the low perception model. Even though this data is simulated, it is still interesting to explore the results as it is obvious how they could be invaluable to the in vivo risk quadruplet methodology.

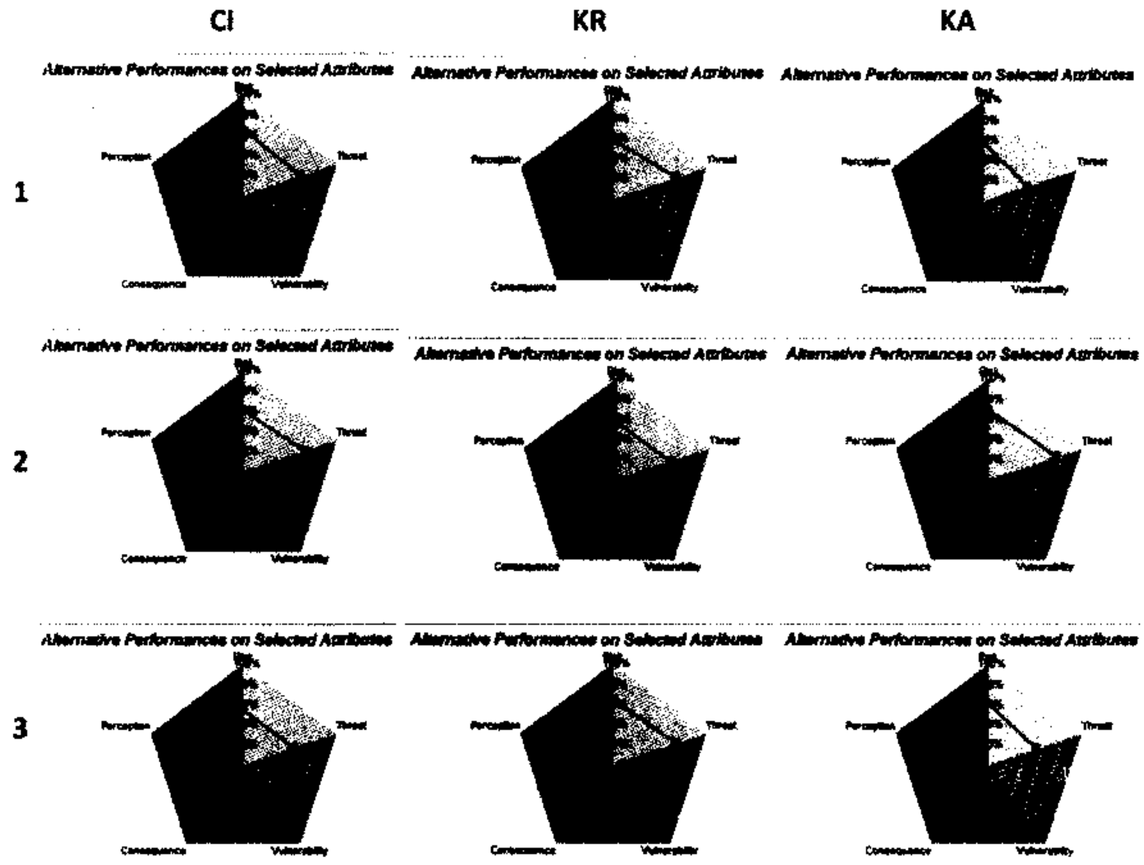


Figure 4.7. Risk and Attributes Radar Plots by Alternative (Low Perception)

4.1 Sensitivity Analysis

Incidentally, two other versions of the IDS model were created which were identical to the low perception risk quadruplet model. One version of the model set the perception attribute weight to be approximately twice as important as the other attributes (where the other attributes were weighted equally) as shown in Figure 4.8. Another version removed the perception attribute completely. These alternate models were used strictly for comparative purposes.

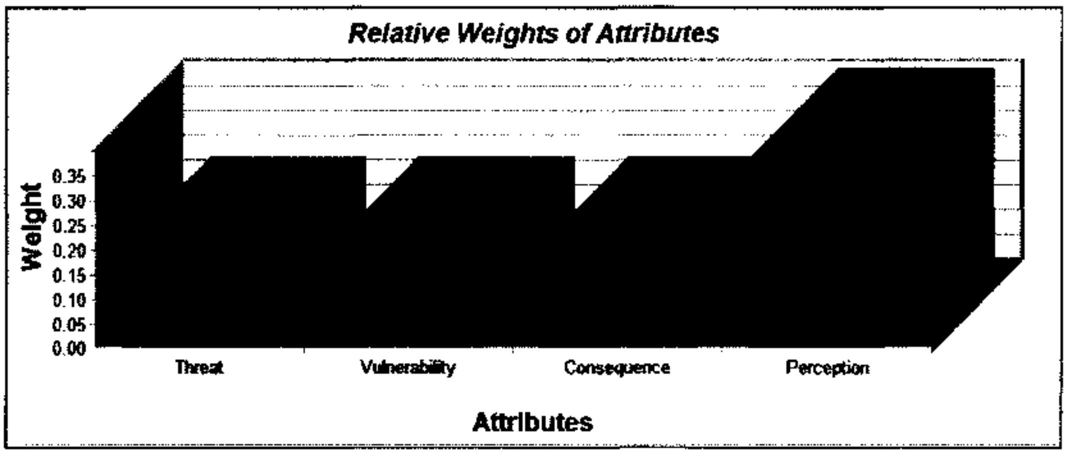


Figure 4.8. Attribute Weights Using Visual Scoring (High Perception)

Recalling our low perception model (Figure 4.4), we can now compare it to our high perception model (Figure 4.9). We see a comparison of the nine CIKRKA alternatives based on their respective overall risk scores. The model for which perception received a lower weight and the model for which perception received a higher weight are essentially identical, aside from the weights of the attributes. The simulated belief degrees input across the threat, vulnerability, consequence, and perception attributes for each of the nine CIKRKA alternatives remain the same. Therefore these breakdown charts are identical for each model.

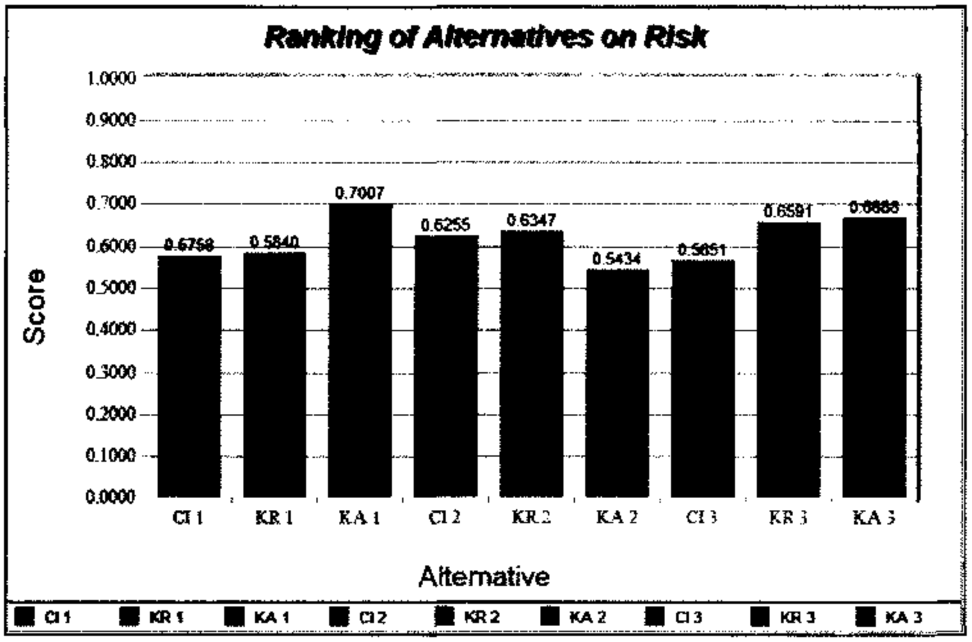


Figure 4.9. Ranking of Alternatives on Risk Attribute (High Perception)

Figure 4.5 (low perception model) and Figure 4.10 (high perception model) show the nine CIKRKA alternatives broken down by the attributes of risk (threat, vulnerability, consequence, and perception). For example, in the high perception model, we see that threat was assessed highest for KA 1, vulnerability was assessed highest for CI 1, consequence was assessed highest for both KA 2 and KA 3, and perception was assessed highest for KA 3. Comparing the two models, we see that in the low perception model, KA 3 did not receive the highest overall risk score even though it was assessed highest for both consequence and perception; it was ranked 4th. However, in the high perception model, KA 3 moved up in the ranking to 2nd.

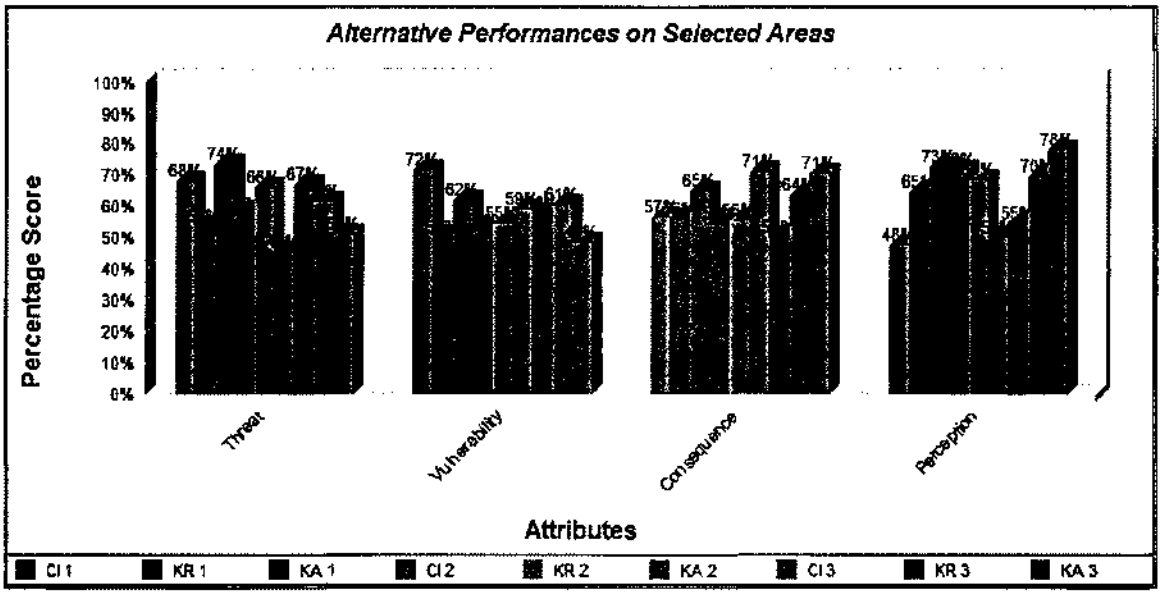


Figure 4.10. Alternative Performances Across Child Attributes (High Perception)

In Table 4.5 we see the threat, vulnerability, consequence, and perception attribute scores for each of the nine CIKRKA alternatives. These child scores remain the same across all versions of the model because they are based on the simulated belief degrees input into the model, which are then related to the parent attribute of risk through the selected belief degrees (based on the identity matrix) and the utilities provided (Table 4.1and Table 4.2). The highlighted values show the assets which received the highest child attribute score. So KA 1 received the highest threat score, CI 1 received the highest vulnerability score, and KA 2 and KA 3 jointly received the highest consequence score, whereas KA 3 received the highest perception score.

In the full risk quadruplet model for which the perception attribute was weighted lower than the other attributes, the overall risk score for CI 1 was 63%. When perception is weighted higher than the other attributes, the overall risk score for CI 1 was 58%. But when perception is removed from the model completely, the overall risk score for CI 1 increases to 66%. Table 4.5 shows the overall risk scores for the reduced model and when compared to the risk quadruplet model (whether perception was weighted low or high compared to the other attributes) all of the CIKRKA alternatives were impacted by the removal of the perception attribute.

Table 4.5. Risk Quadruplet Model Output Comparison

68%	54%	74%	58%	66%	46%	67%	62%	51%
[illegible]	50%	62%	52%	55%	59%	58%	61%	49%
57%	56%	65%	55%	56%	[illegible]	50%	64%	[illegible]
48%	65%	73%	72%	69%	50%	55%	70%	[illegible]
63%	54%	68%	57%	60%	57%	58%	63%	60%
58%	58%	70%	63%	63%	54%	57%	66%	67%
66%	53%	68%	55%	59%	59%	59%	62%	57%

Another interesting comparison is to explore the rank order of the CIKRKA across the three different models. In Table 4.6 we see how the CIKRKA rank changes as the perception attribute is varied. This helps us to visualize how the scores are impacted by perception and why that attribute cannot be ignored in our overall assessment of risk, but should be included in such a way that we can determine how the overall score is impacted by perception and by how much. There are only three assets (KA 1, KR 2, and KR 3) whose risk remains ranked the same across all three models. Other assets swing wildly from a rank of 2 to a rank of 7, in the cases of CI 1 and KA 3.

Table 4.6. Risk Quadruplet Model Ranking Comparison

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	2	7	2
[redacted]	9	6	9
[redacted]	1	1	1
[redacted]	7	5	8
[redacted]	4	4	4
[redacted]	8	9	5
[redacted]	6	8	6
[redacted]	3	3	3
[redacted]	5	2	7

By incorporating perception into the overall risk score, we have influenced the risk score and risk rank for these CIKRKA, which, for the purposes of this methodology, is exactly what we want to see as the entire point of the risk quadruplet is to account for the discrepancy between reality and perception in a systematic, transparent, and reproducible manner. With this approach, we can see exactly how perception is affecting the overall risk score and we also know exactly how the perception attribute is being factored into the overall risk score (based on the visual scoring method for weighting the attributes). This cannot be said of any other risk analysis approach, and certainly none used for ranking assets in homeland security or homeland defense. Future research, might shed some light on how the selected weights, utilities, and parent-child belief degrees affect the influence of perception on the parent attribute of risk.

IDS also offers some built-in sensitivity analyses. Figure 4.11 displays a trade-off analysis chart, found under **Sensitivity > Trade-Off Analysis**, which shows the overall risk scores for the nine CIKRKA alternatives, as well as the perceived scores for the low perception model. We see that the overall risk score for KA 3 was 60% even though it was perceived to be 78%, whereas the overall risk score for CI 1 was approximately 63% while it was only perceived to be 48%.

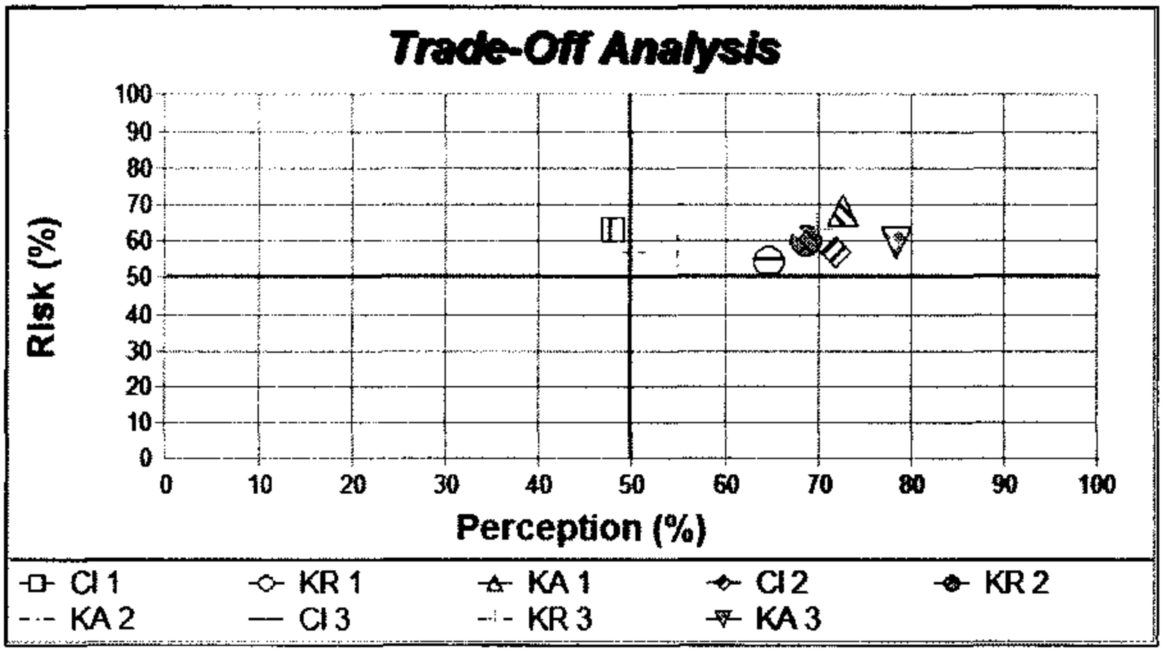


Figure 4.11. Risk and Perception Trade-Off Analysis (Low Perception)

More formally, IDS can produce sensitivity analyses based on the weighting of individual attributes, which look at the overall parent attribute ranking, or the rank change, of alternatives. Users can select the attribute for which they wish to perform sensitivity analyses (in our case, perception), then click **Sensitivity** > **Change Weight**. This brings up a dialog box where the user can select which alternatives to explore (we selected all of them). Initially, we are presented with the weights we input for the model as shown in Figure 4.12 (we conducted our sensitivity analysis from the model for which perception was weighted higher, but either of the models would be sufficient baseline models for the analyses). By clicking **Ranking**, users can manually adjust the weights of the child attributes to see how that affects the overall ranking of alternatives. Weights do not remain normalized automatically, so we manually selected weights for the child attributes that summed to 1 (Figure 4.13). Adjusting the weights of the child attributes, we can see how that affects the overall risk scores for the parent attribute across each of the alternatives.

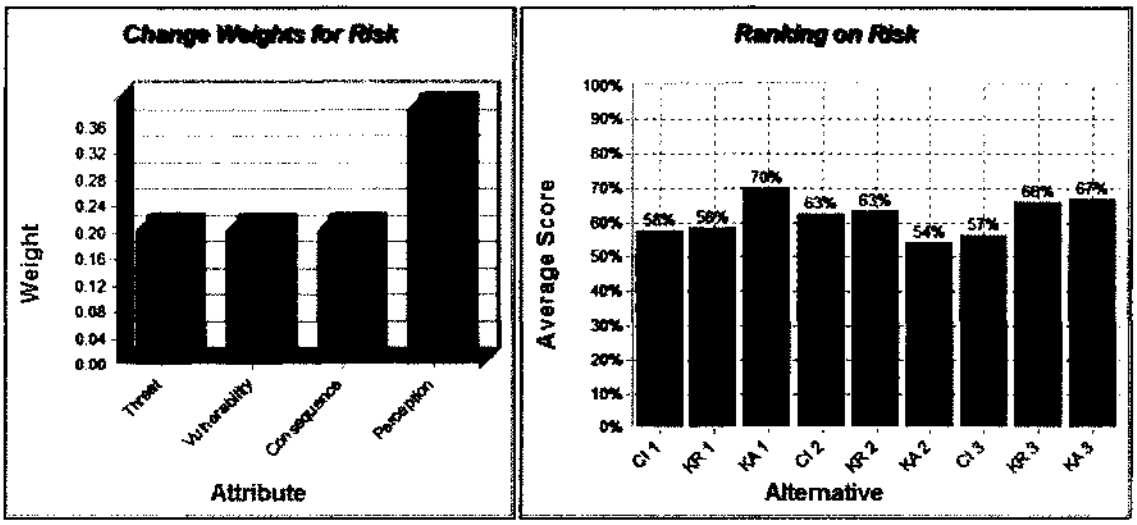


Figure 4.12. Child Attributes on Ranking (Original)

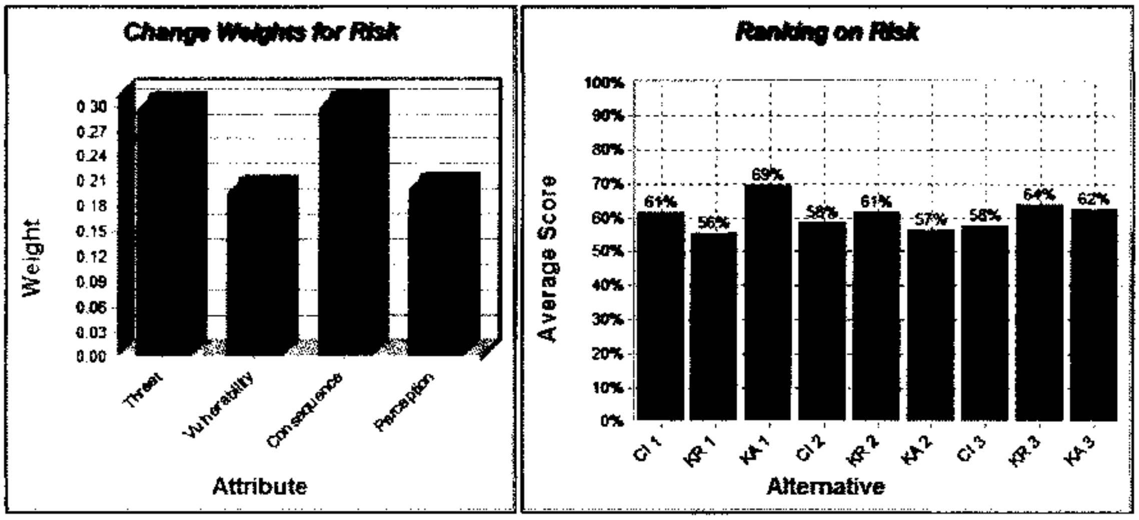


Figure 4.13. Child Attributes on Ranking (Manually Adjusted)

Alternately, and perhaps more efficiently, by clicking **Rank Change**, we can produce a more controlled sensitivity analysis on individual child attributes. The graphic given in Figure 4.14 displays the overall risk scores for each alternative as the weight of the perception attribute is varied from 0 through 1 (we adjusted the y-axis scale, used for the overall risk score, in order to better see the relationship between the weight for perception and the risk rankings). Since we conducted this sensitivity analysis from the model for which perception received a higher weight, that value is displayed as a vertical line, denoted as "Given weight", on the chart so that users can compare their current alternative risk scores and rankings to those that would be produced by adjusting the weight for perception. It is interesting to note that the overall risk score for each asset varies with the weight of the perception attribute, but it is not a linear relationship. And while the majority of the alternative risk scores increase as the weight of perception increases, three of the assets show a negative correlation (CI 1, KA 2, and CI 3).

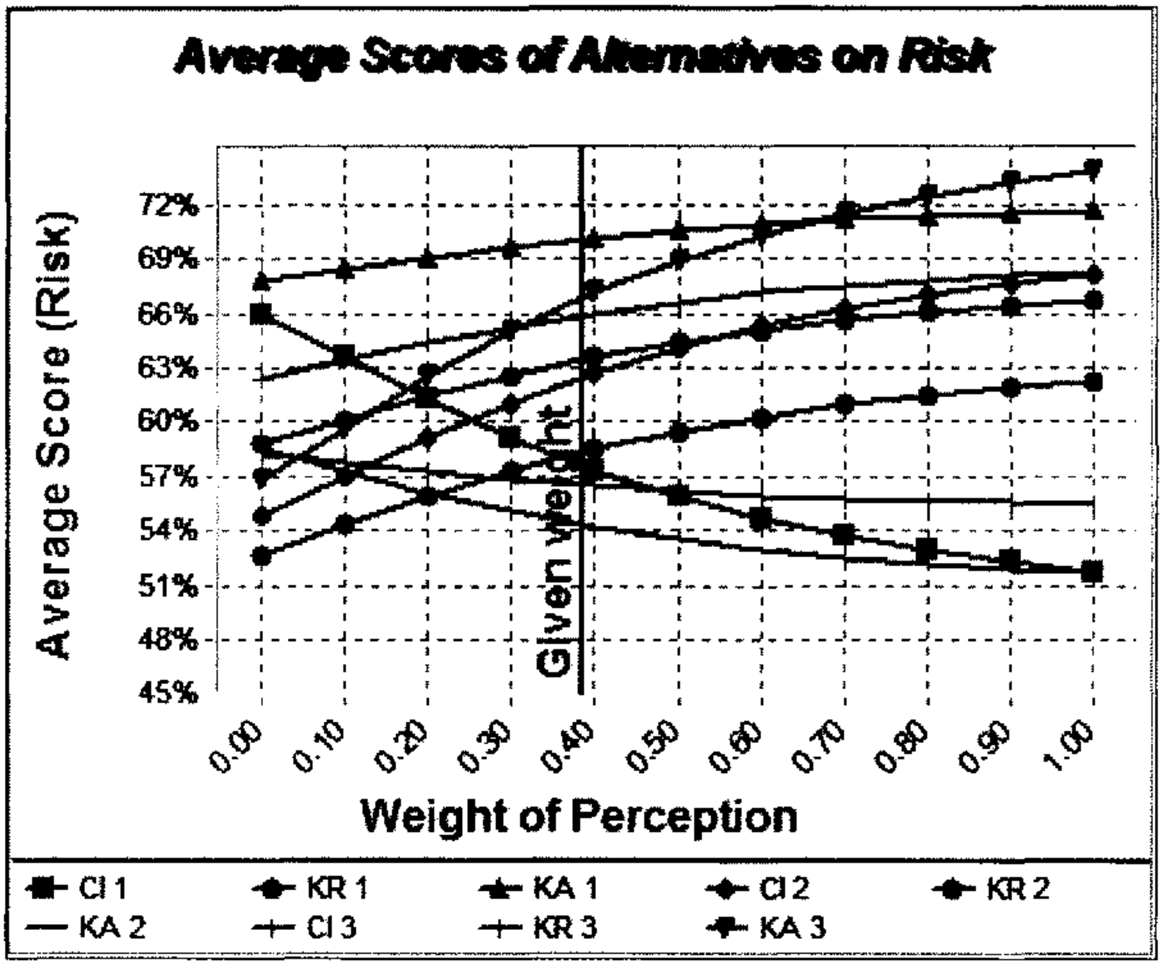


Figure 4.14. Sensitivity Analysis of Perception

IDS can also produce sensitivity analyses of belief degrees based on adjusting the child attribute weights. From the same dialog box, the user simply selects **Belief Degree**. We explored only two alternatives from the model for which perception received a higher weight: CI 1 and KA 3, ranked lowest and highest on their overall risk scores, respectively (Figure 4.15). This shows the belief degrees (our simulated data) for the perception attribute related to the grades (our linguistic set) based on the weights input for the child attributes of threat, vulnerability, consequence, and perception. However, even as we adjust the child attribute weights, the belief degrees do not change, and with good reason. If we recall the belief degree values we chose for relating child attributes to parent attributes (Table 4.2), we used the identity matrix, therefore, the belief degrees input from our simulated data for the perception attribute would not be impacted by adjusting the child attribute weights. Obviously, future research could be conducted to better understand how the belief degrees would change if we used alternative methods for assigning the input values of our belief degrees to relate parent and child attributes.

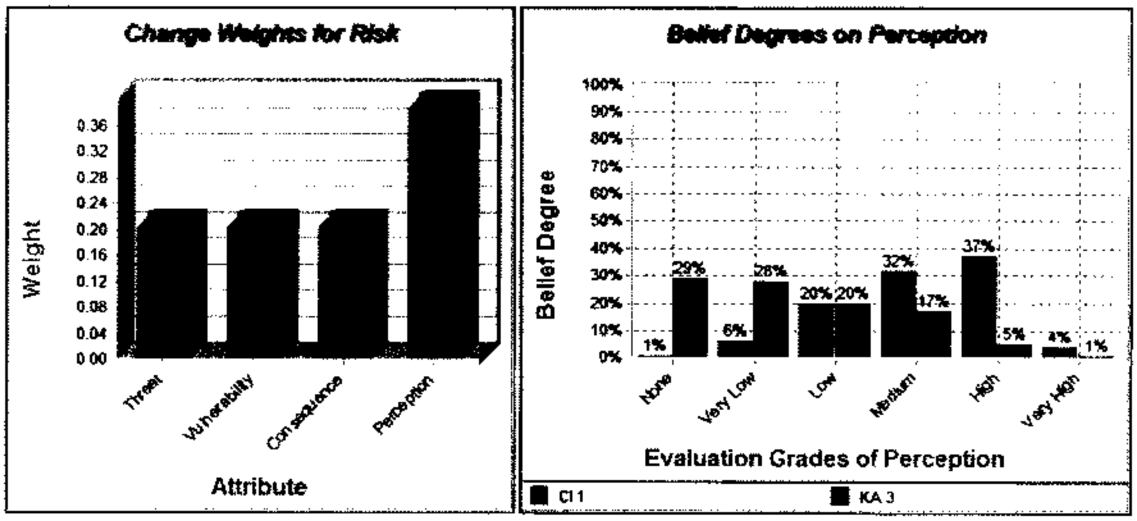


Figure 4.15. Child Attributes on Belief Degrees (Original)

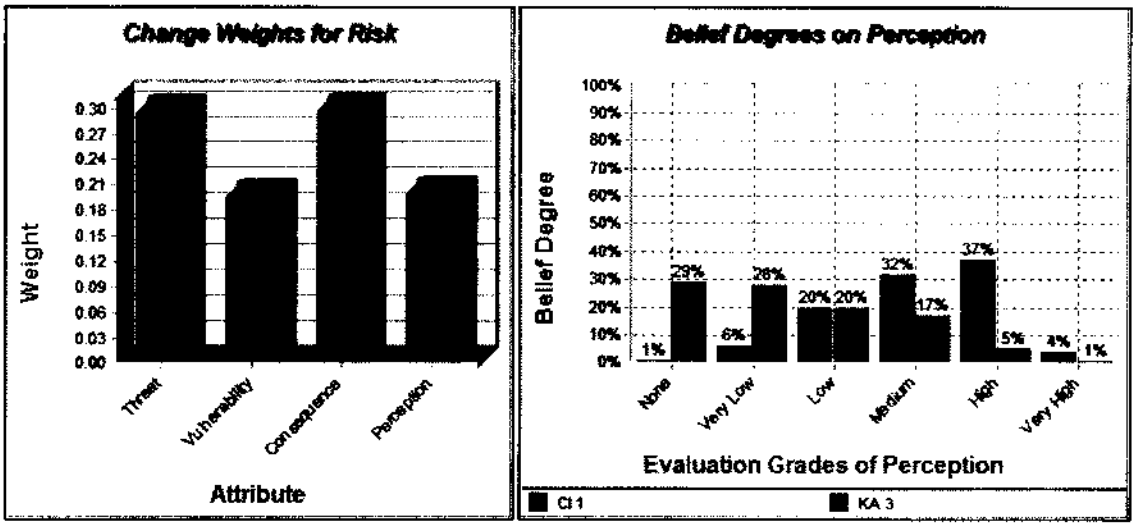


Figure 4.16. Child Attributes on Belief Degrees (Manually Adjusted)

IDS can also produce sensitivity analyses based on the data, itself. Users can select **Sensitivity > Change Input Data**, which brings up a dialog box that produces two side-by-side graphs (Figure 4.17). The first graph displays the belief degrees input for each grade (from our simulated data) for a selected alternative. We selected KA 3, which received the highest perception score (in the model for which perception received a higher weight). The second graph displays the perception score for all of the alternatives (other attributes, such as threat, vulnerability, and consequence can also be explored as desired). The belief degrees do not remain normalized automatically, so we manually adjusted the belief degrees for KA 3, such that the belief degrees summed to 1. Although we did not drastically alter the belief degrees from the original values, we still see a marked change in the overall perception score for KA 3, which dropped from 78% to 68% (Figure 4.18).

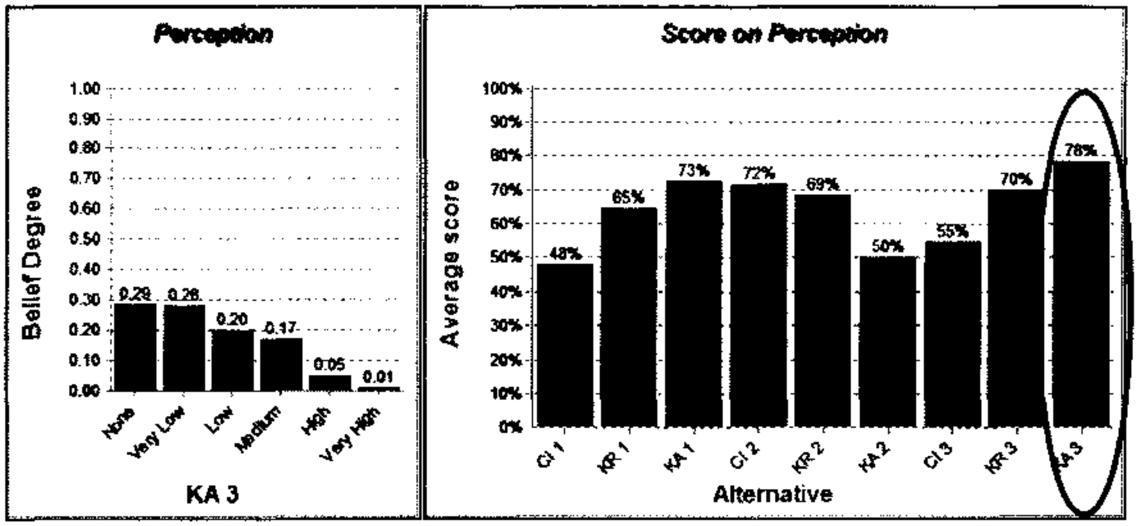


Figure 4.17. Input Data (Original)

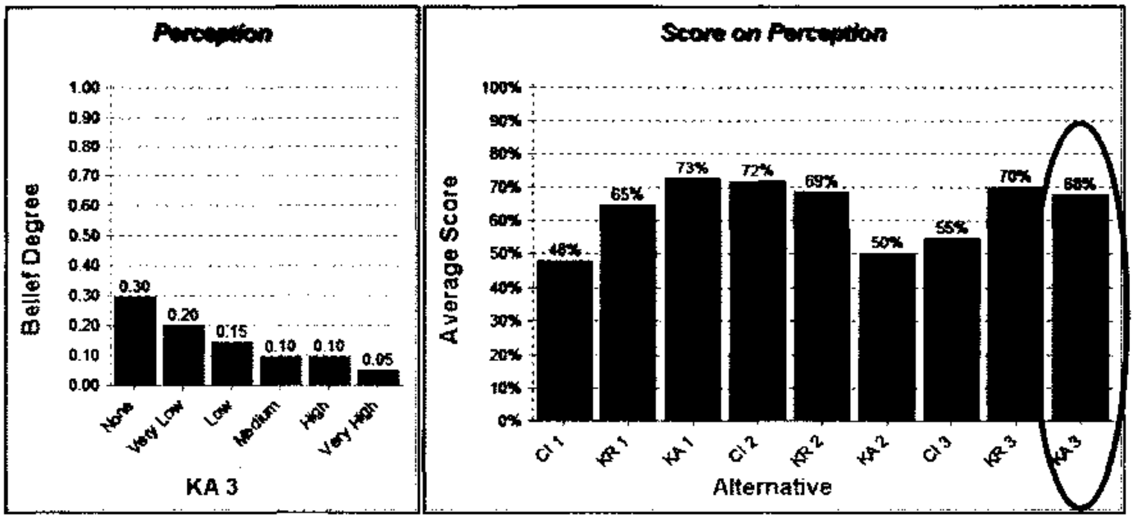


Figure 4.18. Input Data (Adjusted)

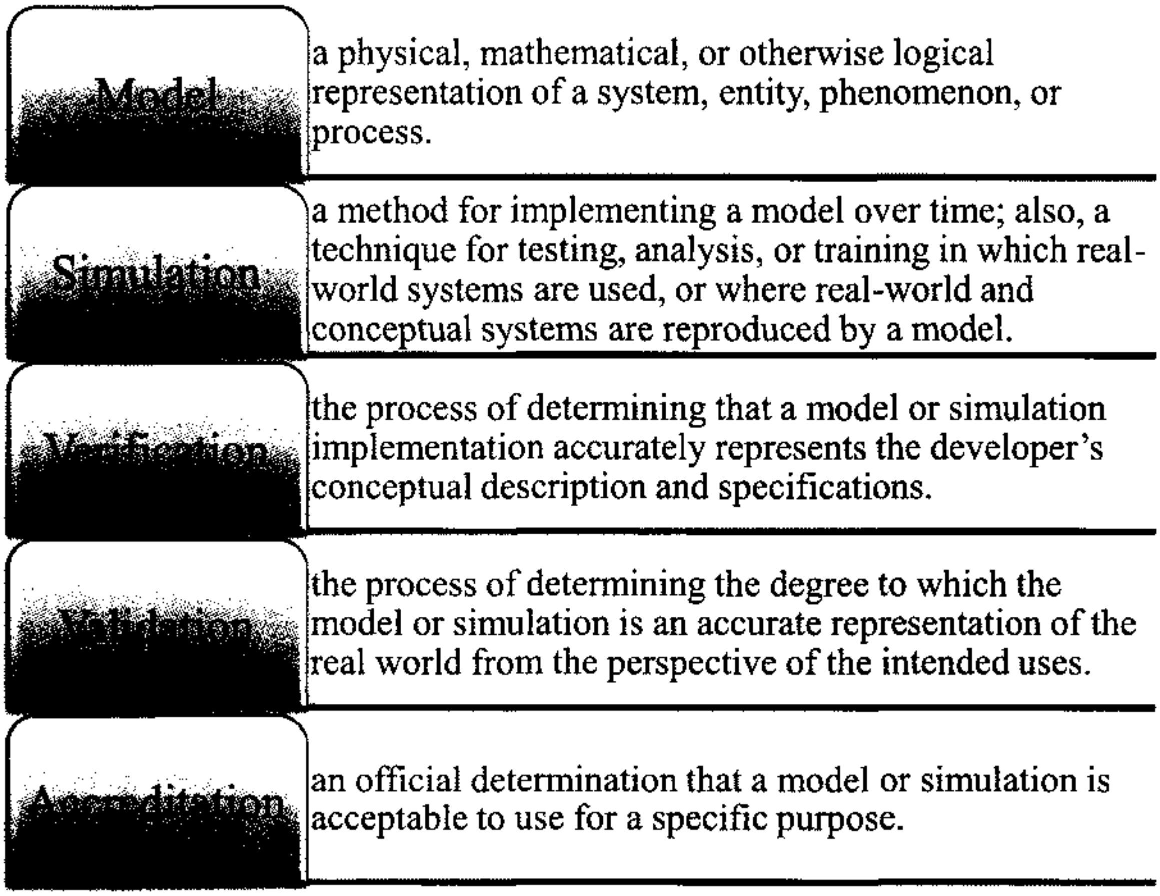
4.2 Verification, Validation, and Accreditation

In addition to the data that must be collected, leveraged, or simulated for threat, vulnerability, consequence, and perception assessments, there is also data required for the MCDA model selected. For example, the IDS software used to implement ER requires values such as weights, utilities, and belief degrees in order to describe the model. These values have nothing to do with the actual assessment data, but rather are used to define the way in which our assessment data will be integrated using the MCDA model. While future research may expand on the in vivo risk quadruplet methodology to include approaches for determining these values, we have assigned these values as necessary in order to complete the in vitro viability testing of the risk quadruplet methodology. Sensitivity analyses were conducted to determine the impact of some of these selected values on the ER model. Further, a preliminary verification and validation of the assessment integration model selected for the risk quadruplet was also performed and is presented below. However, a more thorough Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A) will be necessary in the future.

M&S VV&A is crucial to the development and deployment of a model or simulation, especially if it is to be accepted and employed by stakeholders for decision making (Macal, 2005). The Department of Defense released instructions for VV&A of M&S (*Department of Defense Standard Practice Documentation of Verification, Validation, and Accreditation for Models and Simulations*, 2008) and many other agencies have followed suit. However, DHS does not appear to have a formal instruction for M&S VV&A, even though most of the infrastructure analysis conducted by DHS is heavily reliant upon M&S, such as the work lead by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the National Infrastructure Simulation and Analysis Center (NISAC) ("About the Homeland Infrastructure Threat and Risk Analysis Center," 2012; "About the National Infrastructure Simulation and Analysis Center," 2012).

In 2010, the “Review of the DHS Approach to Risk Analysis” was released (it is discussed further in 5.4APPENDIX C) and it was recommended that DHS improve its documentation, seek model validation, and leverage reviews by technical experts to strengthen its risk M&S practices. Aside from risk analysis models for natural disasters, there are not "any DHS risk analysis capabilities or methods that are yet adequate for supporting DHS decision making, because their validity and reliability are untested," ("Review of the DHS Approach to Risk Analysis," 2010). We do see that the Federal Emergency Management Agency (FEMA), a DHS organization, employs Hazus (a natural disaster model touted as a "nationally applicable standardized methodology that contains models for estimating potential losses from earthquakes, floods, and hurricanes"), which has undergone a series of model validation analyses ("FEMA Releases HAZUS-MH Hurricane Wind Model Validation Study," 2012; "Hazus," 2012; "HAZUS-MH Riverine Flood Model Validation Study," 2012; "Validation of HAZUS Hurricane Model during Ike," 2012). But the risk quadruplet is not specific to natural hazards, which could easily be compared to historical data.

Interestingly, the USCG, another DHS agency, released two Commandant Instructions (CMDTINST) on the subject of M&S VV&A far in advance of the 2010 review of DHS risk analysis approaches. However, these instructions are brief and do not seem to be utilized by DHS for risk analysis models or simulations (*COMDTINST 5200.38: Coast Guard Modeling and Simulation Management*, 2006; *COMDTINST 5200.40: Verification, Validation, and Accreditation of Models and Simulations*, 2006). The USCG official definitions of M&S and VV&A are provided in Figure 4.19 (*COMDTINST 5200.38: Coast Guard Modeling and Simulation Management*, 2006; *COMDTINST 5200.40: Verification, Validation, and Accreditation of Models and Simulations*, 2006).



a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process.

a method for implementing a model over time; also, a technique for testing, analysis, or training in which real-world systems are used, or where real-world and conceptual systems are reproduced by a model.

the process of determining that a model or simulation implementation accurately represents the developer's conceptual description and specifications.

the process of determining the degree to which the model or simulation is an accurate representation of the real world from the perspective of the intended uses.

an official determination that a model or simulation is acceptable to use for a specific purpose.

Figure 4.19. USCG Verification, Validation, and Accreditation Definitions

4.2.1 Risk Quadruplet Model Verification

Verification ensures that a model or simulation is programmed and implemented correctly. In other words, the model should be free from errors, bugs, accidental omissions, misapplications of the model or software, or invalid implementations of any algorithms (Macal, 2005). Verification is the process of determining whether a model is consistent from concept to requirements, including a review of the model's capabilities and the specifications associated with each capability. It is important to understand that no model can ever be completely verified, so the result of model verification is not a verified model, but rather a model that has passed all verification tests. For the purposes of the risk quadruplet, verifying the model relies upon verifying the MCDA assessment integration method selected for the third phase of the risk quadruplet methodology, so ideally we would verify the ER model deployed using IDS. Our verification plan, therefore, addresses the following three questions.

1. Does the risk quadruplet model satisfy the intended use of ER?
2. Does the software code provided by IDS correctly implement ER?
3. Does the risk quadruplet model, implemented with ER via IDS, produce the required results in the desired format to meet the research purpose?

Question 1

Does the risk quadruplet model satisfy the intended use of ER? In an effort to deal with MCDA problems prone to uncertainties and subjectivity, ER was devised, developed, and implemented via IDS by Yang, along with his collaborators (Xu & Yang, 2001). ER and IDS are now used in many areas, such as supply chain management, design decision support, risk and safety analysis, quality management, and government policy consultations ("IDS," 2010). ER uses a set of attributes, weights, utilities, and belief degrees to assess and rank a series of alternatives. This approach lends itself nicely to the complex problem of risk analysis in homeland security which consists of a number of attributes (threat, vulnerability, consequence, and the newly proposed attribute of perception), and also offers a series of alternatives in need of ranking (our CIKRKA assets). ER is used to support decision analyses, assessments, or evaluation activities. The risk quadruplet would also be used to support decision-making, specifically for risk assessments of CIKRKA. So the problem of ranking a number of CIKRKA assets based on a set of attributes (threat, vulnerability, consequence, and perception) is indeed an appropriate application of ER.

Question 2

Does the software code provided by IDS correctly implement ER? Many MCDA problems inevitably deal with information under uncertainty, and that is especially true when dealing with risk. ER provides an alternative way of handling such information systematically and consistently. ER is a powerful MCDA approach based on a recursive algorithm that essentially aggregates information nonlinearly. ER has been compared to other MCDA approaches, such as MAUT, Saaty's left eigenvector method, Belton's normalized left eigenvector procedure, and Johnson's right eigenvector procedure (J.-B. Yang, 1999). The results of those comparisons produced comparable rankings of alternatives. IDS has also been compared to AHP, and while both use a hierarchical structure to model MCDA problems, there are some distinctions (Xu & Yang, 2001). For example, ER alternatives are not part of the hierarchy like they are in AHP. AHP uses a decision matrix whereas ER uses a generalized decision matrix that incorporates belief degrees (which are not employed in AHP); also, AHP uses average scores from pairwise comparisons to aggregate data, but ER aggregates the belief degrees in a progressive manner from lower level attributes to high level attributes. Because of these distinctions, IDS (the software implementation of ER) can: handle large and complex MCDA problems; assess new alternatives independently; produce consistent rakings of alternatives even after new ones are added; create a distributed assessment of alternatives in addition to a ranking of those alternatives; assess an alternative against standards or criteria (AHP can only compare the relative importance of alternatives between attributes); handle mixed data models (with both qualitative and quantitative data, as well as random and deterministic data, under uncertainty); and lastly, IDS can actually use AHP as one of its weighting approaches for attributes (Xu & Yang, 2001).

The detailed problem description, basic evaluation framework, algorithms, axioms, and theorems utilized by ER have been presented in detail (J.-B. Yang & Xu, 2002) and demonstrate that the ER approach and IDS have sound theoretical foundations. ER has undergone mathematical proofs (J.-B. Yang, 1999) and the mechanics of ER along with the results of ER deployed via IDS have been presented in a number of peer-reviewed journals and conferences (Sonmez, Yang, & Holt, 2001; Wang, Yang, & Sen, 1996; Xu, 2004; Xu & Yang, 1999, 2003, 2005; Xu, Yang, & Wang, 2005; J.-B. Yang, 1999; J.-B. Yang & Xu, 2002, 2004; J. B. Yang, Dale, & Siow, 2001). In fact, there is even one example for which ER, using IDS, was used in the fields of risk analysis and homeland security to produce a maritime security assessment (Z. L. Yang, Wang, Bonsall, & Fang, 2009). This example offers a degree of face validity for the methodology, the model, as well as the software code, all of which translates to our research as the risk quadruplet merely leverages IDS to implement an integrated risk assessment based on threat, vulnerability, consequence, and perception attributes used to rank CIKRKA alternatives, which is a valid application of ER. Additionally, as evidenced by the sensitivity analyses provided earlier, as well as the model validations which will be provided in the next section, we have demonstrated that the model behaves logically, which implies that the software code is free from mathematical errors.

Question 3

Does the risk quadruplet model, implemented with ER via IDS, produce the required results in the desired format to meet the research purpose? The research purpose requires that the output of the risk quadruplet is a ranked assessment of CIKRKA (Figure 1.3). ER is an MCDA approach, which, like other MCDA approaches such as AHP, produces a ranked list of alternatives as its output. The IDS software implementation of ER thus also produces a ranked list of alternatives. We have designated the CIKRKA assets as alternatives in the risk quadruplet model. We have defined threat, vulnerability, consequence, and perception as attributes in the model, and assigned risk as the overall parent attribute. We have supplied the model with sufficient information (including attribute weights, utilities, and belief degrees) to relate parent and child attributes, as well as to relate our data (from the threat, vulnerability, consequence, and perception assessments) to the attributes and alternatives. The output of our model is, indeed, a ranked list of CIKRKA based on an integrated risk assessment and thus adequately meets the needs of this research.

4.2.2 Risk Quadruplet Model Validation

Validation ensures that the model is useful (Macal, 2005). In other words, the model should address the correct problem and provide accurate information about the system or phenomenon being modeled. Validation could also consist of a series of challenges designed to purposefully address any doubts about the application of the model, in which case, similar to verification, the results of validation do not necessarily produce a validated model, but rather a model that has passed all validation tests (or perhaps a model that has failed some tests, but may be able to pass them in the future after additional model improvements have been made). Validation of complex models involves demonstrating that the model has the appropriate underlying relationships to permit an acceptable representation of the real world. Our validation plan addresses the following three questions.

1. Is the risk quadruplet model a valid construct of risk for homeland security?
2. Are the results produced by the risk quadruplet close to the results of the real world?
3. Under what range of inputs are the risk quadruplet results useful?

Question 1

Is the risk quadruplet model a valid construct of risk for homeland security? Typically, validation requires that a newly proposed model be compared to some existing "gold standard" model. However, there really is no such model for risk, so, let us instead explore whether the model constructed for risk makes sense in the context of homeland security. This validation depends on the purpose of the model and its intended use, so it is valuable to understand why we are using a model in the first place. In the case of the risk quadruplet, we are modeling risk as a function of threat, vulnerability, consequence, and perception, in order to make qualitative or quantitative predictions about the future, namely to rank CIKRKA assets based on their integrated risk assessment value (produced by the risk quadruplet model). But we are also using the model to gain insight into how perception affects threat, vulnerability, consequence, and risk, overall. The risk quadruplet model uses ER which allows us to explore all four attributes of risk (threat, vulnerability, consequence, and perception), as well as to explore how those attributes interact, depending on the weights, utilities, and belief degrees supplied for the model. We have already seen that the homeland security definition of risk includes threat, vulnerability, and consequence. The introduction of perception is now obvious after conducting this research, so the risk quadruplet model seems like a valid construct for homeland security.

Face validation is another technique for validating a model or simulation. Essentially, face validation determines whether a model or simulation appears to measure a certain criterion. It is often conducted via peer reviews accompanied by surveys or interviews to seek the opinions of subject matter experts regarding the model or simulation. There are even examples of this type of validation being conducted in the fields of homeland security and homeland defense, once for a vulnerability assessment model (Ezell, Keating, & Old Dominion University. Dept. of Engineering Management and Systems Engineering., 2005), and again for a serious gaming approach to infrastructure analysis (Ancel, 2011). The specific risk quadruplet model proposed in this research has undergone some preliminary, informal face validation through conference presentations and papers (Norman Hill & Ezell, 2011; Norman Hill & Gheorghe, 2011), the feedback from which has resulted in improvements to the research presented in this dissertation. Further, ER and IDS have undergone extensive face validation by presenting the methodology, mathematics, and software implementation in numerous peer-reviewed journals and conference proceedings (Huynh, Nakamori, Ho, & Murai, 2006; Sonmez, et al., 2001; Wang, et al., 1996; Xu & Yang, 1999, 2003, 2005; Xu, et al., 2005; J.-B. Yang, 1999; J.-B. Yang & Xu, 2002, 2004; J. B. Yang, et al., 2001; Z. L. Yang, et al., 2009; Zhou, Liu, & Yang, 2010). Therefore, any model which correctly implements ER and IDS can claim some level of transitive face validation.

Question 2

Are the results produced by the risk quadruplet close to the results of the real world? We could validate new models by comparing model predictions to historical data, but how would we conduct controlled experiments on risk models when historical data is limited, inconsistent, and deterministic? The maritime security assessment that leverages ER and IDS validates its model with benchmarking and sensitivity analysis (Z. L. Yang, et al., 2009). While we have conducted sensitivity analyses of the risk quadruplet model, a benchmarking study is not possible within the scope of this research. Ideally, a benchmarking study would use an existing model supplied with existing data to generate results. These results would then be compared to the results achieved with the new model (our risk quadruplet), based on the same data. Therefore, benchmarking requires some current best practice or model to which we could compare the results of our risk quadruplet. However, the risk quadruplet actually proposes a shift in the paradigm of risk calculation. Risk is not currently calculated in homeland security by including perception alongside threat, vulnerability, and consequence, so there is no comparable model to compare and contrast against the risk quadruplet. Furthermore, even if a comparable model existed, we have already discussed the limitations of the data in this research. We were unable to access threat, vulnerability, or consequence data due to its sensitivity, and we were unable to collect that data due to the limitations of the scope and schedule of the research. Therefore, we tested the viability of the model using simulated data, but we have no actual data with which to compare our results. This is a limitation of the research, but it could (and should) be addressed in the future through a more formal M&S VV&A process.

Question 3

Under what range of inputs are the risk quadruplet results useful? We have already conducted sensitivity analyses to explore different versions of the risk quadruplet model. We have compared the risk quadruplet to the current homeland security risk triplet (consisting of only threat, vulnerability, and consequence). We have gained a better understanding of the effects of weights for the perception attribute on the overall parent attribute of risk. We have determined the sensitivity of the belief degrees to the selected weights. And we even explored how changing the input data impacts the perception attribute score. However, we can conduct some other sensitivity analyses to further validate the risk quadruplet model.

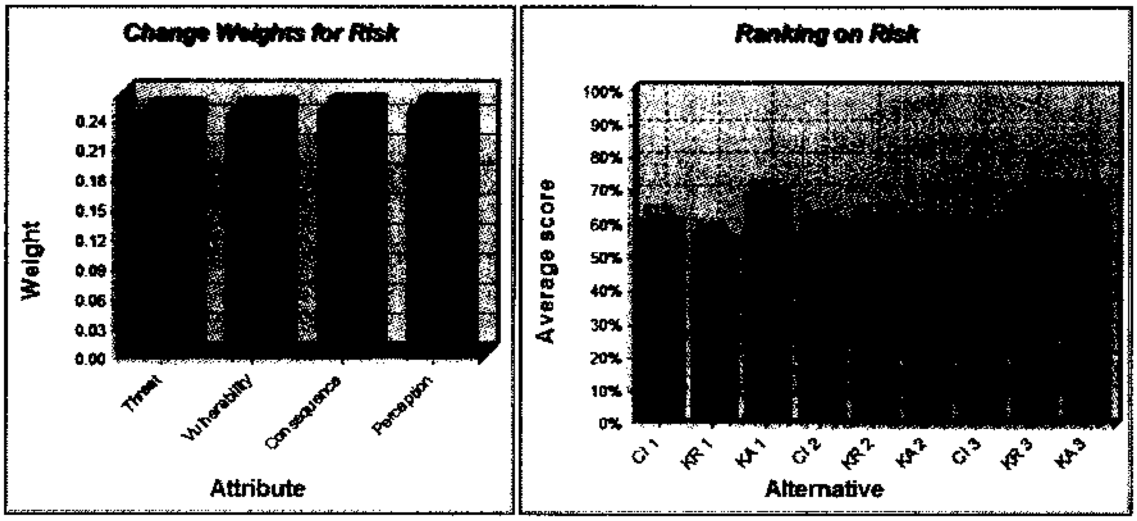


Figure 4.20. Attribute Weights Using Visual Scoring (Equal Weights Model)

The output of the risk quadruplet model (the ranked CIKRKA) should change depending on the weights selected for the child attributes, so we will explore some extreme weighting cases to test the validity of the model by ensuring that the results align with our intuitions. From Table 4.5, we know that KA 1 received the highest threat score, CI 1 received the highest vulnerability score, and KA 2 and KA 3 jointly received the highest consequence score, whereas KA 3 received the highest perception score. In Figure 4.20 we create a baseline case version of the in vitro risk quadruplet model (Equal Weights Model) for which we have set all weights equal across the four attributes. The resulting rank of alternatives (from highest risk to lowest risk) is KA 1, CI 1, CI 3, KR 2, KR 3, CI 2, KR 1, KA 3, and KA 2. We will now systematically explore the four weighting schemes presented below. We would expect the resulting CIKRKA ranks to adjust accordingly. For example, for the Max Threat Model, we would expect KA 1 (the asset which received the highest threat score) to be ranked highest with regards to the overall parent attribute of risk.

1. Max Threat Model: threat weight=1.0, vulnerability weight=0.0, consequence weight=0.0, and perception weight=0.0 (Figure 4.21)
2. Max Vulnerability Model: threat weight=0.0, vulnerability weight=1.0, consequence weight=0.0, and perception weight=0.0 (Figure 4.22)
3. Max Consequence Model: threat weight=0.0, vulnerability weight=0.0, consequence weight=1.0, and perception weight=0.0 (Figure 4.23)
4. Max Perception Model: threat weight=0.0, vulnerability weight=0.0, consequence weight=0.0, and perception weight=1.0 (Figure 4.24)

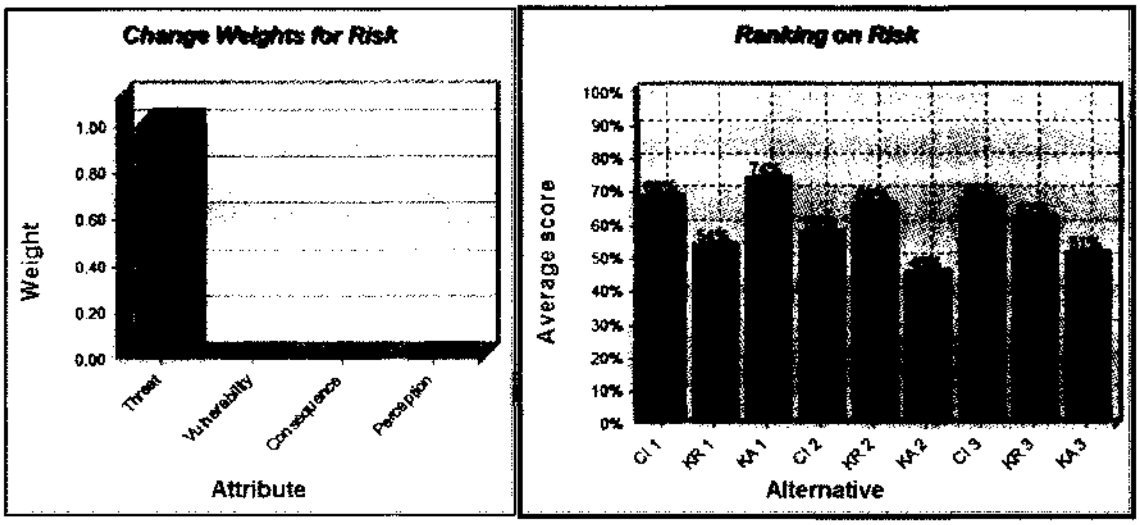


Figure 4.21. Attribute Weights Using Visual Scoring (Max Threat Model)

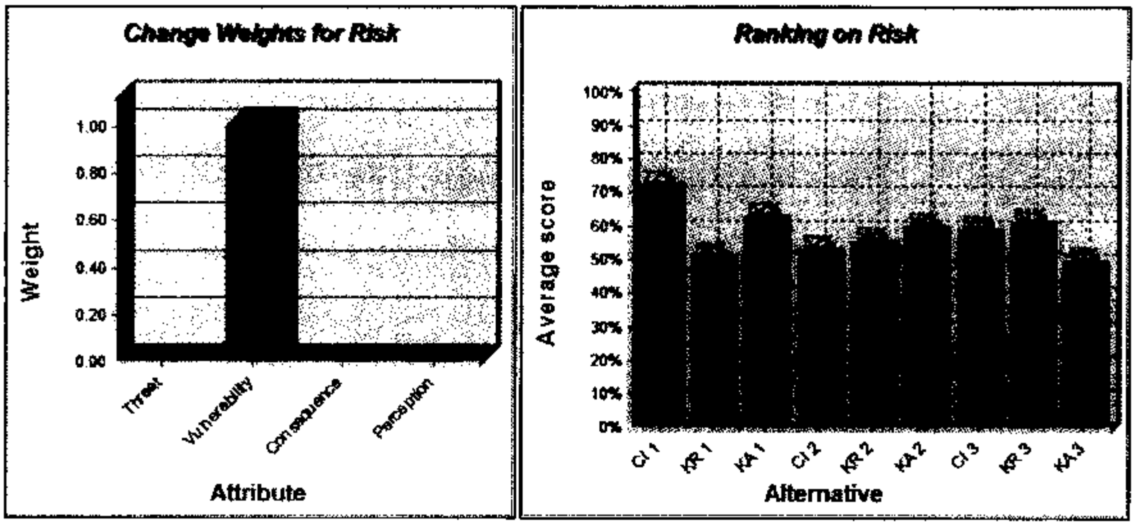


Figure 4.22. Attribute Weights Using Visual Scoring (Max Vulnerability Model)

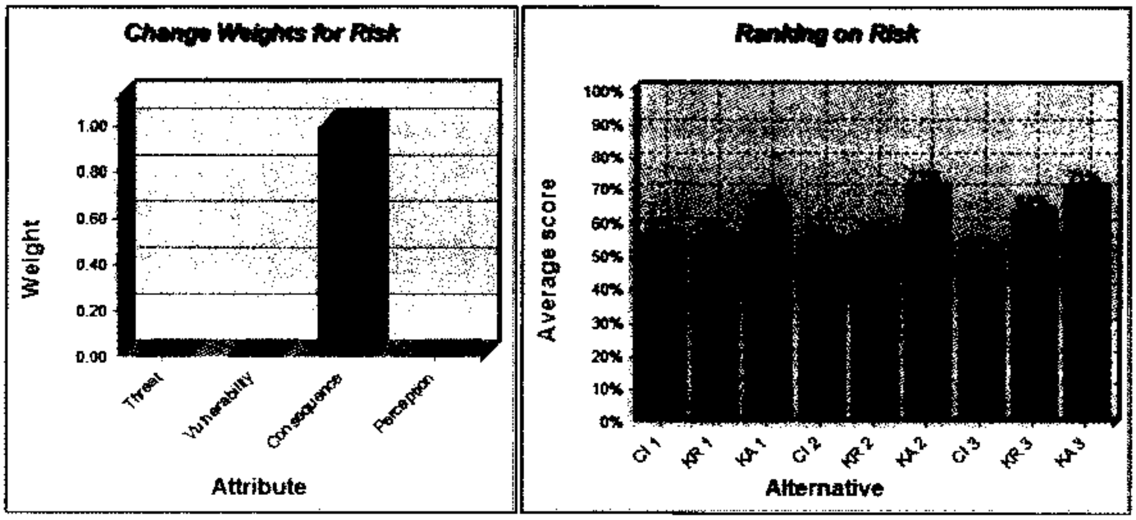


Figure 4.23. Attribute Weights Using Visual Scoring (Max Consequence Model)

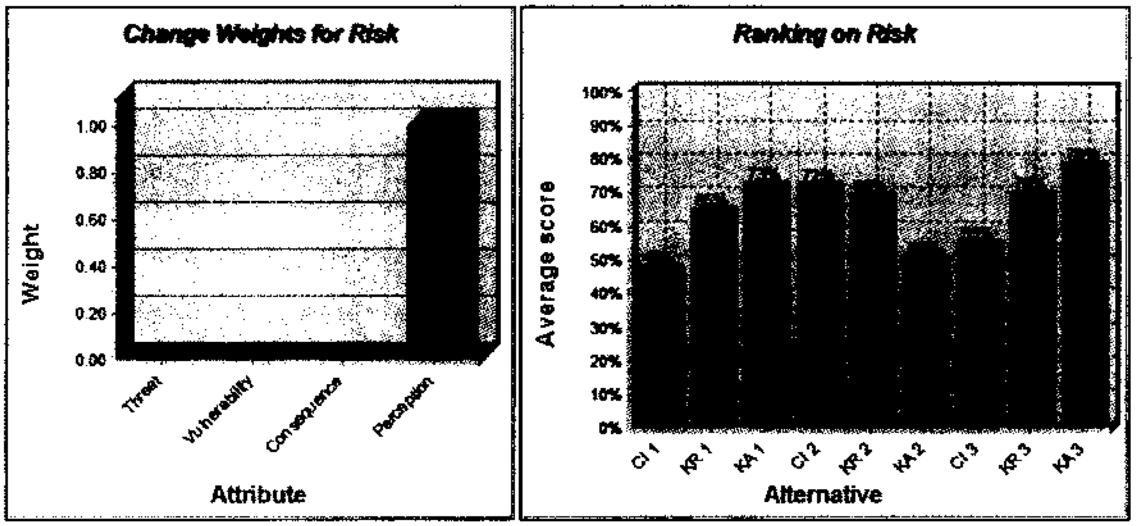


Figure 4.24. Attribute Weights Using Visual Scoring (Max Perception Model)

We condense the results of these different models in Table 4.7 and the highlighted values were the assets which received the highest overall risk score for that model. For the baseline case (Equal Weights Model), KA 1 received the highest overall risk score. For the Max Threat Model, we would expect KA 1 to be ranked highest as it received the highest threat score, and that is exactly what we see. In fact, when compared to the Equal Weights Model, the overall risk score for KA 1 increases from 69% to 74% in the Max Threat Model. This shows that the emphasis of the weight on threat has a positive correlation with the overall parent attribute of risk. Since CI 1 received the highest vulnerability score, we expect to see it ranked the highest for risk in the Max Vulnerability Model and that is again what we see. Since KA 2 and KA 3 jointly received the highest consequence score, it is no surprise that we see both of them tied for the overall risk score in the Max Consequence Model. And because KA 3 received the highest perception score, it only makes sense that KA 3 received the highest overall risk score for the Max Perception Model.

Table 4.7. Model Validation Comparison of Weighting Schemes

	61%	56%	[illegible]	59%	61%	56%	57%	64%	63%
	68%	54%	74%	58%	66%	46%	67%	62%	51%
	72%	50%	62%	52%	55%	59%	58%	61%	49%
	57%	56%	65%	55%	56%	[illegible]	50%	64%	71%
	48%	65%	73%	72%	69%	50%	55%	70%	78%

4.2.3 Risk Quadruplet Model Accreditation

Accreditation is the final step in a full M&S VV&A process. Accreditation is used to approve a model or simulation that has demonstrated that it can be employed successfully and that its results would be beneficial to the decision-making process. Obviously the entire VV&A process, but especially accreditation, would require close work with the stakeholders or agency which would be interested in employing the model or simulation. For the purposes of our research, we would initially look to market the risk quadruplet to DHS, and perhaps later share the approach with other EPR&R agencies. However, direct interaction with DHS regarding the risk quadruplet model has been extremely limited. A few DHS employees were introduced to the risk quadruplet during the 2011 Institute for Operations Research and the Management Sciences (INFORMS) Annual Meeting, and responded favorably to the proposed model; however, the model has not yet been formally presented to DHS.

While the data in these in vitro models were simulated, it is easy to see how the quick visual analyses, sensitivity analyses, and preliminary verification and validation of the model would be valuable once the risk quadruplet is deployed in vivo with actual data and stakeholders reviewing the results to inform their decisions. As evidenced by this preliminary model testing, the risk quadruplet has the potential to assess perceptions of subject matter experts using an ER model. An integrated assessment methodology, based on ER, can be employed to integrate threat, vulnerability, consequence, and perception assessments. And this methodology systematically integrates all four types of data in a meaningful, traceable, and reproducible approach, and provides a ranked CIKRKA list as its output. Future research would be necessary to better understand the sensitivity of the model to the selected weights, utilities, and belief degrees selected for the model, but it is easy to see how IDS could be useful in producing these analyses. Further, these sensitivity analyses would be invaluable for communicating with participants and stakeholders in the risk quadruplet integrated assessment.

Many versions of the risk quadruplet model have been tested, in vitro, using simulated data to rank nine CIKRKA assets. This same risk quadruplet model could be used, in vivo, to assess the actual perceptions of subject matter experts. It could also incorporate threat, vulnerability, and consequence assessment data leveraged or collected during the second phase of the risk quadruplet methodology. The output of this in vivo approach would again be a ranking of assets, based on the proposed ER approach (using IDS), which could combine subjective and objective data, both quantitative and qualitative, to improve our understanding of the risks to CIKRKA.

CHAPTER 5

CONCLUSION AND FUTURE RESEARCH

"This paper, by its very length, defends itself against the risk of being read."
– Winston Churchill

The three purposes of this research were to assess perceptions of CIKRKA, determine a risk quadruplet methodology for integrating threat, vulnerability, consequence, and perception assessments, and to rank CIKRKA based on an integrated risk quadruplet assessment methodology. Additionally, the two initial contributions of this research were to propose an MCDA risk quadruplet model for integrating assessments of threat, vulnerability, consequence, and perception, as well as a methodology for deploying the risk quadruplet model. The risk quadruplet methodology proposed is capable of integrating threat, vulnerability, consequence, and perception assessments. While the risk quadruplet methodology was not deployed in vivo, it does detail the approach necessary for all three phases of the risk quadruplet methodology, from collecting perception data, leveraging or collecting threat, vulnerability, and consequence data, as well as systematically integrating those data in a meaningful, traceable, and reproducible model. Further, this methodology has been subjected to preliminary testing and analysis, in vitro, and has proven to be a viable approach for ranking CIKRKA in order to improve decision making for homeland security and homeland defense.

And in fact, though not defined at the onset of the research, additional contributions have been made to the fields of risk perception, risk analysis, systems engineering, as well as homeland security and homeland defense. This research challenged the existing paradigm for risk, not just as it is defined in homeland security (as a function of threat, vulnerability, and consequence), but as it is typically defined in risk analysis, in general (as a function of probability and consequence). This research asserts that risk is inherently related to our perceptions and that we construct risk methodologies and models based on those perceptions.

This paradigm shift has a direct and corresponding impact on the practical application of risk analysis. If we agree that perception affects our assessments of risk, then it is only logical that we include those perceptions in our risk assessment approaches. This argues for more robust methods to incorporate perceptions into an integrated risk assessment approach, as has been proposed by the risk quadruplet. The practical, and potentially disturbing, implication of this new risk model is that if we change our perceptions, we then influence our calculated risk. However, this is already the case, although it has not been formalized. If we conducted an assessment on a given asset's risk in 2000, we might have produced very different results than if we had repeated that assessment in 2010 (considering all of the risk scenarios that have impacted our psyche since 2000, including the September 11th attacks and the Fukushima disaster). And in fact, this correlation between risk and our perceptions could be further exploited to improve risk communication and strategic risk planning. As perceptions of risk are incorporated into risk assessments, decision makers can better understand where gaps exist between our perceptions of risk and the actual threat, vulnerability, and consequence data known about those risks. This information can be developed into improved risk visualizations, such as risk maps, or even graphics like those produced by the WEF for their Global Risks reports. Improving the risk communication could have a positive effect on risk perceptions, which would, in turn, result in improved risk assessments.

5.1 Methodology Improvements

Obviously, future research should include an in vivo test of the risk quadruplet methodology since the risk quadruplet model has only been subjected to in vitro testing using simulated data. While the in vitro testing proved the viability of the risk quadruplet model, it did not ensure the entire research methodology was viable, since risk perception data was not collected from subject matter experts directly. However, had we implemented the in vivo methodology, we could have encountered a number of issues. For example, in the proposed in vivo methodology, respondents would have been given CIKRKA local to them (as volunteer participants would have lived or worked in the National Capitol Region at the time of perception data collection). It was noted that this might introduce some bias. Would their perceptions be influenced by their proximity to the region? What if we presented them with CIKRKA examples specific to Hampton Roads or another region with which they were less familiar? Further, respondents would only have been asked to consider Motor Gasoline for VA, as this information was unavailable for DC. However, these regional choices could introduce some bias to the perception data as respondents were asked to consider a CI in DC, a KA in DC, but a KR covering the entire state of VA.

Future methodological improvements might also include the exploration of perceptions from the general public, instead of focusing on subject matter expert opinions. The model could even be expanded to accommodate a combination of perceptions from both experts and non-experts. For example, the perception attribute could branch into two sub-attributes: private and public, where private perception assessments would come from the owners and operators of the asset and public perception assessments could be split further into assessments collected from general citizens, regulatory committees, as well as federal, state, and local government agencies. All of these different entities provide valid perceptions which could affect decision-making. We have seen that risk is a construct, so it may be valuable to not only include perception in the assessment process, but to include multiple perceptions to ensure we are seeing all of the potential risk associated with an asset from numerous different perspectives.

In addition to the approach presented for collecting perception data, the risk quadruplet methodology could also be expanded to include options for collecting threat, vulnerability, and consequence data. It would also be good to explore whether that data could or should be collected as qualitative or quantitative data, since ER can handle mixed data models. While it may be valid to continue collecting risk perception using a qualitative linguistic set, that might not be appropriate for all combinations of CIKRKA and risk scenarios with regards to the other three attributes of the risk quadruplet model.

It was suggested that threat, vulnerability, and consequence data could be collected or leveraged from historical assessments for use during the in vivo risk quadruplet approach. One option would be to code the results (of either collected or leveraged data) to the ER linguistic set. However, this additional step could introduce some bias as someone would have to judge how the results align to the linguistic set, but it would treat all data in the risk quadruplet on a common qualitative scale. Threat, vulnerability, and consequence assessments are often ad hoc and typically produce inconsistent data, so coding the results to a single linguistic set would give them commonality. But due to the flexibility of the ER assessment integration phase of the risk quadruplet, we could collect or leverage threat, vulnerability, and consequence data however it is available (qualitative or quantitative, for example). ER can integrate both qualitative and quantitative data and IDS provides that option when defining attributes, so we could explore the impact to the risk quadruplet model when using mixed data. For example, if the attribute is defined as quantitative, then the user can also decide whether it is a certain or uncertain attribute. This would be useful for defining uncertain quantitative attributes, which could be random numbers, may be difficult to assess, or could suffer from missing data ("IDS Multicriteria Assessor Quick Guide," 2010). We could revisit the in vitro model used to test the risk quadruplet, and replace some of the simulated qualitative data with simulated quantitative data by inputting threat and consequence as quantitative variables, using the tornado frequencies and property damage data presented in 5.4APPENDIX D. However, this research could require significant contributions to the methodological approach.

The number and types of assets under study in the proposed in vivo methodology would have been limited to a single CI, KR, and KA, and would have only explored a single scenario. Even the in vitro viability testing of the risk quadruplet model limited the number of assets to three CI, three KR, and three KA, and again assumed a single risk scenario. Future iterations of the risk quadruplet model should explore an increased number of assets and scenarios (both natural and unnatural). Additionally, it has been shown that not all assets clearly align to a single type of asset (CI, KR, or KA); many assets are interrelated. For example, the Hoover Dam produces electricity and serves as a major transportation route (making it a CI), however it outputs electricity and maintains water supplies (which are both KRs), but it is also a thriving tourist attraction (making it a KA). There is no methodology for integrating multiple risk assessments for a single entity from different perspectives, such as when a CI is aligned to multiple sectors, or when it is also considered a KA, which is where perception could play a starring role. Future research could explore ways to handle interrelated CIKRKA. Expanding the risk quadruplet methodology to include additional (and potentially interrelated) assets and risk scenarios would drastically improve its value and applicability.

Additionally, the methodology is also adaptable as more research on the model, itself, is conducted. For example, the risk quadruplet methodology could be expanded to include details for determining child attribute weighting, utility scoring, and the assignment of parent-child belief degrees. This could open up a number of areas of research to further improve the risk quadruplet methodology, such as comparing the child attribute weighting methods (visual scoring versus pairwise comparison), or the derivation of utility inputs. Perhaps this could be an opportunity to revisit the MCDA MAUT approach which was discarded as an improper approach for the assessment integration phase of the risk quadruplet, but might be a valuable approach for determining those utility values required by the ER model. This research could also benefit from the study of the selection of parent to child belief degrees (which were input using the identity matrix for the purposes of this research, but which could be further explored using sensitivity analyses).

5.2 Model Improvements

First and foremost, the risk quadruplet should undergo formal M&S VV&A (a preliminary verification and validation of the model was discussed in CHAPTER 4). It was recommended that "DHS should have a well-funded research program to address social and economic impacts of natural disasters and terrorist attacks" ("Review of the DHS Approach to Risk Analysis," 2010). Existing risk analyses for infrastructure protection could be improved by verifying and validating models, improving documentation, or submitting models to external subject matter experts for peer review ("Review of the DHS Approach to Risk Analysis," 2010). The risk quadruplet offers a unique proposal, to not only shift the paradigm for how risk is calculated by DHS, but to potentially be one of the first models accredited which formalizes the DHS approach to integrating threat, vulnerability, consequence, and perception assessments in a meaningful, traceable, and reproducible manner. Further, as DHS does not have a formal instruction for M&S VV&A, there is an opportunity for future research to ensure DHS creates such guidance and that it is tailored to the specific needs for models, simulations, and assessments used by DHS for strategic decision-making, risk mitigation plans, and budget allocation.

The model could also be expanded to rank a much larger number of CIKRKA assets. Additionally, replicating the model would allow for the comparison of multiple risk scenarios. In other words, we would set up one instance of the model to analyze threat, vulnerability, consequence, and perception data based on a single risk scenario. Another instance of the model (identical in every way, except for the data) would be used to analyze a second scenario, and so on. This would allow for apples to apples comparisons of the same CIKRKA assets (alternatives) across the same attributes. Although it could be argued that the models should be adjusted to account for differences in utilities, belief degrees, and weighting depending on the risk scenario (in other words, does perception receive the same weight when exploring a flood risk scenario for which threat, vulnerability, and consequence data might be very reliable versus a terrorist attack risk scenario for which data is less reliable and perceptions tend to be driven by fear more than facts?).

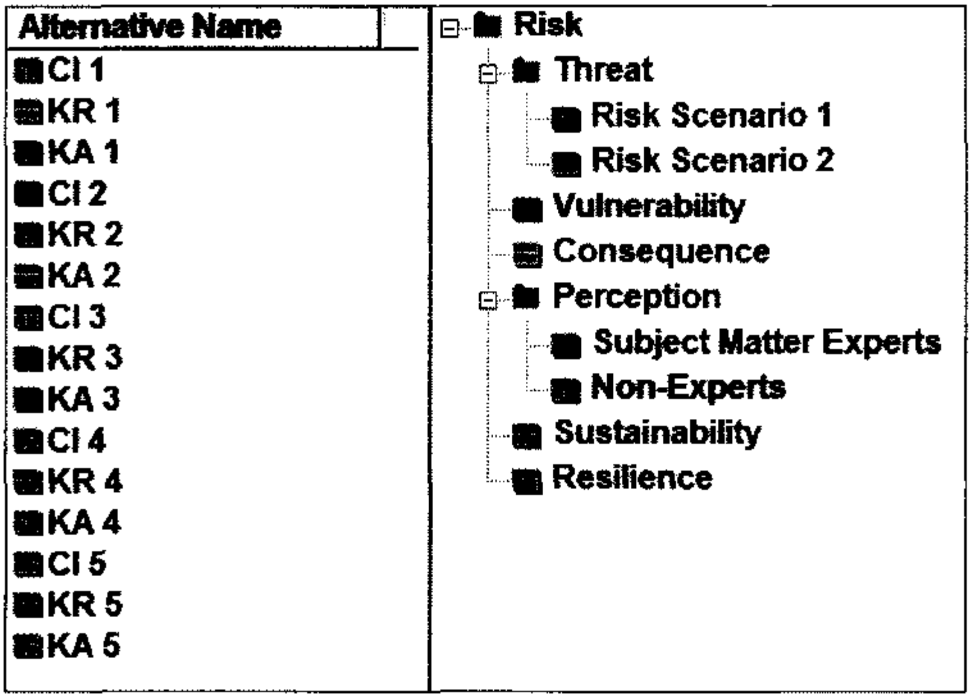
Prospective versions of the model could work with subject matter experts to complete the pairwise comparison approach for weighting attributes in the ER integration assessment phase. This tool is provided with the IDS software and is basically an AHP approach for weighting the child attributes (threat, vulnerability, consequence, and perception) as they relate to the parent attribute (risk). Additionally, utilities for the parent attribute (risk) were assigned to grades arbitrarily for this example, but it may be worth exploring how to assess and incorporate the utilities of those providing inputs for the ER model. These values could be easily revised in future iterations of the model. Similarly, to relate parent and child attributes, the belief degrees were assigned arbitrarily for each child (threat, vulnerability, consequence, and perception). These values could be adjusted in future iterations of the model. For example, if the child grade is very low, that could relate to a parent grade of none, very low, and low with belief degrees of .25, .50, and .25, respectively. Developing a methodology for determining how to define these weights, utilities, and belief degrees would improve the flexibility and robustness of the risk quadruplet model. Additionally, it would allow for sensitivity analyses, which might shed some light on how the selected weights, utilities, and belief degrees affect the influence of perception on all attributes, as well as the parent attribute of risk.

Similarly, future research could be conducted to better understand how the belief degrees would change if we used alternative methods for assigning the input values of our belief degrees to relate parent and child attributes. More intense sensitivity analyses would be necessary to better understand how the model would behave as the utilities, weights, and belief degrees that relate child to parent attributes are adjusted. It is easy to see how IDS could be useful in producing these analyses and how these sensitivity analyses would be invaluable for communicating with participants and stakeholders in the risk quadruplet integrated assessment.

5.3 Generalizability of the Risk Quadruplet Model

Determining how to generalize the risk quadruplet model would be worthwhile to demonstrate its applicability across a wider range of homeland security and homeland defense risk issues, as well as risk challenges in other fields. Conveniently, the risk quadruplet model is extensible and adaptable, mainly because ER is a flexible and robust assessment integration approach.

A more complex model could also be explored to address multiple risk scenarios by introducing them as child attributes of the threat attribute, rather than just replicating the model. Additionally, the model could be expanded to address additional child attributes, such as sustainability or resilience (Figure 5.1). Expanding the risk quadruplet methodology to include additional (and potentially interrelated) assets and risk scenarios would drastically improve its value and applicability.



Alternative Name

CI 1
KR 1
KA 1
CI 2
KR 2
KA 2
CI 3
KR 3
KA 3
CI 4
KR 4
KA 4
CI 5
KR 5
KA 5

- Risk
  - Threat
    - Risk Scenario 1
    - Risk Scenario 2
  - Vulnerability
  - Consequence
  - Perception
    - Subject Matter Experts
    - Non-Experts
  - Sustainability
  - Resilience

Figure 5.1. Risk Quadruplet Model (Generalized Example)

Lastly, additional child attributes that relate to the overall parent attribute of risk could be explored in future iterations of the risk quadruplet. For example, sustainability and resilience have both become very popular terms in the homeland security and homeland defense literature. Resilience is defined by DHS as the "ability of systems, infrastructures, government, business, communities, and individuals to resist, tolerate, absorb, recover from, prepare for, or adapt to an adverse occurrence that causes harm, destruction, or loss" (*DHS Risk Lexicon*, 2010). Sustainability is generally defined as the development of infrastructure that not only meet the needs of the present, but do not impact the ability of future generations to meet their evolving needs (for example, adapting existing infrastructure, or building new infrastructure, that is compatible with alternative energy sources). The term sustainability is mentioned in 15 homeland security and homeland defense documents, but was not specifically defined in any of them (*Agriculture and FooD Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007; *Communications: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007; *Critical Foundations: Protecting America's Infrastructures*, 1997; *Defense Industrial BasE Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007; *Energy: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007; *Information Technology: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007; *Interim National Infrastructure Protection Plan*, 2005; *National Infrastructure Protection Plan*, 2006; *National Infrastructure Protection Plan*, 2009; *National Response Framework*, 2008; *National Response Plan*, 2004; *NSHS*, 2002; *NSPPCIKA*, 2003; *Quadrennial Homeland Security Review Report*, 2010; *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007). It is not too much of a stretch to see how DHS and other agencies might wish to conduct sustainability or resilience assessments in the future, and the results of those assessments could be easily incorporated alongside threat, vulnerability, consequence, and perception assessments into a *risk quintuplet* or *risk sextuplet*.

Further generalizing the risk quadruplet approach, we could use the risk quadruplet model to explore anything that would need to be ranked in an overall integrated assessment of risk for homeland security or homeland defense. For example, it is possible that an adaptation of the risk quadruplet approach could be useful in future Regional Resiliency Assessment Program (RRAP) and Strategic National Risk Assessment (SNRA) efforts to rank regions, cities, or areas, or to rank risk scenarios. Or the risk quadruplet could be used to rank countries, similar to the country risks reported by WEF ("Global Risks," 2006; "Global Risks," 2007; "Global Risks," 2008; "Global Risks," 2009; "Global Risks," 2010; "Global Risks," 2011; "Global Risks," 2012; "OECD Studies in Risk Management: Innovation in Country Risk Management," 2009). Or the risk quadruplet could be used to evaluate decisions and lessons learned from crises, to measure the effectiveness of risk mitigation efforts, to reevaluate risks once vulnerabilities have been addressed, or to ensure funds for mitigation efforts are allocated based on risk rankings. These areas are critical deficiencies in many countries' enterprise risk management processes, as identified in the OECD risk management report ("OECD Studies in Risk Management: Innovation in Country Risk Management," 2009). Additionally, the risk quadruplet could be used to explore risk mitigation. Pinto asserts that it is "essential that alternative (risk mitigation) actions be evaluated" and ranked based on the attributes of cost and benefits (Pinto, 2006). The risk quadruplet methodology could easily be reengineered for this particular problem by defining actions as alternatives in the ER model and by defining attributes in the ER model for cost and benefit, thus outputting a ranked list of mitigation actions. Most importantly, it is vital to recognize that the risk quadruplet model is not restricted to only analyzing risk to CIKRKA assets.

And, in fact, the risk quadruplet model is also not limited to the homeland security or homeland defense markets. The Center for Strategic and International Studies (CSIS) conducted a survey of risk analysis in a number of government agencies, as well as throughout the international community (Murdock, Squeri, Jones, & Smith, 2011). CSIS found a number of key similarities and key differences in both the risk assessment phase ("how risk is defined, identified, analyzed, and assessed") as well as the implementation phase (how risk assessment affects decision-making and how risk is communicated). Similar to our findings, the overall risk lexicon was deemed to be inconsistent and incomplete. Another lesson learned was the need for risk management techniques to acknowledge uncertainty and variance in risk assessment approaches. Interestingly, CSIS also notes that "simple models are almost always better than complicated ones" (Murdock, et al., 2011). A series of case study matrices are presented for DHS, National Aeronautics and Space Administration (NASA), EPA, Nuclear Regulatory Committee, Office of Management and Budget, Food and Drug Administration, as well as a number of countries such as Singapore, the United Kingdom, Canada, New Zealand, and France, as well as a number of international organizations like the United Nations, World Bank, and OECD. The case studies explore how the agencies or countries define, identify, assess, and communicate risk, along with information about the organization's strategic environment and objectives, culture, leadership, and the overall effectiveness of the organization's risk management approach (Murdock, et al., 2011). The risk quadruplet may be a good fit for some of the risk analysis approaches employed by these agencies and countries.

Additionally, many other risk analysis research areas could benefit from this general model. For example, project management risk analysts are typically interested in technical risks and programmatic risks (Pennock & Haimes, 2002), where technical risks are those issues that would keep a project from meeting its performance criteria and programmatic risks are related to cost and schedule overruns. Often these attributes are assessed independently and attempts to provide an overall integrated assessment, so as to rank risk scenarios to the project for the purposes of risk mitigation, are often oversimplified; for example, some risk analysts might use a straight average of the attribute assessment scores. The risk quadruplet model could be applied here, where the risk scenarios become the alternatives and the child attributes underneath the parent attribute of risk would be cost, schedule, safety, and quality.

5.4 Additional Research Areas

There are also a number of additional research areas that could be explored which do not directly relate to the risk quadruplet methodology or the model itself, but are still related to the research presented here. For example, studying the regional component of risk and perception for homeland security, in and of itself, could open up an entire area of research, already being explored to some extent in conjunction with Geographic Information Systems (GIS). For example, are there regional differences in perceptions of risk to CIKRKA and could that impact risk assessments (if a region does not often experience flooding, would that risk scenario be overlooked, rendering them vulnerable should a flood occur)? And could differences in perceptions across different geographical areas allow national, regional, or local policy-makers, or infrastructure planners and vendors, to determine where new CIKR would be best received by local residents (a sort of geomarketing of CIKR)?

And although it did not make sense to propose a complete Psychometric Model for the in vivo risk quadruplet methodology presented in this research (given the constraints of the ER model selected for attribute integration), it would be worth exploring an expanded Psychometric Model in the future. A full psychometric study could analyze the perceptions of CIKRKA to see if there is a statistically significant difference between perceptions of those different assets, the results of which would be very interesting and worthwhile as DHS continues to refine its definitions and risk analysis approaches for CIKRKA. Further, surveying experts could result in perceptions different from those of the layperson. Future iterations of the model could explore perceptions from the general public, or even a combination of perceptions from both experts and non-experts.

Lastly, it was suggested that KA do not have a traditional systemic purpose and are not seeking to produce, transform, or transport anything. Future research might shed some light on how this might impacts the inclusion of KA in the greater CIKR system of systems, especially for the purposes of ranking those assets based on risk. At the very least, it would be worthwhile for DHS to revisit and improve their definitions for assets, risk, and risk-related terms, as it could only have a positive impact on their overall risk management and analysis program.

REFERENCES

Agriculture and Food: Critical Infrastructure and Key Resources Sector-Specific Plan. (2007). Retrieved from http://www.vet.utk.edu/cafsp/resources/pdf/Department%20of%20Homeland%20Security%20-%20Agriculture%20and%20Food%20SSPs.pdf

Althaus, C. E. (2005). A Disciplinary Perspective on the Epistemological Status of Risk. *Risk Analysis*, 25(3), 22.

Ancel, E. (2011). A systemic approach to next generation infrastructure data elicitation and planning using serious gaming methods. . Engineering Management and Systems Engineering. Dissertation. Old Dominion University. Norfolk, VA.

Apostolakis, G. E. (2004). How Useful is Quantitative Risk Assessment? *Risk Analysis*, 24(3), 6.

Apostolakis, G. E., & Lemon, D. M. (2005). A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. *Risk Analysis*, 25(2), 361-376.

Becker, U., Dunwoody, S., Holzheu, F., Hunnius, G., Jungermann, H., Kemp, R., et al. (1993). *Risk is a Construct: Perceptions of Risk Perception.* Munich, Germany: Knesebeck GmbH & Co.

Bronfman, N. C., & Cifuentes, L. A. (2003). Risk Perception in a Developing Country: The Case of Chile. *Risk Analysis*, 23(6), 1271-1285. doi: 10.1111/j.0272-4332.2003.00400.x

COMDTINST 5200.38: Coast Guard Modeling and Simulation Management. (2006). Retrieved from http://www.uscg.mil/directives/ci/5000-5999/CI_5200_38.pdf

COMDTINST 5200.40: Verification, Validation, and Accreditation of Models and Simulations. (2006). Retrieved from COMDTINST 5200.40

Commercial Facilities Sector: Critical Infrastructure and Key Resources. (2010, March 22, 2010) Retrieved September 9, 2010, 2010, from http://www.dhs.gov/files/programs/gc_1189101907729.shtm

Communications: Critical Infrastructure and Key Resources Sector-Specific Plan. (2007). Retrieved from http://www.hsdl.org/?view&did=474324

Conrow, E. H. (2005). Risk Management for Systems of Systems. *The Journal of Defense Software Engineering*, 5.

Cox, L. A. (2008). Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks". *Risk Analysis*, 28(6), 1749-1761.

Critical Foundations: Protecting America's Infrastructures. (1997). Retrieved from http://www.cyber.st.dhs.gov/docs/PCCIP%20Report%201997.pdf

Critical Infrastructure and Key Assets: Definition and Identification. (2004). (Order Code RL32631). Congressional Research Service. Retrieved from http://www.fas.org/sgp/crs/RL32631.pdf

Critical Infrastructure Information Act. (2002). Retrieved from http://www.fas.org/sgp/crs/RL31762.pdf

Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan. (2007). Retrieve from http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf

Department of Defense Standard Practice Documentation of Verification, Validation, and Accreditation for Models and Simulations. (2008). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/500061p.pdf

Dillman, D. A. (2000). *Mail and Internet Surveys: The Tailored Design Method (Second ed.)*. New York: John Wiley & Sons, Inc.

EIA. (2011, December 22, 2011). Energy Information Administration State Energy Profiles - Virginia Data Retrieved December 22, 2011, from http://www.eia.gov/state/state-energy-profiles-data.cfm?sid=VA

Energy: Critical Infrastructure and Key Resources Sector-Specific Plan. (2007). Retrieved from http://www.naruc.org/Publications/Energy_SSP_Public3.pdf

Executive Order 13010: Critical Infrastructure Protection. (1996). Federal Register. Retrieved from http://www.fas.org/irp/offdocs/eo13010.htm

Expert Elicitation. (2011, 18 November 2011 19:27 UTC) Retrieved 23 December 2011 20:10 UTC from http://en.wikipedia.org/w/index.php?title=Expert_elicitation&oldid=461318585

Ezell, B. C. (2007). Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis*, 27(3), 571-583.

Ezell, B. C., Keating, C. B., & Old Dominion University. Dept. of Engineering Management and Systems Engineering. (2005). Quantifying Vulnerability to Critical Infrastructure. Thesis (PhD), Old Dominion University, 2005. Retrieved from http://www.proxy.lib.odu.edu/login?url=http://proquest.umi.com/pqdweb?did=920937791&sid=9&Fmt=2&clientId=3505&RQT=309&VName=PQD

FEMA Releases HAZUS-MH Hurricane Wind Model Validation Study. (2012, Wednesday, 11-Aug-2010 14:32:33 EDT) Retrieved March 27, 2012, from http://www.fema.gov/plan/prevent/hazus/hz_windvalidationstudy.shtm

Fischbeck, P. S. (2001). Improving regulation: cases in environment, health, and safety: Resources for the Future.

Fischhoff, B. (2010). Judgment and decision making. *Wiley Interdisciplinary Reviews: Cognitive Science*, 1(5), 724-735. doi: 10.1002/wcs.65

Fischhoff, B., & Bruine De Bruin, W. (1999). Fifty–Fifty=50%? *Journal of Behavioral Decision Making*, 12(2), 149-163. doi: 10.1002/(sici)1099-0771(199906)12:2<149::aid-bdm314>3.0.co;2-j

Fischhoff, B., De Bruin, W. B., Perrin, W., & Downs, J. (2004). Travel Risks in a Time of Terror: Judgments and Choices. *Risk Analysis*, 24(5), 1301-1309. doi: 10.1111/j.0272-4332.2004.00527.x

Fischhoff, B., Slovic, P., & Lichtenstein, S. (1982). Lay Foibles and Expert Fables in Judgments about Risk. *The American Statistician*, 36(3), 240-255.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How Safe Is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits. *Policy Sciences*, 9(2), 127-152.

Garvey, P. R., & Pinto, C. A. (2009). An index to measure risk co-relationships in engineering enterprise systems. *International Journal of System of Systems Engineering*, 1(3), 22.

Gheorghe, A. V., Masera, M., & Voeller, J. G. (2008). *Critical Infrastructures at Risk: A European Perspective*. Springer.

Global Risks. (2006) (pp. 26): World Economic Forum. Retrieved from https://members.weforum.org/pdf/CSI/Global_Risk_Report.pdf

Global Risks. (2007) (pp. 34): World Economic Forum. Retrieved from https://members.weforum.org/pdf/CSI/Global_Risks_2007.pdf

Global Risks. (2008) (pp. 54): World Economic Forum. Retrieved from https://members.weforum.org/pdf/globalrisk/report2008.pdf

Global Risks. (2009) (pp. 37): World Economic Forum. Retrieved from https://members.weforum.org/pdf/globalrisk/2009.pdf

Global Risks. (2010) (pp. 52): World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2010.pdf

Global Risks. (2011) (pp. 60): World Economic Forum. Retrieved from http://reports.weforum.org/wp-content/blogs.dir/1/mp/uploads/pages/files/global-risks-2011.pdf

Global Risks. (2012) (pp. 64): World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

Google Public Alerts. (2012) Retrieved March 1, 2012, from http://www.google.org/publicalerts

Government Facilities Sector: Critical Infrastructure and Key Resources. (2010, December 29, 2008) Retrieved September 9, 2010, 2010, from http://www.dhs.gov/files/programs/gc_1189011910767.shtm

GWU. (2011). The George Washington University Hospital Retrieved December 22, 2011, from http://www.gwhospital.com

Haimes, Y. Y. (1999). The Role of the Society for Risk Analysis in the Emerging Threats to Critical Infrastructures. *Risk Analysis*, 19(2), 153-157.

Hazus. (2012, Thursday, 23-Feb-2012 22:00:19 EST) Retrieved March 27, 2012, 2012, from http://www.fema.gov/plan/prevent/hazus/index.shtm

HAZUS-MH Riverine Flood Model Validation Study. (2012, Wednesday, 11-Aug-2010 14:33:12 EDT) Retrieved March 27, 2012, 2012, from http://www.fema.gov/plan/prevent/hazus/hz_utfldvalstudy.shtm

Homeland Security Act of 2002. (2002). Retrieved from http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

Homeland Security Advisory System. (2010, September 10, 2010) Retrieved September 11, 2010, 2010, from http://www.dhs.gov/files/programs/Copy_of_press_release_0046.shtm

Homeland Security Presidential Directive 3: Homeland Security Advisory System. (2002). Retrieved from http://www.fas.org/irp/offdocs/nspd/hspd-3.htm

Homeland Security Presidential Directive 5: Management of Domestic Incidents. (2003). Retrieved from http://www.fas.org/irp/offdocs/nspd/hspd-5.html

Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. (2003). Retrieved from http://fas.org/irp/offdocs/nspd/hspd-7.html

Homeland Security Presidential Directive 8: National Preparedness. (2003). Retrieved from http://www.fas.org/irp/offdocs/nspd/hspd-8.html

Homeland Security Presidential Directive 9: Defense of United States Agriculture and Food (2004). Retrieved from http://www.fas.org/irp/offdocs/nspd/hspd-9.html

Huynh, V. N., & Nakamori, Y. (2005). Multi-Expert Decision-Making with Linguistic Information: A Probabilistic-Based Model. Paper presented at the 38th Hawaii International Conference on System Sciences.

Huynh, V. N., Nakamori, Y., Ho, T.-B., & Murai, T. (2006). Multiple-Attribute Decision Making Under Uncertainty: The Evidential Reasoning Approach Revisited. IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A SYSTEMS AND HUMANS, 36(4), 19.

IDS Multicriteria Assessor Quick Guide. (2010). Retrieved from www.eids.co.uk

Information Technology: Critical Infrastructure and Key Resources Sector-Specific Plan. (2007). Retrieved from http://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf

Inquisite. (2011), from http://www.inquisite.com/

Intelligent Decision System. (2010) Retrieved August 13, 2011, 2011, from http://www.e-ids.co.uk/

Interim National Infrastructure Protection Plan. (2005). Retrieved from http://www.michigan.gov/documents/Interim_National_Infrastructure_Protection_Plan_140123_7.pdf

Kaplan, S. (1997). The Words of Risk Analysis. *Risk Analysis*, 17(4), 11.

Kaplan, S., Haimes, Y. Y., & Garrick, B. J. (2001). Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk. *Risk Analysis*, 21(5), 807-807.

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., et al. (1988). The Social Amplification of Risk: A Conceptual Framework. *Risk Analysis*, 8(2), 177-187. doi: 10.1111/j.1539-6924.1988.tb01168.x

Keating, C. B., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A., Safford, R., et al. (2003). System of Systems Engineering. *Engineering Management Journal*, 15(3), 10.

Keating, C. B., Sousa-Poza, A., & Mun, J. H. (2004). System of Systems Engineering Methodology. Engineering Management & Systems Engineering. Old Dominion University.

Lerner, J. S., Gonzalez, R. M., Small, D. A., & Fischhoff, B. (2003). Effects of Fear and Anger on Perceived Risks of Terrorism: A National Field Experiment. *Psychological Science*, 14(2), 144-150.

Lincoln Memorial. (2011a, 22 December 2011 22:40 UTC) Retrieved 22 December 2011 23:01 UTC, from http://en.wikipedia.org/w/index.php?title=Lincoln_Memorial&oldid=467255945

Lincoln Memorial. (2011b, August 24, 2011 at 05:51 MST) Retrieved December 22, 2011, from http://www.nps.gov/linc/index.htm

Luiijf, H. A. M., & Nieuwenhuijs, A. H. (2008). Extensible threat taxonomy for critical infrastructures. *International Journal of Critical Infrastructures*, 4(4), 409-417.

Macal, C. M. (2005, April 7-9, 2005). Model Verification and Validation. Paper presented at the Threat Anticipation: Social Science Methods and Models, The University of Chicago and Argonne National Laboratory.

Maier, M. W. (1998). Architecting principles for systems-of-systems. *Systems Engineering*, 1(4), 267-284. doi: 10.1002/(sici)1520-6858(1998)1:4<267::aid-sys3>3.0.co;2-d

Mallor, F., García-Olaverri, C., Gómez-Elvira, S., & Mateo-Collazas, P. (2008). Expert Judgment-Based Risk Assessment Using Statistical Scenario Analysis: A Case Study—Running the Bulls in Pamplona (Spain). *Risk Analysis*, 28(4), 1003-1019. doi: 10.1111/j.1539-6924.2008.01098.x

McGill, W. L., Ayyub, B. M., & Kaminskiy, M. (2007). Risk Analysis for Critical Asset Protection. *Risk Analysis*, 27(5), 1265-1281.

Millet, I., & Wedley, W. C. (2002). Modelling risk and uncertainty with the analytic hierarchy process. *Journal of Multi-Criteria Decision Analysis*, 11(2), 97-107. doi: 10.1002/mcda.319

Morgan, M. G. (1993). Risk Analysis and Management. *Scientific American*, 269, 32-35+.

Moser, C. A. (1951). Interview Bias. *Revue de l'Institut International de Statistique / Review of the International Statistical Institute*, 19(1), 28-40.

Murdock, C. A., Squeri, M., Jones, C., & Smith, B. S. (2011). Risk Management in Non-DoD US Government Agencies and the International Community. In D. a. N. S. G. Center for Strategic and International Studies (Ed.), (pp. 117).

National Disaster Recovery Framework. (2011). Retrieved from http://www.fema.gov/pdf/recoveryframework/ndrf.pdf

National Infrastructure Protection Plan. (2006). Retrieved from http://www.vet.utk.edu/cafsp/resources/pdf/National%20Infrastrucure%20Protection%20Plan.pdf

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

National Monuments and Icons: Critical Infrastructure and Key Resources Sector-Specific Plan. (2007). Retrieved from http://www.pmcgroup.biz/downloads_files/DHS%20NIPP%20SSP%20National%20Monuments%202009.pdf

National Preparedness Goal. (2011). Retrieved from http://www.fema.gov/pdf/prepared/npg.pdf

National Preparedness Guidelines. (2007). Retrieved from http://www.fema.gov/pdf/emergency/nrf/National_Preparedness_Guidelines.pdf

National Preparedness System. (2011). Retrieved from http://www.fema.gov/pdf/prepared/nps_description.pdf

National Response Framework. (2008). Retrieved from http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

National Response Plan. (2004). Retrieved from http://it.ojp.gov/fusioncenterguidelines/NRPbaseplan.pdf

The National Strategy for Homeland Security. (2002). Retrieved from http://georgewbush-whitehouse.archives.gov/homeland/book/index.html

The National Strategy of the Physical Protection of Critical Infrastructures and Key Assets. (2003). Retrieved from http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

NOAA. (2012a). Fujita Tornado Damage Scale, from http://www.spc.noaa.gov/faq/tornado/f-scale.html

NOAA. (2012b). NCDC Storm Events Retrieved January 2, 2012, 2012, from http://www4.ncdc.noaa.gov/cgi-win/wwcgi.dll?wwEvent~Storms

Norman Hill, K., & Ezell, B. C. (2011). A Risk Quadruplet for Homeland Security. Paper presented at the INFORMS Annual Meeting, Charlotte, NC.

Norman Hill, K., & Gheorghe, A. V. (2011). The Risk Quadruplet: An Integrated Assessment of Threat, Vulnerability, Consequence, and Perception. Paper presented at the Annual International Conference on Infrastructure Systems, Norfolk, VA.

OECD Studies in Risk Management: Innovation in Country Risk Management. (2009) (pp. 45). Retrieved from http://www.oecd.org/dataoecd/33/18/42226946.pdf

One Team, One Mission, Securing Our Homeland: US Department of Homeland Security Strategic Plan Fiscal Years 2008–2013. (2008).

Pennock, M. J., & Haimes, Y. Y. (2002). Principles and guidelines for project risk management. *Systems Engineering*, 5(2), 89-108.

Pinto, C. A. (2006). Challenges to Sustainable Risk Management: Case Example in Information Network Security. *Engineering Management Journal*, 18(1), 8.

Pinto, C. A. (2008). Risk Management. Engineering Management and Systems Engineering. Old Dominion University.

Presidential Decision Directive (PDD-63/NSC-63). (1998). Retrieved from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

Presidential Policy Directive (PPD-8): National Preparedness. (2011). Retrieved from http://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf

Principal Component Analysis. (2010, December 18, 2010) Retrieved December 29, 2010 2010, from http://en.wikipedia.org/w/index.php?title=Principal_component_analysis&oldid=403072267

Quadrennial Homeland Security Review Report. (2010). Retrieved from http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

Regional Resiliency Assessment Program. (2012, March 31, 2010) Retrieved February 12, 2012, from http://www.dhs.gov/files/programs/gc_1265397888256.shtm

Review of the Department of Homeland Security's Approach to Risk Analysis. (2010). Retrieved from http://www.nap.edu/catalog.php?record_id=12972

Risk Perception. (2010, December 17, 2010) Retrieved December 28, 2010, 2010, from http://en.wikipedia.org/w/index.php?title=Risk_perception&oldid=402895750

Risk Steering Committee: DHS Risk Lexicon. (2008). Retrieved from http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf

Risk Steering Committee: DHS Risk Lexicon. (2010). Retrieved from http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

Secretary Napolitano Announces New National Terrorism Advisory System to More Effectively Communicate Information about Terrorist Threats to the American Public. (2011, January 27, 2011) Retrieved April 6, 2011, from http://www.dhs.gov/ynews/releases/pr_1296158119383.shtm

Sheard, S. A., & Mostashari, A. (2009). Principles of complex systems for systems engineering. *Systems Engineering*, 12(4), 295-311. doi: 10.1002/sys.20124

Sjöberg, L. (1999). Risk Perception in Western Europe. *Ambio*, 28(6), 543-549.

Sjöberg, L. (2000). Factors in Risk Perception. *Risk Analysis*, 20(1), 1-12. doi: 10.1111/0272-4332.00001

Skyttner, L. (2005). General Systems Theory: Problems, Perspectives, Practice. *World Scientific.*

Slovic, P. (1987). Perception of Risk. *Science*, 236(4799), 280-285.

Slovic, P. (1999). Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield. *Risk Analysis*, 19(4), 689-701. doi: 10.1111/j.1539-6924.1999.tb00439.x

Slovic, P. (2002). Perception of Risk Posed by Extreme Events. Paper presented at the Risk Management strategies in an Uncertain World, Palisades, New York.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1979). Rating the Risks. *Environment*, 21(3), 14.

Small, D. A., Lerner, J. S., & Fischhoff, B. (2006). Emotion Priming and Attributions for Terrorism: Americans' Reactions in a National Field Experiment. *Political Psychology*, 27(2), 289-298. doi: 10.1111/j.1467-9221.2006.00007.x

Sonmez, M., Yang, J. B., & Holt, G. D. (2001). Addressing the contractor selection problem using an evidential reasoning approach. *Engineering, Construction and Architectural Management*, 8(3), 13.

Starr, C. (1969). Social Benefit versus Technological Risk. *Science*, 165(3899), 1232-1238.

Strategic National Risk Assessment. (2012, December 9, 2011) Retrieved February 12, 2012, from http://www.dhs.gov/xabout/structure/rma-strategic-national-risk-assessment-ppd8.shtm

The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation. (2011). Retrieved from http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf

Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan. (2007). Retrieved from http://www.hsdl.org/?view&did=474328

Triangular Distribution. (2012, 4 February 2012 21:43 UTC), from http://en.wikipedia.org/w/index.php?title=Triangular_distribution&oldid=475025000

Turner, B. A. (1994). The Future for Risk Research. *Journal of Contingencies and Crisis Management*, 2(3), 146-156. doi: 10.1111/j.1468-5973.1994.tb00037.x

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. (2001). Retrieved from http://epic.org/privacy/terrorism/hr3162.html

Validation of HAZUS Hurricane Model during Ike. (2012, 10/13/2010 11:40 AM) Retrieved March 27, 2012, 2012, from http://www.fema.gov/library/viewRecord.do?id=4133

Vamanu, D. V., Gheorghe, A. V., Acasandrei, V. T., & Vamanu, B. I. (2011). Environmental modelling for blue collars. *International Journal of Environment and Pollution*, 46(3/4), 21.

Wang, J., Yang, J. B., & Sen, P. (1996). Multi-person and multi-attribute design evaluations using evidential reasoning based on subjective safety and cost analysis. *Reliability Engineering and System Safety*, 52(1996), 16.

Washington Metropolitan Area. (2012, 20 December 2011 02:06 UTC) Retrieved 2 January 2012 21:01 UTC, from http://en.wikipedia.org/w/index.php?title=Washington_Metropolitan_Area&oldid=466796092

Wellerstein, A. (2012). NukeMap Retrieved February 18, 2012, from http://nuclearsecrecy.com/nukemap/

Willis, H. H. (2007). Guiding Resource Allocations Based on Terrorism Risk. *Risk Analysis*, 27(3), 597-606. doi: 10.1111/j.1539-6924.2007.00909.x

Willis, H. H., DeKay, M. L., Fischhoff, B., & Morgan, M. G. (2005). Aggregate, Disaggregate, and Hybrid Analyses of Ecological Risk Perceptions. *Risk Analysis*, 25(2), 405-428. doi: 10.1111/j.1539-6924.2005.00599.x

Wright, G., Bolger, F., & Rowe, G. (2002). An Empirical Test of the Relative Validity of Expert and Lay Judgments of Risk. *Risk Analysis*, 22(6), 1107-1122. doi: 10.1111/1539-6924.00276

XKCD. (2010). Conditional Risk: xkcd: A webcomic of romance, sarcasm, math, and language.

Xu, D.-L. (2004). An Analysis on Whether UK Should Join the Euro: the "Intelligent Decision System" Solution.

Xu, D.-L., & Yang, J.-B. (1999). Intelligent Decision System via Evidential Reasoning. Paper presented at the ACE Software Group Meeting.

Xu, D.-L., & Yang, J.-B. (2001). Introduction to Multi-Criteria Decision Making and the Evidential Reasoning Approach (M. S. o. Management, Trans.) (pp. 21): University of Manchester Institute of Science and Technology.

Xu, D.-L., & Yang, J.-B. (2003). Intelligent Decision Systemfor Self-Assessment. Journal of Multi-Criteria Decision Analysis, 12, 18.

Xu, D.-L., & Yang, J.-B. (2005). Intelligent decision system based on the evidential reasoning approach and its applications. *Journal of Telecommunications and Information Technology*, 3, 8.

Xu, D.-L., Yang, J.-B., & Wang, Y.-M. (2005). The evidential reasoning approach for multi-attribute decision analysis under interval uncertainty. *European Journal of Operational Research*, 174(2006), 30.

Yang, J.-B. (1999). Rule and Utility Based Evidential Reasoning Approach for Multiattribute Decision Analysis Under Uncertainties. *European Journal of Operational Research*, 131(2001), 31.

Yang, J.-B., & Xu, D.-L. (2002). On the Evidential Reasoning Algorithm for Multiple Attribute Decision Analysis Under Uncertainty. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 32(3), 16.

Yang, J.-B., & Xu, D.-L. (2004). Intelligent Decision System for Supplier Assessment. Paper presented at the International Federation for Infomation Processing Working Group 8.3: Decision Support Systems, Prato, Italy.

Yang, J. B., Dale, B. G., & Siow, C. H. R. (2001). Self-assessment of excellence: an application of the evidential reasoning approach. *International Journal of Production Research*, 39(16), 24.

Yang, Z. L., Wang, J., Bonsall, S., & Fang, Q. G. (2009). Use of Fuzzy Evidential Reasoning in Maritime Security Assessment. *Risk Analysis*, 29(1), 95-120. doi: 10.1111/j.1539-6924.2008.01158.x

Zhou, M., Liu, X.-B., & Yang, J.-B. (2010). Evidential reasoning-based nonlinear programming model for MCDA under fuzzy weights and utilities. *International Journal of Intelligent Systems*, 25(1), 31-58. doi: 10.1002/int.20387

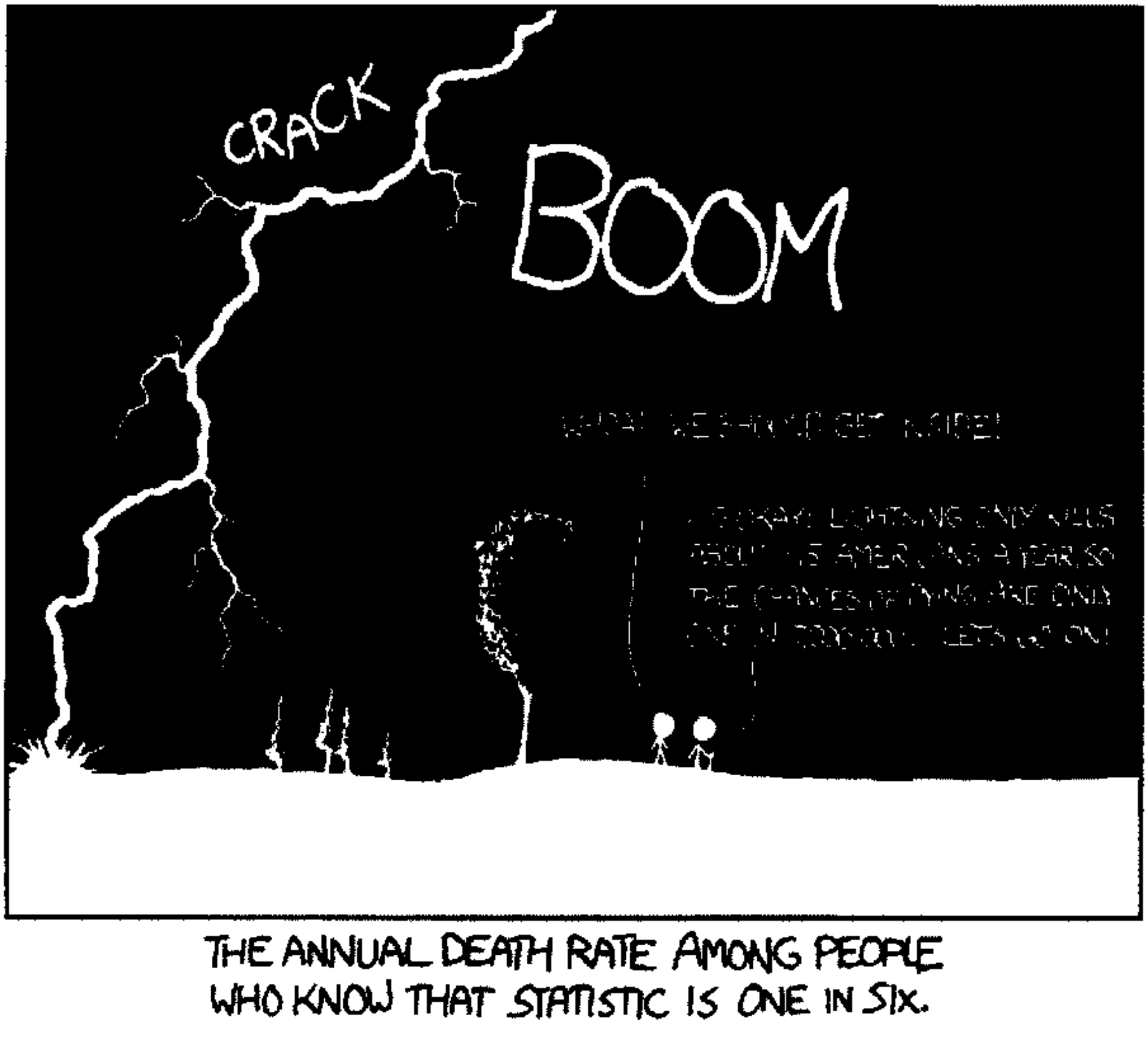

CRACK
BOOM
WHOA! WE SHOULD GET INSIDE!
IT'S OKAY! LIGHTNING ONLY KILLS ABOUT 45 AMERICANS A YEAR, SO THE CHANCES OF DYING ARE ONLY ONE IN 7,000,000. LET'S GO ON!
THE ANNUAL DEATH RATE AMONG PEOPLE WHO KNOW THAT STATISTIC IS ONE IN SIX.

Figure 5.2. Conditional Risk (XKCD, 2010)

APPENDICES

APPENDIX A

GLOBAL RISKS REPORTS ANALYSIS

Table A.1. Global Risks Reports: Core Global Risks by Year

2006	2007	2008	2009	2010	2011	2012
[illegible]						
Asset prices/Indebtedness	Blow up in asset prices/excessive indebtedness	Asset price collapse	Asset price collapse	Asset price collapse	Asset price collapse	
China	Chinese economic hard landing	Slowing Chinese economy (6%)	Slowing Chinese economy (6%)	Slowing Chinese Economy (<6%)	Slowing Chinese economy (<6%)	
Coming fiscal crises	Fiscal crises caused by demographic shift	Fiscal crises in advanced economies	Fiscal crises	Fiscal crises	Fiscal crises	
Oil prices/energy supply	Oil price shock/energy supply interruptions	Oil and gas price spike	Oil and gas price spike	Oil price spikes		
US Current Account deficit and US dollar	US current account deficit/fall in US$	Major fall in US$	Major fall in US$	Major Fall in the US $		
Critical infrastructures			Underinvestment in infrastructure	Underinvestment in infrastructure	Infrastructure fragility	Prolonged infrastructure neglect
		Retrenchment from globalization (developed)	Retrenchment from globalization (developed)	Retrenchment from globalization (developed)	Retrenchment from globalization	
		Retrenchment from globalization (emerging)	Retrenchment from globalization (emerging)	Retrenchment from globalization (emerging)		

Economic						
2006	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**
			Food price volatility	Food price volatility		
			Regulation cost	Burden of regulation	Regulatory failures	Unforeseen negative consequences of regulations
					Liquidity/credit crunch	Recurring liquidity crises
					Extreme energy price volatility	Extreme volatility in energy and agriculture prices
					Global imbalances and currency volatility	Chronic fiscal imbalances
					Extreme commodity price volatility	
					Extreme consumer price volatility	
						Unmanageable inflation or deflation
						Chronic labour market imbalances
						Hard landing of an emerging economy
						Major systemic financial failure
						Severe income disparity
Environmental						
Climate change	Climate change	Extreme climate change related weather	Extreme climate change-related weather	Extreme weather	Climate change	Persistent extreme weather

2006	2007	2008	2009	2010	2011	2012
Tropical cyclones	Natural catastrophE Tropical storms	NatCat: Cyclone	Natural catastrophE cyclone	NatCat: Cyclone	Storms and cyclones	
Earthquakes	Natural catastrophE Earthquakes	NatCat: Earthquake	Natural catastrophE earthquake	NatCat: Earthquake	Earthquakes and volcanic eruptions	
Loss of ecosystem services						
	Natural catastrophE Inland flooding	NatCat: Extreme inland flooding	Natural catastrophE inland flooding	NatCat: Inland flooding	Flooding	
	Loss of freshwater services	Loss of freshwater	Loss of freshwater	Water scarcity		
		Heatwaves & droughts	Droughts and desertification reduces agricultural yields	Droughts and desertification		
			Natural catastrophE coastal flooding	NatCat: Coastal flooding		
			Air pollution	Air pollution	Air pollution	Irremediable pollution
						Rising greenhouse gas emissions
			Biodiversity loss	Biodiversity loss	Biodiversity loss	Species overexploitation
					Ocean governance	
						Land and waterway use mismanagement
						Mismanaged urbanization
						Vulnerability to geomagnetic storms

2006	2007	2008	2009	2010	2011	2012
						Unprecedented geophysical destruction
						Antibiotic-resistant bacteria
						Failure of climate change adaptation
[illegible]						
Terrorism	International terrorism	International terrorism	International terrorism	International terrorism	Terrorism	Terrorism
European dislocation						
Current and future hotspots						
	Transnational crime and corruption	Transnational crime and corruption	Transnational crime and corruption	Transnational crime and corruption	Organized crime	Entrenched organized crime
					Corruption	Pervasive entrenched corruption
	Interstate and civil wars	Interstate & civil wars				
	Proliferation of weapons of mass destruction (WMD)				Weapons of mass destruction	Diffusion of weapons of mass destruction
	Retrenchment from globalization					
	Failed and failing states	Failed & failing states			Fragile states	Critical fragile states
		Collapse of Non-Proliferation Treaty of Nuclear Weapons	Collapse of Non-Proliferation Treaty of Nuclear Weapons	Nuclear proliferation		
	Middle East instability	Middle East instability	Afghanistan instability	Afghanistan instability	Geopolitical conflict	

2006	2007	2008	2009	2010	2011	2012
			Israel-Palestine conflict	Israel - Palestine		
			Violence in Iraq	Iraq		
			US/Iran conflict	Iran		
			US/Democratic People's Republic of Korea conflict	North Korea		
			Global governance gaps	Global governance gaps	Global governance failures	Global governance failure
					Space security	Militarization of space
					Illicit trade	Widespread illicit trade
						Failure of diplomatic conflict resolution
						Unilateral resource nationalization
Societal						
Global pandemics	Pandemics	Pandemic	Pandemic	Pandemic		Vulnerability to pandemics
Epidemic disease (developing world)	Infectious diseases in the developing world	Infectious disease, Pandemic, developing world	Infectious disease	Infectious diseases	Infectious diseases	
Slow and chronic diseases (industrialized world)	Chronic disease in the developed world	Chronic disease, developed world	Chronic disease	Chronic diseases	Chronic diseases	Rising rates of chronic disease
Liability regimes	Liability regimes	Liability regimes	Liability regimes	Liability regimes		
Regulation						
Corporate governance						
Intellectual Property rights						
Organized crime						

2006	2007	2008	2009	2010	2011	2012
		Food insecurity			Food security	Food shortage crises
			Migration	Migration	Migration	Unmanaged migration
					Water security	Water supply crises
					Demographic challenges	Mismanagement of population aging
						Unsustainable population growth
					Economic disparity	
						Backlash against globalization
						Ineffective drug policies
						Rising religious fanaticism
Technological						
Nanotechnology	Emergence of risks associated with nanotechnology	Emergence of nanotechnology risks	Emergence of nanotechnology risks	Nanoparticle toxicity		Unintended consequences of nanotechnology
Electromagnetic fields						
Pervasive computing						
Convergence of technologies						
	Breakdown of critical information infrastructure (CII)	CII breakdown	Critical Information Systems (CII) breakdown	Critical information infrastructure (CII) breakdown	Critical information infrastructure breakdown	Critical systems failure
			Data fraud/loss	Data fraud/loss		Massive incident of data fraud or theft

2006	2007	2008	2009	2010	2011	2012
					Online data and information security	Cyber attacks
					Threats from new technologies	Unintended consequences of new life science technologies
						Massive digital misinformation
						Proliferation of orbital debris
						Mineral resource supply vulnerability
						Unintended consequences of climate change mitigation
						Failure of intellectual property regime

APPENDIX B

RESEARCH LIMITATIONS (IN VIVO)

Phase 1. Perception Assessment

"The fear of death is the most unjustified of all fears, for there's no risk of accident for someone who's dead."
– Albert Einstein

Data Collection

The first phase (the perception assessment) must consider a means for collecting perception data, the framework for obtaining that data, the selection of respondents who will voluntarily contribute their perceptions, as well as an approach for analyzing the perception data once it is collected. Expert elicitation is a way to gather the opinions of experts, often seeking a consensus, regarding a subject characterized by uncertainty, usually due to insufficient data ("Expert Elicitation," 2011). For that reason, it seems like a logical approach for gathering perceptions.

Expert elicitation is often used when researching rare events, which typically lack adequate data to conduct more traditional probabilistic approaches ("Expert Elicitation," 2011). Expert opinion is also used when observation, experimentation, or simulation is not possible due to limited resources. Subject matter experts are employed to estimate new, uncommon, or complicated issues and may also be utilized to forecast future outcomes. Multiple methods exist to elicit expert judgments, such as focus groups, surveys, interviews, or even interactive exercises like wargames (Ancel, 2011).

A common goal of expert elicitation is to quantify uncertainty ("Expert Elicitation," 2011), which lends the technique nicely to risk analysis. There is also a precedence for employing expert elicitation techniques to the research and design of next generation infrastructure (Ancel, 2011), but it is not without its flaws and limitations. Research on risk judgments usually shows that expert judgments are more valid or accurate than those of the general public (Wright, Bolger, & Rowe, 2002). However, it has been shown that lay people are not completely irrational or inaccurate in their judgments of risk-related values (Baruch Fischhoff, Slovic, & Lichtenstein, 1982). The selection of respondents for the perception assessment will be important and it will be important to note whether participants are considered experts, non-experts, or a mix of both.

It will also be important to determine how to aggregate perception assessment results. If perception data is to be collected via expert elicitation, then the number of perception values produced is dependent upon the number of survey respondents. And the number of values for the threat, vulnerability, and consequence assessments would not depend on the number of respondents, so synthesizing those two different sized data sets could pose a problem during the assessment integration phase.

Early work on perception models focused on the variation among means of perception ratings across multiple risk scenarios and did not examine the variation among the individual respondents (those rating the risks). This means that, for better or worse, higher levels of explanatory power can be achieved by stabilizing the means through large samples (Lennart Sjöberg, 1999). However, some perception models have been scrutinized for their use of aggregate data (versus disaggregate data), but it is generally recognized that using disaggregate data changes the focus of the analysis to an exploration of the distinctions among respondents, rather than an exploration of the distinctions among risk scenarios (Henry H. Willis, DeKay, Fischhoff, & Morgan, 2005). Since the purpose of this research is not to explore the differences between the perceptions of individual respondents, but rather to explore the differences of their collective perceptions across a series of combinations of CIKRKA and risk scenarios, this should not have an impact on the research.

Another challenge to overcome is bias as numerous studies have shown inherent biases in perception data. There is often a difference between perceived personal risk (risk to oneself) and perceived general risk (risk to others), where general risk is usually judged to be higher, especially those risks perceived as uncontrollable along the Controllable – Uncontrollable risk scale (Lennart Sjöberg, 1999). Also, women tend to rate risks higher than men (Lennart Sjöberg, 1999). It is important to note that some studies have shown that demographic and other participant factors were very weakly related to perception (L. Sjöberg, 2000).

And not only can bias be introduced in the perception data, but also in the expert elicitation tool, itself. Survey studies often display a bias, especially in terms of the respondents' educational levels, but that bias does not appear to be serious in studies of perception (L. Sjöberg, 2000). One alternative to a survey might be structured interviews although there is no evidence that suggests that interviews are more valid than surveys (Lennart Sjöberg, 1999). And while survey questions might introduce bias (Dillman, 2000), an interviewer could also introduce bias (Moser, 1951). Furthermore, there is always a risk of low response rates for any survey (Dillman, 2000), and sample sizes for focus groups or interviews are typically much smaller due to limited resources and time constraints (Moser, 1951), so generalizability and interpolation to the rest of the population is limited, especially since the sample may not be representative of the entire population, given the respondents will primarily be subject matter experts.

Respondents would likely be volunteers, so response rates may be low. Requests for participation could be announced via email and websites to public organizations that share common interests in homeland security, homeland defense, Critical Infrastructure Protection (CIP), risk, threat, vulnerability, and consequence assessments, risk management, risk mitigation, risk analysis, and Emergency Preparedness, Response, and Recovery (EPR&R). As a result, many of these potential respondents would be subject matter experts, so the perceptions gathered would be those of experts.

We are then assuming some level of homogeneity across the respondents, which might not be the case if we selected non-experts to provide their perceptions. Future research might explore a comparison of the risk quadruplet eliciting subject matter expert perceptions versus common citizen perceptions. Or, perhaps both types of respondents should participate in the perception assessment phase in order to seek a more complete picture of the perceived risks to the assets under study. The in vivo risk quadruplet methodology is easily adaptable to exploring these alternatives in the future.

Other concerns affecting the data collection methodology are the scope of the research. We will need perceptions within the context of CIKRKA, but how many types of CIKRKA can be explored in a survey? A reduced number of assets must be selected to the risk quadruplet research. Should the data be collected via survey or focus group, and would it make sense to use a blocked experimental design where a certain percentage of respondents explore CI, the next group provides data on KR, and so on? Furthermore, how many combinations of threats and assets should be studied? Will each respondent focus on one scenario, perhaps a power plant asset combined with a terrorist attack threat? Or will a list of potential threats be used to gauge perceptions of the asset overall, like a power plant subjected to threats of flood, earthquake, tornado, insider threat, and terrorist attack?

Perception Models

The models typically used for collecting and analyzing perception data are the Social Amplification of Risk Framework, the Cultural Theory Model, and the Psychometric Model. There are pros and cons to each methodology, so they will be explored and the final perception model will be selected accordingly. This research will explore how a perception model performs when applied to CIKRKA, but also how the resulting data can be integrated with threat, vulnerability, and consequence data, so those constraints will affect our decision and determine which model is selected for the risk quadruplet.

Social Amplification of Risk Framework

The social amplification of risk framework is an interdisciplinary approach, combining psychology, sociology, anthropology, and communications ("Risk Perception," 2010). It assumes that communications of risk events travel from the sender to the receiver through intermediate stations (such as individuals, groups, and the media) and in that process, the receiver's perceptions are amplified or diminished. The framework attempts to ascertain why some risks are considered more important and thus receive public attention, and why other risks are considered less important and thus receive little to no public attention ("Risk Perception," 2010). While interesting, this framework seems inappropriate and overly complicated for this research, which is less interested in the impacts of risk communication and more interested in the perception of risks from certain risk scenarios to CIKRKA.

Cultural Theory Model

The cultural theory model assumes that people choose to worry about certain risk scenarios based on their social engagements and the model tends to link world views (egalitarian, hierarchy, individualistic, and fatalistic) and perceptions using group and grid indices (Lennart Sjöberg, 1999). Group indices measure one's membership in certain groups and one's freedom of expressing opinions differing from the norm, whereas grid indices measure one's respect for others, specifically authority figures. This model usually only explains approximately 5%-10% of the variance of perceived risk (Lennart Sjöberg, 1999), and again it does not appear to lend itself to easily gauging perceptions of CIKRKA.

Psychometric Model

Psychometrics is a field that studies the measurement of knowledge, perception, abilities, or personality characteristics. The psychometric model appears to be the preferred method for studying perceptions of risk. According to the traditional psychometric model approach, perception is a function of risk scales, usually nine dimensions (Slovic, Fischhoff, & Lichtenstein, 1979):

1. Voluntary – Involuntary
2. Chronic – Catastrophic
3. Common – Dread
4. Certainly Not Fatal – Certainly Fatal
5. Known to Exposed – Unknown to Exposed
6. Immediate – Delayed
7. Known to Science – Unknown to Science
8. Uncontrollable – Controllable
9. New – Old

Using this approach up to approximately 85% of the (aggregate) variance in risk ratings can be explained (Henry H. Willis, et al., 2005). However, the psychometric model has been scrutinized for its use of aggregate data (versus disaggregate data). It is true that the psychometric method explains less variance when data are not averaged over participants prior to analysis. But, it is generally recognized that using the psychometric model for disaggregate data changes the focus of the analysis to an exploration of the distinctions among participants, rather than an exploration of the distinctions among risk scenarios (Henry H. Willis, et al., 2005). The traditional psychometric model is focused on aggregate-level risk scenario-focused analysis, which is the goal of this research. Should the psychometric model be selected, the data will be aggregated to emphasize the distinctions between risk scenarios (Henry H. Willis, et al., 2005).

But are the nine traditional risk scales (Slovic, et al., 1979) still valid for homeland security and CIKRKA? In addition to the nine traditional risk scales previously mentioned, the psychometric model can be further improved by including another risk scale, described as “Tampering with Nature” or “Immoral Risk” (Lennart Sjöberg, 1999). This risk scale might be explained as “Natural – Unnatural” where natural risk scenarios fall on one extreme and terrorism falls along the other, with manmade accidents perhaps falling somewhere near the unnatural end of the scale. This scale could be used to address the all-hazards approach to homeland security and homeland defense that must deal with EPR&R to both natural hazards, as well as accidents and terrorist attacks. And for the purposes of our research, perhaps a new scale could be introduced, something along the lines of “CIKR – KA” where the extremes are used to determine whether the type of asset affects risk perceptions.

For the past quarter century, research on perception has been dominated by Slovic, Fischhoff, and Liechtenstein’s psychometric model. Traditionally, participants rank a large number of risk scenarios with regard to their perceived benefit to society, perceived risk (personal and/or social), the acceptability of the current risk, and their position along each of the nine risk scales (Bronfman & Cifuentes, 2003; B. Fischhoff, Slovic, Lichtenstein, Read, & Combs, 1978; Slovic, et al., 1979). The ratings of the nine risk scales are averaged over participants and the resulting risk scenario versus dimension matrix is analyzed, often using principal component analysis since many of the risk scales tend to be inter-correlated.

Principal component analysis is a mathematical procedure that converts a set of correlated variables to a set of uncorrelated variables, or principal components, where the number of principal components is always less than or equal to the number of original variables ("Principal Component Analysis," 2010). The principal components are selected to account for as much of the variability in the data as possible, subject to the constraint that they are uncorrelated with each other ("Principal Component Analysis," 2010). These principal components can then be used in regression analyses.

Principal components analysis can be used to explain the variation in risk ratings (including variation unique to individual attributes) by factoring out the principal components (comprised of the correlated risk scales) which are often named for their shared characteristics, such as dread risk or unknown risk. Typically, a few components or factors account for a majority of the variation (Slovic, 1987). These principal components are then used as independent variables in regressions to predict the mean ratings of pertinent dependent variables, such as perceived benefit to society, perceived risk (personal and/or social), and the acceptability of the risk. Principal components analysis seems like an unnecessary step in the psychometric model, at least for the purposes of this research as this additional analysis would not likely be needed for the MCDA model selected for the assessment integration.

The psychometric model is often used to explore perceptions, and an interesting example is given for Chile (Bronfman & Cifuentes, 2003). The study examined risk scenarios along 16 risk scales: Newness, Voluntariness, Catastrophic Potential, Dread, Immediacy, Severity, Social Knowledge, Social Control, Social Benefit, Number of Exposed People, Personal Knowledge, Personal Control, Personal Benefit, Personal Effect, Current Regulation Status, and Desired Regulation. These were defined and rated on 7 or 10 point rating scales (psychometric scales often used with questionnaires). Three risk constructs were explored, including social risk, personal risk, and acceptability. Finally, 54 risk scenarios were analyzed, grouped by type of risk scenario, and each risk scenario was scored along the risk scales and risk constructs in a survey. The design was blocked into four surveys and administered to approximately 500 people, only 100 of which actually completed all four surveys (Bronfman & Cifuentes, 2003).

Once the data was collected, principal components analysis was performed and three main factors were identified. Factor 1 (Dread Risk) included Catastrophic Potential, Dread, Severity, Voluntariness, and Social Control. Factor 2 (Unknown Risk) included Social Knowledge, Newness, and Immediacy. Factor 3 (Personal Effect) included Number of Exposed People, and Personal Effect. Additional analysis compared social versus personal results, using regression models with the three factors to model personal risk, social risk, and risk denial (the difference of the two). Analysts also conducted regressions using the three factors to model acceptability, desired regulation, and the difference between the desired regulation and the current regulation.

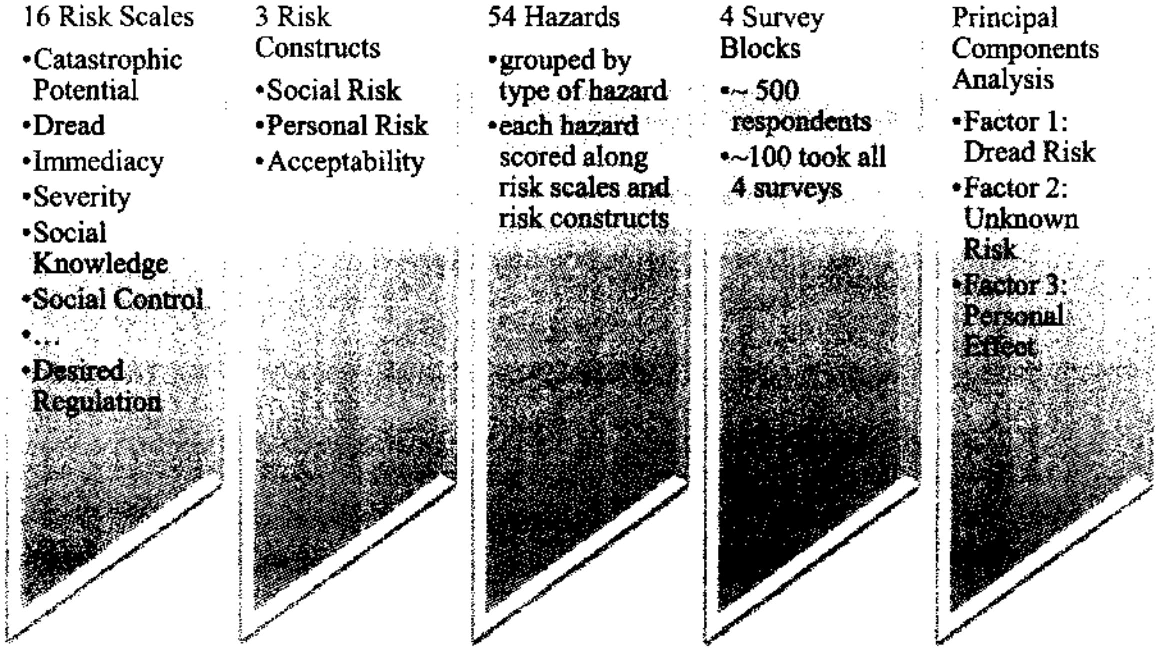


Figure B.1. Psychometric Model Example

Using this example as a guideline for the first phase of the risk quadruplet methodology might be the most appropriate application of a risk assessment methodology to the risk quadruplet. Participants could be asked to rate a number of risk scenarios, specific to CIKRKA along a series of risk scales. Mean ratings could be computed for each risk scenario along each scale. The resulting risk scenarios versus risk scales matrix could be analyzed using principal components analysis to determine which factors explain the most variance. The survey could be limited to social risk scales and risk constructs. It may not be possible to test so many risk scenarios, but it may be possible to test a small sample of natural and unnatural risk scenarios, perhaps using a taxonomy to randomly select risk scenarios. The survey design could be blocked into three surveys, one each for CI, KR, and KA, so that perceptions could be compared and contrasted across asset type. The CIKRKA could even be randomly selected from the DHS Infrastructure Data Taxonomy (IDT).

However, given the many challenges discussed already, a full blown psychometric model may not be possible or even necessary. While the psychometric model is probably the best candidate for collecting and analyzing perception data for CIKRKA, that is not the only goal of this research. The other goal of this research is to determine a risk quadruplet methodology for integrating threat, vulnerability, consequence, and perception assessments, ultimately ranking CIKRKA based on that integrated assessment. The outcomes of the traditional psychometric model may not be compatible with the assessment integration model selected for the third phase of the risk quadruplet.

It is common to use questionnaire studies to consider the levels of acceptable risk or the perceived seriousness of a wide variety of natural and man-made hazards (B. Fischhoff, et al., 1978). And expert judgment-based risk methodologies might use descriptive words like high, medium, or low to describe the characteristics that play a role in the risk scenario (Mallor, García-Olaverri, Gómez-Elvira, & Mateo-Collazas, 2008). Therefore, a reduced psychometric model, based on a much simpler questionnaire that elicits qualitative expert judgments could still be a valid perception assessment approach for the purposes of this research.

So, after reviewing the risk perception models available to us, the psychometric model seemed like the most appropriate candidate for the first phase of the in vivo risk quadruplet methodology. However, given the ER model and IDS software selected for the assessment integration phase, a full blown psychometric model seems unnecessary, especially as it would not provide data immediately compatible with ER, the selected assessment integration model. Therefore, a reduced psychometric model, based on a much simpler questionnaire that elicits qualitative expert judgments will be employed for the purposes of the risk quadruplet methodology. Inquisite provides a survey tool for designing and deploying the survey, as well as for collecting the perception data. IDS provides a data input tool and data warehouse for us to load the perception data after it has been collected. This risk quadruplet methodology will be discussed further in APPENDIX D.

Technology

Many of the research limitations discussed in the first phase of the risk quadruplet would drastically affect the collection of perceptions. Concerns such as respondent selection and participation, as well as the design of a survey (or other data collection tool) could greatly impact the type and amount of data able to be collected. The data collection tool and analysis could become unwieldy if multiple assets and risk scenarios are considered. And while blocking by CIKRKA may reduce respondent burden, it could pose a technological challenge whether disseminating a survey or conducting a focus group. All of these matters will be intertwined with the perception model chosen, as well as the technology available at the time of the study.

Regardless of the data collection methodology, or the model selected, the first phase of the risk quadruplet will require a means to assess perceptions. Technology can be used to assist with some of these challenges. Inquisite is software that can be used to design and deploy surveys, collect data, as well as analyze respondent data ("Inquisite," 2011). Using this software it would be possible to select a sample of experts and ask them a series of perception questions tailored to fit the models selected for the first and third phases of the risk quadruplet methodology.

Phase 2. Threat, Vulnerability, and Consequence Assessments

> *"The dangers of life are infinite, and among them is safety."*
> – Goethe

Data Collection

Understanding the different types of threat, vulnerability, and consequence assessment data, whether those data are available to be leveraged, collected, or simulated is extremely important to the risk quadruplet methodology. One option would be to leverage data from threat, vulnerability, and consequence assessments. However, risk data are not often collected or displayed consistently. However, risk data are often not collected or displayed consistently. This data could still contain an element of subjectivity, depending on how the assessments were conducted, but it could also incorporate objective data. For example, if the risk scenario under study was flooding, there is historical data available on the impact of flooding to a particular region and its assets. There would be documented information on the consequences such as causalities or cost to repair damages. It might even be possible to determine whether any recommended fortifications provided additional security against flood damage over the years to provide some insight on vulnerabilities. These assessments might provide scores, which could be used directly or which could be coded to a linguistic set, similar to one used for collecting perception data. Assessments that use risk scores are rarely normalized, so comparing a risk score from one study to that from another study is like comparing apples to oranges. For example, some may calculate risk where threat has an associated threat severity probability distribution, vulnerability is a conditional probability (the probability of a successful attack, given the attack is identified), and consequence is based on some loss function (McGill, Ayyub, & Kaminskiy, 2007). Other assessments use risk words like low, medium, or high, or color coding like red, yellow, or green to describe the severity of a risk. For example, expert judgment-based risk methodologies might use descriptive words like high, medium, or minimal to describe certain characteristics that play a role in the threat scenario (Mallor, et al., 2008). However, access to this type of information is obviously restricted due to its sensitivity.

If the data are not available, it is possible that those assessments could be conducted to produce results, but this would have a significant impact on the time and scope of the research. We could attempt to collect that data during the perception assessment phase of the risk quadruplet methodology, but that would again impact the time and scope of the research. Additionally, it could make it more difficult to segregate perception data from threat, vulnerability, and consequence data. We would basically be forced to collect perception data on the impact of a risk scenario to CIKRA, as well as perception data on threat, vulnerability, and consequence to CIKRA. Actual threat, vulnerability, and consequence assessments might rely in part on subject matter expertise, but could also contain quite a bit of objective data, as well, so relying solely on perceptions would defeat the purposes of integrating threat, vulnerability assessments with perception assessments.

The goals of this research are to assess perceptions of CIKRKA, determine a methodology for integrating threat, vulnerability, and consequence assessments with the CIKRKA perception assessment, and to ultimately rank those CIKRKA accordingly (Figure 1.3). Therefore, it is not within the scope of this research to determine a methodology to collect (or to translate leveraged) threat, vulnerability, or consequence data. These assessments are already being conducted by asset owners and operators, DHS, or DoD. We can assume that real-world data for threat, vulnerability, and consequence assessments exists and could be fit to our model, allowing us to focus on how to integrate that data with the perception data.

Phase 3. Assessment Integration

"Living at risk is jumping off the cliff and building your wings on the way down."
– Ray Bradbury

The final phase (assessment integration) is the most crucial. Many approaches exist that could integrate these disparate perception, threat, vulnerability, and consequence assessments. Based on the goals of this research, the result of this phase of the risk quadruplet methodology must be a ranking of CIKRA from highest risk to lowest risk (Figure 3.5).

Multi Criteria Decision Analysis Models

The research is dependent upon the MCDA model used to integrate the threat, vulnerability, consequence, and perception assessments. Options for an integrated risk quadruplet assessment methodology include AHP, ANP, ER, and MAUT. However, each of these approaches would require complex software. The research may be limited based on the availability of software at the time of analysis. It is valuable to analyze these different alternatives in order to select the most appropriate MCDA model.

Analytic Hierarchy Process

There are benefits to using AHP and there is precedence for using it to assess risk (Millet & Wedley, 2002). The hierarchy provides a means for systematically evaluating the complex problem of ranking CIKRKA. It also provides a method for quantifying the relative weights of different criteria and factors making it easier to compare incommensurable items (such as CI versus KA; or loss of life versus loss of money).

However, AHP is not without criticism. When ranking alternatives in terms of their attributes, some experts would argue that as new alternatives are added to a problem, the ranking of the old alternatives must not change, in other words, rank reversal should not be permitted. But, as we know all too well, especially in the realm of homeland security and homeland defense, new alternatives do (and should) cause rank reversal sometimes. For example, the September 11th terrorist attacks were considered a black swan event, unforeseeable, and forever changing the landscape of threat, vulnerability, and consequence assessments for CIKRKA. Most AHP software can handle both approaches, either allowing for rank reversal or not, depending on the preference of the user.

Furthermore, AHP is sensitive to the hierarchical model proposed. If the model is incomplete, or otherwise inadequate, then all results of the AHP would be questionable. The AHP model would need to be vetted with stakeholders and experts, in the hopes of adequately reflecting the complex decision making problem of integrating threat, vulnerability, consequence, and perception assessments to rank CIKRKA. If AHP were selected for this research, Figure B.2 offers an example of our potential model. The goal would be to rank CIKRKA using threat, vulnerability, consequence, and perception assessments.

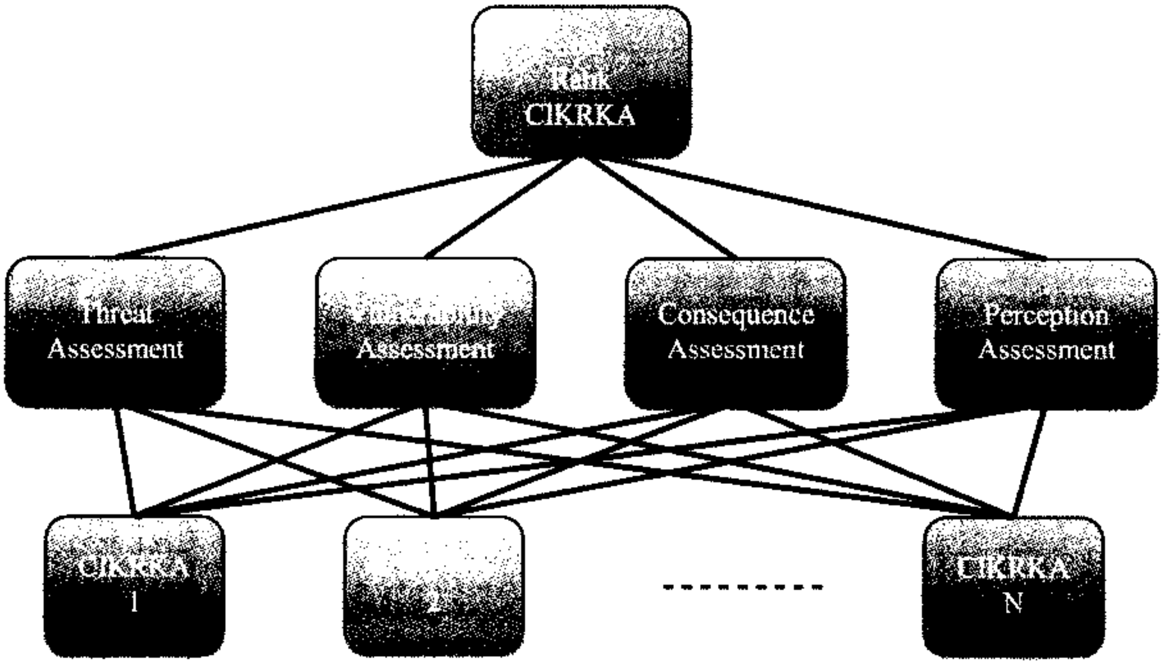
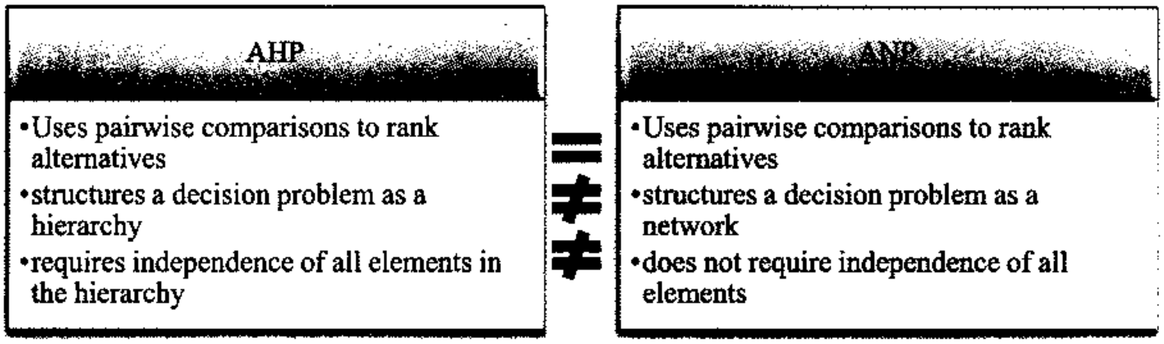


Figure B.2. Analytic Hierarchy Process Example

Analytic Network Process

While both AHP and ANP use pairwise comparisons to measure weights and rank alternatives, there are some fundamental differences between these two approaches (Figure B.3). AHP structures a decision problem as a hierarchy with a goal, decision criteria, and alternatives. It also requires independence of all elements in the hierarchy, so the decision criteria must be independent, and the alternatives to be considered must also be independent, not only from each other, but also from the decision criteria. ANP, on the other hand, does not require independence among elements. Often there is interdependence among alternatives and decision criteria, so this is an improvement over AHP. The way ANP handles this is to structure the decision problem as a network, which might be useful for the purposes of our research as threat, vulnerability, consequence, and perception are most likely interrelated, not independent.



AHP

- Uses pairwise comparisons to rank alternatives
- structures a decision problem as a hierarchy
- requires independence of all elements in the hierarchy

=

≠

≠

ANP

- Uses pairwise comparisons to rank alternatives
- structures a decision problem as a network
- does not require independence of all elements

Figure B.3. Analytic Hierarchy Process versus Analytic Network Process

Multi Attribute Utility Theory

MAUT builds utility functions for multiple attributes, independently, then combines these utility functions using weighted multi attribute models (additive models are common, but more complicated models exist). Next, one must determine the indifference probability between a sure thing and a gamble. This requires strong assumptions of independence, including (mutual) preferential independence and (mutual) utility independence.

Attribute Y is preferentially independent of X if preferences for specific outcomes of Y do not depend on the level of X. For example, say that Y is number of days to complete a job, maybe 5 or 10 days. And the cost to perform the job, X, is either $100 or $200. Assume that the cost is $100 no matter what, whether it takes 5 days or 10 days. If we prefer a 5 day time frame, then even if we raise the cost to $200 (again, for both 5 and 10 days), then we would still prefer 5 days. In this case, Y is preferentially independent of X. For mutual preferential independence, we also need X to be preferentially independent of Y, so we need to prefer the lower cost, no matter how many days it takes to perform the job.

Utility independence is basically a stronger form of preferential independence. Y is utility independent of X if preferences for uncertain choices involving different levels of Y are independent of the value of X. In other words, if there is a 50% chance that Y is 5 days, and a 50% chance that Y is 10 days, then regardless of whether X is fixed at \$100 or \$200, we would still prefer 5 days. For mutual utility independence, then we just need to reverse X and Y and see if the independence still holds.

If these assumptions are validated, then we would set up a reference gamble to determine the indifference probability. In our example, the sure thing would be that X is some cost between the best case (X+) and worse case (X-) scenarios (\$100 ≤ X ≤ \$200), and Y would be some duration for the job to be completed. In this case Y+ would be the lesser of the two values, assuming we wish the job to be completed in a shorter period of time, so Y+ ≤ Y ≤ Y- (or 5 ≤ Y ≤ 10). We are interested in the utility, U(X, Y) versus the utility of a gamble. The gamble would have two scenarios based on a chance outcome. There is a best case scenario, (X+, Y+) or (\$100, 5), which has probability p. There is also a worst case scenario, (X-, Y-) or (\$200, 10), which has probability 1-p. Then we find p such that we are indifferent between the sure thing and the gamble (Figure B.4).

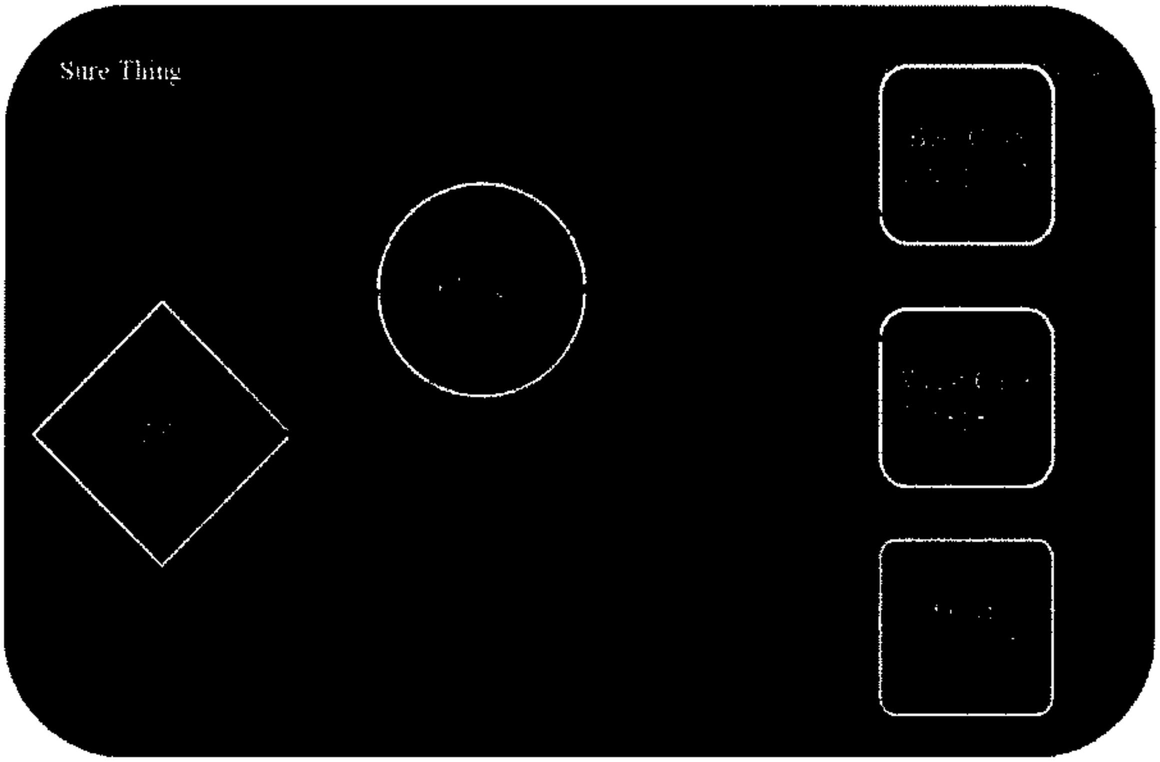
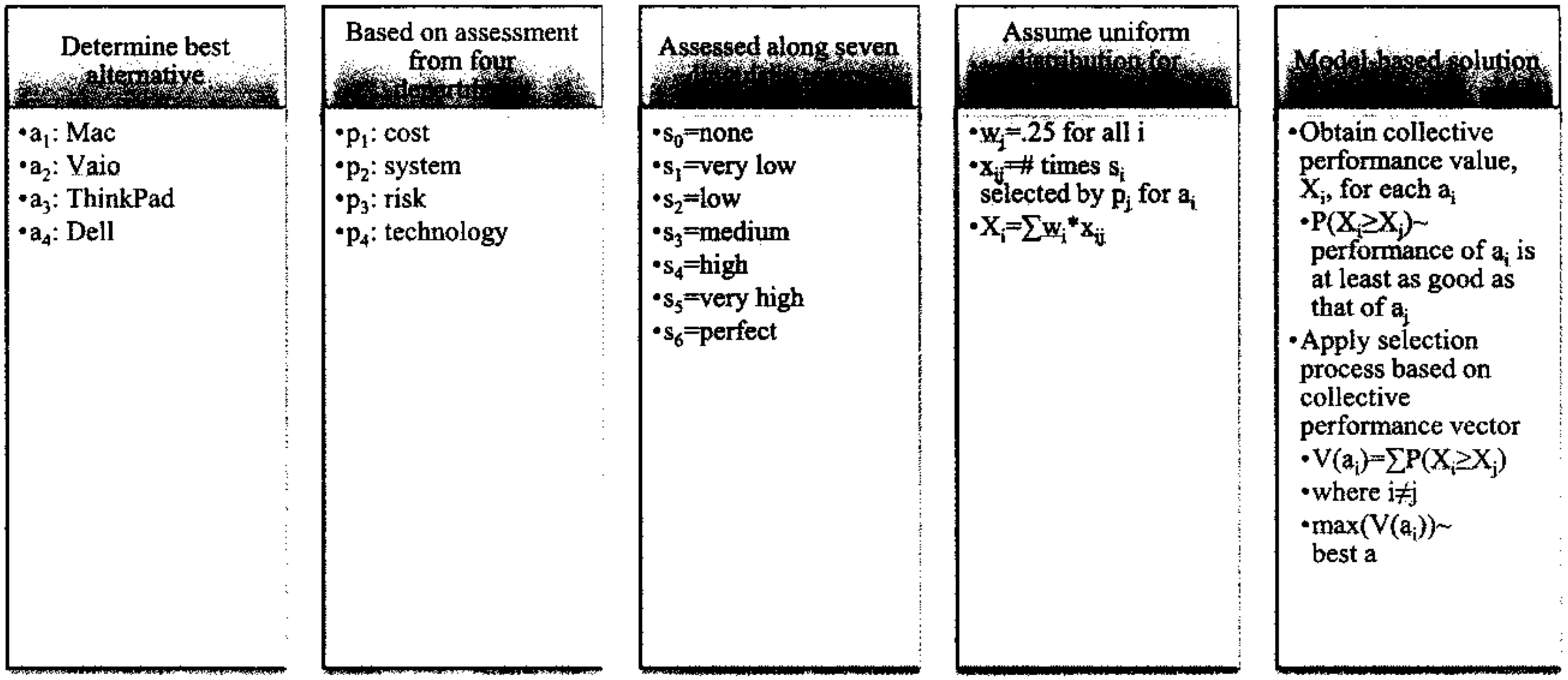


Figure B.4. Multi Attribute Utility Theory Example

However, these assumptions of independence do not always hold. Without the assumptions of independence, MAUT could become extremely challenging to implement. Furthermore, this model requires significantly more time in order to conduct these reference gambles and determine each respondent's utility. Due to lack of resources, MAUT is not a viable option for this research. In fact, regardless of resources, the model does not lend itself to integrating the types of data available for threat, vulnerability, consequence, and perception assessments.

Evidential Reasoning

An appealing option for a risk quadruplet integrated assessment methodology is ER, which deals with problems having both quantitative and qualitative criteria under uncertainty, such as ignorance or randomness (Huynh & Nakamori, 2005; Huynh, et al., 2006). It is used to support decision analyses, assessments, or evaluation activities. It addresses the decision problem using a belief structure to model an assessment with uncertainty, a belief decision matrix to represent a problem under uncertainty, ER algorithms to aggregate criteria for generating distributed assessments, and belief and plausibility functions to generate a utility interval which measures the degree of ignorance. It may be easier to understand ER by walking through an example (Figure B.5).



Determine best alternative

- a_1: Mac
- a_2: Vaio
- a_3: ThinkPad
- a_4: Dell

Based on assessment from four departments

- p_1: cost
- p_2: system
- p_3: risk
- p_4: technology

Assessed along seven [illegible]

- s_0=none
- s_1=very low
- s_2=low
- s_3=medium
- s_4=high
- s_5=very high
- s_6=perfect

Assume uniform distribution for

- w_j=.25 for all i
- x_{ij}=# times s_i selected by p_j for a_i
- $X_i=\sum w_i * x_{ij}$

Model-based solution

- Obtain collective performance value, X_i, for each a_i
  - $P(X_i \geq X_j)$~ performance of a_i is at least as good as that of a_j
- Apply selection process based on collective performance vector
  - $V(a_i)=\sum P(X_i \geq X_j)$
  - where $i \neq j$
  - $\max(V(a_i))$~ best a

Figure B.5. Evidential Reasoning Example

Assume that your company wants to upgrade their computers, so they hire a consulting company to choose between Macs, Vaios, ThinkPads, and Dells. The consulting company has four departments: cost analysis, system analysis, risk analysis, and technology analysis. Each department provides an evaluation vector, assessed in linguistic terms (none, very low, low, medium, high, very high, and perfect). A model is used to solve the problem consisting of two steps. First, obtain a collective performance value, X_i, for each option. Where $P(X_i \geq X_j)$ loosely translates as the "performance of a_i is as at least as good as that of a_j". Then apply a selection process based on collective performance vector $V(a_i)=\sum P(X_i \geq X_j)$ where $i \neq j$ and the best alternative would be the one for which $V(a_i)$ was maximized.

We could use a similar approach for our integrated risk assessment. The alternatives would be different assets. The evaluation vectors would be threat, vulnerability, consequence, and perception. The linguistic set would be very similar (none, very low, low, medium, high, and very high) to describe the level of threat, vulnerability, consequence, or perception for that particular asset. IDS will ensure that the data is captured consistently for all four assessments. Then the ranked performance vectors would output an overall ranking of assets from highest (riskiest) to lowest.

Both ER and AHP use a hierarchy to model a MCDA problem, however, ER differs from AHP in a number of ways. With AHP all of the alternatives comprise the lowest level of the hierarchy, but with ER the alternatives are not included in the hierarchy at all (Xu & Yang, 2001). Further, ER uses a generalized decision matrix where each element of the matrix is an assessment of a given attribute using belief degrees. The decision matrix in AHP merely describes the relative importance of one attribute over another, therefore, "ER can be used to assess an alternative against a set of standards, while AHP can only compare the relative importance between attributes" (Xu & Yang, 2001). Finally, ER aggregates the belief degrees of lower level attributes to higher level attributes gradually, until it achieves and overall score, whereas AHP aggregates average scores based on pairwise comparison (Xu & Yang, 2001). One implication of these differences is that ER can tackle large-scale MCDA problems (without limits on the number of alternatives or attributes). Also, as new attributes are added, an ER model does not need to be re-evaluated since each attribute is scored for each alternative separately. ER also does not suffer from a common AHP problem known as rank reversal, which can occur when new attributes are added to an AHP model. Perhaps most importantly, ER can handle mixed data, including random and deterministic, qualitative and quantitative, as well as incomplete data for some attributes. And ER can even incorporate AHP procedures into certain aspects of a model, such as using pairwise comparisons to weight attributes against each other (Xu & Yang, 2001).

Technology

Technology will have a significant impact on the MCDA models, as the availability of software to conduct such analyses at the time of research could be limited. Software for AHP is widely available, but can be very expensive. Software for ANP and MAUT are not as common. ER appears to be the preferred MCDA approach for the risk quadruplet and conveniently, there is free ER software available. IDS uses a belief decision matrix to model MCDA problems under uncertainty, "including subjectivity, randomness, and incompleteness" ("IDS," 2010). It can communicate risk and decisions through graphical data visualizations, making it a logical choice for this research.

APPENDIX C

LITERATURE REVIEW

International Risks: Risk Management and Risk Perception in a Global Context

Risk Management by Country

The OECD is a collection of 30 democratic governments which work together to address the economic, societal, and environmental challenges of globalization. OECD members include Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the US ("OECD Studies in Risk Management: Innovation in Country Risk Management," 2009). The OECD provides a neutral forum for governments to compare policy experiences, seek answers to shared concerns, and identify best practices. A recent OECD report commented on National Level Risk Assessments conducted by six countries, including the United Kingdom, Canada, the Netherlands, Singapore, and Japan, as well as the US which conducted its SNRA with FEMA soon after the OECD report. The report focused on each country's risk management approach to large scale events such as natural disasters, terrorist attacks, and pandemic diseases, all of which pose serious consequences for the country's population and national assets.

Risk Management Programs

Each of the six countries have assigned at least one government agency to oversee an all-hazards risk management framework (DHS and FEMA are the main entities for the US, but they obviously work closely with many other agencies). All six countries have also adopted an all-hazards approach to risk management (for example, the US follows the DHS National Response Framework and National Preparedness Goal). Singapore's Whole-of-Government Integrated Risk Management framework stood out as a best practice as it identifies cross-agency risks, not just the risks associated with disasters, themselves. Additionally, each country has a policy coordination body in place (the US equivalent is the Homeland Security Council), which conducts policy-planning for large-scale disasters, usually reporting to the highest levels of government (the Homeland Security Council consists of Secretaries from a number of related departments and agencies and reports directly to the president). The report also reviews each country's approach to mitigation planning, cost-wise risk mitigation, resilience and continuity of operations, risk financing, risk transference, but of particular interest to this research, OECD also explored protection of CI. Only four of the six countries maintain an infrastructure protection program ("OECD Studies in Risk Management: Innovation in Country Risk Management," 2009); in the US, this is covered by the NIPP. While it is recognized that there is not a unanimous view across countries about which infrastructure sectors are critical, each of the four countries understood the need to protect both physical and cyber systems "essential to the minimum operations of government and their individual economies". All six countries recognize the importance of risk concepts such as interdependent vulnerabilities which can lead to cascading effects. And even though only four of the six countries have a program in place to address infrastructure protection, each of the six countries has identified those assets it considers crucial ("OECD Studies in Risk Management: Innovation in Country Risk Management," 2009).

The OECD study identified 16 CI sectors (some of which we would classify as KR and/or KA sectors based on our definitions). Of these sectors, most of them map to those given in Table C.5, with a few exceptions. OECD listed Public Safety as a sector, and the US does not include that in its 18 CIKR sectors. Furthermore, the US identifies three additional categories not included in the OECD report (Information Technology, Postal and Shipping, and Critical Manufacturing). OECD also noted that approximately 80% of CI in the four countries listed above were privately owned and operated, making public-private coordination extremely important.

Risk Management Tools

Also of interest to this research is the OECD review of the risk management tools leveraged by the six participating countries. The United Kingdom uses a National Risk Assessment, which is basically a traditional risk matrix used for visually scoring risks along a scale of likelihood and impact (Figure C.1). The descriptions of likelihood, impact, and risk are given qualitatively using terms like "negligible" to describe an estimated likelihood of less than 0.005%, which is also given as a ratio of less than a 1 in 20,000 chance.

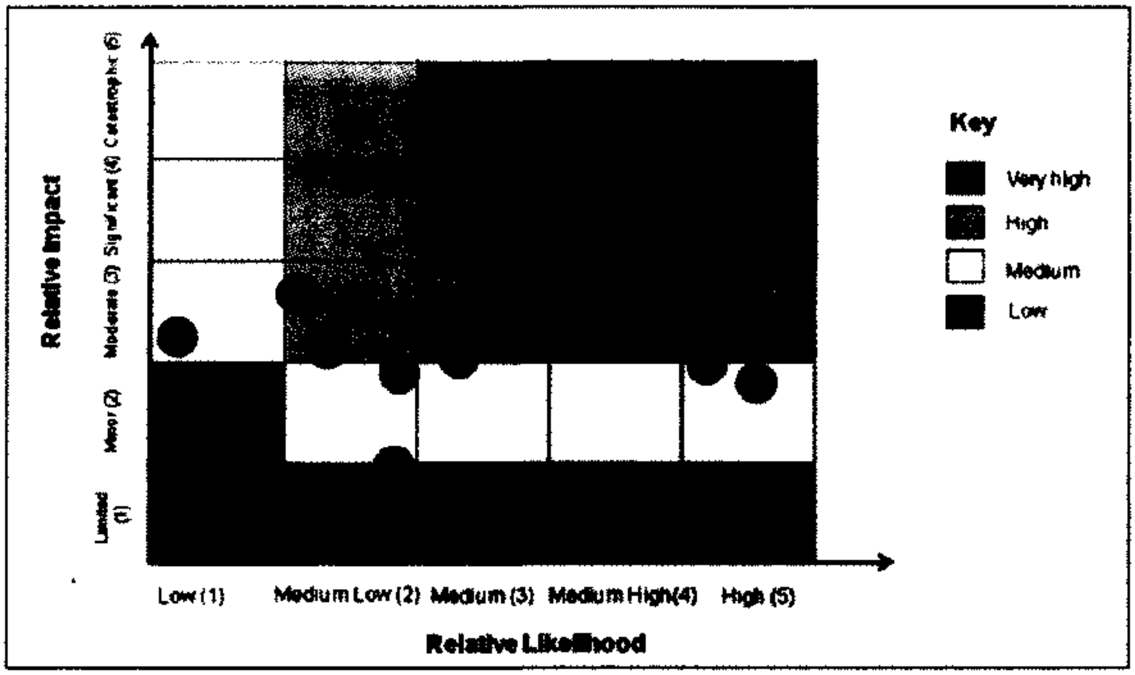


Figure C.1. United Kingdom National Risk Assessment

Three of the countries in the study conduct short-, medium-, and long-term risk assessments. In Singapore, risk scenarios are identified and reviewed every three years ("OECD Studies in Risk Management: Innovation in Country Risk Management," 2009). Many of the countries are also looking at multidisciplinary risk assessment approaches, combining GIS and probabilistic risk assessment models to produce hazard maps, a valuable tool for communicating risk. Other disciplines are being leveraged, as well, including economics, sociology, and of special note for our research (as it relates to risk perception), the field of psychology.

Global Risks

In 2006, the WEF began to release an annual series of reports in an effort to work “towards a more sophisticated understanding of global risks” ("Global Risks," 2006). The original purpose of these reports was to identify and assess current and emerging global risks, study their interdependencies, determine the potential consequences for different markets, and to improve the mitigation of these global risks. WEF consistently categorized global risks into five classes in their annual Global Risks Reports from 2006 to 2012 (Figure C.2).

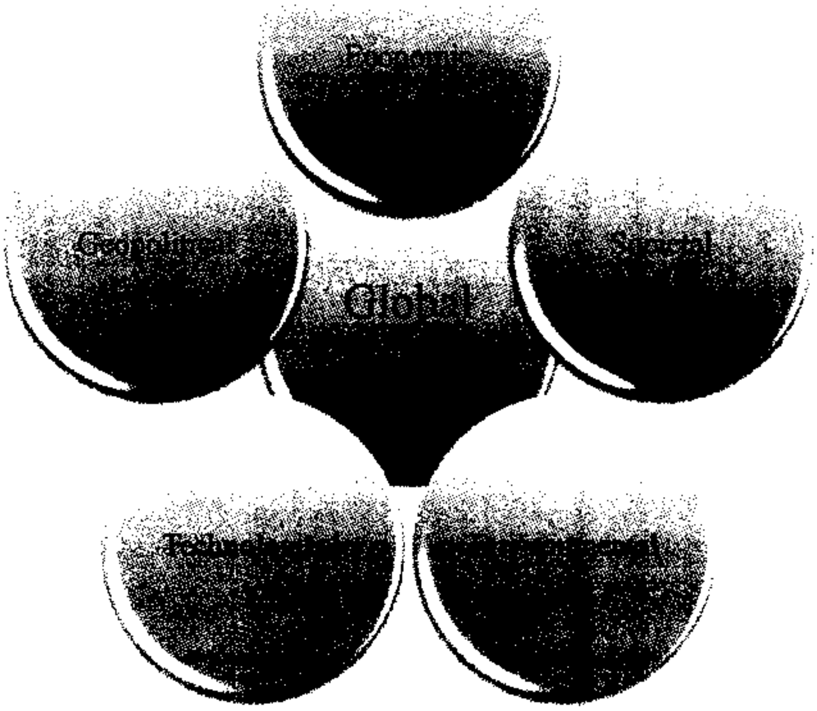


Figure C.2. Global Risks: Risk Categories

In 2006, economic risks included oil prices and energy supply, asset prices and indebtedness, the current account deficit and state of the dollar in the US, impending fiscal crises, China, and critical infrastructures. Societal risks included regulation, corporate governance, intellectual property rights, organized crime, global pandemics, chronic diseases in the industrialized world, epidemic diseases in the developing world, and liability regimes. Environmental risks included tropical cyclones, earthquakes, climate change, and the loss of ecosystem services. Technological risks included convergence of technologies, nanotechnology, electromagnetic fields, and pervasive computing.

Geopolitical risks included terrorism, European dislocation, as well as current and future hotspots.

While the five main global risk categories remain the same from 2006 through 2012, the number and categorization of risk events within those categories evolves over time (Table C.1). For example, retrenchment from globalization was considered a Geopolitical risk in 2007, but from 2008 through 2011 it was considered an economic risk. Interestingly, at least for the purposes of this research, we see that critical infrastructures (to include underinvestment in infrastructures, infrastructure fragility, and infrastructure neglect) are considered economic risks in 2006, 2009, 2010, 2011, and 2012. But critical information infrastructures (and specifically, the breakdown of those infrastructures) appear under technological risks from 2007 through 2012. A more detailed comparison of the risks cited over the years by the WEF Global Risk Reports can be found in Table A.1.

Table C.1. Global Risks: Core Global Risks by Year

Global Risks	Core Global Risks
2006	25
2007	23
2008	26
2009	36
2010	36
2011	37
2012	50

Risk Assessment

The risk assessment process in 2006 was basically a risk matrix approach, where the likelihood (Table C.2) and consequence severity (Table C.3) of different risk scenarios (events) for each risk category, were predominantly estimated by subject matter experts on a scale of 1 to 4 ("Global Risks," 2006). When sufficient data existed, WEF employed statistical and actuarial methods to analyze data, but most of the estimates were qualitative.

Risks were estimated along two timelines (short-term and long-term), and across two cases (base-cases, or the likely trend for the risk given current information, and worst-cases, representing the most severe outcome). Consequences were broken down into three dimensions: asset damage, human impact, and financial impact as measured by the percent growth of the aggregate global Gross Domestic Product.

Table C.2. Global Risks 2006: Likelihood Key

1	Below 1%	Low
2	1-10%	Moderate
3	10-20%	High
4	Above 20%	Very High

Table C.3. Global Risks 2006: Severity Key

Asset Damage	
1	US$ 10-50 Billion
2	US$ 50-250 Billion
3	US$ 250 Billion - US$ 1 Trillion
4	> US$ 1 Trillion
Human Impact	
1	< 100
2	100-10,000
3	10,000 – 1 Million
4	> 1 Million
Financial Impact	
1	< .2
2	.2 - .7
3	.7 – 1.5
4	> 1.5

So, for example, in the Economic global risks category, four impending fiscal crisis scenarios were explored: a short-term base-case where fiscal deficits decline modestly, a short-term worst-case where fiscal positions become unsustainable, a long-term base-case where fiscal positions come under demographic pressure, and a long-term worst-case where fiscal deficits are seriously challenged by demographic pressure ("Global Risks," 2006). The likelihood and severity estimates collected and aggregated by WEF for these four scenarios are given by (3, 1), (1, 1), (2, 2), and (3, 3), respectively.

In 2007, the WEF seems to maintain a similar risk assessment methodology to the one described for 2006. While the 2007 Global Risks Report alludes to a more detailed description of their methodology ("Global Risks," 2007), the link to the extended version of the report is broken and an online search proved fruitless. However, the number of dimensions of consequences is obviously reduced (asset damage is eliminated), as there are two graphics alluding to severity, one for economic loss, another for number of deaths. Additionally, an examination of the core global risks analyzed in each year of the WEF Global Risks Report (Table A.1) shows that the number of risks decreased slightly from 2006 to 2007 (Table C.1).

In 2008, the number of core risks increases slightly, but aside from the addition of a completely new risk, food security, the risk assessment process is comparable to previous years. We see that the likelihood and severity scales evolved (Table C.4) from those displayed in 2006. One anomaly in the methodology appears when reviewing the 2008 report appendices, one of which includes a detailed taxonomy of global risks, comprising 31 risks even though only 26 core global risks were explored in the report.

Table C.4. Global Risks 2008: Likelihood and Severity Tables

1	below 1%	2-10 billion	below 1%	1,600-8,000
2	1-5%	10-50 billion	1-5%	8,000-40,000
3	5-10%	50-250 billion	5-10%	40,000-200,000
4	10-20%	250 billion-1 trillion	10-20%	200,000-1 million
5	above 20%	>1 trillion	above 20%	> 1 million

In 2009, the number of core global risks jumps from 26 to 36. The risk assessment methodology appears to remain comparable to that of previous years; however, the Global Risk Network conducted a series of additional workshops and meetings, focusing on regional risk and released three regional risk reports for Africa, Europe, and India, as well as one topical report on global growth which looked at emerging markets and high-growth companies ("Global Risks," 2009).

The 2009 Global Risks Report also discusses its general methodology for a number of the tables and graphics presented. The Risk Interconnection Map is derived from results of the WEF Global Risks Perceptions Survey, which was a web-based survey completed by approximately 120 risk experts in 2009. The 2009 regional risk maps were created using a methodology similar to statistical cluster analysis. Most interestingly, in 2009 what constitutes a global risk is defined and, in general, the criteria includE global scope, cross-industry relevance, uncertainty, economic impact, public impact, and a multi-stakeholder approach ("Global Risks," 2009).

In 2010, the core global risks remained identical to the 36 reviewed in 2009. The methodology for the Risk Interconnection Map and the Global Risks Perception Survey remains the same in 2010, although the number of experts which completed the survey increases to 200. The 2010 regional risk maps were again created using a methodology similar to statistical cluster analysis. And the criteria for what constitutes a global risk also remain the same ("Global Risks," 2010).

In 2011, the number of core global risks increases by one to 37, however, it is not a simple addition of one new risk. Rather, a number of core global risks from previous years are dropped from the assessment, while many others are introduced, such as extreme energy price volatility, ocean governance, space security, demographic challenges, or threats from new technologies. The number of experts that responded to the Global Risk Perceptions Survey increases to 580. The criteria for what constitutes a global risk also remain the same ("Global Risks," 2011).

In 2012, the number of core global risks shot from 37 to 50, which included the introduction of a number of new risks, such as severe income disparity, antibiotic-resistant bacteria, failure of diplomatic conflict resolution, rising religious fanaticism, and proliferation of orbital debris. While only 489 experts participated in the 2012 survey, the details of the survey, including the questions, demographics, and detailed results, are included in appendices of the Global Risks Report ("Global Risks," 2012). Interestingly, there is no breakdown of risks comparing severity by economic loss or number of deaths, rather impact is measured on a scale of 1 to 5, as is likelihood. However, it is implied in the appendix detailing the Global Risks Perception Survey that impact is "to be interpreted in a broad sense, beyond just economic consequences" ("Global Risks," 2012), so impact in this case could include economic loss, number of deaths, and even other types of consequences.

Risk Communication

Similarly, the WEF worked to stay at the cutting edge of risk communication and risk visualization techniques. In 2006, the WEF Global Risks Report only a few graphics were used to display and communicate risk ("Global Risks," 2006). There was a summary table of the likelihood and severity of the core global risks, displayed by the five risk categories (economic, environmental, societal, technological, and geopolitical) and four cases (short-term base-case, short-term worst-case, long-term base-case, and long-term worst-case). There was also a set of graphics to display the top short-term risks with the highest severity, the top long-term risks with the highest severity, and similar graphics were broken down by the 5 risk categories (Figure C.3).

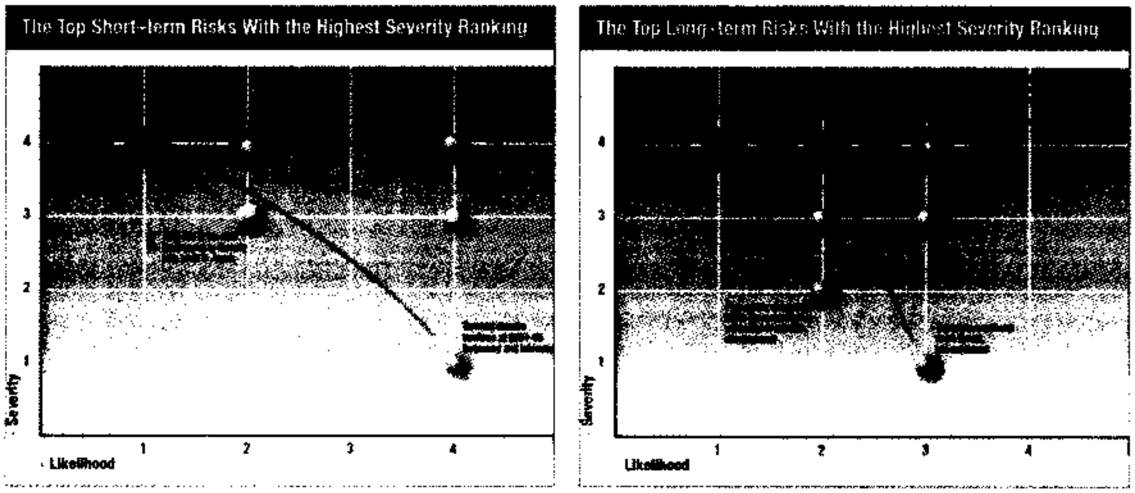


Figure C.3. Global Risks 2006: Top Risks

The 2007 WEF Global Risks Report displayed 23 core global risks in three dimensions (Figure C.4): likelihood, severity (in terms of economic loss), as well as a dimension described as "increasing consensus around risk" ("Global Risks," 2007). Each risk was displayed along its coordinates for likelihood and severity, but its marker was displayed as varying hues of blue to denote the level of consensus around the risk. A similar graphic was displayed for the 23 core global risks, only severity was displayed in terms of the number of deaths associated with the risk. WEF also introduced a global risk barometer, a table that showed the 23 core global risks and whether their overall risks had increased, stabilized, decreased, or caused expert disagreement. The barometer was used to compare these risks not to the past, but to the future, looking at whether the significance of the risk for the next ten years has become more or less critical ("Global Risks," 2007). Additionally, the report included a correlation matrix graphic, which helped to visualize, through the use of a network diagram (Figure C.5), the fact that risks do not manifest independently, but are often interrelated with other risks ("Global Risks," 2007). The correlation matrix helps us visualize the strength of the high-level correlations between risks, as they are perceived by experts to exist. The strength of the correlation is represented by the thickness of the lines connecting the risks ("Global Risks," 2007).

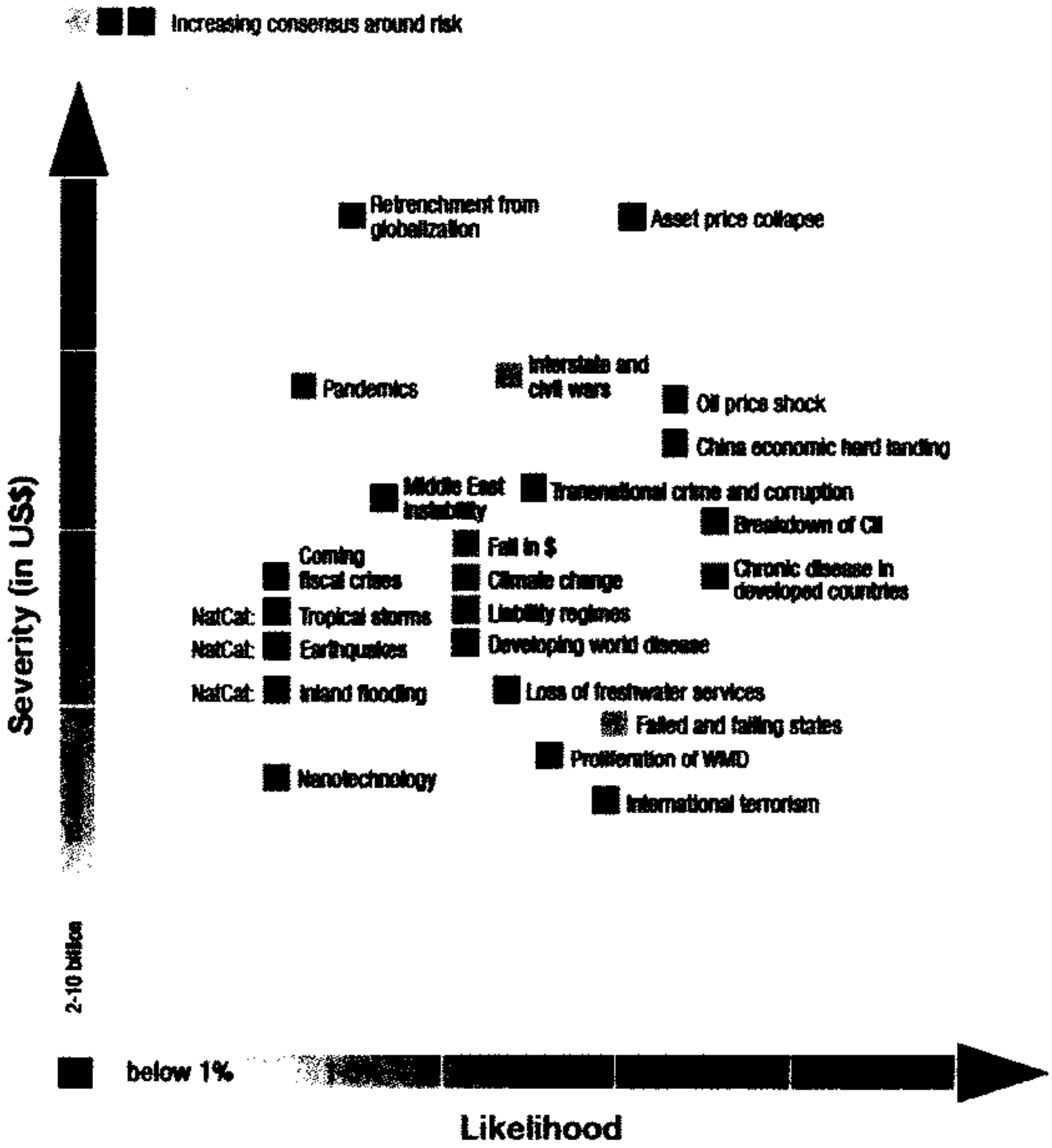


Figure C.4. Global Risks 2007: 23 Core Global Risks

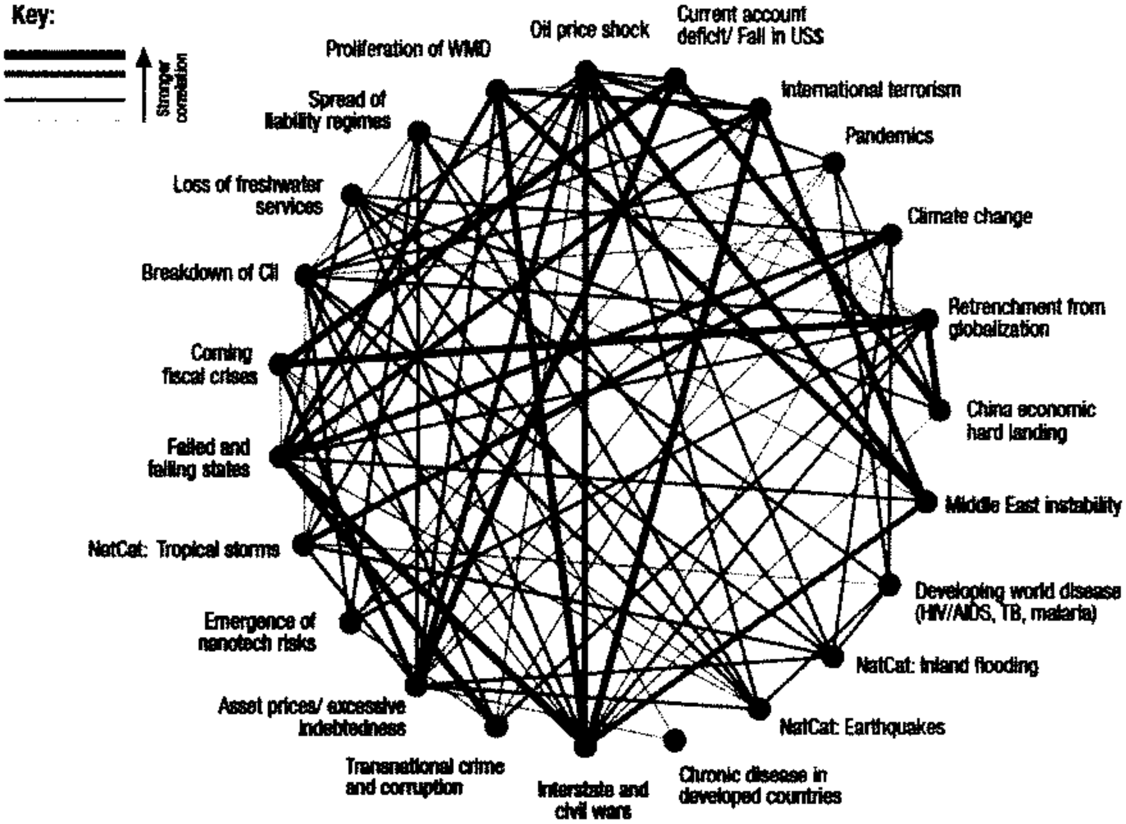

Key:
Stronger correlation
Proliferation of WMD
Oil price shock
Current account deficit/ Fall in US$
International terrorism
Pandemics
Climate change
Retrenchment from globalization
China economic hard landing
Middle East instability
Developing world disease (HIV/AIDS, TB, malaria)
NatCat: Inland flooding
NatCat: Earthquakes
Chronic disease in developed countries
Interstate and civil wars
Transnational crime and corruption
Asset prices/ excessive indebtedness
Emergence of nanotech risks
NatCat: Tropical storms
Failed and failing states
Coming fiscal crises
Breakdown of CII
Loss of freshwater services
Spread of liability regimes

Figure C.5. Global Risks 2007: Correlation Matrix

The 2008 Global Risks Report used a graphic very similar to the 2007 one to display likelihood and severity (by economic loss, as well as number of deaths), but abandoned the additional dimension regarding the consensus around the risk. It also display a network graphic to depict the interrelationships amongst the core global risks, however the graphic is reimagined and includes additional risk information ("Global Risks," 2008). Though originally called a correlation matrix, in 2008 the graphic is referred to as a social networking diagram (Figure C.6). Again, the thickness of the lines represents the strength of the correlation between the risks connected, but now the size of the nodes indicates the assessment of the risk and the proximity of the nodes relates to the similarity of the correlations.

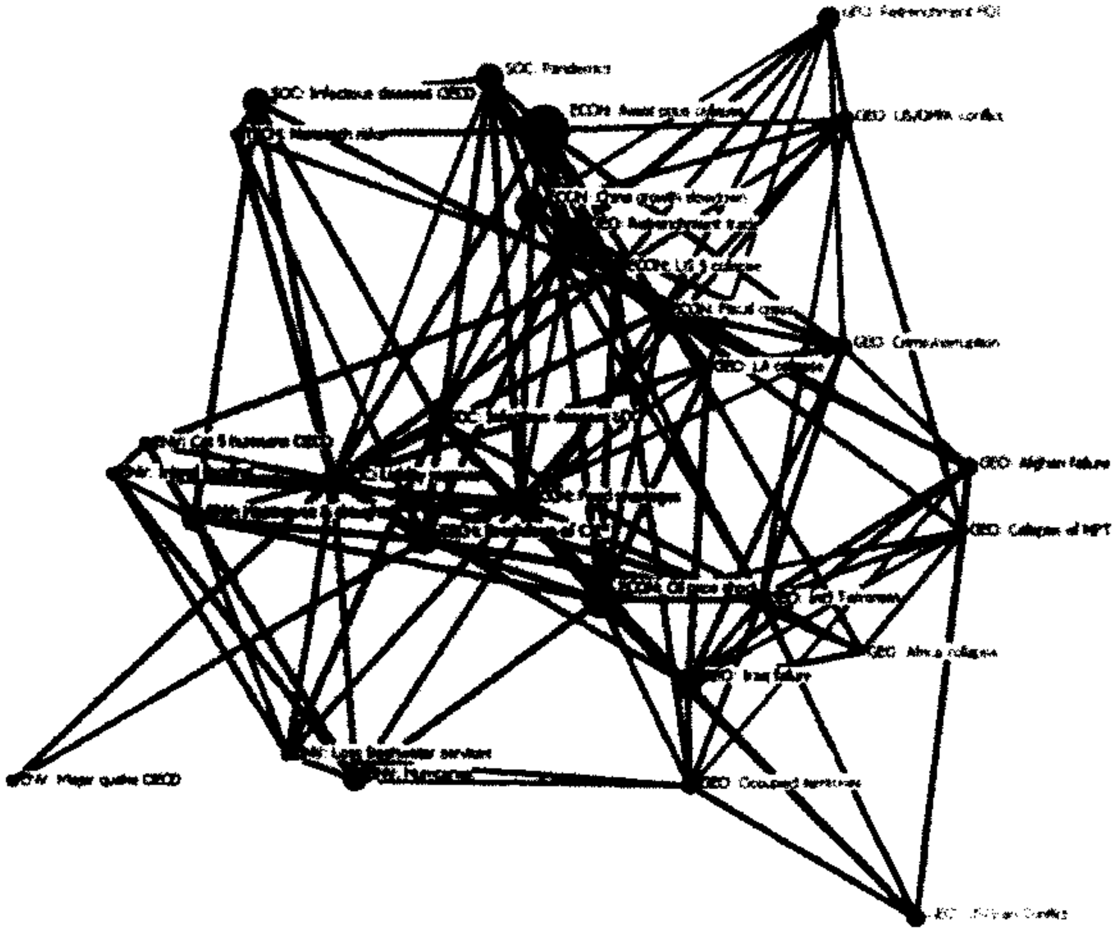


Figure C.6. Global Risks 2008: Social Network Diagram of Global Risks

In 2009, the 36 core global risks were visualized by likelihood and severity, both economic loss and number of deaths (Figure C.7), however, this time around they used color coding to show whether that risk was a new risk, or if it had increased, decreased, or remained stable since the 2008 Global Risks Report ("Global Risks," 2009). Additionally, some nodes were split to show that the likelihood had increased, but the severity had decreased (or vice versa). It appears that this is merely a way of communicating the information from the risk barometer alongside all of the other global risk information. The risk barometer is still included in the report, but as an appendix.

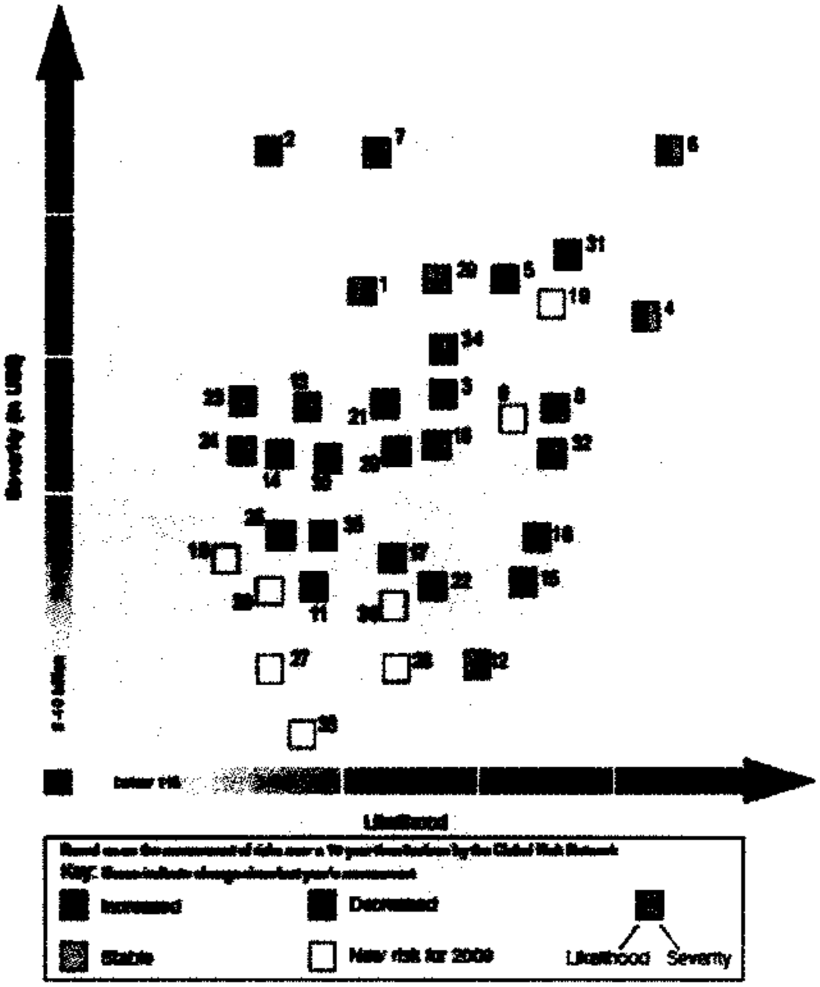


Figure C.7. Global Risks 2009: 36 Core Global Risks

The Risks Interconnection Map (Figure C.8) evolved slightly. Node size continued to denote severity, line thickness continued to refer to the strength of the interconnection between nodes. And the proximity of the nodes indicates that those risks are closely interlinked. Additionally, the node colors which indicate to which category the risk is aligned (red – economic; dark green – geopolitical; light green – environmental; purple – technological; blue – societal). And the direction of a thicker line segment demonstrates that of the two interconnected risks, one risk has a stronger dependence or interdependence ("Global Risks," 2009).

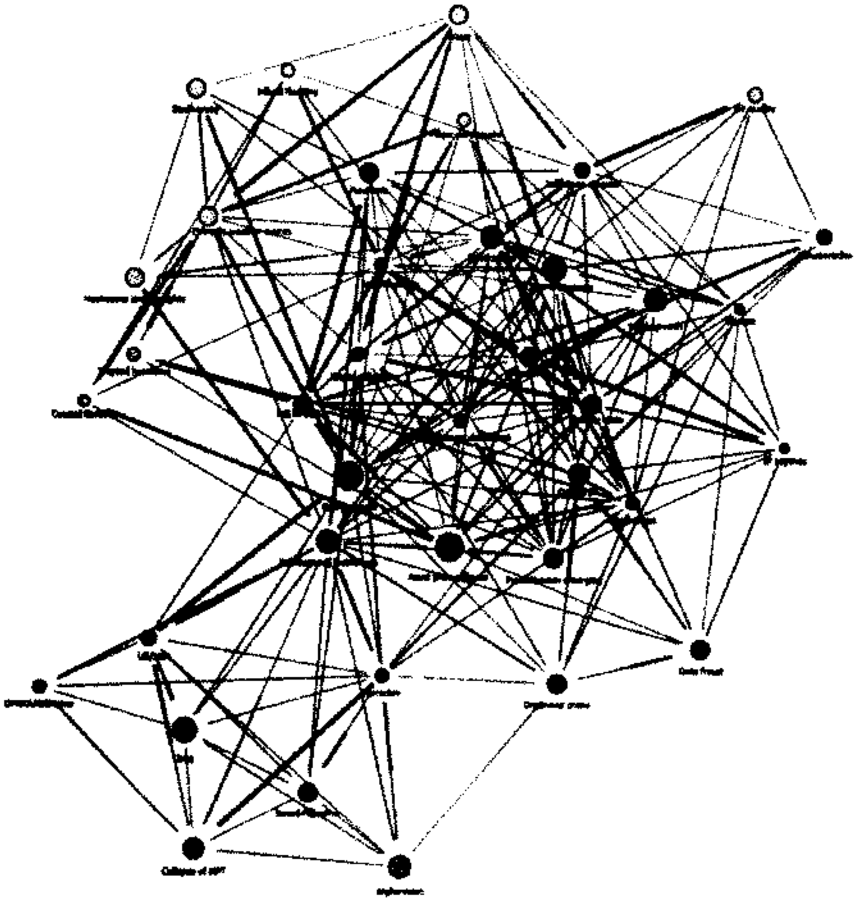


Figure C.8. Global Risks 2009: Risks Interconnection Map

A new graphic was introduced in 2009, which shows a country's exposure to risks (Figure C.9). Interestingly, four of the risk categories displayed in the graphic align to the global risk categories, but one (health) seems to be a substitute for the societal global risk category. The graphic aligns the country's exposure to risk along two scales: economic risks versus a combined scale of geopolitical, environmental, health, and technical risks ("Global Risks," 2009). Similar graphics were included in the report to display a country's exposure to asset bubbles and economic risks, as well as geopolitical risks versus oil dependency.

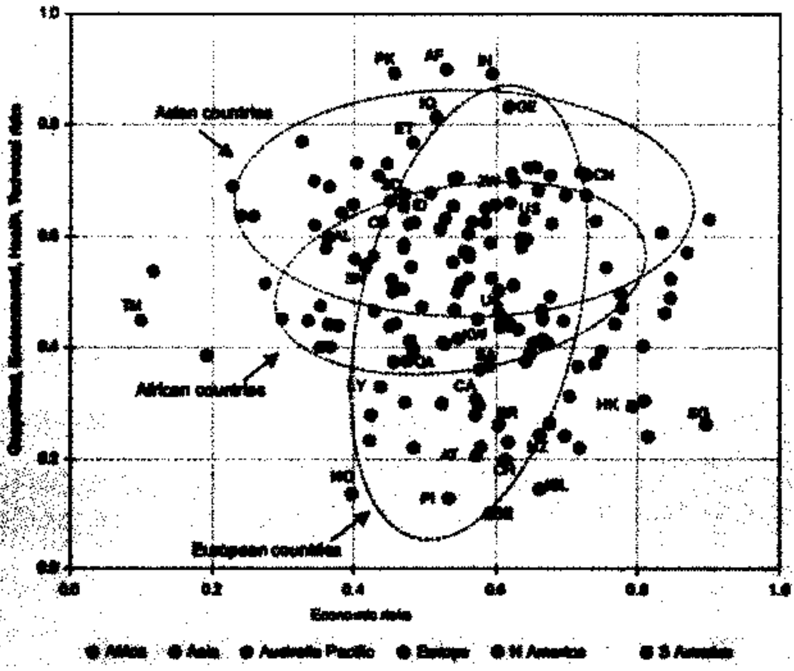


Figure C.9. Global Risks 2009: Exposure of 160 Countries to Global Risks

Also new in this report, the Risks Interconnection Map is spliced and reorganized in later sections of the report to highlight certain risks and their relationships, such as water, which is described as being at the "nexus of many risks", including infectious disease, infrastructure, food prices, amongst others ("Global Risks," 2009). An example pertinent to this research is given in Figure C.10, which shows the infrastructure risk and all of its many interconnected risks, noting that an investment in risk mitigation for infrastructure is extremely important as it could impact so many related risks ("Global Risks," 2009).

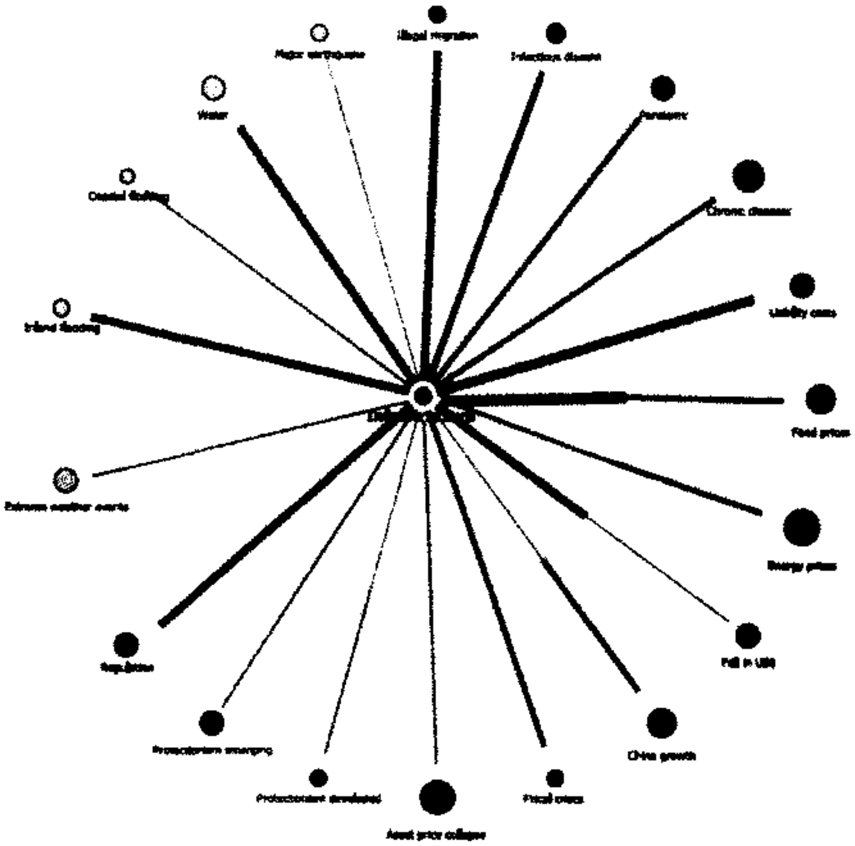


Figure C.10. Global Risks 2009: Infrastructure

The 2010 Global Risks Report again displayed 36 core global risks (Figure C.11), but this time it only displays those risks by severity of economic loss; there is not a separate graphic showing the severity by number of deaths ("Global Risks," 2010). Additionally, the graphic did not include the barometer information (whether the risk had increased or decreased), although the barometer was again included in an appendix. Instead, the color coding only shows the categories to which each risk aligns (economic, geopolitical, environmental, societal, and technological).

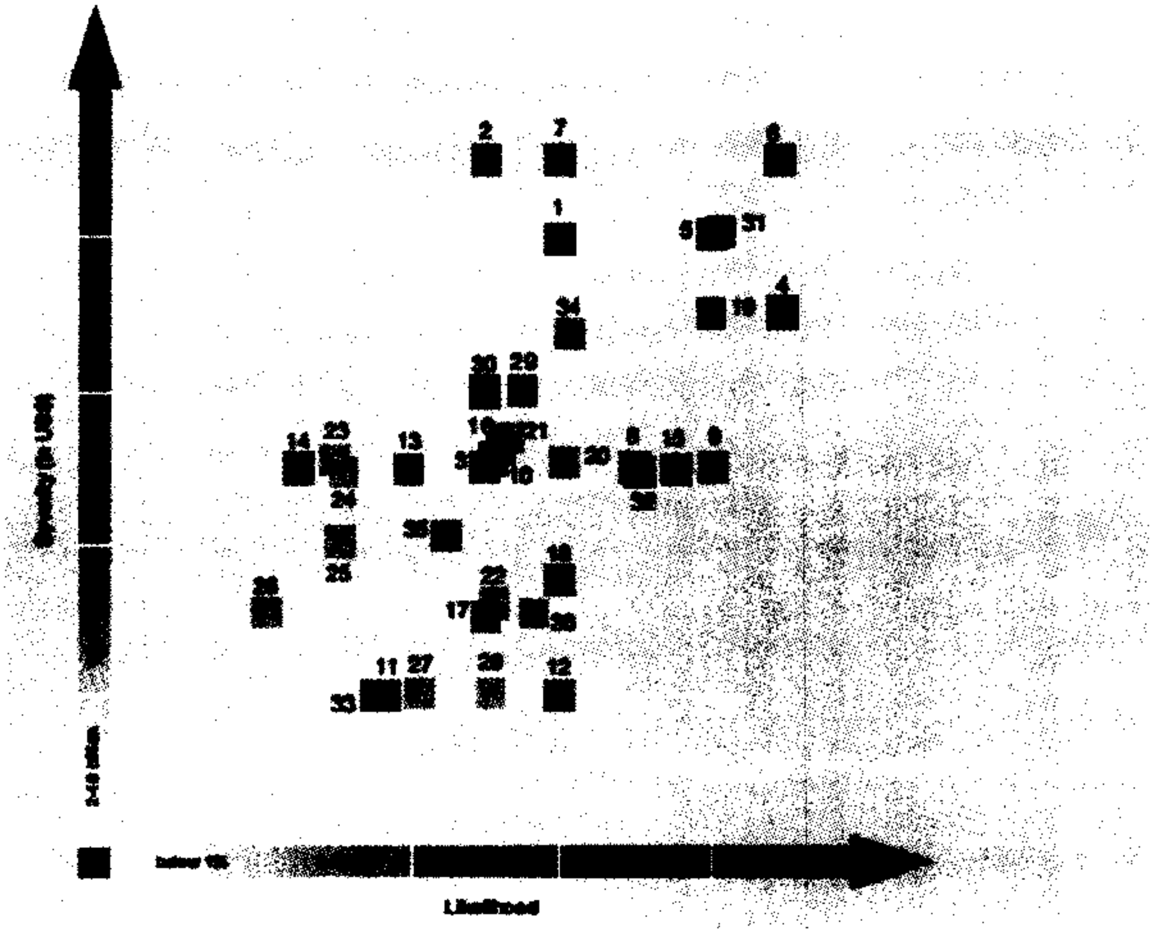


Figure C.11. Global Risks 2010: 36 Core Global Risks

An example of a breakdown of the 2010 Risk Interconnected Map is given in Figure C.12 for the risk of underinvestment in infrastructure. The severity of the risk is denoted by the width of the line around the node, the likelihood of the risk is given by the size of the node, the category of the risk is shown in the color of the node, the proximity of the risks indicate they are highly interconnected, and the degree of interconnectedness is displayed in the width and darkness of the line between nodes ("Global Risks," 2010). A country risk map, similar to Figure C.9 is given in the 2010 report, but only to compare the global retrenchment risk versus the global governance gap risk. A Risks Interconnection Map similar to Figure C.8 is also displayed, though it is much more complex and dense given the increase in the number of core global risks.

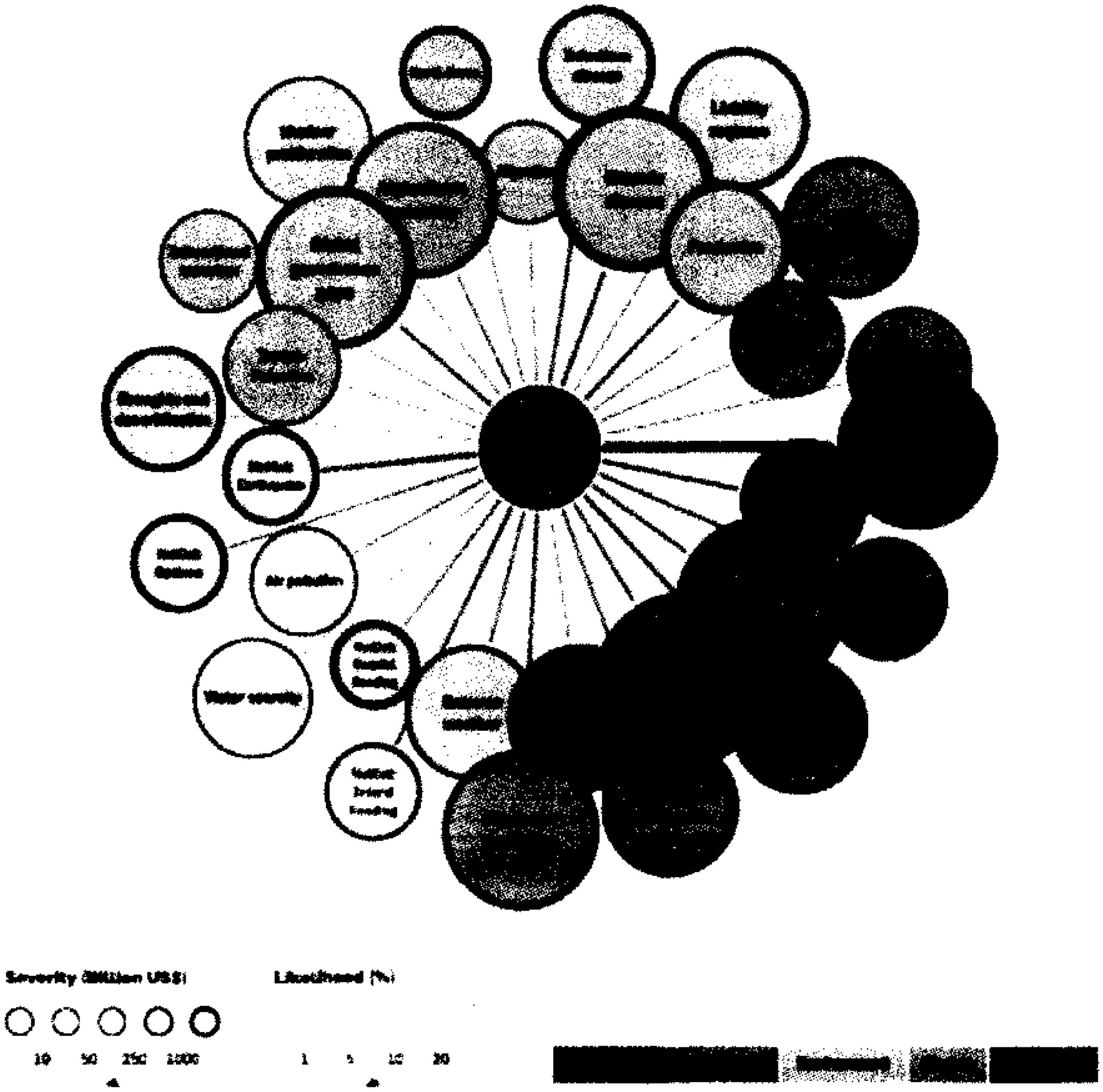


Figure C.12. Global Risks 2010: Infrastructure Interconnect Risks

The 2011 report again displayed the core global risks by likelihood and (economic) severity (Figure C.13), where the size of the node related to an increased perceived likelihood, the darkness of the node related to an increased perceived severity, and the color of the node related to the category of the risk ("Global Risks," 2011). The Risks Interconnection Map received a comparable face-lift (Figure C.14), where the nodes provide the same information as the core global risks chart, and again the thickness and darkness of the line indicate a strong, perceived interrelationship between the nodes.

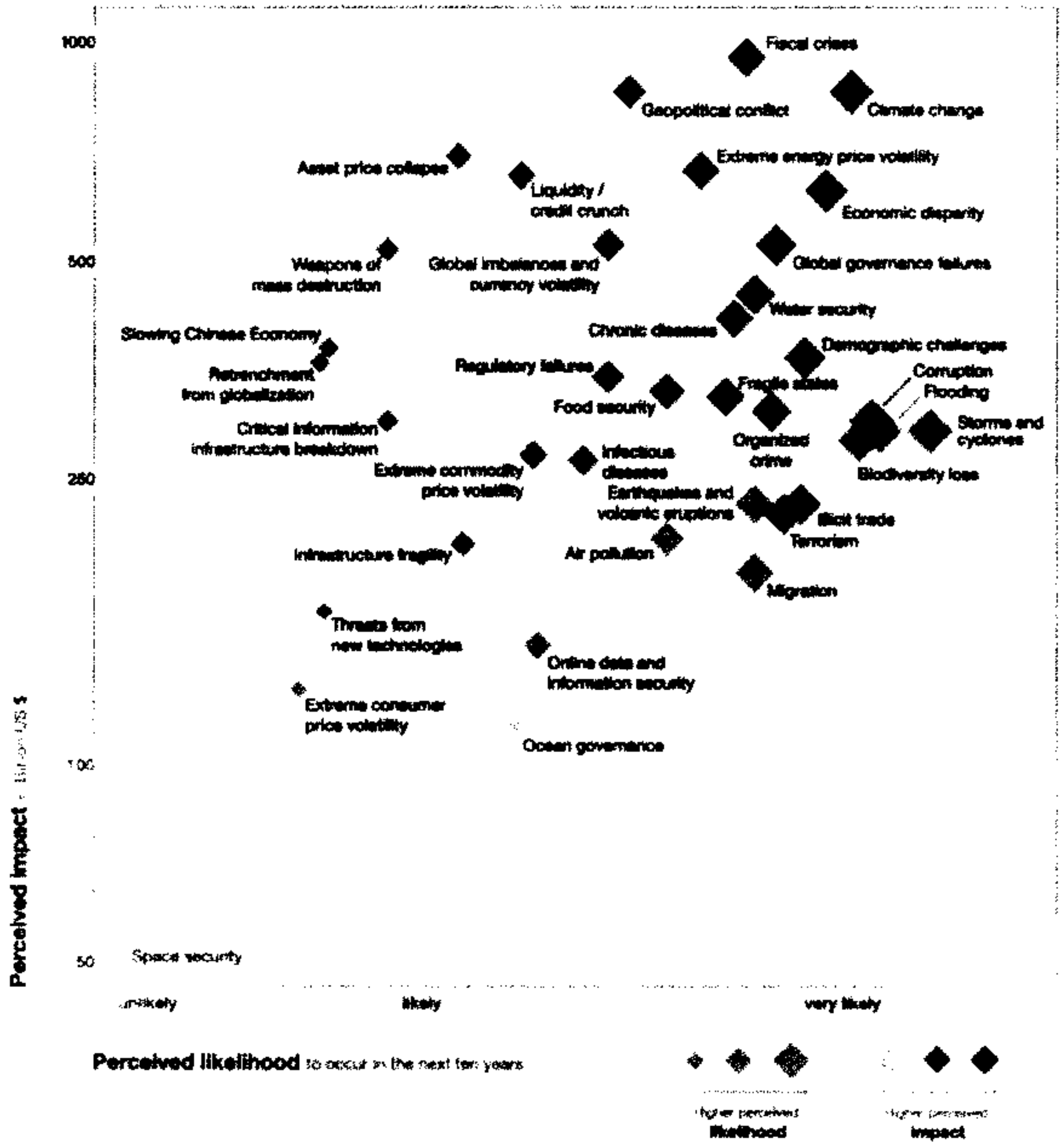


Figure C.13. Global Risks 2011: 37 Core Global Risks

In 2011, the fact that the estimates of risk likelihood, severity, and connectedness are based on perceptions is really highlighted in the 2011 report. It was always described in previous reports that these charts and graphs were based on data collected in the Global

Risks Perception Survey, but now the charts and graphs actually include the word *perceived* in their keys. The report breaks down the Risks Interconnection Map to examine a subset of risks, dubbed "risks in focus" (Figure C.15), to include the macroeconomic imbalances nexus, the illegal economy nexus, and the water-food-energy nexus ("Global Risks," 2011).

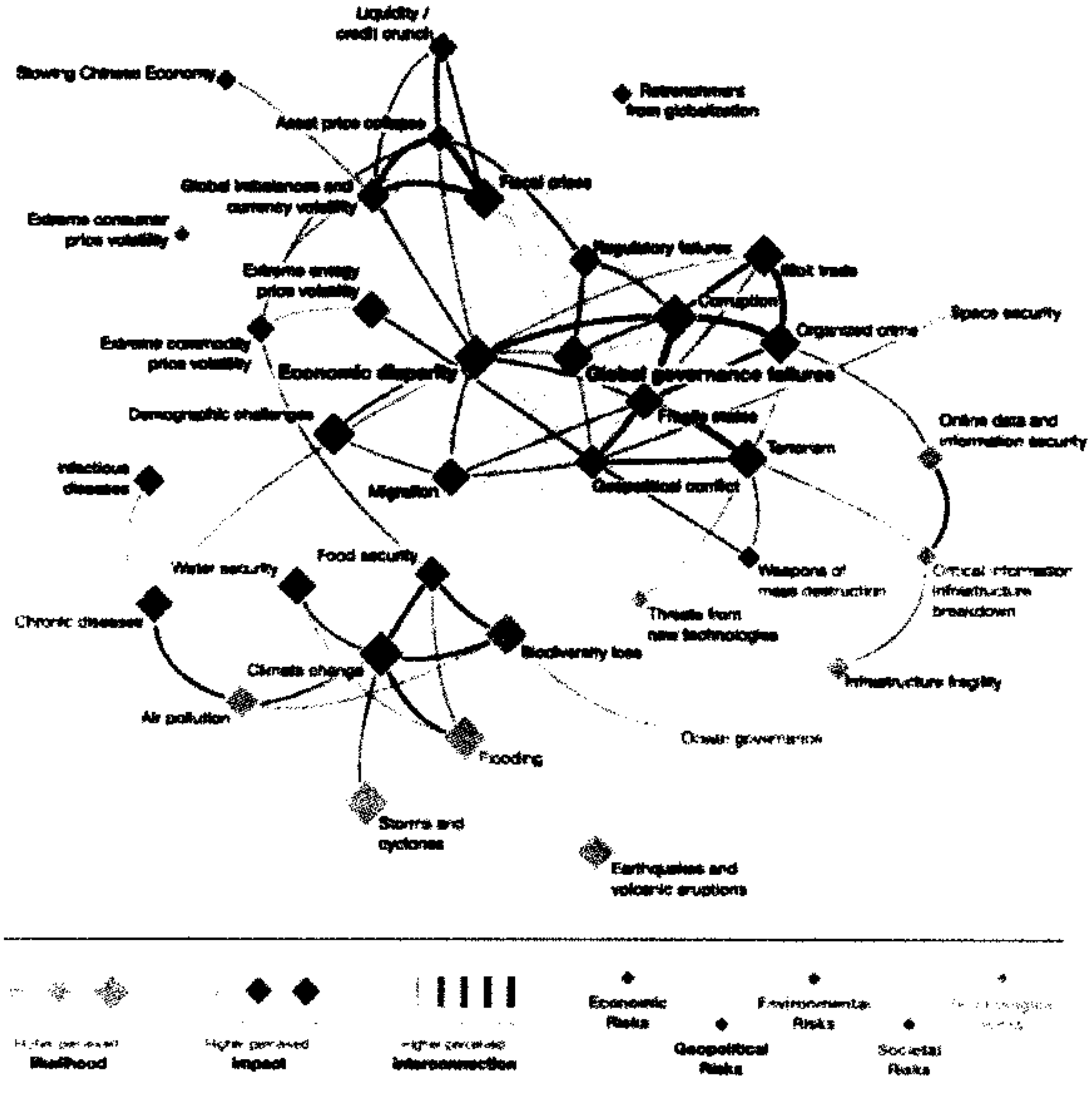
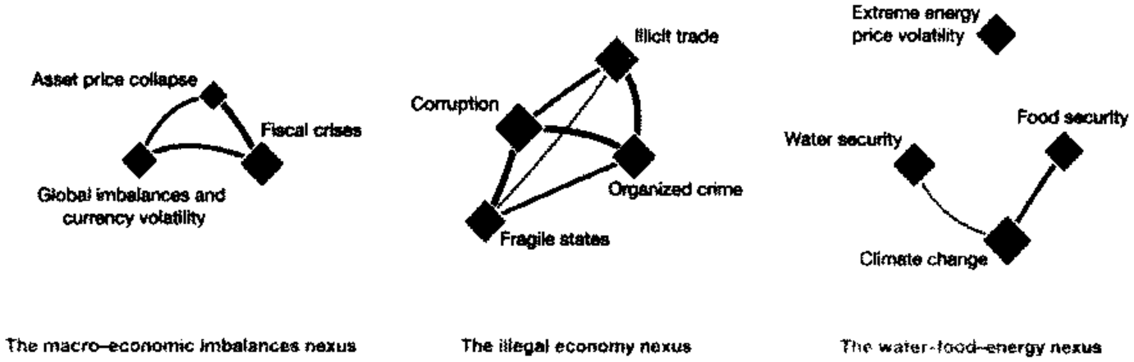


Figure C.14. Global Risks 2011: Risks Interconnection Map



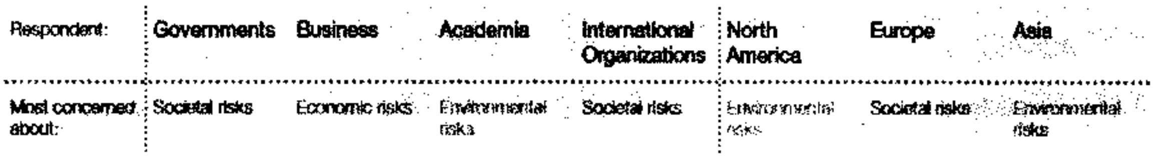
The macro-economic imbalances nexus

The illegal economy nexus

The water-food-energy nexus

Figure C.15. Global Risks 2011: Risks in Focus

In the 2011 report appendices, we see a breakdown of the survey results, to include a top ten list of risks by combined likelihood and impact, the highest ranking of which was global climate change. Further analysis of the Risks Interconnection Map also results in a top ten list of risks based on the average strength of their interconnections, the highest ranking of which was economic disparity. Very interestingly, the survey results also include a comparison of the risk perceptions amongst respondents given basic demographic information (Figure C.16), such as whether they were representatives of government, business, academia, or international organizations, and whether they are from North America, Europe, or Asia ("Global Risks," 2011). The categories of risk about which each group was most concerned seems pretty logical. For example, government representatives were concerned mostly with societal risks, whereas business representatives were concerned with economic risks. This was the first Global Risks Report to explore how our unique perspectives affect our risk perceptions. The global risks barometer is mentioned in an appendix, but it is relocated to the web as an online resource.



Respondent:	Governments	Business	Academia	International Organizations	North America	Europe	Asia
Most concerned about:	Societal risks	Economic risks	Environmental risks	Societal risks	Environmental risks	Societal risks	Environmental risks

Figure C.16. Global Risks 2011: Differences in Risk Perception Among Respondents

In 2012, the graph of the 50 core global risks displays likelihood and impact, instead of severity (Figure C.17), where impact is shown along a generic scale from 1 to 5, which is also the scale used for likelihood ("Global Risks," 2012). The color of the node relates to the category of risk to which it is aligned. It appears that the size of the node relates to its combined increase in likelihood and severity, but there is no key to confirm this. There are also 5 charts which break down the core global risks by each category of risk (economic, environmental, geopolitical, societal, and technological).

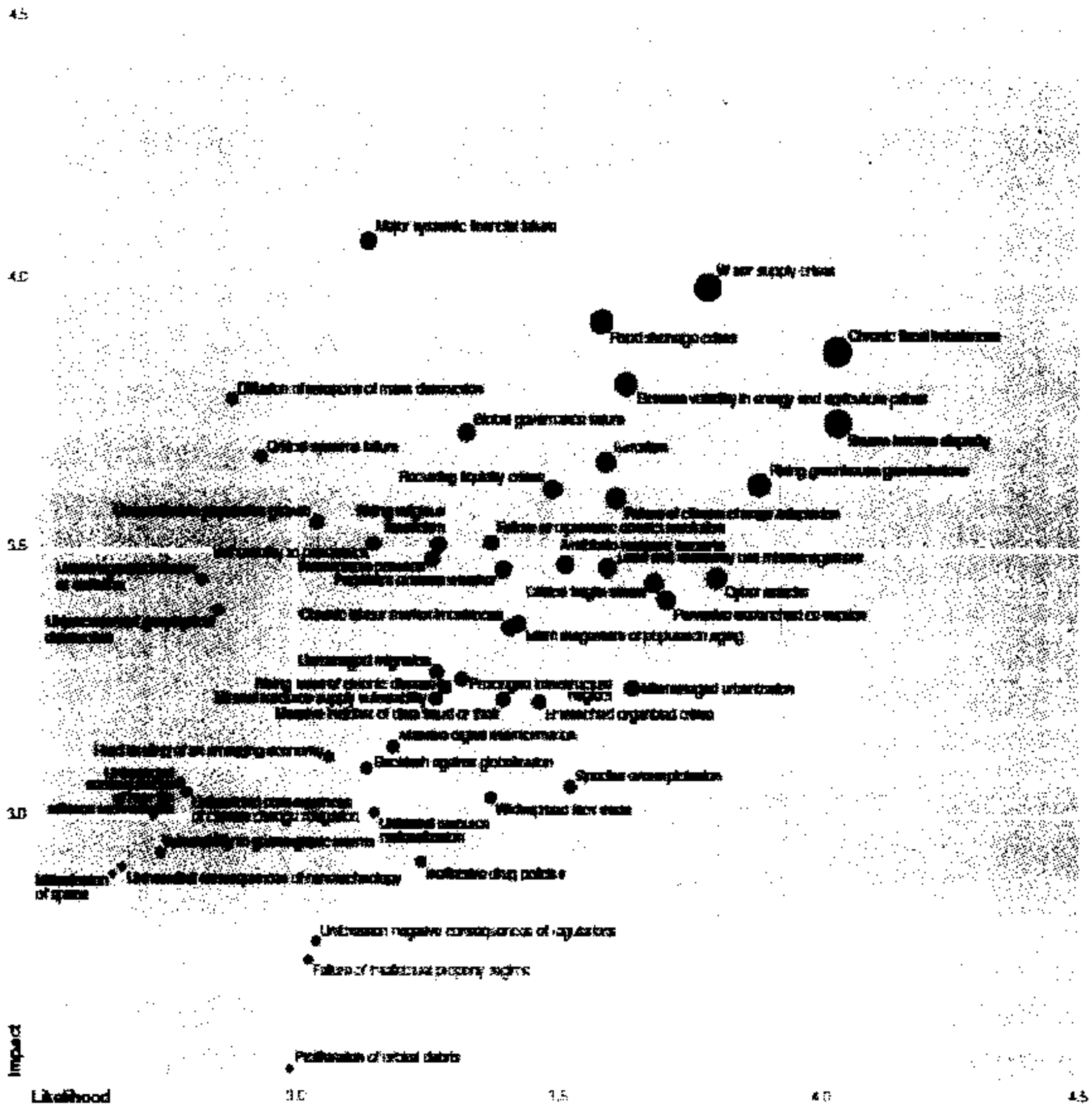


Figure C.17. Global Risks 2012: 50 Core Global Risks

Again, the 2012 report included information on the participants in the Global Risk Perception Survey, as well as additional graphics detailing the risk landscape broken down by respondent regions (Figure C.18). Similar charts were shown to compare the risk landscape broken down by respondent affiliation (business, academia, government, etc.). A new, and interesting visual comparison was presented in this report, which showed how risk perceptions differed between experts in different areas. For example, a risk landscape is shown in Figure C.19 for respondents who claimed to be experts on issues related to one of the risk categories (economic, environmental, geopolitical, societal, or technological) versus all other respondents (also considered experts, but perhaps not in that particular area). Interestingly, the only risk landscapes that appear to differ is the one for environmental issues, otherwise, subject matter area experts and other respondents seem to agree on the likelihood and impact of risks across the different categories ("Global Risks," 2012).

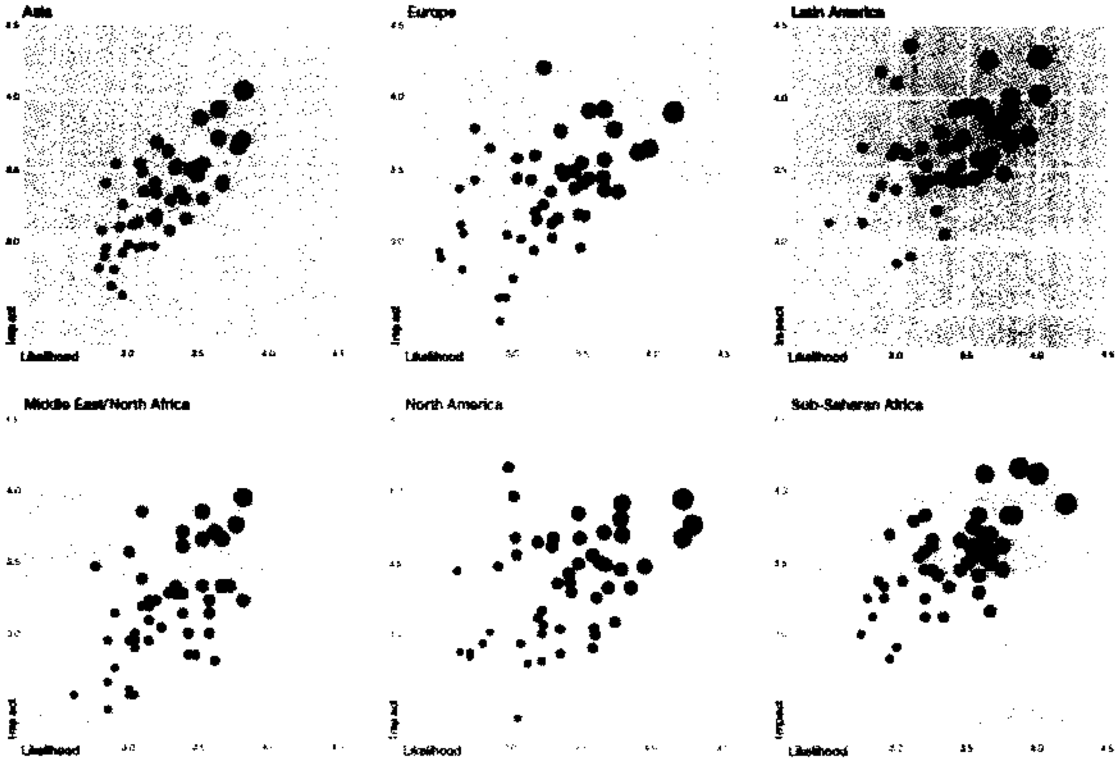


Figure C.18. Global Risks 2012: Risk Landscapes by Region

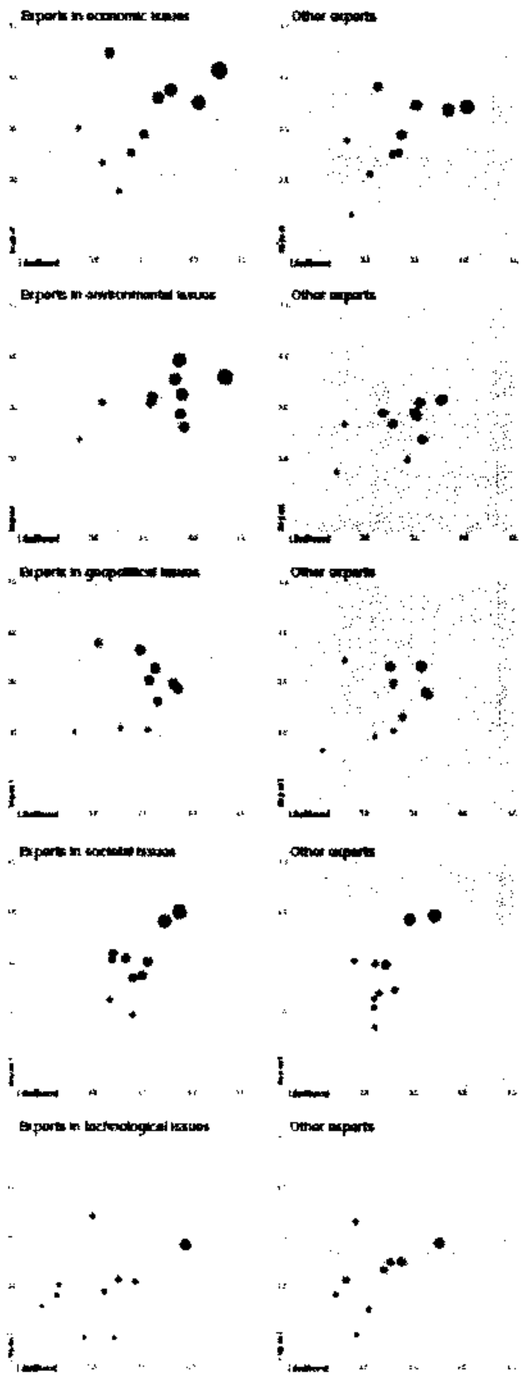


Figure C.19. Global Risks 2012: Risk Perception Comparison of Experts

National Risks: Homeland Security in the United States

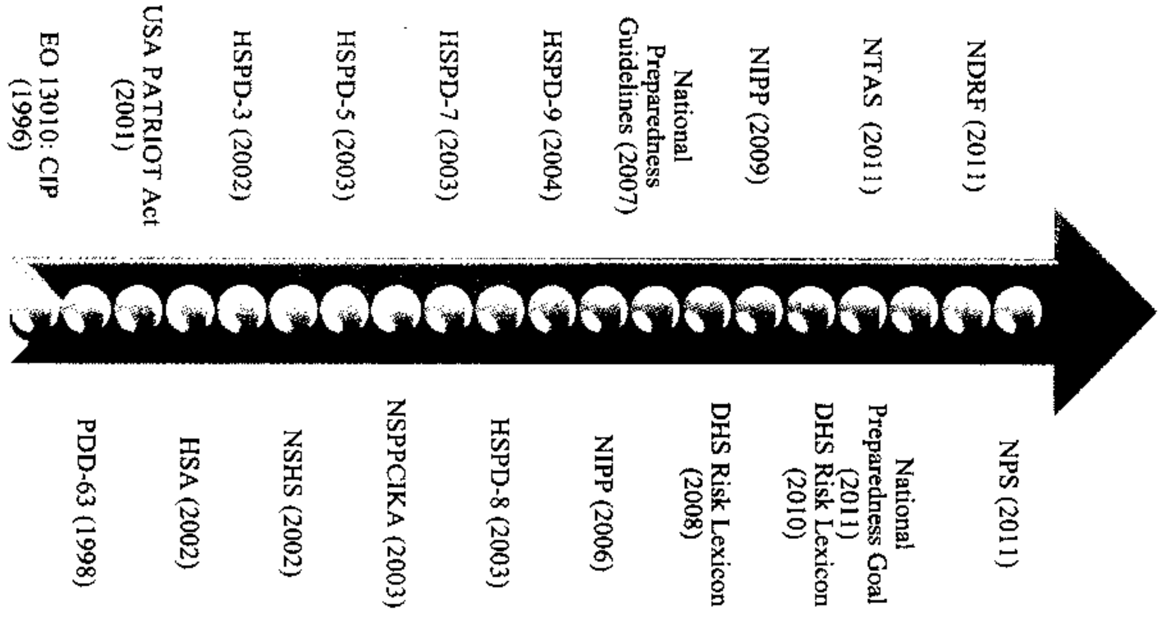


Figure C.20. Homeland Security Timeline

In Figure C.20, a timeline of homeland security and CIP in the United States (US) is provided, consisting of government directives, acts, and plans. In 1996, Executive Order 13010 (EO 13010) introduced the concept of cyber threats and their potential impact to CI (*Executive Order 13010: Critical Infrastructure Protection*, 1996). In 1998, Presidential Decision Directive NSC-63 (PDD-63) set up a national program of CIP (*Presidential Decision Directive (PDD-63/NSC-63)*, 1998). After the September 11th attacks, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) authorized additional measures to prevent terrorism (*USA PATRIOT Act*, 2001). By 2002, the Homeland Security Act (HSA) created DHS, whose mission was to protect the US from terrorists and natural disasters. It also included the Critical Infrastructure Information Act (CIIA), which allows for the voluntary submission of sensitive information regarding CIKR to DHS with the assurance that the information will be protected from public disclosure (*Homeland Security Act of 2002*, 2002).

Homeland Security Presidential Directive 3 (HSPD-3) created a Homeland Security Advisory System (HSAS) with color-coded threats to inform government and public of the current risk of terrorist acts (*HSPD-3*, 2002). The National Strategy for Homeland Security (NSHS) outlined the strategic considerations for cooperation between federal, state, and local government, as well as the private sector, in order to anticipate future terrorist attacks, natural disasters, or other incidents of national significance. It included the National Response Framework (NRF) which acts as a comprehensive emergency management guideline for implementing EPR&R (*NSHS*, 2002). HSPD-5 established the National Incident Management System (NIMS) to cover the prevention of, preparation for, response to, and recovery from terrorist attacks, disasters, and emergencies (*HSPD-5*, 2003). The National Strategy of the Physical Protection of Critical Infrastructure and Key Assets (NSPPCIKA) established a national policy to protect CI and KA from terrorist attacks (*NSPPCIKA*, 2003). In 2003, HSPD-7 added cybersecurity and additional risk management functions to the DHS mission and established the National Infrastructure Protection Plan (NIPP), a framework for CI identification, prioritization, and protection (*HSPD-7*, 2003). HSPD-8 mandated the development of a National Preparedness Goal and the National Preparedness Guidelines, aimed at helping entities at all levels of government build and maintain the capabilities to prevent, protect against, respond to, and recover from major events "to minimize the impact on lives, property, and the economy," (*HSPD-8*, 2003). HSPD-9 merely added agriculture to the list of industries for CIP (*HSPD-9*, 2004).

The 2006 NIPP established a partnership structure for coordination across 18 CIKR sectors, as well as a Risk Management Framework (RMF) to identify assets, systems, networks, and functions whose loss or compromise would pose the greatest risk (*National Infrastructure Protection Plan*, 2006). In 2007, the National Preparedness Guidelines were released and were considered to be a call to action for an all-hazards, risk-based, umbrella for a range of readiness activities (*National Preparedness Guidelines*, 2007). In 2008, DHS introduced the DHS Risk Lexicon, which attempted to establish a comprehensive list of terms and meanings relevant to the practice of homeland security risk management and analysis (*DHS Risk Lexicon*, 2008). The NIPP was updated in 2009 (*National Infrastructure Protection Plan*, 2009) and the DHS Risk Lexicon was updated in 2010 (*DHS Risk Lexicon*, 2010). In 2011, the National Terrorism Advisory System (NTAS) replaced the color-coded threat alert system HSAS ("National Terrorism Advisory System," 2011).

Even more recently, DHS released the National Preparedness Goal, the National Disaster Recovery Framework (NDRF), as well as the National Preparedness System (NPS) (*National Disaster Recovery Framework*, 2011; *National Preparedness Goal*, 2011; *National Preparedness System*, 2011). The National Preparedness Goal defines its mission areas as prevention, protection, mitigation, response, and recovery (*National Preparedness Goal*, 2011). The NDRF provides guidance that enables effective recovery support to disaster-impacted state and local areas, allowing disaster recovery managers at all levels of government to operate in a collaborative effort. It emphasizes restoration, redevelopment, and revitalization, specifically in the areas of health, social, economic, natural, and environmental aspects of the community, making the nation more resilient to disasters or attacks (*National Disaster Recovery Framework*, 2011). The NPS relates directly to the National Preparedness Goal and the National Preparedness Guidelines. It has six mission area components which repeat cyclically: identifying and assessing risk, estimating capability requirements, building and sustaining capabilities, planning to deliver capabilities, validating capabilities, and reviewing and updating (*National Preparedness System*, 2011).

Risk in Homeland Security

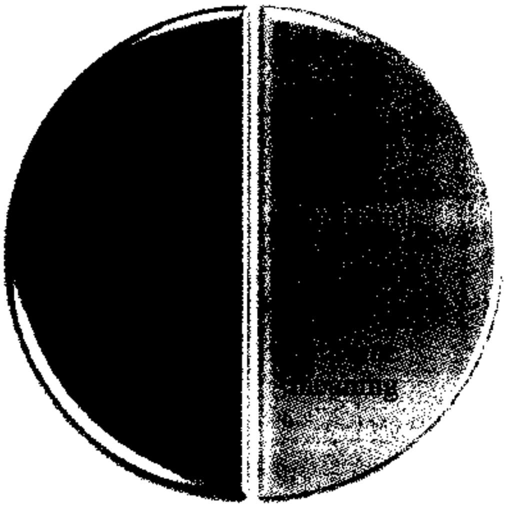


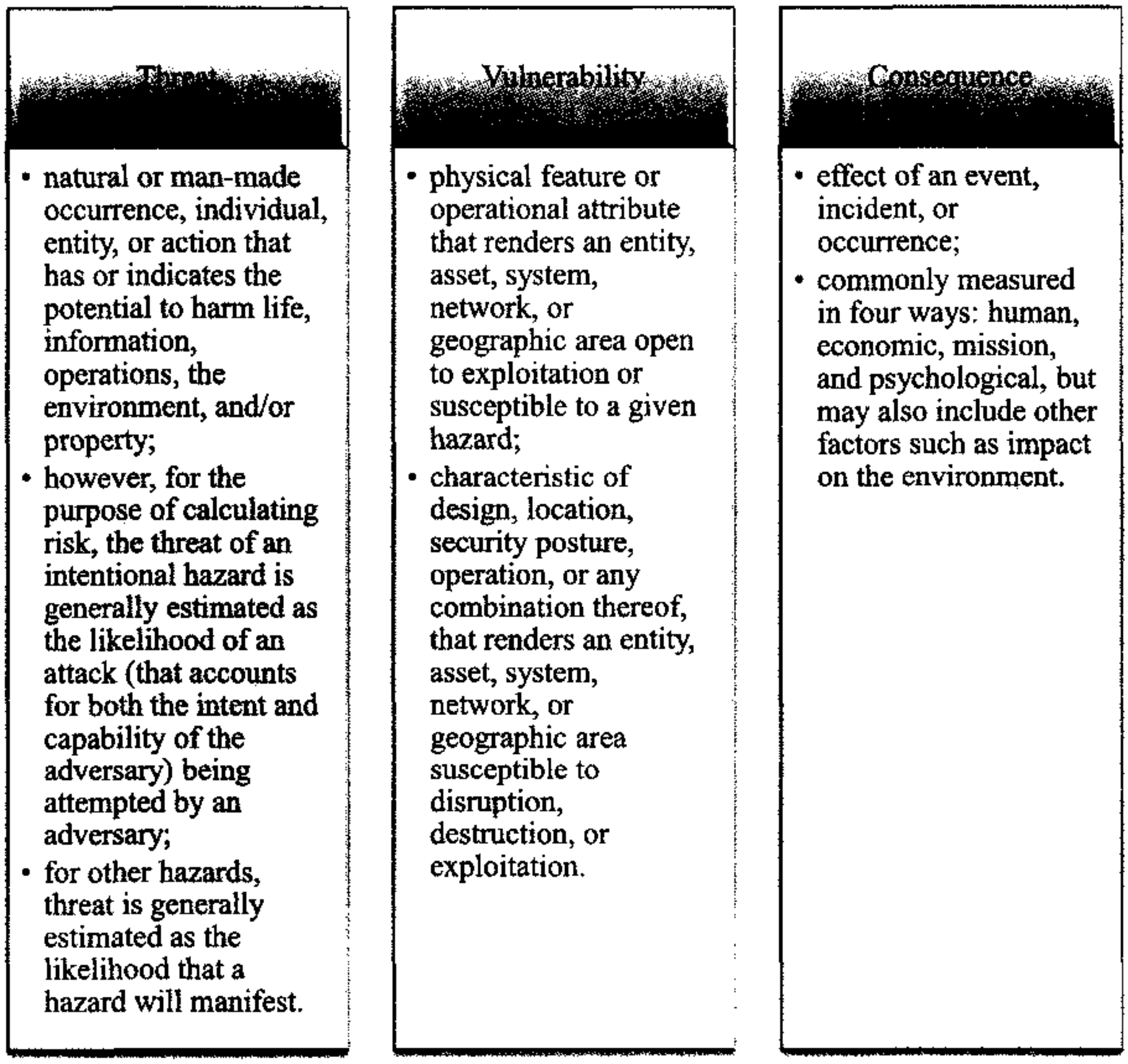
Figure C.21. Theorems on Communication

"Not infrequently confusion arises when experts from different fields attempt to communicate with one another or with laymen about risks," (Becker, et al., 1993). This can probably be attributed to Kaplan's two theorems of communication (Kaplan, 1997) presented in Figure C.21. Kaplan also defined his risk triplet as the set of a scenario, a likelihood, and consequences (Kaplan, 1997), which is still a very common definition throughout the risk literature today.

$$R = f(Threat, Vulnerability, Consequence)$$

Equation C.1. Homeland Security Risk Function

However, risk, at least in the context of homeland security (Equation C.1), is considered to be quite a different triplet, a function of threat, vulnerability, and consequence (*National Infrastructure Protection Plan*, 2009). It is challenging to integrate these disparate assessments to establish an overall picture of risk and exploring their definitions helps us to understand why (Figure C.22). Threat is defined as a likelihood of accident or attack (*DHS Risk Lexicon*, 2010). This may be hard to measure, but at least we know what to measure: a probability. However, risk analysis literature sometimes refers to threat as a scenario and not a probability at all. And the probabilities of certain events (like low probability high consequence events, such as terrorist attacks) are unknown and difficult to estimate due to their infrequency. Vulnerability is more loosely defined and the actual measurement is not defined at all, making it difficult to know what kind of data we would need to collect and analyze (*DHS Risk Lexicon*, 2010). Is vulnerability also a probability? Is it a state of the system where either you are, or are not, vulnerable? Or is it a conditional probability, where the likelihood of vulnerability is contingent upon a successful risk scenario?



Threat

- natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property;
- however, for the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary;
- for other hazards, threat is generally estimated as the likelihood that a hazard will manifest.

Vulnerability

- physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard;
- characteristic of design, location, security posture, operation, or any combination thereof, that renders an entity, asset, system, network, or geographic area susceptible to disruption, destruction, or exploitation.

Consequence

- effect of an event, incident, or occurrence;
- commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment.

Figure C.22.Threat, Vulnerability, and Consequence (DHS Risk Lexicon)

It is acknowledged that consequences could include loss of life (measured in number of deaths or injuries) or loss of money (measured in loss of profit or cost of repairs), but the other types of consequences are more abstract (*DHS Risk Lexicon*, 2010). How would we measure mission or psychological impacts? For example, what were the psychological impacts of 9/11 or of the combined disasters in Japan? Since natural disasters or attacks will almost certainly have psychological impacts, this seems like a pretty important aspect of risk, however, no means of measuring psychological impacts is given. And, perhaps more importantly, how do these psychological impacts affect our future perceptions of risk? Furthermore, how do we integrate different types of consequences, let alone all three components of risk?

Risk

- potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences;
- potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence the potential for an unwanted outcome is often measured and used to compare different future situations;
- may manifest at the strategic, operational, and tactical levels; for terrorist attacks or criminal activities, the likelihood of an incident, event, or occurrence can be estimated by considering threats and vulnerabilities

Risk Analysis

- systematic examination of the components and characteristics of risk

Risk Assessment

- product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making;
- resulting product created through analysis of the component parts of risk

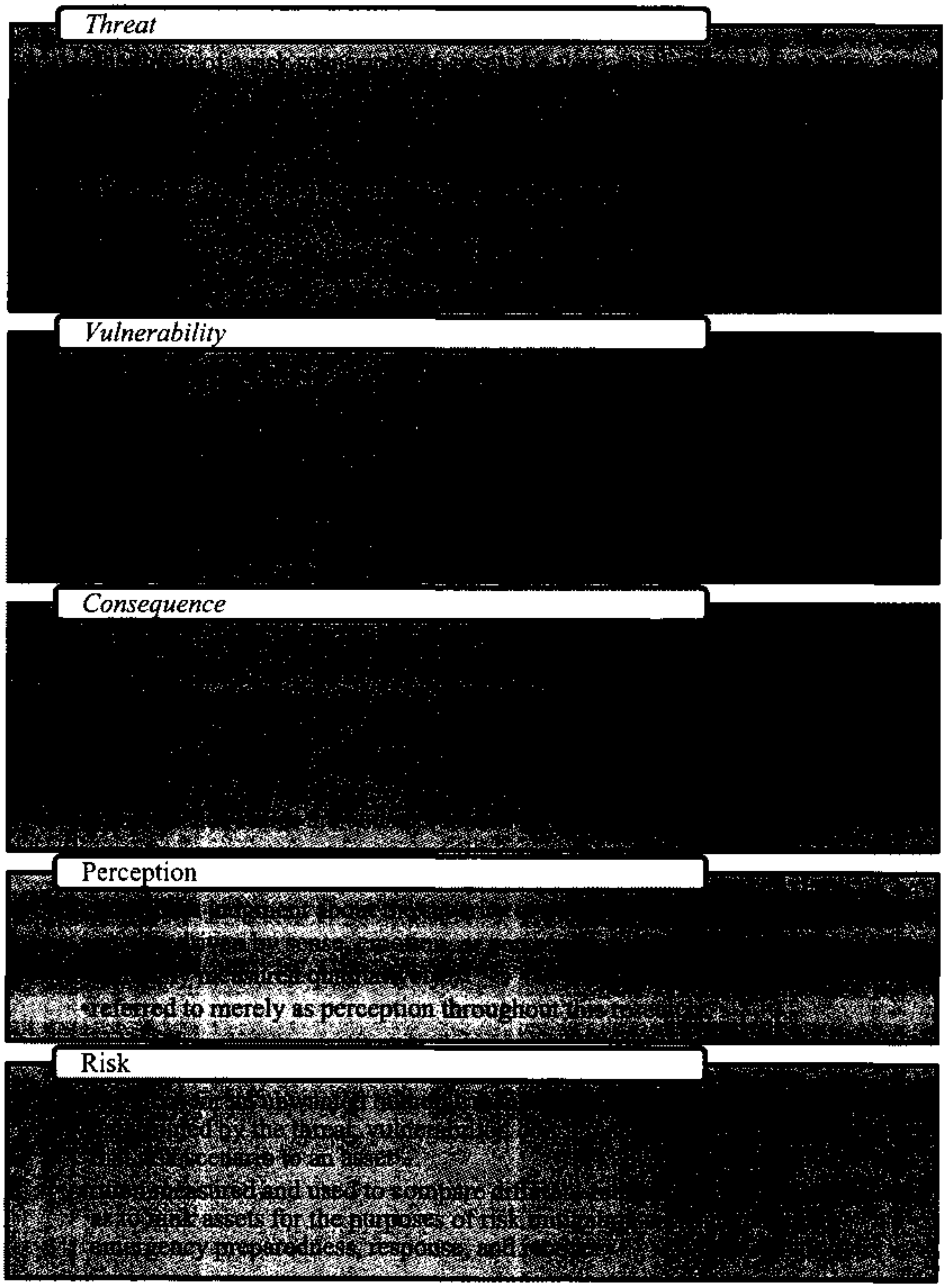
Risk Perception

- subjective judgment about the characteristics and/or severity of risk; may be driven by sense, emotion, or personal experience

Figure C.23. Risk and Related Terms (DHS Risk Lexicon)

In Figure C.23, we see definitions of risk and other related terms (*DHS Risk Lexicon*, 2010). By its very definition, risk analysis is the process by which the components of risk are studied. And risk assessment is the process of collecting data and calculating risk values. But perception, which seems to be a significant component of risk, is segregated, almost ignored, as mere opinion.

Additional definitions from the literature add to the confusion. Ezell reviewed the many definitions of vulnerability, which ranged from the ability to resist and recover from adversity, the actual susceptibility to a threat or risk scenario, or the resilience or survivability of a system to a hazard (Ezell, et al., 2005). He further expands on this by saying that, "vulnerability is a term that is often confused with risk," (Ezell, 2007). While he concludes that vulnerability is a condition of a system, as understood within the context of a risk scenario, others see vulnerability as a probability, or even a conditional probability. For example, risk might be calculated where threat is a scenario with an associated threat severity probability distribution, vulnerability is a conditional probability (the probability of a successful attack, given the attack is identified), and consequence is based on a loss function (McGill, et al., 2007). Other expert judgment-based risk methodologies might simply use descriptive words like high, medium, or low to describe the characteristics of risk (Mallor, García-Olaverri, Gómez-Elvira, & Mateo-Collazas, 2008). Many risk keywords have numerous, and sometimes conflicting, definitions, such as threat which might be considered the description of a scenario or the likelihood of a scenario. And there are also many words which have similar definitions, such as threat, hazard, and scenario, all of which refer to an event, but not necessarily its probability. In order to be consistent throughout this research, we will redefine a number of pertinent terms (Figure C.24).



Threat

[illegible]

Vulnerability

[illegible]

Consequence

[illegible]

Perception

[illegible] referred to merely as perception throughout this [illegible]

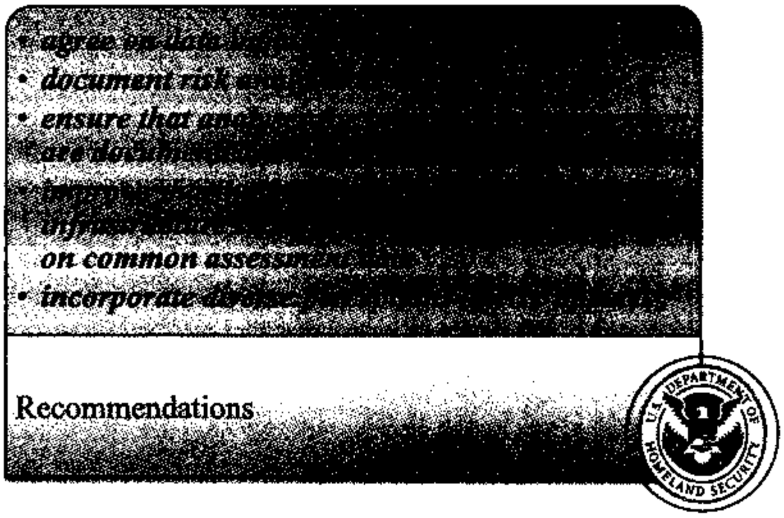
Risk

[illegible] and used to compare [illegible] to rank assets for the purposes of risk [illegible] emergency preparedness, response, and [illegible]

Figure C.24. Threat, Vulnerability, Consequence, and Perception (Revised)

Similar to Kaplan, we will also use the term risk scenario. Basically, risk scenarios are the answers we provide when we are asked, "What can go wrong?" (Kaplan, Haimes, &

Garrick, 2001). More formally, a risk scenario is a natural or man-made occurrence, hazard, individual, entity, or action that has or indicates the potential to damage an asset. So this distinguishes the term risk scenario from threat, and when we refer to threat, we speak of the likelihood of a risk scenario. Vulnerability is considered the ability of an asset to endure a risk scenario (Gheorghe, et al., 2008). And consequence is a measure of the impacts resulting from a successful risk scenario. Risk perception is a subjective judgment about the severity of a risk scenario to an asset, and will be referred to as perception throughout this research. For the purposes of this research it is considered possible to estimate threat, vulnerability, consequence, and perception quantitatively or qualitatively. Finally, we define risk as the potential for an unwanted outcome resulting from a risk scenario, as determined by the threat, vulnerability, consequence, and perception of that risk scenario to an asset.



- *agree on data* [illegible]
- *document risk* [illegible]
- *ensure that an* [illegible]
  are docum [illegible]
- *impr* [illegible]
  inform [illegible]
  on common assess [illegible]
- *incorporate diverse* [illegible]

Recommendations

Figure C.25. Review of the DHS Approach to Risk Analysis Recommendations

In 2010, based on a request from congress, the National Research Council (NRC) established a committee which issued the "Review of the DHS Approach to Risk Analysis" ("Review of the DHS Approach to Risk Analysis," 2010). The committee examined how

DHS was building its capabilities in risk analysis for decision making. It evaluated the quality of the current DHS approach to estimating risk and applying those estimates in its management, planning, and resource allocation (including grant-making) activities, through the review of a committee-selected sample of models and methods. It assessed the capability of DHS risk analysis methods to appropriately represent and analyze risks from across the spectrum of activities and responsibilities, including both terrorist threats and natural disasters and how well they support DHS decision making. The committee reviewed the feasibility of creating integrated risk analyses covering the entire DHS program areas, including both terrorist threats and natural disasters, and made recommendations for best practices, including outreach and communications. And finally, the committee made recommendations for how DHS could improve its risk analyses and how those analyses could be validated to provide improved decision support. The committee uncovered many of the problems already discussed, including a recommendation to "incorporate diverse perceptions of risk impacts", a key element of the proposed risk quadruplet. Some highlighted recommendations are given Figure C.25.

DHS maintains the Regional Resiliency Assessment Program (RRAP) to assess CIKR, including interdependencies, along with a regional analysis of the surrounding area ("Regional Resiliency Assessment Program," 2012). Similarly, DHS conducts a Strategic National Risk Assessment (SNRA) to support FEMA with respect to the National Preparedness Presidential Policy Directive (PPD-8) and the DHS National Preparedness Goal (*National Preparedness Goal*, 2011; *Presidential Policy Directive (PPD-8): National Preparedness*, 2011; "Strategic National Risk Assessment," 2012). PPD-8 states that, "The national preparedness goal shall be informed by the risk of specific threats and vulnerabilities…" (*Presidential Policy Directive (PPD-8): National Preparedness*, 2011). The National Preparedness Goal states that, "All levels of government and the whole community should present and assess risk in a similar manner to provide a common understanding of the threats and hazards confronting our Nation…" (*National Preparedness Goal*, 2011), noting that the information gathered during a risk assessment also allows for the prioritization of preparedness efforts. While the specific results of the SNRA are classified, it affirmed the need for an all-hazards, capability-based approach to preparedness planning. The analytic approach to the SNRA leveraged "data and information from a variety of sources, including existing Government models and assessments, historical records, structured analysis, and judgments of experts from different disciplines" (*The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*, 2011). The SNRA assessed the risk of identified risk scenarios (which were broken down into three categories: natural, technological or accidental, and adversarial or human-caused). Interestingly, risk for the SNRA was assessed as a function of frequency (that a risk scenario would occur) and consequence (the impacts should the risk scenario occur); vulnerability was not assessed. Additionally, six categories of consequence were explored including, "loss of life, injuries and illnesses, direct economic costs, social displacement, psychological distress, and environmental impact" (*The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*, 2011).

Critical Infrastructure, Key Resources, and Key Assets

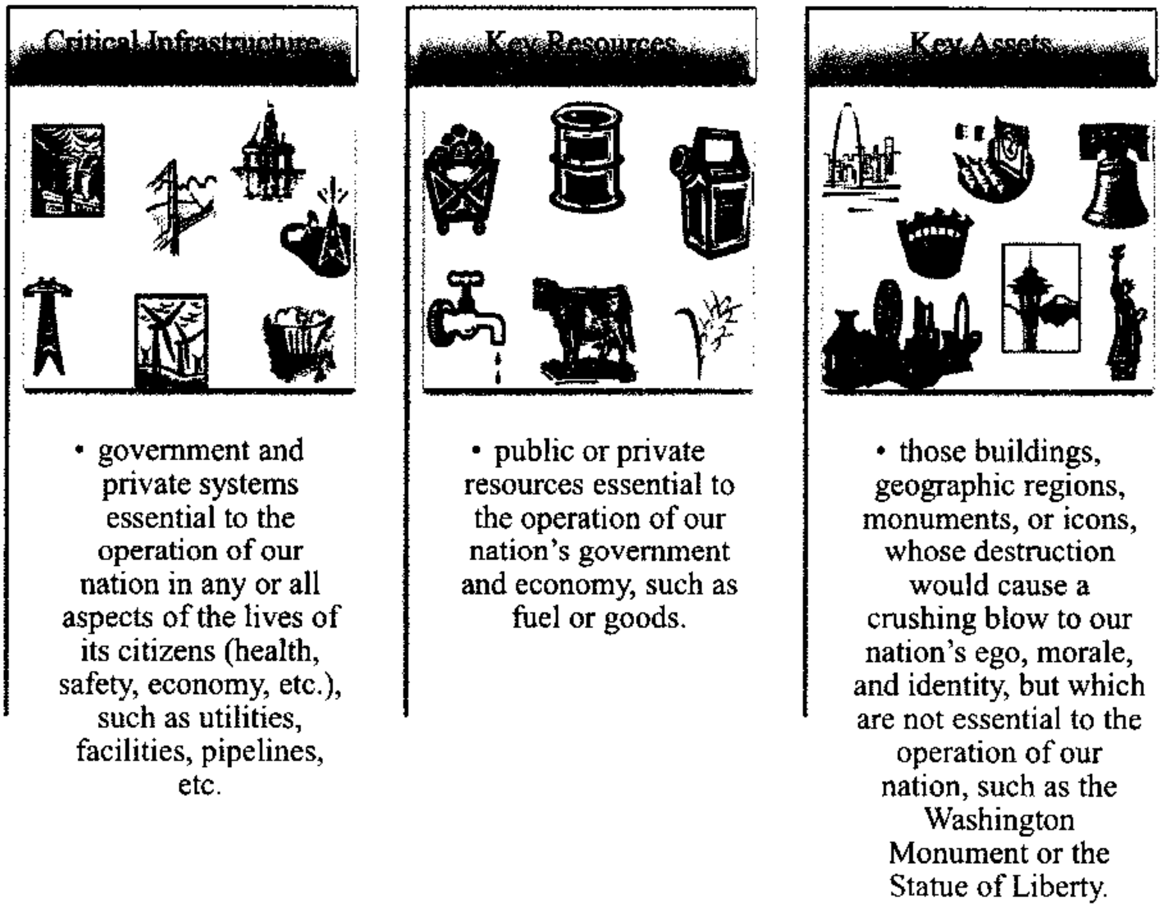
The definitions of CIKRKA have evolved over time (*Critical Infrastructure and Key Assets: Definition and Identification*, 2004). After a review of the authoritative literature which addresses CIKRKA, it is clear that there exists some confusion over these terms, which provide the foundation of, and context for, CIP in the realm of homeland security and homeland defense. Most federal documents now refer to the combined term CIKR. KA is now an outdated term after being officially replaced by DHS in a footnote of the NIPP (*National Infrastructure Protection Plan*, 2006). However, it is recommended that we resurrect the defunct definition because these items are unique and deserve to be explored independently.

The official definitions are given below:

- *Critical infrastructure:* assets, systems, and networks, whether physical or virtual, so vital to the US that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof (*DHS Risk Lexicon*, 2010)
- *Key resources:* publicly or privately controlled resources essential to the minimal operations of the economy and government (*DHS Risk Lexicon*, 2010)
- *Key assets:* individual targets whose attack—in the worst-case scenarios—could result in not only large-scale human casualties and property destruction, but also profound damage to our national prestige, morale, and confidence (*NSPPCIKA*, 2003)

But even these definitions are not ideal; they are self-referential and they are not mutually exclusive. Of course, given the inherent overlap between CIKRKA, such as the

Hoover Dam, it may be impossible to craft mutually exclusive definitions. Revised definitions are proposed below (Figure C.26). Additionally, we will define the term assets, the collective, generalized term used to represent the combination of all CIKRKA.



Critical Infrastructure

- government and private systems essential to the operation of our nation in any or all aspects of the lives of its citizens (health, safety, economy, etc.), such as utilities, facilities, pipelines, etc.

Key Resources

- public or private resources essential to the operation of our nation's government and economy, such as fuel or goods.

Key Assets

- those buildings, geographic regions, monuments, or icons, whose destruction would cause a crushing blow to our nation's ego, morale, and identity, but which are not essential to the operation of our nation, such as the Washington Monument or the Statue of Liberty.

Figure C.26. Critical Infrastructure, Key Resources, and Key Assets (Revised)

In a Congressional Research Service (CRS) report, the definitions of CIKRKA were explored. A table was presented that illustrated the introduction of CIKR sectors over time, based on their mention throughout different government documents (*Critical Infrastructure and Key Assets: Definition and Identification*, 2004). This table has been updated (Table C.5) and is presented below to show how the list of sectors has evolved over time, even since the table was first presented in 2004.

Table C.5. History of Critical Infrastructure and Key Resources Sectors

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Banking and Finance	X	X	X	X	X	X
Communications	X	X	X	X	X	X
Emergency Services	X	X	X	X	X	X
Energy	X	X	X	X	X	X
Government Facilities	X	X	X	X	X	X
Transportation Systems	X	X	X	X	X	X
Water	X	X	X	X	X	X
Healthcare and Public Health		X	X	X	X	X
Information Technology		X	X	X	X	X
Agriculture and Food			X	X	X	X
Chemical			X	X	X	X
Defense Industrial Base			X	X	X	X
Commercial Facilities				X	X	X
National Monuments and Icons				X	X	X
Postal and Shipping				X	X	X
Dams					X	X
Nuclear Reactors, Materials and Waste					X	X
Critical Manufacturing						X

There are greater system of systems comprised of multiple CI, which in conjunction with the KR (the inputs and outputs from these system of systems), aim to meet the daily essential operating needs of our nation. For example, a water treatment plant (CI) requires electricity (KR) to operate and that electricity reaches the plant through an electric power grid connected to a power plant. But that power plant requires fuel in order to generate electricity, and in most cases, that fuel must be transported to the power plant via train or truck, and so on. So that water treatment facility might be directly compromised by any number of CI failures, such as a delayed delivery of fuel to a power plant, which leads to a power outage. But, that same water treatment plant not only requires power, but it also requires water (KR), so if water pipelines (a CI system necessary for delivering a KR) are compromised, or if there is a drought, then a similar problem exits: there would be no clean drinking water. Furthermore, this domino-effect could continue, because the lack of clean drinking water could cause a local health epidemic, which could create a strain on hospitals, which may lack the capacity to treat the influx of patients or which may also be suffering from the power loss. Examining individual CI is not sufficient if the goal is the protection of the greater system of systems of CIKR.

Below is a list of the latest DHS CIKR sectors (Table C.6). Using the new definitions of CIKRKA given above, the National Monuments and Icons, Commercial Facilities, and Government Facilities sectors are comprised mostly of KA, not CI or KR. The remaining sectors typically consist of both CI and KR. For example, the Energy sector consists of not only power plants and power lines, but also of the coal or gas used to generate that power, and the Critical Manufacturing sector consists of the iron and steel which it produces and processes in mills or plants. There are also many obvious dependencies and interdependencies which add to the complexity of CIKRKA protection. For example, the Energy sector is dependent upon the Communications sector to provide the information technology infrastructure required to operate power plants or natural gas pipelines, such as Supervisory Control and Data Acquisition (SCADA) systems, while the Communications sector would be nearly paralyzed if there were a power failure.

Table C.6. Critical Infrastructure and Key Resource Sectors

Agriculture and Food	Energy
Banking and Finance	*Government Facilities*
Chemical	Healthcare and Public Health
Commercial Facilities	Information Technology
Communications	*National Monuments and Icons*
Critical Manufacturing	Nuclear Reactors, Materials and Waste
Dams	Postal and Shipping
Defense Industrial Base	Transportation Systems
Emergency Services	Water

Furthermore, there is also an obvious overlap between some CI and KA (Figure C.27). In these situations, if the KA has a primary function as a CI, then it is aligned to that sector, although the secondary sector, for which the CI is a KA, may also collaborate with the primary sector, at least for the purposes of risk assessment. For example, the Hoover Dam, while iconic, is aligned to the Dam sector (*National Monuments and Icons: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007).

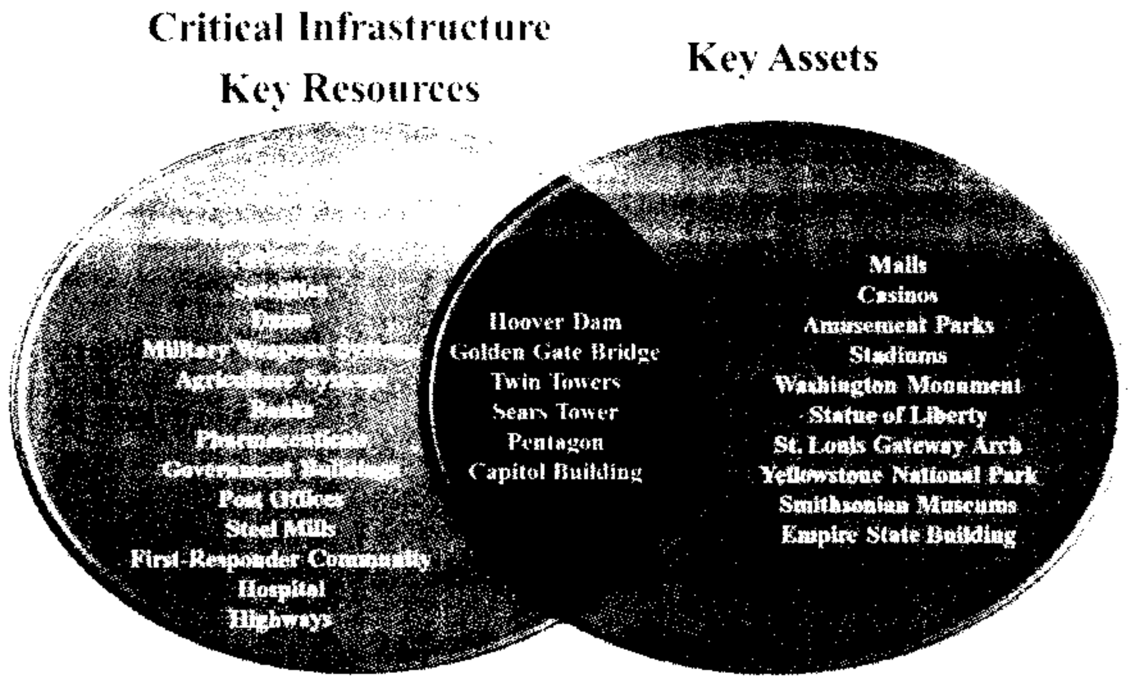
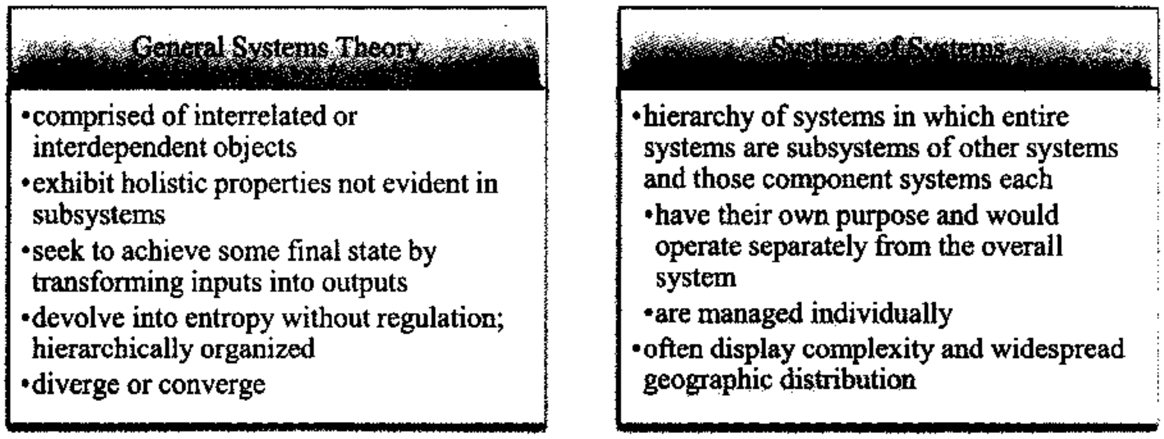


Figure C.27. Intersection of Critical Infrastructure and Key Assets

Systems and System of Systems

According to general systems theory, there are a number of attributes that define systems. Systems are comprised of interrelated or interdependent objects. Systems exhibit holistic properties not necessarily evident at the level of individual objects or subsystems. Systems seek to achieve some final goal or state, and in order to reach this goal they transform inputs into outputs. Systems tend to devolve into entropy without regulation and are typically organized in a hierarchical system of nested subsystems where the subsystems are specialized with different functions within the system. Finally, a system either diverges, in which case it has many ways of achieving a single goal, or it converges, where, from an initial state, it could achieve many different goals (Skyttner, 2005).

Quite simply, many of these same attributes hold true for a system of systems, just on a much larger scale (Figure C.28). Skyttner describes the system of systems phenomenon as a "hierarchy of systems" in which systems are components of, or rather, subsystems of, other systems (Skyttner, 2005). A system would be considered a "system of systems" when its component systems each have a purpose of their own and would continue to operate even if separated from the overall system, and if those component systems are managed individually, rather than being managed within the context of the entire system of systems (Maier, 1998). However, this does not address the issue of scale. By this definition, a single condominium unit could be a system of systems, having many subsystems such as heating and running water, each of which are managed separately by the different utility companies, or, examined from a different perspective, the entire condominium complex could be a system of systems where each condo is managed separately by its owner, and so on. Often, the concepts of complexity and geographic distribution are also introduced when referring to system of systems (Maier, 1998).



General Systems Theory

- •comprised of interrelated or interdependent objects
- •exhibit holistic properties not evident in subsystems
- •seek to achieve some final state by transforming inputs into outputs
- •devolve into entropy without regulation; hierarchically organized
- •diverge or converge

Systems of Systems

- •hierarchy of systems in which entire systems are subsystems of other systems and those component systems each
  - •have their own purpose and would operate separately from the overall system
  - •are managed individually
- •often display complexity and widespread geographic distribution

Figure C.28. General Systems Theory and System of Systems

It is obvious that system of systems face different issues from traditional systems (Sheard & Mostashari, 2009). Typically, system of systems seek to integrate many independent systems which were built for other, albeit related, purposes. These system of systems must often develop quickly in order to continue to meet the demands of the user, as well as the demands of the overall system of systems, such as policy demands or technological demands. As with complex systems problems, there are many different stakeholders, each with different perspectives and requirements, some of whom do not wish to participate in, or simply do not understand that they are a part of, a greater system of systems. System of systems also usually depend on integrated computing infrastructure. Further complicating things, there is distributed development for these systems, not just geographically, but managerially, and technologically. For example, the individual management of one system in California could require its computing infrastructure to be upgraded, but the upgrade then renders the individual system incapable of communicating with its related systems in New York (Sheard & Mostashari, 2009).

Traditional systems engineering can solve system problems and even some complex system problems. However, systems are increasingly complex, and systems engineers are inundated with systems information, some of which may be conflicting without clear authoritative sources, they are overwhelmed by the seemingly infinite interdependencies of systems, and they struggle to keep up with the constantly changing missions and policies governing different systems (Keating, Sousa-Poza, & Mun, 2004). Systems engineers typically focus on a single complex problem and engineer (or modify) a single complex system to address that problem. System of Systems engineers must focus on "integrating multiple complex systems," which could be achieved by integrating existing systems into a larger system of systems, or by engineering new systems in order to integrate existing systems, or by replacing existing subsystems so that the larger system of systems is more interoperable, or by replacing the entire system of systems all together (Keating, et al., 2003).

The risk management approach to system of systems also presents its own list of issues. For example, differences in the perspectives and goals of multiple stakeholders could lead to problems with funding or scheduling; differences in risk management practices across different subsystems could lead to risk oversights; and risk integration, or interdependencies, are often not evaluated, rather subsystems focus on their individual risks (Conrow, 2005). All of these concerns may ultimately increase risk for system of systems.

The 2009 NIPP mentions system of systems once, and only in reference to the international dimension of homeland security and CIP (*National Infrastructure Protection Plan*, 2009). The Critical Infrastructure Information Act of 2002 makes reference to a protected system, which is defined as "any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of CI or KR; and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage" (*Critical Infrastructure Information Act*, 2002). It could be argued that the more appropriate term here would be a protected system of systems as the viability of a single CIKRKA could be compromised by its interaction with, and interdependence upon, multiple systems.

System of Systems: Critical Infrastructure and Key Resources

It can be easily argued that CI are not only systems, but system of systems. It is also quite simple to extend the definition of system of systems to include the systems responsible for KR as they relate directly to CI. In fact, infrastructure (not just CI, but all infrastructure) has already been defined as a system of systems which transfers fundamental goods or services from one point in the system to another point in the system (Gheorghe, et al., 2008).

Maier suggests that each component system must have a purpose of its own such that it would continue to operate even if disconnected from the overall system of systems and he also argues that the component systems must be primarily managed individually, rather than managed from within the context of the entire system of systems (Maier, 1998). There are a number of ways of disaggregating system of systems and there are many more models for managing systems, but the Transportation Systems sector has actually generated an elegant approach for disconnecting and reconfiguring its unwieldy system of systems (Figure C.29). They propose four different risk views, used for the purposes of analyzing risk, which offer a systematic way of disaggregating or reorganizing system of systems into more manageable components, and one of those views even teases out the system owners and operators (the individual system managers). These four views include modal, geographic, functional, and ownership and are depicted in Figure C.29 (*Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007). Looking at the Transportation Systems infrastructure from different perspectives also allows for the observation of emergent system of systems properties which might not be apparent across all perspectives.

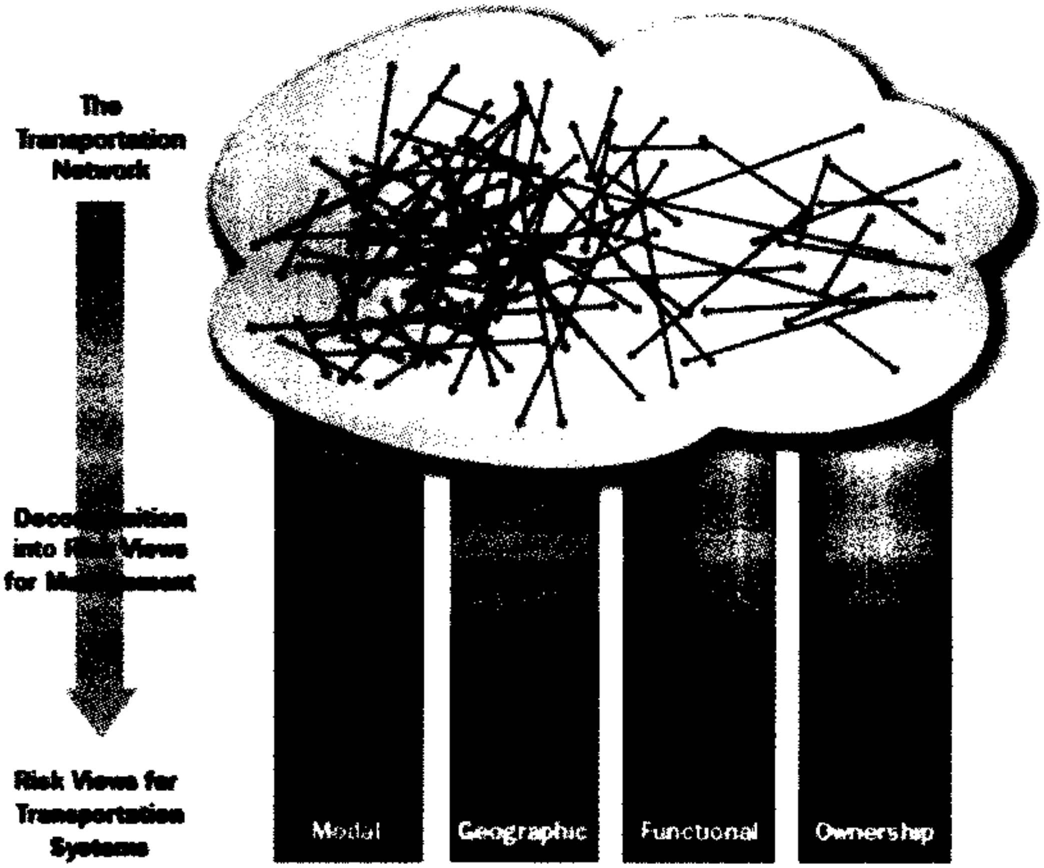

The Transportation Network
Decomposition into Risk Views for Management
Risk Views for Transportation Systems
Modal
Geographic
Functional
Ownership

Figure C.29. Transportation Systems Sector Risk Views

The modal view consists of six modes: aviation, maritime, mass transit, highway, freight rail, and pipeline. Delineating the sector along its different modes of transportation is the most common way of viewing the sector and it allows all assets from a given mode to be collectively evaluated as a single system. The functional view disaggregates the Transportation Systems sector by function, which is described as "the service, process, capability, or operation performed by specific infrastructure assets, systems, or networks". In this view, all assets that share a specific function or service, usually supply chain-focused, are grouped together. The geographic view looks at the system of all transportation assets in a particular region, state, or city. The ownership view groups all assets that are owned and operated by the same company or agency. Together, these four views capture different ways of looking at transportation systems and their dependencies and interdependencies, allowing for a robust assessment of the sector.

From a system of systems perspective, these different views offer a very interesting approach, which in and of itself, almost perfectly addresses Maier's two components for defining a system of systems. Each of these component systems would function independently, regardless of whether they comprise a greater system of systems. For example, the aviation system operates independently from the highway system or, geographically speaking, the Seattle system operates independently from the Miami system. Furthermore, many of these systems (or groups of systems) are managed individually, so while highways might be managed by their respective state's department of transportation, marine ports might be managed by the navy or the state's port authority. The complicated integration of these systems through necessity (transportation is a vital service for any nations' citizens) or through overarching policies (like those of the National Transportation Safety Board, in this case) creates a massive system of systems, which, itself is only one system within the even greater and even more complex system of systems which includes all of the nation's CIKR (for example, the Transportation Systems sector is extremely dependent upon the Energy sector for fuel).

Interestingly, Gheorghe's definition of a system of systems refers directly to CI (Gheorghe, et al., 2008). A system of systems is defined by Gheorghe as the combination of several interdependent CI showing the characteristics of a single system, but lacking on overarching management entity. In the latter part of the definition, he and Maier seem to agree that the greater system of systems lack centralized command and control, so to speak. However, with the advent of DHS and its CIKR protection initiatives, do these CIKR system of systems now possess central management?

Another attribute often ascribed to system of systems is the notion of geography; typically a system of systems is spread over a much larger geographic region than a single system. Gheorghe notes that the "ever-accelerated geographical expansion of the energy, transportation, and telecommunications infrastructure has resulted in the emergence of enormous networks that transcend national borders and even continental shores" (Gheorghe, et al., 2008). Again, the Transportation Systems sector offers itself as a wonderful example of how a large system of systems can quickly span a major metropolitan area through highways and mass transit, then suddenly expand to include the air above the region, the water along its coastlines, even the pipelines beneath the ground.

A geographically widespread system composed of independent and individually managed CIKR systems, which, when integrated, exhibit dependent, or even interdependent, component systems, should most definitely be considered a system of systems. However, describing such a system of systems is sort of like describing a fractal; every time you get to one node in the complex system of systems, there are multiple nodes which split and regenerate in similar or slightly altered ways, some even turning back in on themselves. Starting at what might be considered an initial system node in the Energy sector, we can pinpoint the CI, such as oil rigs, which are designed specifically for the production of KR, such as oil and gas. Then there are CI designed to distribute that crude oil and gas to nearby refineries or processing plants. Refineries and processing plants transform KR, as they are designed to input crude oil and gas, and output refined oil and gas fit for end users. Additionally, there are CI systems which further distribute these KR, such as pipelines which transport natural gas to homes for cooking or heating. Sometimes the fuel is further transformed by a system, like when natural gas is used in a power plant to generate electricity. And speaking of electricity, there are even more CI to distribute the KR of electricity, which powers countless other assets, including the very oil and gas production facilities described at the beginning of this example.

System of Systems: Key Assets

The National Monuments and Icons sector is composed of assets, systems, networks, and functions throughout the US, many of which are listed in the National Register of Historic Places or the List of National Historic Landmarks (*National Monuments and Icons: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007). In general, these assets do not have a purpose or function which aligns to one of the other CIKR sectors. This sector includes KA which may be physical structures like monuments, operational staff (and visitors), historical or significant documents and objects, as well as geographic areas, like parks or historical areas.

The Commercial Facilities sector is similar to the National Monuments and Icons sector in that it is also comprised of KA, such as arenas, stadiums, museums, casinos, amusement parks, and malls ("Commercial Facilities Sector: Critical Infrastructure and Key Resources," 2010). The Government Facilities sector consists of buildings such as embassies and courthouses, which could also be considered KA ("Government Facilities Sector: Critical Infrastructure and Key Resources," 2010). Further distinguishing these sectors, is their lack of extreme interdependencies with other sectors, which is so apparent when examining other CIKR system of systems. These KA usually depend on other sectors for the operation of the physical structures (power, water, communications, etc.), but the relationship is one way; there is no case where a CI or a KR would be directly dependent on a KA, unless that KA overlapped with another sector, in which case it would be classified as a CI. For example, the Hoover Dam, while iconic, is aligned to the Dam sector, and considered primarily a CI, and similarly the Golden Gate Bridge is aligned to the Transportation Systems sector.

Maier's definition for system of systems seems to apply when first examining KA. KA are individually managed and would, indeed, operate for their own purpose if separated from a greater system of systems. For example, the Statue of Liberty would continue to operate even if the Mall of America in Minneapolis was closed, and KA are not typically managed by the same agency or company, although some groups of monuments are managed collectively such as the Lincoln Memorial and the Washington Monument (among others), which are all part of the National Mall and Memorial Parks, operated by the National Park Service with the US Department of the Interior (DOI) ("Lincoln Memorial," 2011b). However, Maier's definition requires KA to first be considered a system, before being considered components of a greater system of systems (Maier, 1998). And, according to Skyttner, KA may not be considered systems because they do not seek to achieve some final goal or state by transforming inputs into outputs (Skyttner, 2005). KA do not have a traditional systemic purpose and are not seeking to produce, transform, or transport anything. Future research might shed some light on how this distinction impacts the inclusion of KA in the greater CIKR system of systems, especially for the purposes of ranking those assets based on risk.

Risk Analysis

Defining risk and risk management is no easy feat. However, it is a necessary step before we can explore how we calculate risk, or how we perceive risk. Linguistically, risk suffers from *risk-archipelago syndrome* (Althaus, 2005), in other words, a number of distinct specializations have evolved due to the wide range of definitions for risk (such as risk perception, risk analysis, risk mitigation, and so on). The origin of the term is disputed, but reviewing the possible etymology of the word may explain why we still struggle to define this word today. Risk could be derived from the Arabic word *risq* which basically translates as something you received from which you can profit; or from the Latin word *risicum* which refers to the challenge posed to sailors by a barrier reef (Althaus, 2005). More recently, different professional organizations describe risk as "the potential for realization of unwanted, adverse consequences", the "(perceived) feeling of insecurity and fear due to undesirable consequences", the "probability of the occurrence of (the risky) event multiplied by the consequence of the event, given that it has occurred", or even as "events that if they occur can jeopardize the successful completion of the projects" (Pinto, 2008).

Further complicating risk analysis, systems now consist of many separate parts which, together, provide an overarching capability not achievable at the level of the individual subsystems (Garvey & Pinto, 2009). These system of systems do not have clear boundaries, requirements, or specifications, so managing these risks is much more challenging (Garvey & Pinto, 2009). Additionally, the analysis of risk is typically considered to be scenario-driven, in other words, we cannot analyze a risk unless we can conceive of such a risk (Pinto, 2008), and obviously that brings us back to our perceptions of risk.

Risk Calculation

Risk is often calculated as the product of the probability that a risk event will occur and the magnitude of the consequences should the risk event occur (Kasperson, et al., 1988). Quantitative Risk Assessment (QRA) and Probabilistic Risk Assessment (PRA) are direct applications of this definition, in which both assessments typically aim to answer the same three questions: 1) what can go wrong? 2) how likely is it? and 3) what are the consequences? (Apostolakis, 2004). Later, the concept of vulnerability was introduced to form the current risk triplet often shown in a deceivingly straightforward equation given in Equation C.1 where Risk is a function of threat, vulnerability, and consequence. Threat is usually the probability of an attack (or accident) occurring, vulnerability is often considered to be the probability of a successful attack, and consequence is the magnitude of the impact given that the attack occurs and that it was successful (based on the level of vulnerability at the time of the attack). Others have argued that this equation is inadequate and misleading (Cox, 2008), citing a multitude of reasons. Just one example would be the arithmetic distortions which could reverse the proper risk ranking of two risks if one has high vulnerability and low consequence while the other has high consequence and low vulnerability. Algebraically reorganizing Equation C.1 produces an alternate equation (Equation C.2) that, when examined, would lead to some interesting results.

$$Vulnerability = Risk / (Threat * Consequence)$$

Equation C.2. Homeland Security Risk Function (Rearranged)

Ignoring for the moment that threat and vulnerability are probabilities, and simply examining the relationships implied by Equation C.2, we see that vulnerability is inversely proportional to threat, so as threat increases, vulnerability would decrease, but that does not make sense. Vulnerability, intuitively, cannot decrease unless measures are taken to either reduce the likelihood of an attack (if that is possible to control), or to reduce the potential for success of an attack. This might be akin to a soccer team which wants to have a good offense, and failing that, a good defense. Vulnerability is also inversely proportional to consequence, so as consequence increases, vulnerability would decrease. Again, vulnerability can only be altered by the measures taken to reduce the probability of success of an attack, and increasing the potential consequences of an attack would not be a good way of reducing the vulnerability of an attack.

More interesting relationships are uncovered when we account for the fact that threat and vulnerability are often both considered probabilities and while the product of positive integers results in a larger integer, the product of probabilities results in smaller probabilities. Table C.7 shows the variables from Equation C.2 and assigns random numbers between 0 and 1 to represent the probabilities and random numbers between 0 and 100 to represent the consequences. We also include a baseline which we will use to compare different scenarios.

Table C.7. Risk Equation

[illegible]		
Threat	0.233234094	0.5
Vulnerability	0.601075973	0.5
Consequence	86	50
Risk	12.05646128	12.5

Because there are four variables and there are two possible deviation options from their baseline values (up or down), we have 4^2, or 16, possible scenarios, given in Table C.8. There was a randomly generated instance for each of the following scenarios, except for the completely illogical ones (down-down-down-up and up-up-up-down). The down-down-down-down and up-up-up-up scenarios make sense, intuitively. However the remaining scenarios are not intuitive and could greatly misrepresent risk. Even if we hold consequence constant, we see similar results in Table C.9.

Table C.8. Risk Equation Simulation Scenarios

[illegible]								
Threat	Down	Up	Down	Down	Down	Down	Down	Down
Vulnerability	Down	Down	Up	Down	Down	Up	Up	Down
Consequence	Down	Down	Down	Up	Down	Up	Down	Up
Risk	Down	Down	Down	Down	Up	Down	Up	Up
[illegible]								
Threat	Up	Down	Up	Up	Up	Up	Up	Up
Vulnerability	Up	Up	Down	Up	Up	Down	Down	Up
Consequence	Up	Up	Up	Down	Up	Down	Up	Down
Risk	Up	Up	Up	Up	Down	Up	Down	Down

Table C.9. Risk Equation Simulation Scenarios (Constant Consequence)

[illegible]									
Threat	Down	Up	Down	Down	Down	Up	Up	Up	Up
Vulnerability	Down	Down	Up	Down	Up	Up	Down	Up	Down
Consequence	Same	Same	Same	Same	Same	Same	Same	Same	Same
Risk	Down	Down	Down	Up	Up	Up	Up	Down	Down

These results do not necessarily jive with our feelings about risk, in general. For example, if threat is reduced from a probability of 0.50 to 0.10, but vulnerability increases from 0.50 to 0.99 and consequence increases from 50 to 99, Risk actually *decreases* from 12.5 to 9.8. While the probability of a successful threat has been reduced, there is still some level of threat, and now, if that threat were to occur, there is such a dramatic increase in the probability of success of that attack, coupled with an increase in the potential consequence of that impact, the attack would be devastating. These low-probability, high-consequence events really throw a wrench into the mix when trying to calculate risk.

The type of consequence and the order of magnitude of the consequence can also cause problems. For example, if threat and vulnerability are both increased to 0.70, but consequence is reduced to 20 instead of 50, then Risk *decreases* from 12.5 to 9.8. If consequence is defined by billions of dollars, then reducing the Risk from 12.5 to 9.8 billion dollars does not seem all that significant. But if consequence is defined by thousands of fatalities, then the difference between 13,000 deaths and 10,000 deaths does seem significant. But is death even acceptable for the risk under discussion? And how do we integrate multiple consequences? We could determine a risk value based on monetary consequences, then another risk value based on fatalities, and somehow try to integrate them. Or we could assign death a monetary value, based on life insurance policies, perhaps. Or we maybe could perform a weighted linear model, where the weight for consequence of fatalities is significantly higher than that of money, then we could integrate the consequences and try to calculate an overall risk. But with either approach, we are still adding apples and oranges in the hopes of producing pears.

Furthermore, how do we integrate multiple assessments into a single, meaningful assessment, score, or report? Data from multiple assessments could be drastically different depending on data collection methods or data sources. And what about risk assessments for CI that are also considered KA? Or what if the asset falls into multiple CI sectors, as well as KA sectors? How do we integrate risk assessments from all of these different perspectives? While traditional probabilistic risk assessments might be applicable to CIKR, are they applicable to KA? The current risk assessment methodology for handling KA is basically a semi-quantitative risk prioritization approach (*National Monuments and Icons: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007). But the Hoover Dam can be aligned to the Dam, Water, Transportation, and Energy sectors, not to mention the National Monuments and Icon sector since it is also a KA, so which sector produces the *right* risk assessment? Are all of the different risk assessments incorporated into a single estimate of risk for the Hoover Dam? Can that overall score be compared against the risk scores of other CIKRKA?

Risk Perception

Risk has been described as a *construct*. In other words, "risk is all in the mind"; it is not just something that we can observe, rather it is something which affects everything that we observe (Becker, et al., 1993). Depending on the filter affecting our perceptions, we may see risks differently. A policeperson might see a busy intersection and see the risk of car accidents, where as an environmentalist might see the risk of pollution from all of the car exhaust, yet the driver of a car whizzing through the intersection sees only the risk of a speeding ticket as he notices the police car in his rear view mirror. The way we attempt to define, assess, and model risk, is thus, a construct, as well.

Early risk perception research focused on the cognitive aspects of the acceptability of risk, such as how and why we make the decisions we do, how we factor risk into those decisions, what we consider to be acceptable risk, whether or not we are capable of estimating risk accurately, and why we underestimate or overestimate some risks. The question we are seeking to answer through risk analysis and risk assessments is whether or not a given product (action, technology, asset, resource, or infrastructure) is safe. But risk perception asks, "How safe is safe enough?" (B. Fischhoff, et al., 1978).

In more recent years, risk perception has been introduced to the field of homeland defense and homeland security, or, rather, the pressing issues of homeland defense and homeland security have unfolded before our very eyes, no doubt affecting our collective risk perceptions. During the September 11th attacks, we became aware of our own vulnerability in an instant (Small, Lerner, & Fischhoff, 2006). Risk perceptions after a tragic event are bound to be shaped by emotions (Small, et al., 2006), but reacting based on those risk perceptions, rather than based on unbiased evidence, could lead to further tragedy. Risk perceptions changed so drastically after this pivotal event that the US went to war (to reduce threat likelihood) and simultaneously created a new department, DHS with its mission to protect our nation's borders, CIKRKA, and citizens (to reduce vulnerability likelihood).

Fischhoff was one of the first to realize the implications for the field of risk perception and subsequently contributed a handful of articles dealing with terrorism. He even supported the proposal to allow the public to rank (some of the) risks for regulatory policy (Fischbeck, 2001). This approach was intended to be expanded to "ecological, social, and other quality-of-life risks" (Fischbeck, 2001), but it could definitely be extended to

CIKRKA risks. Soon after the September 11th attack, “Effects of Fear and Anger on Perceived Risks of Terrorism: A National Field Experiment” was published and it explored the effects of anger or fear on risk perceptions and policy partiality, determining that fear increased risk estimates of terrorism and the desire for protective measures, whereas anger had the opposite effect (Lemer, Gonzalez, Small, & Fischhoff, 2003).

Fischhoff also noted the importance of September 11th in our quotidian risk perception, remarking that the attack “has thrown many everyday choices into sharp relief” (B. Fischhoff, De Bruin, Perrin, & Downs, 2004). Deciding where and when to travel is no longer just a matter of personal preference or price, but could require consulting the current HSAS to determine the threat level (B. Fischhoff, et al., 2004). Of course, the threat level is almost always yellow, which is described as “Significant Risk of Terrorist Attack” ("Homeland Security Advisory System," 2010), so how does that play into our risk perceptions of terrorism? When the threat level is truly elevated, does anyone even notice? Are we the nation who cried terrorist?

Slovic also offered some unique post-September 11th opinions on risk perception, beginning with an emphasis on a persistent problem with the risk quantification of large-scale terrorist attacks such as September 11th; they are extreme events, black swans, high-consequence low-probability events (Slovic, 2002). Slovic actually called these events “a new species of trouble” (Slovic, 2002). Slovic stated that people “respond to the hazards they perceive” (Slovic, et al., 1979). And if the risk perceptions of those risk scenarios are not in sync with reality, decision makers cannot make adequate judgments in order to mitigate those risks.

Slovic was aware that risk management had become political and controversial in 1999, but it undoubtedly became more so after September 11th (Slovic, 1999). He argues that "danger is real, but risk is socially constructed" and since the government controls the definition of risk, it also controls the risk response and risk mitigation plans, which can cause the public to mistrust the government if the public disagrees with the definition of risk or the proposed response to, or mitigation of, that risk (Slovic, 1999). Judgments about risk are influenced by emotion and this is the only common denominator amongst the public, policy makers, and even risk analysts who supposedly look at risk as a science; none of us are immune to the effects that our emotions have on risk determination. For example, the Environmental Protection Agency (EPA) spent the majority of its budget for years on hazardous waste because the public perceived that to be the most serious environmental priority for the nation, even though indoor air pollution is actually considered to be a more serious health risk by experts (Slovic, 1999). Slovic proposes that public participation in both the risk assessment and risk decision making process would improve the scientific assessments of risk, as well as increase the public's acceptance of the resulting decisions (Slovic, 1999).

The supposed laws of acceptable risk (Table C.10) were first developed by Starr early in the history of risk perception (B. Fischhoff, et al., 1978). They were derived from an analysis of risk versus benefit based on historical data of fatalities per hours, an approach that is very similar to a failure rate analysis in reliability engineering. Risk was defined as the expected value of the number of fatalities for every hour that one was exposed to the risk event. Benefit was defined as the average amount of money spent on the risk activity or the average amount of money the risk activity would contribute to one's annual income (Starr, 1969).

Table C.10. Laws of Acceptable Risk

Risk Acceptability (RA) is proportional to the cube of the Risk Rewards (RR)	$(RA \alpha RR^3)$
The public generally accepts risks from voluntary activities that are about 1,000 greater than involuntary activities, even if both activities offer equivalent rewards	$(RA_I = 1{,}000*RA_V)$
RA is inversely related to the size of the population exposed to that risk	$(RA \alpha (1/n_E))$
The level of risk tolerated for voluntarily accepted hazards is approximately equal to the level of Risk from Disease (RD)	$(RA_V \approx RD)$

Do Starr's laws of acceptable risk still hold true? Are they applicable to CIKRKA risks? If RA is still proportional to the cube of RR, then what constitutes a RR in risk assessments of CIKRKA? Does the public still tend to accept risks from voluntary activities more than involuntary activities? If RA is inversely related to the size of the population exposed to that risk, how does RA relate to the region of the risk, or the time of the risk, both of which could affect the size of the population exposed to the risk? Is RD still a good measuring stick for voluntarily accepted risk scenarios, or has the communication of information about RD (an involuntary risk, after all) over the past 30 years altered this relationship?

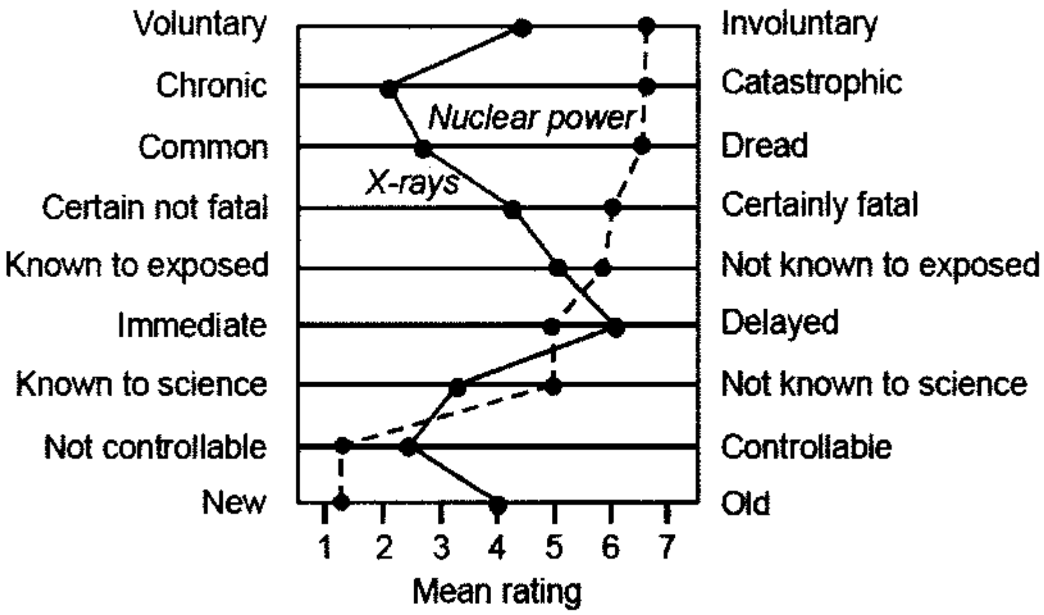


Figure C.30. Perceived Risk Scales

Many talk about risk as a function of threat, vulnerability, and consequence (H. H. Willis, 2007), but it seems obvious that the risk triplet is inadequate. Risk is also a function of our risk perceptions, and through risk perception, other factors influencing our risk perception of risk can be explored, such as those given in Figure C.30. And other factors may influence our risk perceptions, such as the location of an asset, the time of day, month, or year of an attack on that asset, or even the type of asset at risk (CI, KR, or KA).

It has long been a challenge to evaluate multiple assessments of risk. Multiple risk assessments, even those which all seek to assess the same risk event or facility, etc., could vary widely. Risk assessments could be based on risk data or risk perceptions. The data from one assessment could be drastically different from the data of another assessment if the data collection methods or data sources differ significantly; furthermore, one assessment could incorporate factors such as whether the risk was voluntary or involuntary, while another might attempt to calculate risk using traditional risk equations (Turner, 1994). Even the definition of consequences can drastically affect the risk calculations, and there are many types of consequences (economic, environmental, or in some cases loss of life) which must all be assessed in order to give the best possible overall risk picture.

A great example here would be the integration of risk assessments for CI which are also considered KA. Traditional probabilistic risk assessments, which might be applicable to CIKR, are probably not applicable to KA such as the Washington Monument or the St. Louis Arch. Still, an attack on such assets would have significant repercussions on our nation's morale and would, in turn, affect our risk perceptions. Haimes remarks that it may not matter whether the threat to CIKRKA is a natural risk scenario or an unnatural risk scenario, as the consequences may be similar, however "the psychological and political impacts are likely to be significantly different" (Haimes, 1999) and an attack on a KA is most likely to be a manmade attack, aiming to affect our national psyche.

The current risk assessment methodology for handling KA is basically a semi-quantitative risk prioritization approach (*National Monuments and Icons: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007). Could risk perceptions be incorporated into an overall risk assessment methodology for KA? Could risk perceptions be used to integrate multiple risk assessments of the same asset? For example, the Hoover Dam would have a traditional risk assessment viewing the facility from the perspective of CIKR (the structure itself, as well as the water it controls), but it could also have a risk assessment which views the facility from the perspective of a KA (in addition to its primary function as a dam, the structure is also a national icon and tourist site). But how are these two risk values aggregated to provide an overall risk profile?

Perhaps risk perception could learn from the field of CIP in this case. The Transportation Systems sector introduced the concept of risk views. These risk views describe the types of transportation systems in terms of four views: mode, geography, function, and ownership (*Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan*, 2007). Together, these four views capture different ways of viewing transportation systems, allowing for a robust assessment of the sector. From a systems analysis perspective, this is a very interesting systematic risk management approach incorporating risk perception. Furthermore this approach could be expanded to all other sectors and subsectors. In addition to the Transportation Systems views, there could be Energy risk views for Oil, Gas, as well as Electricity.

Even if we calculate risks accurately, we may not be able to subjectively estimate those risks independently. We might not be able to accurately recall the frequency of risk events, which would influence our estimates of risk. Or we might give weight to other factors in our subjective estimates of risk, such as whether the risk is voluntary or not (Kasperson, et al., 1988). We are often called upon to factor risk into our everyday decisions, but we are not likely to refer to calculated risks, or any other data for that matter, in order to make common decisions, like whether to go for a run after dark, or whether it is safer to take a plane or a ship to reach our vacation destinations.

Risk biases can even be introduced by our vernacular. For example, when asked the chances of a rainy day next Saturday, a person might respond, “fifty-fifty”. It is possible that the speaker places equal probability on both hypotheses (either it will rain, or it will not rain), but it is probably more likely that the speaker is not sure which probabilities to use in order express her belief, because quite frankly she does not know whether it will rain or not and has no information to make a more educated guess, so rather than researching data to inform her response, ignoring the question all together, or saying, "I don't know," she offers a pseudo-probability (B. Fischhoff & Bruine De Bruin, 1999). Incidentally, when attempting to incorporate perceived risks into risk calculation, the misuse of this "I don't know" probability of 0.50 could artificially inflate the average response for events which might typically be assigned smaller probabilities or vice versa (B. Fischhoff & Bruine De Bruin, 1999).

We can also introduce bias through the availability heuristic (Slovic, et al., 1979), the result of which makes us more likely to focus on frequently occurring risk events, or events with a vivid impact (such as the September 11th attack). Slovic is quick to point out that even the mere "discussion of any low-probability hazard may increase the judged probability of that hazard" regardless of whether the evidence contradicts that conclusion (Slovic, et al., 1979). Well, the future is ripe with unforeseen low-probability risk scenarios, and if the availability heuristic, or any other bias, precludes us from imagining potential threats, or inadvertently ignoring threats which are infrequent, then we cannot prepare for those threats, rendering us vulnerable.

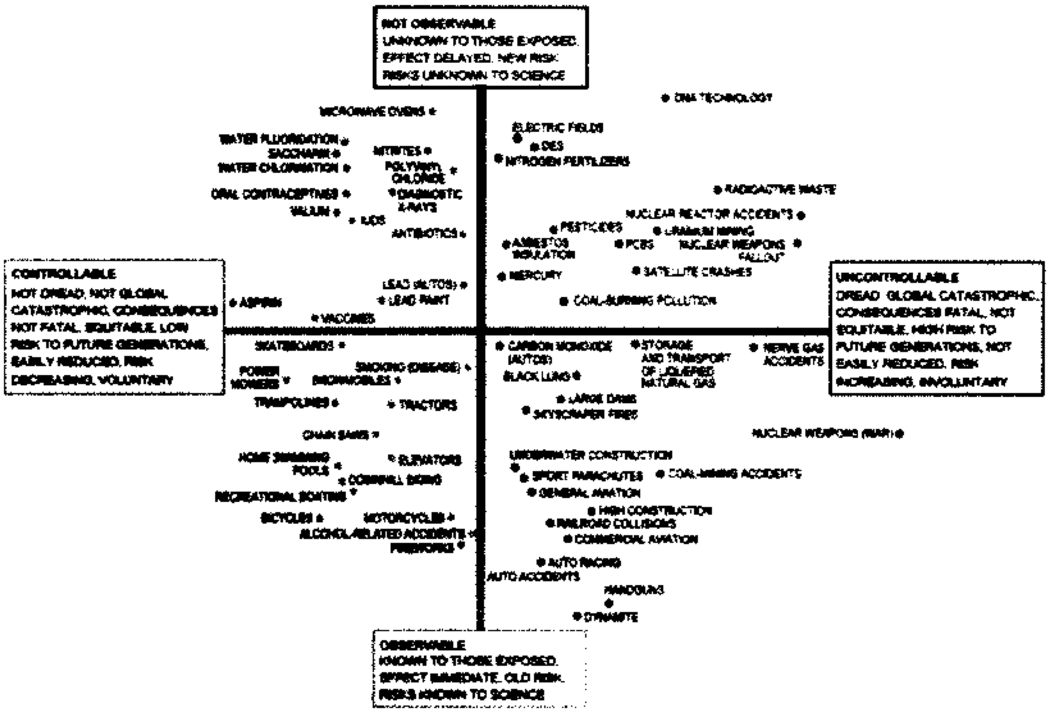


Figure C.31. Observed Risk Versus Controllable Risk

Our estimates of risks are affected by extraneous factors which can cloud our quantitative judgments. Figure C.31 introduces two scales or dimensions of risk: observability and controllability (Morgan, 1993). Observable risks are described here as old risks. These are risks for which the consequences are immediate and noticeable and because of this, there exist rich data sets which have been studied extensively. Furthermore, those exposed to these kinds of risks are aware of the potential consequences; automobile accidents are plotted here as observable risks because we are all aware that we could end up in an accident any time we drive or ride in a vehicle (Morgan, 1993). Unobservable risks are those risks for which those exposed to the risks are unaware of the consequences because the consequences might remain unknown or could be delayed, therefore data and research on these risks may be limited or unavailable (Morgan, 1993). The controllability scale basically boils down to two factors, whether the risk is voluntary or involuntary, and whether the consequences incite dread or not (Morgan, 1993).

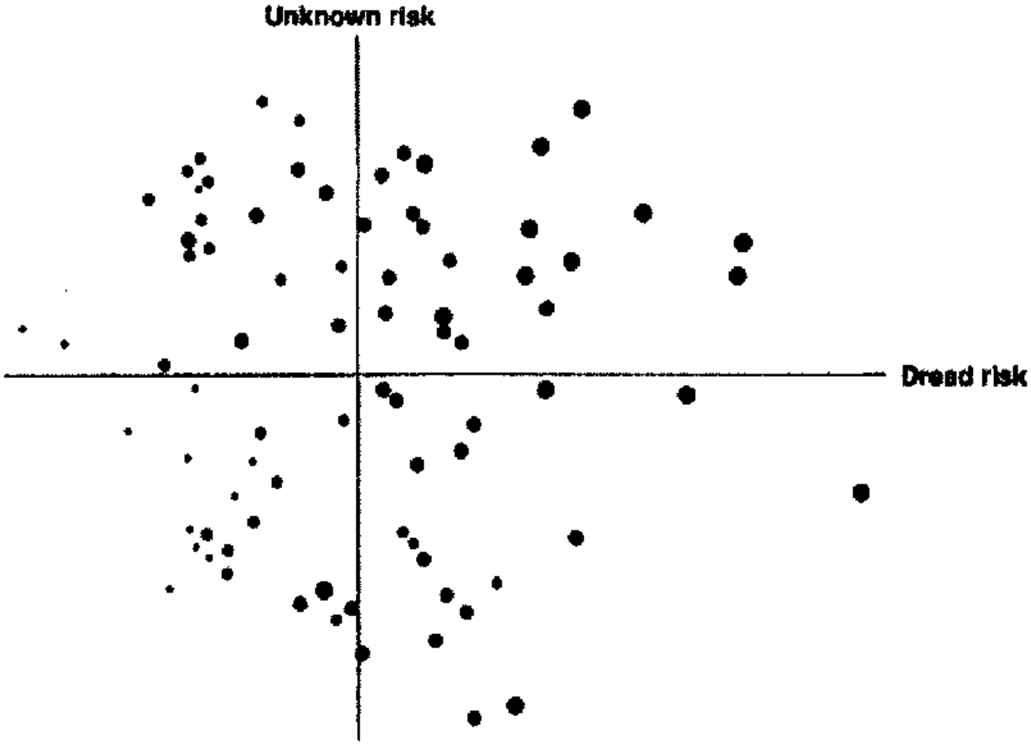


Figure C.32. Unknown Risk Versus Dread Risk

Slovic also mentions voluntariness, knowledge (or observability), and dread when discussing risk perception (Slovic, 2002). However, as opposed to only two scales, he proposes nine risk scales. We see in Figure C.30 that nuclear power has a more negative risk profile (looking across the nine risk characteristics), than that of x-rays. These risk scales influence our risk perceptions, and as a result, the public required a greater reduction in nuclear power risk before that risk would be tolerated by society. In Figure C.32, we see that risk perception can also be visualized in three dimensions with powerful results. Risk events are shown on the known/unknown and dread/non-dread risk scales, but for each risk event, the size of the point increases as the public's desire for risk regulation increases

(Slovic, 1987). We see points where the risk is known and there is no dread associated with the risk, and yet the public still demands increased risk regulation, because other factors are influencing their risk perceptions.

The tools for capturing risk perceptions can even introduce bias in our responses. For example, people are generally not as comfortable with decimals, leading them to overestimate very small risks if a survey asks for answers in the form of percentages, rather than asking for answers in the form of odds (B. Fischhoff, 2010). Thankfully, a well-designed survey can be crafted to reduce most of these biases, and surveys are still an extremely useful method for determining the levels of socially acceptable risk, as well as other risk perceptions (B. Fischhoff, et al., 1978).

For some risk scenarios, we can temper our risk perceptions with objective statistical data and robust risk assessments. For other, more nebulous risk scenarios, such as terrorist attacks, we lack reliable data and must depend on our risk perceptions. This is analogous to going with our gut and sometimes our gut is wrong. This bias can ripple through the risk-based decision making process and result in disproportionately allocated budgets. For example, DHS allocated $675 million in Fiscal Year (FY) 2004 to 50 metropolitan regions, all of which were perceived to be most vulnerable to terrorist attacks, based on a formula that supposedly accounts for a number of factors, including the presence of CIKRKA, vulnerability, population size and density, as well as law enforcement activity (H. H. Willis, 2007). Based on a new approach which focused on regional risk, $765 million was allocated in FY 2006, but only 35 metropolitan areas were eligible (H. H. Willis, 2007). Someone thought that looking at risk regionally was a better approach, and it may be, but as a result of the discrepancies in budget allocation, DHS was criticized for its inability to adequately calculate risk, especially risk as abstract as that of a terrorist attack, for which there is insufficient data to use traditional probabilistic risk analysis methods. Risk perception is most certainly playing a role here, both in the ability of DHS to calculate these risks and allocate resources appropriately, but also in the public's criticism of DHS. A better understanding of risk perception, calculated risk, along with the communication of that valuable risk information, could pave the way for mutual understanding between the public and DHS.

If the risk of a terrorist attack is perceived to be significant, regardless of the actual risk, then policy makers may decide to allocate the majority of available funds to protecting assets against terrorist attacks, when perhaps the true risk to an asset is deterioration due to age and lack of repairs. We have all seen examples of overlooked infrastructure failing with disastrous results, such as the incapacitation of the levies during Hurricane Katrina. Risk assessments are supposed to protect us from this bias by omission, but in fact, a risk assessment, itself, could introduce bias by drawing the decision maker's attention to all of the potential risks, some of which might not have been obvious and could cause the decision maker to emphasize those new risks over other more significant risks.

We ask our policy makers to "weigh the benefits against the risks" (B. Fischhoff, et al., 1978), but there are few tools for them to determine societal RA. Fischhoff proposes expressed preferences, a method using surveys to measure the public's attitudes towards the risks and benefits from various activities (B. Fischhoff, et al., 1978). An approach like this could be extended with the significant advancements in survey methodology (which could reduce risk biases), along with online survey applications or even online tools for performing MCDA.

The vision statement of DHS is "a secure America, a confident public, and a strong and resilient society and economy" (*One Team, One Mission, Securing Our HomelanD US Department of Homeland Security Strategic Plan Fiscal Years 2008–2013*, 2008). One way to ensure the public is confident in its nation's CIKRKA is for them to actively participate in determining the acceptable risks of those assets. Risk perception models could be used to gauge the public's risk perceptions regarding risk to CIKRKA, similar to the public risk ranking methods proposed for environmental, health, and safety policies (Fischbeck, 2001).

Now let us examine how perception might affect risk calculation. Often in order to estimate threat, vulnerability, and consequence, we rely on subject matter expertise because actual data is unavailable or difficult to collect. So, perception is inadvertently and haphazardly incorporated into Risk (Equation C.3). In other words, we are already integrating perception into the risk equation, but we are doing it in such a way that we cannot tease apart what is fact and what is opinion.

$$Risk = f(Threat_{Perception}, Vulnerability_{Perception}, Consequence_{Perception})$$

Equation C.3. Current Risk Calculation Revisited

We need a way to systematically incorporate subject matter expertise, or even public opinion, alongside actual data (no matter how limited that data may be). With the risk quadruplet, we propose separating perception from threat, vulnerability, and consequence, as its own component of Risk (Equation C.4). We would collect actual data for threat, vulnerability, and consequence in a consistent and systematic approach, and then integrate that data with perception data in a transparent and reproducible manner.

$$Risk = f(Threat, Vulnerability, Consequence, Perception)$$

Equation C.4. Proposed Risk Calculation

APPENDIX D

RISK QUADRUPLET METHODOLOGY (IN VIVO)

The in vivo risk quadruplet methodology describes the data collection and model building efforts that must be accomplished to complete this research. This is not the methodology which will be used to test the viability of the risk quadruplet; the in vitro methodology was discussed in CHAPTER 3 and CHAPTER 4. Rather, this is the methodology that would be used in vivo, vice in vitro, to actually deploy the methodology in the real world. The first phase is the perception assessment. The second phase consists of threat, vulnerability, and consequence assessments. The final phase of the research is the assessment integration phase, where the assessments of threat, vulnerability, consequence, and perception are all assimilated. The three-phased methodology for the risk quadruplet consists of three sub-methodologies, one for each phase (Figure 3.3).

To deploy the risk quadruplet in vivo, a perception survey, crafted with Inquisite, would be used to capture perception scores along a six level scale (the linguistic set of none, very low, low, medium, high, and very high). The survey results would be aggregated across all respondents to determine the frequencies with which respondents selected different grades of the perceived risk to a CI, KR, or KA given a risk scenario. ER, via IDS, would be used to integrate the survey results for the perception attribute with the data leveraged or collected for the remaining attributes (threat, vulnerability, and consequence). The output of the ER model would be a ranking of the CIKRKA in order of most to least risk, where risk is defined in the model as a systematic, traceable, and reproducible function of threat, vulnerability, consequence, and perception.

The main driver of the in vivo methodology was the MCDA model selected for the final phase. ER was an ideal choice for integrating the four disparate types of CIKRKA assessments as it can cope with relationships between parent and child attributes, as well as across all child attributes, through the use of weighting, utilities, and belief degrees. It can also handle both quantitative and qualitative data. And lastly, it can output a ranked series of assets based on all attributes. Once this ER model was selected and the free IDS software was identified as the tool which could be used to implement this model, it was soon realized that IDS could be leveraged throughout all three phases of the risk quadruplet.

In order to implement the risk quadruplet model in vivo, we would need to provide consistent definitions and examples for the CIKRKA, as well as an overall risk scenario. The risk quadruplet model can be adapted and expanded to handle more complex and lengthy lists of CIKRKA alternatives, multiple risk scenarios, improved threat, vulnerability, and consequence assessment data, and could even be used to integrate perception data from experts and non-experts. However, for the purposes of demonstrating how the risk quadruplet approach would be implemented in the real world, a simple model is proposed consisting of a CI, a KR, a KA, and one risk scenario. Threat, vulnerability, and consequence data would be leveraged from existing assessments or collected anew, and perception data would be gathered via survey from volunteer experts.

The risk scenario would describe the hazard which poses a danger to the CIKRKA. Providing a single risk scenario would allow respondents to consider their perception of risk across the different CIKRKA. Once those common elements have been defined, the respondent would select their perception (based on the risk scenario) for the three separate

CIKRKA selected. That perception data would be used, in conjunction with the leveraged or collected threat, vulnerability, and consequence data in order to provide an overall integrated assessment of the CIKRKA.

To demonstrate how the in vivo methodology might look, it was assumed that this methodology might first be deployed in a small setting with subject matter experts as the survey participants. It was assumed that those experts would live and work in the Washington, DC metropolitan area, so that region was chosen to set the stage for the examples of CIKRKA, as well as the risk scenario. This means that we could be introducing some bias, as we would not only be eliciting the perceptions of homeland security experts, but we would also be seeking their opinions based on familiar assets and regions. In practice, this methodology could be expanded to include a much larger and more diverse list of assets, as well as an increased sample of respondents, which might eliminate this regional bias. However, for the purposes of explaining how to deploy the risk quadruplet in vivo, it makes sense to scope the model. The National Capital Region (as it is often called by DHS) includes the cities, counties, and districts shown in Table D.1 ("Washington Metropolitan Area," 2012).

Table D.1. National Capitol Region

DC	Washington
MD	Calvert County
MD	Charles County
MD	Frederick County
MD	Montgomery County
MD	Prince George's County
VA	Arlington County
VA	Clarke County
VA	Fairfax County
VA	Fauquier County
VA	Frederick County
VA	Loudoun County
VA	Prince William County
VA	Spotsylvania County
VA	Stafford County
VA	Warren County
VA	City of Alexandria
VA	City of Fairfax
VA	City of Falls Church
VA	City of Fredericksburg
VA	City of Manassas
VA	City of Manassas Park
WV	Jefferson County

We chose a representative example for each CIKRKA in the National Capitol Region (Table D.2). The CIKRKA were chosen such that they were mutually exclusive. In other words, there was no ambiguity as to whether the CI could also be categorized as a KA or if it could have a direct impact on KR. Obviously these overlaps and interactions exist, as discussed in the Literature Review (APPENDIX C), and future research of the risk quadruplet model could explore ways to handle these interrelated CIKRKA, but for the current exercise, we wanted the CIKRKA to be unique and unambiguous.

Table D.2. Definitions and Examples for Alternatives

CI	government and private systems essential to the operation of our nation in any or all aspects of the lives of its citizens (health, safety, economy, etc.), such as utilities, facilities, pipelines, etc.	The George Washington University Hospital 900 23rd St., NW Washington, DC 20037	**Facts and Figure s (2010 Statistics)** 371 beds 17,016 inpatient admissions 86,414 outpatient visits a year Over 810 physicians on the hospital medical staff Nursing staff of over 713 The emergency department is a Level I Trauma Center seeing 71,242 patients a year. **Additional Information** Street parking is limited and metered. Access via Metro is recommended, if possible.
KR	public or private resources essential to the operation of our nation's government and economy, such as fuel or goods.	Motor Gasoline in Virginia	Energy Information Administration **Reserves & Supply (September 2011)** Motor Gasoline Stocks (Excludes Pipelines): 266K barrels (US Share: 0.7 %) **Distribution & Marketing (2008)** Fueling Stations: 4,140 (US Share: 2.6%) **Consumption (2009)** Motor Gasoline Consumed: 94.5M barrels (US Share: 2.9 %) **Environment (2008/2009)** Alternative-Fueled Vehicles in Use: 21,505 (US Share: 2.8 %) Ethanol Plants: 0 Ethanol Consumed: 8,616K barrels (US Share: 3.3 %)

KA	those buildings, geographic regions, monuments, or icons, whose destruction would cause a crushing blow to our nation's ego, morale, and identity, but which are not essential to the operation of our nation, such as the Washington Monument or the Statue of Liberty.	Lincoln Memorial	Located on the National Mall in Washington, DC Surrounded on three sides by water Approximately 6M people visit annually Open to the public 24 hours a day Free to visit The memorial was built to honor Abraham Lincoln, but it has become a symbol of the American Civil Rights movement as it is also the site of Martin Luther King, Jr.'s famous "I Have a Dream" speech.

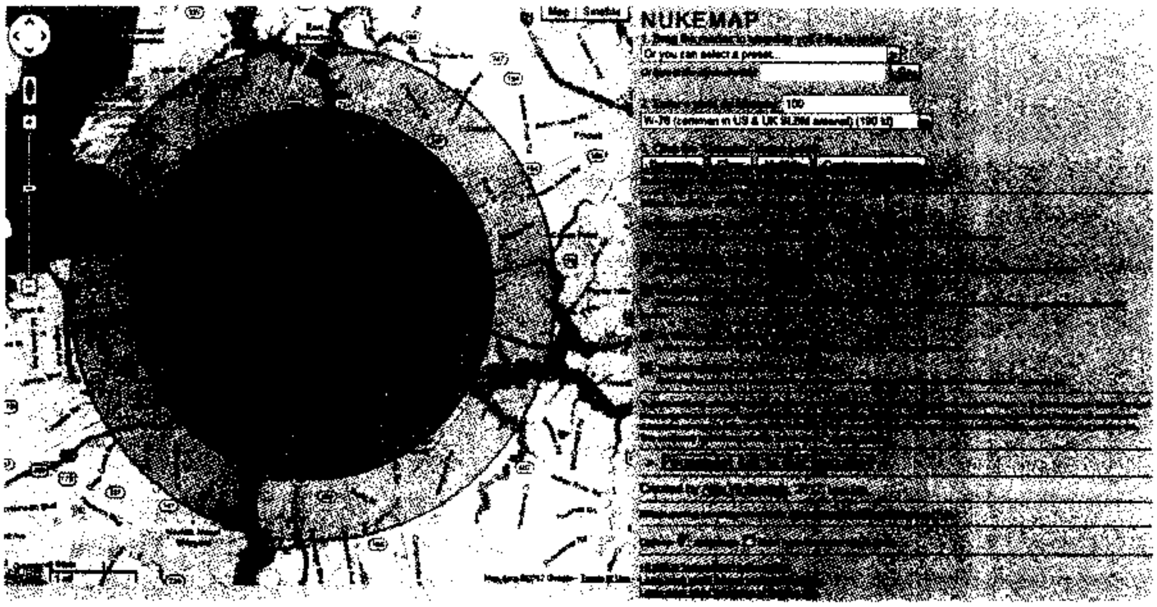
The CI selected for testing the risk quadruplet model was The George Washington University (GWU) Hospital, located at 900 23rd St., NW, Washington, DC 20037. From their website, a list of quick facts and figures was available to provide additional context for the facility. The hospital (according to 2010 statistics) has 371 beds, 17,016 inpatient admissions, 86,414 outpatient visits a year, over 810 physicians on the hospital medical staff, a nursing staff of over 713, and its emergency department is a Level I Trauma Center seeing 71,242 patients a year (GWU, 2011). Additional information available on their website noted that street parking is limited and metered, so accessing the hospital via Metro is recommended, if possible (GWU, 2011).

The KR selected for this exercise was motor gasoline for the state of VA. The Energy Information Administration (EIA) publishes state energy profiles including economic, price, reserves and supply, distribution and marketing, consumption, as well as environmental data (EIA, 2011). In the month of September 2011, VA had 266 thousand barrels of motor gasoline in stocks (excluding pipelines). This represents 0.7% of the US share. In 2008, VA had 4,140 fueling stations for motor gasoline, a 2.6% share of the US.

VA consumed 94.5 million barrels of motor gasoline (a 2.9% share of the US) in 2009. Additionally, some related information was also provided on this KR for context. VA had 21,505 alternative-fueled vehicles in use (a 2.8% share of the US) in 2008, and while there were no plants to produce ethanol (as of 2008), VA consumed 8,616 thousand barrels of ethanol in 2009, which is a 3.3% share of the US totals for ethanol consumption (EIA, 2011).

The KA selected for research was the Lincoln Memorial in Washington, DC, which is operated as part of the National Mall and Memorial Parks by the National Park Service with the US DOI ("Lincoln Memorial," 2011b). It was a memorial built to honor Abraham Lincoln, the 16th President of the US, although it has also become a symbol of the American Civil Rights movement as it is the site of Martin Luther King, Jr.'s famous "I Have a Dream" speech ("Lincoln Memorial," 2011a). It is located on the National Mall, approximately 6 million people visit the memorial annually, it is open to the public 24 hours a day, and it is free to visit ("Lincoln Memorial," 2011a). The location is surrounded on three sides by water, meaning, from an EPR&R perspective, that incidents could be easily contained ("Lincoln Memorial," 2011a).

Scenarios are one of the main elements of models, simulations or serious games, (Ancel, 2011). It would be possible to choose any type of risk scenario and use all sorts of resources for describing and exploring those scenarios with stakeholders. For example, a recently developed website, NukeMap, went viral amongst social media sites. The website's author was interested in visualizing the impacts of nuclear detonations in different cities and regions (Figure D.1). Using Google's interactive base map, NukeMap allows users to select a location and type of bomb, then detonate it to see the impacts, represented visually as concentric color coded circles ranging out from the impact site which describe the consequences most likely to be experienced in those regions (Wellerstein, 2012).



NUKEMAP

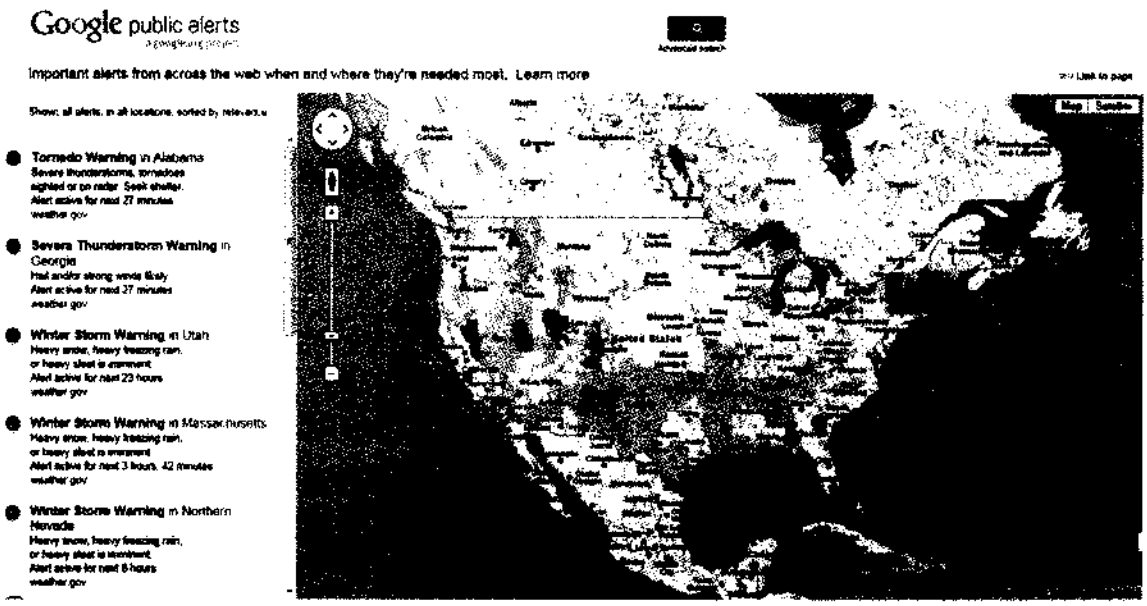
Or you can select a preset...

100

W-76 (common in US & UK [illegible] arsenal) (100 kt)

Figure D.1. NukeMap

Google has announced the release of Public Alerts, a new emergency alert system developed by their Crisis Response division ("Google Public Alerts," 2012). It is designed to display alerts issued by the National Occanic and Atmospheric Administration (NOAA), the National Weather Service, and the US Geological Survey right on Google Maps, offering an instantaneous visualization of risk (Figure D.2). Google is encouraging authorized local public safety officials to post alerts at no cost. These visualizations could make consequence and perception assessments much more informative and interactive.



Important alerts from across the web when and where they're needed most. Learn more

Show: all alerts, in all locations, sorted by relevance

- ● **Tornado Warning** in Alabama
  Severe thunderstorms, tornadoes sighted or on radar. Seek shelter.
  Alert active for next 27 minutes
  weather.gov
- ● **Severe Thunderstorm Warning** in Georgia
  Hail and/or strong winds likely
  Alert active for next 27 minutes
  weather.gov
- ● **Winter Storm Warning** in Utah
  Heavy snow, heavy freezing rain, or heavy sleet is imminent
  Alert active for next 23 hours
  weather.gov
- ● **Winter Storm Warning** in Massachusetts
  Heavy snow, heavy freezing rain, or heavy sleet is imminent
  Alert active for next 3 hours, 42 minutes
  weather.gov
- ● **Winter Storm Warning** in Northern Nevada
  Heavy snow, heavy freezing rain, or heavy sleet is imminent
  Alert active for next 8 hours
  weather.gov

Figure D.2. Google Public Alerts

The risk scenario selected for the risk quadruplet in vivo methodology was a tornado. Table D.3 below gives descriptions of the Fujita Tornado Damage Scale, used by the NOAA National Climatic Data Center (NCDC) to determine the magnitude of tornadoes (NOAA, 2012a). In February of 2007, this scale was revised (NOAA, 2012a) and the Enhanced Fujita Tornado Damage Scale is now based on 28 damage indicators from which a degree of damage is calculated and then translated to the magnitude scale, however, the definitions and damage descriptions for the original scale are sufficient for the purposes of this research, especially considering the majority of the dataset provided by NOAA NCDC was data collected prior to the implementation of the Enhanced Fujita Tornado Damage Scale.

Table D.3. Fujita Tornado Damage Scale

[illegible]	[illegible]	[illegible]
[illegible]	<73	Some damage to chimneys; branches broken off trees; shallow-rooted trees pushed over; sign boards damaged.
[illegible]	74-112	Peels surface off roofs; mobile homes pushed off foundations or overturned; moving autos blown off roads.
[illegible]	113-157	Roofs torn off frame houses; mobile homes demolished; boxcars overturned; large trees snapped or uprooted; light-object missiles generated; cars lifted off ground.
[illegible]	158-206	Roofs and some walls torn off well-constructed houses; trains overturned; most trees in forest uprooted; heavy cars lifted off the ground and thrown.
[illegible]	207-260	Well-constructed houses leveled; structures with weak foundations blown away some distance; cars thrown and large missiles generated.
[illegible]	261-318	Strong frame houses leveled off foundations and swept away; automobile-sized missiles fly through the air in excess of 100 meters (109 yds); trees debarked; incredible phenomena will occur.

We examined NCDC historical records from April 30, 1950 (the start date of the NOAA storm events data set) through September 30, 2011 (the most recent data published at the time of this research) and recorded all tornadoes to hit the National Capitol Region, as it was defined earlier (NOAA, 2012b). We also collected data about the magnitude of the tornadoes, the number of deaths and injuries, as well as the cost of property damage. Table D.4 shows the summary of these results. It is interesting to note that out of 83 tornadoes to hit the National Capitol Region, only one touched down in Washington, DC, an F0 at the Lincoln Memorial, resulting in $2,000 worth of damage.

Table D.4. National Capitol Region Tornadoes

Location or County	Date	Magnitude	[illegible]	[illegible]	Property Damage
Lincoln Memorial	9/24/2001	F0	0	0	$2,000
Frederick	4/5/1952	F1	0	0	$25,000
Frederick	4/5/1952	F1	0	1	$25,000
Montgomery	8/31/1952	F1	0	0	$25,000
Prince George's	5/26/1953	F1	0	0	$3,000
Frederick	5/3/1954	F0	0	0	-
Montgomery	7/1/1959	F1	0	0	$3,000
Frederick	11/19/1960	F1	0	0	$3,000
Frederick	4/16/1961	F1	0	0	$3,000
Frederick	7/19/1963	F1	0	0	$25,000
Prince George's	7/19/1963	F1	0	0	$25,000
Frederick	2/13/1966	F1	0	0	$25,000

Frederick	6/28/1966	F1	0	0	$25,000
Montgomery	8/26/1967	F1	0	0	$25,000
Prince George's	9/12/1971	F2	0	0	$250,000
Frederick	3/3/1972	F1	0	0	$250,000
Charles	4/1/1973	F1	0	0	$25,000
Charles	1/28/1974	F1	0	0	$3,000
Montgomery	5/12/1974	F1	0	0	$3,000
Charles	6/5/1975	F0	0	0	$3,000
Charles	7/13/1975	F1	0	0	$250,000
Calvert	6/27/1978	F2	0	0	$250,000
Charles	6/20/1978	F2	0	0	$25,000
Frederick	7/31/1978	F2	0	0	$25,000
Frederick	8/28/1978	F2	0	0	-
Calvert	9/5/1979	F1	0	1	$250,000
Charles	9/5/1979	F0	0	0	$25,000
Frederick	5/30/1982	F1	0	0	$3,000
Calvert	10/13/1983	F2	0	0	$25,000
Frederick	5/22/1983	F3	0	0	$25,000
Calvert	5/8/1984	F0	0	0	$25,000
Frederick	5/13/1990	F1	0	0	$250,000
Montgomery	10/18/1990	F1	0	1	$2,500,000
Montgomery	8/20/1991	F1	0	0	$25,000
Prince George's	8/4/1992	F1	0	0	-
Prince George's	8/4/1992	F0	0	0	$25,000
Prince George's	11/23/1992	F1	0	0	$2,500,000
Calvert	8/17/1994	F0	0	0	$1,000
Frederick	6/16/1998	F0	0	0	$10,000
Frederick	8/14/1999	F1	0	0	$800,000
Frederick	6/6/2002	F0	0	0	$15,000
Fairfax	8/31/1952	F1	0	0	$25,000
Fauquier	5/17/1953	F1	0	0	$3,000
Fauquier	9/7/1954	F1	0	0	$25,000
Loudoun	5/3/1954	F0	0	0	$3,000
Stafford	2/18/1960	F1	0	0	-
Frederick	7/13/1961	F2	0	1	$3,000
Frederick	6/2/1962	F1	0	0	$25,000
Fairfax	8/9/1969	F2	0	0	$250,000
Warren	7/9/1970	F0	0	0	$3,000
Fairfax	4/1/1973	F3	0	37	$25,000,000
Fauquier	4/1/1973	F3	0	0	$25,000
Clarke	8/4/1975	F2	0	0	$250,000
Clarke	3/21/1976	F0	0	0	$25,000
Prince William	1/26/1978	F3	1	10	$250,000
Fairfax	9/5/1979	F3	1	6	$2,500,000
Loudoun	9/5/1979	F2	0	2	$250,000
Loudoun	9/5/1979	F2	0	0	$250,000
Stafford	9/5/1979	F1	0	0	$25,000
Loudoun	6/3/1980	F2	0	0	$25,000
Fairfax	7/28/1981	F2	0	0	$25,000
Fairfax	10/13/1983	F0	0	0	-
Falls Church	10/13/1983	F2	0	0	$2,500,000
Fauquier	10/13/1983	F0	0	0	$3,000

Clarke	8/2/1986	F1	0	0	-
Clarke	8/2/1986	F1	0	0	-
· Fairfax	7/12/1987	F1	0	0	$3,000
Loudoun	7/12/1987	F1	0	0	$3,000
Prince William	7/21/1987	F0	0	0	$2,500,000
Fairfax	10/18/1990	F0	0	0	-
Fauquier	7/12/1990	F0	0	0	-
Fauquier	10/18/1990	F1	0	0	$250,000
Fairfax	8/4/1992	F1	0	0	$3,000
Fauquier	4/16/1993	F0	0	0	$5,000
Fauquier	4/16/1993	F1	0	0	$500,000
Loudoun	4/16/1993	F1	0	0	$500,000
Fredericksburg	7/24/1999	F1	0	0	$20,000
Alexandria	9/24/2001	F0	0	0	$8,000
Arlington	9/24/2001	F1	0	2	$1,000,000
Fredericksburg	9/17/2004	F0	0	0	-
Manassas	9/17/2004	F1	0	0	-
Manassas Park	9/17/2004	F1	0	0	-
Jefferson	4/28/2008	F1	0	0	$15,000

Over the 61 years reviewed, the National Capitol Region suffered 83 tornadoes, none of which were F4 or F5 tornadoes. The counts of tornadoes by magnitude, as well as the sums of deaths, injuries, and property damage are provided in Table D.5. Percentages are also provided to show the percentage contribution by tornado magnitude (based on the total sum of counts, deaths, injuries, and property damage, respectively). The total property damage for all years was $8,049,000, approximately 75% of which was the result of F0 and F1 tornadoes. Only 2 lives were lost in the National Capitol Region as a result of tornadoes, both of which were caused by F3 tornadoes, however 61 injuries were caused by tornadoes.

Table D.5. Percentages of National Capitol Region Tornadoes, Casualties, and Costs

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	20	24%	0	0%	0	0%	$2,653,000	33%
[redacted]	44	53%	0	0%	5	8%	$3,468,000	43%
[redacted]	14	17%	0	0%	3	5%	$1,628,000	20%
[redacted]	5	6%	2	100%	53	87%	$300,000	4%
[redacted]	0	-	-	-	-	-	-	-
[redacted]	0	-	-	-	-	-	-	-
[redacted]	83		2		61		$8,049,000	

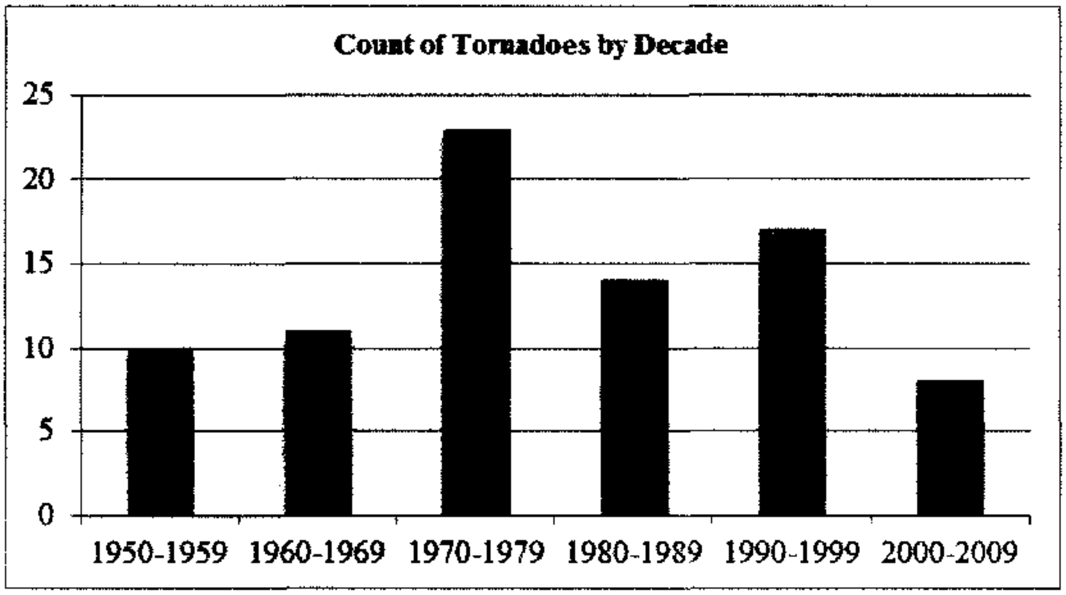


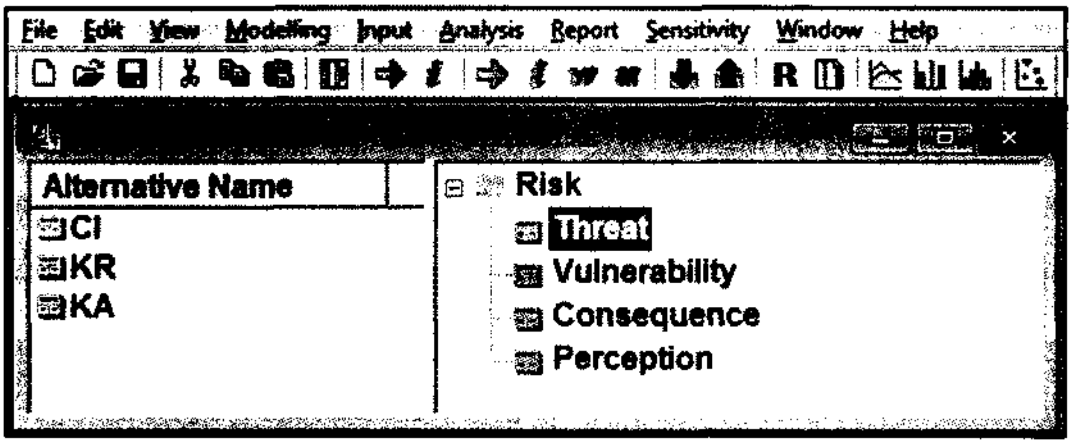
Figure D.3. Count of Tornadoes by Decade

Tornadoes were also counted by decade and the distribution is shown in Figure D.3. Table D.6 below shows the average number of casualties (deaths and injuries combined), as well as costs over the period from which the data was collected. F3 tornadoes were responsible for the highest average number of casualties over the 61 years; however, F0 tornadoes had the highest average property damages.

Table D.6. Average Casualties and Property Damages

	0	$132,650
	0.113636364	$78,818
	0.214285714	$116,286
	12.6	$60,000
	-	-
	-	-

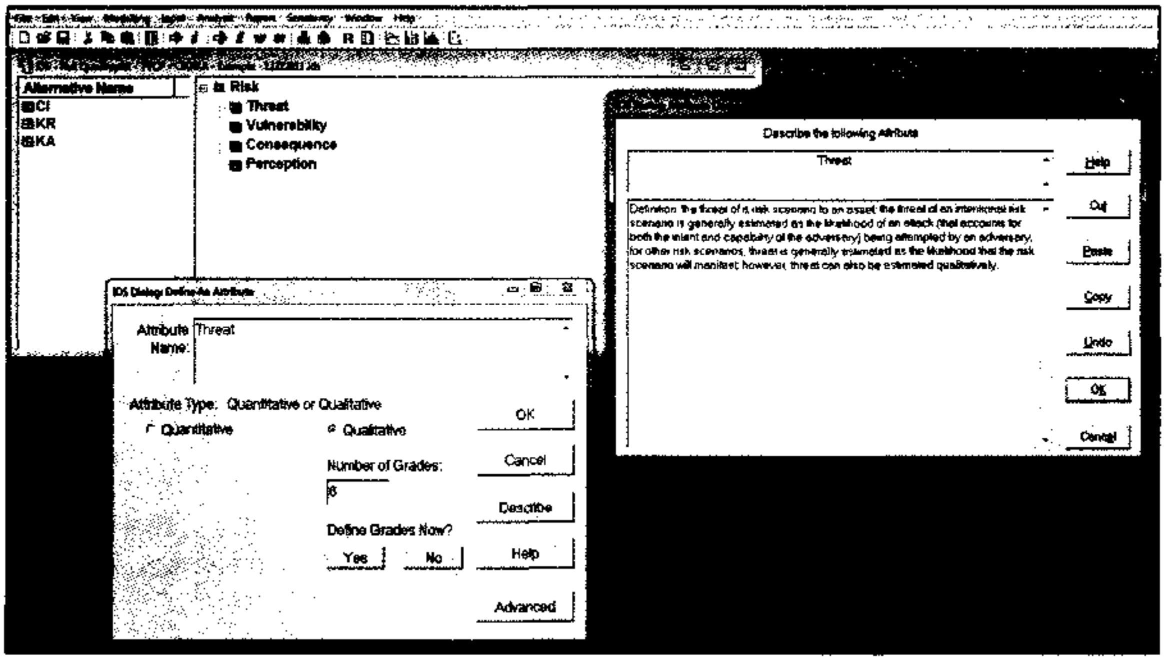
With IDS we are able to build an ER model for the risk quadruplet using a combination of collected perception data and simulated threat, vulnerability, and consequence data. A simple model was described in IDS to demonstrate the in vivo methodology, consisting of three alternatives (CI, KR, and KA), and four child attributes (threat, vulnerability, consequence, and perception) nested under an overall parent attribute (risk). The model also uses weighting (to determine the contribution of the child attributes to the parent attribute), utilities (to determine the relationship between the grades and the child attributes), and belief degrees (to determine the beliefs held for the grades selected).



Alternative Name
CI
KR
KA

Risk
Threat
Vulnerability
Consequence
Perception

Figure D.4. Risk Quadruplet Model (In Vivo)



Attribute Name: Threat

Attribute Type: Quantitative or Qualitative

○ Quantitative ● Qualitative

Number of Grades: 6

Define Grades Now?

Threat

Definition: The threat of a risk scenario to an asset; the threat of an intentional risk scenario is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary; for other risk scenarios, threat is generally estimated as the likelihood that the risk scenario will manifest; however, threat can also be estimated qualitatively.

Figure D.5. Dialog Box for Description of Attributes

An example of how this model appears in IDS is shown in Figure D.4. The definitions for each attribute (threat, vulnerability, consequence, and perception) were input into IDS, based on the definitions provided in CHAPTER 1 (Figure D.5). The attributes were then assigned six possible grades, mapped from the following linguistic set: none, very low, low, medium, high, and very high. A threat of none was defined as, "This risk scenario poses no risk to this CI, KR, or KA," and similar definitions were used across all combinations of grades and attributes (Table D.7).

Table D.7. Definitions and Examples for Attributes and Grades

Threat	the threat of a risk scenario to an asset; the threat of an intentional risk scenario is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary; for other risk scenarios, threat is generally estimated as the likelihood that the risk scenario will manifest; however, threat can also be estimated qualitatively.	None	This risk scenario poses no risk to this CI, KR, or KA.
		Very Low	This risk scenario poses very low risk to this CI, KR, or KA.
		Low	This risk scenario poses low risk to this CI, KR, or KA.
		Medium	This risk scenario poses medium risk to this CI, KR, or KA.
		High	This risk scenario poses high risk to this CI, KR, or KA.
		Very High	This risk scenario poses very high risk to this CI, KR, or KA.
Vulnerability	ability of an asset to endure a risk scenario despite physical features, operational attributes, characteristics of design, location, security posture, operation, or any combination thereof that renders an asset open to exploitation or susceptible to a given risk scenario; can be estimated qualitatively, or quantitatively as the likelihood of a successful risk scenario given the risk scenario is identified, which implies that vulnerability is also related to resilience.	None	This CI, KR, or KA has no vulnerability to this risk scenario.
		Very Low	This CI, KR, or KA has very low vulnerability to this risk scenario.
		Low	This CI, KR, or KA has low vulnerability to this risk scenario.
		Medium	This CI, KR, or KA has medium vulnerability to this risk scenario.
		High	This CI, KR, or KA has high vulnerability to this risk scenario.
		Very High	This CI, KR, or KA has very high vulnerability to this risk scenario.
Consequence	effect of a successful risk scenario on an asset; consequence is commonly assessed along four scales: human, economic, mission, and psychological, but may also include other factors such as impact on the environment; consequence can also be measured qualitatively either along a set of scales or along a single integrated consequence scale for which all consequence scales are considered as a whole.	None	This CI, KR, or KA would have no consequences from this risk scenario.
		Very Low	This CI, KR, or KA would have very low consequences from this risk scenario.
		Low	This CI, KR, or KA would have low consequences from this risk scenario.
		Medium	This CI, KR, or KA would have medium consequences from this risk scenario.
		High	This CI, KR, or KA would have high consequences from this risk scenario.
		Very High	This CI, KR, or KA would have very high consequences from this risk scenario.
Perception	subjective judgment about the severity of a risk scenario to an asset; may be driven by sense, emotion, or personal experience; generally measured qualitatively; referred to merely as perception throughout this research.	None	I perceive this CI, KR, or KA to have no risk from this risk scenario.
		Very Low	I perceive this CI, KR, or KA to have very low risk from this risk scenario.
		Low	I perceive this CI, KR, or KA to have low risk from this risk scenario.
		Medium	I perceive this CI, KR, or KA to have medium risk from this risk scenario.
		High	I perceive this CI, KR, or KA to have high risk from this risk scenario.
		Very High	I perceive this CI, KR, or KA to have very high risk from this risk scenario.

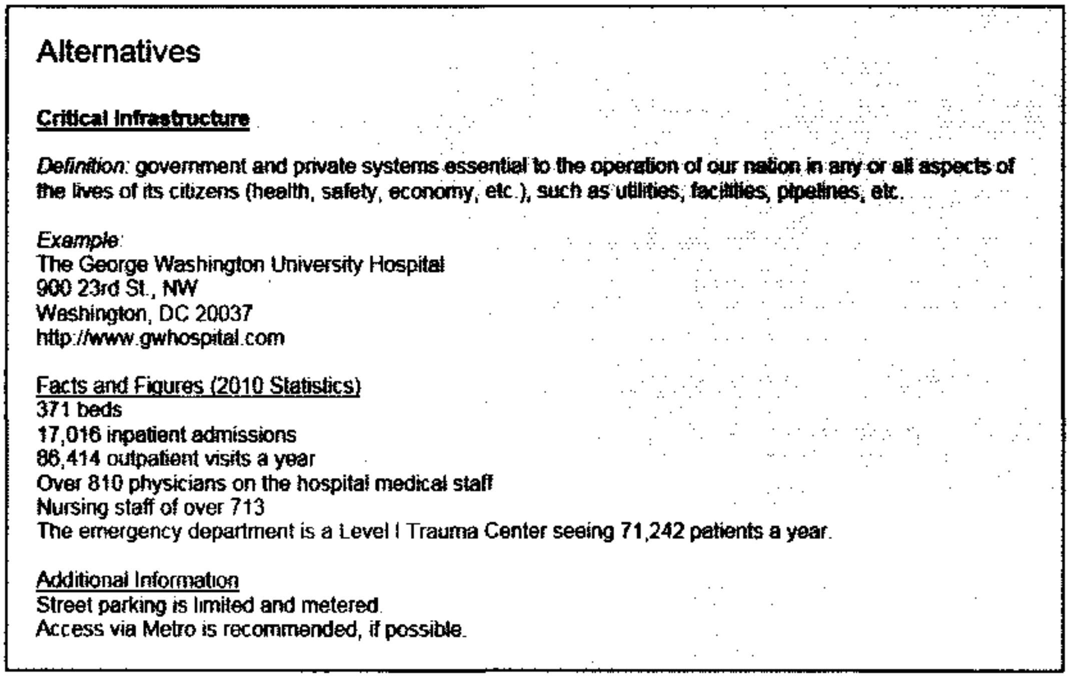
Phase 1. Perception Assessment Methodology

The survey proposed for the in vivo methodology also provides the definitions and examples for the CIKRKA, definitions of the attributes, as well as the overall risk scenario which poses a danger to the CIKRKA. Providing a consistent risk scenario is necessary in order for respondents to consider their perception of risk across the different CIKRKA. After reviewing those common elements, the respondent would select a grade to qualify the perceived risk (based on the risk scenario) to the three separate CIKRKA selected.

In IDS the perception data would be captured as qualitative data, aligned to the linguistic set defined above. This same linguistic set would be used for the grades across all of the different attributes (threat, vulnerability, consequence, and perception). IDS could be used to collect perception data for a single respondent, however there is not an immediate and obvious way to incorporate the perceptions of multiple respondents into an ER model.

Upon further examination, one way this could be done is to use the distribution of the frequencies of respondents' selections from the linguistic set as the belief degrees for the grades. For example, we would create a simple survey that would collect the data required for the IDS data entry dialog box. The linguistic set would be used as the perception options in the survey. If that survey had ten respondents and for the CI alternative, one of them choose a grade of very low for the perception attribute, one of them chose low, and eight of them choose medium, then the belief degrees could be assigned to those grades as .1, .1, and .8, respectively.

Inquisite is software that can be used to design and deploy surveys, collect data, as well as analyze respondent data ("Inquisite," 2011). Using this software, it would be possible to select a sample of experts, ask them a series of perception questions tailored to fit the ER model selected for the third phase of the risk quadruplet. The definitions for each attribute were input into Inquisite and each CIKRKA alternative definition and example as discussed above was populated in Inquisite (Figure D.6). The attributes were then assigned six possible grades, mapped from the same linguistic set as the one used in IDS: none, very low, low, medium, high, and very high.



Alternatives

Critical Infrastructure

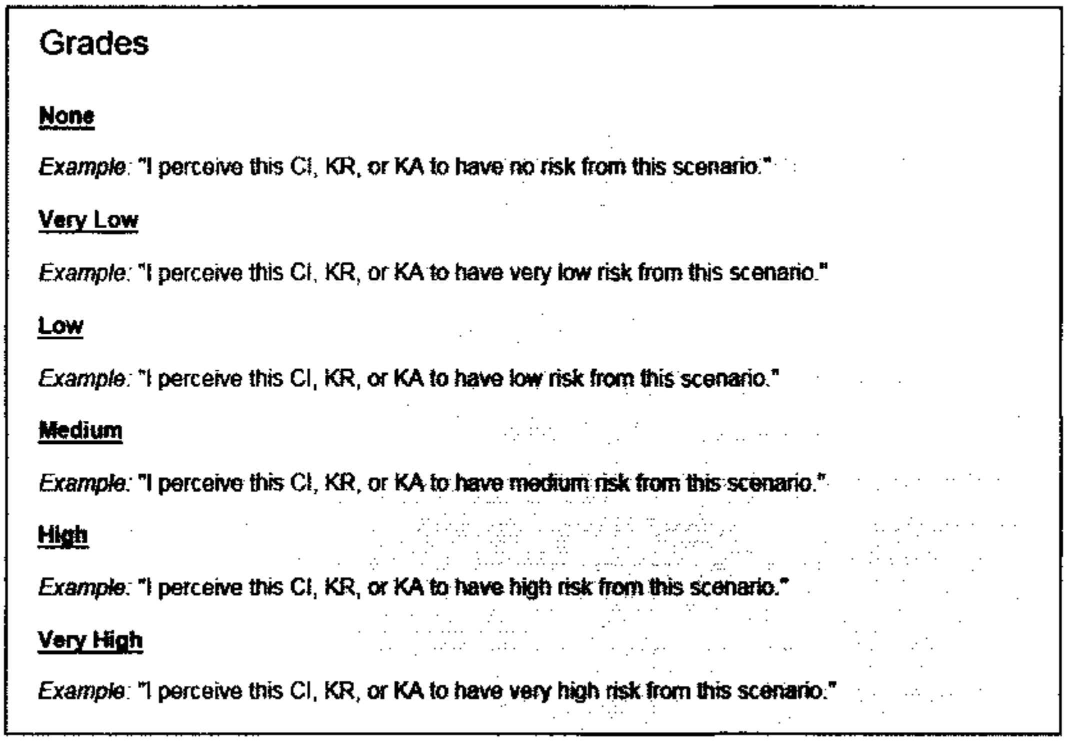
Definition: government and private systems essential to the operation of our nation in any or all aspects of the lives of its citizens (health, safety, economy, etc.), such as utilities, facilities, pipelines, etc.

Example:
The George Washington University Hospital
900 23rd St., NW
Washington, DC 20037
http://www.gwhospital.com

Facts and Figures (2010 Statistics)
371 beds
17,016 inpatient admissions
86,414 outpatient visits a year
Over 810 physicians on the hospital medical staff
Nursing staff of over 713
The emergency department is a Level I Trauma Center seeing 71,242 patients a year.

Additional Information
Street parking is limited and metered.
Access via Metro is recommended, if possible.

Figure D.6. CI Example



Grades

None

Example: "I perceive this CI, KR, or KA to have no risk from this scenario."

Very Low

Example: "I perceive this CI, KR, or KA to have very low risk from this scenario."

Low

Example: "I perceive this CI, KR, or KA to have low risk from this scenario."

Medium

Example: "I perceive this CI, KR, or KA to have medium risk from this scenario."

High

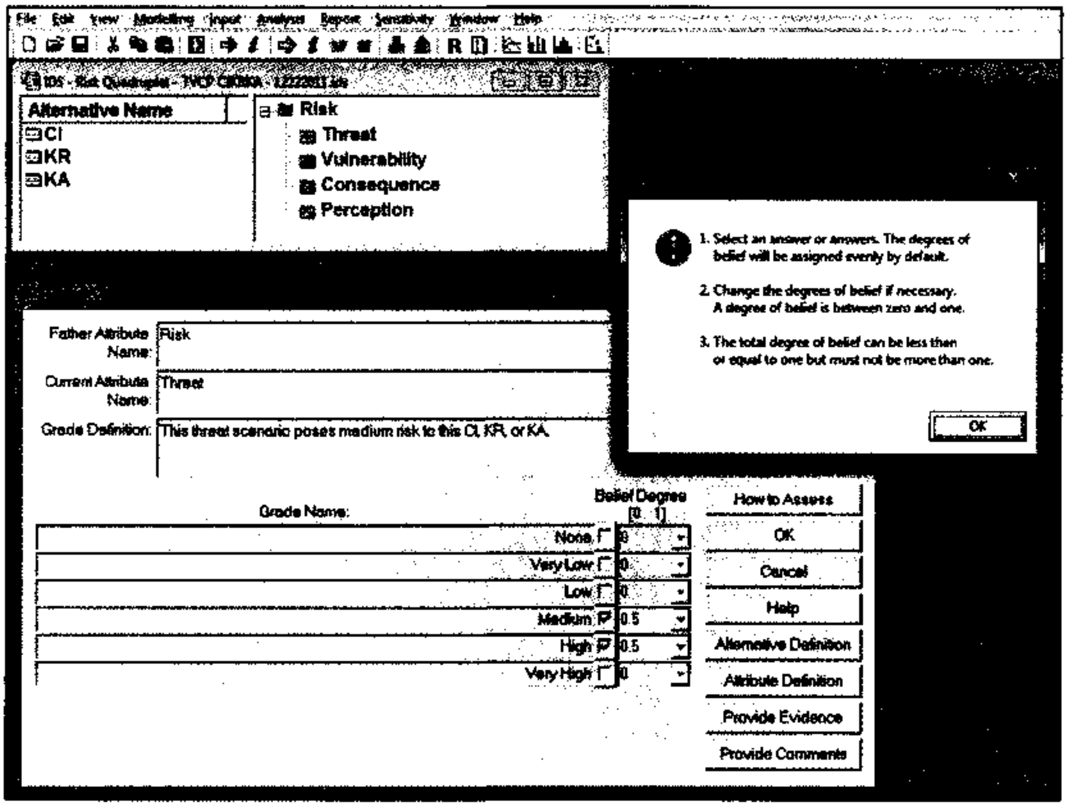
Example: "I perceive this CI, KR, or KA to have high risk from this scenario."

Very High

Example: "I perceive this CI, KR, or KA to have very high risk from this scenario."

Figure D.7. Grade Examples

The threat, vulnerability and consequence attributes will not be explored in the survey as they would be leveraged or collected and then entered into IDS separately, so they are not defined nor described in the survey. However, the grades, along with their definitions from above, were populated for the perception attribute in the Inquisite survey, as well as for the threat, vulnerability, and consequence attributes in IDS (Figure D.7 and Figure D.8). If one user was providing perception input into IDS, that user could select very low with a belief degree of .5 and low with a belief degree of .5, so long as a belief degree between 0 and 1 was entered for each grade selected, and so long as the sum of all belief degrees was less than or equal to 1 (similar to the example we see in Figure D.8).



1. Select an answer or answers. The degrees of belief will be assigned evenly by default.
2. Change the degrees of belief if necessary. A degree of belief is between zero and one.
3. The total degree of belief can be less than or equal to one but must not be more than one.

Father Attribute Name: Risk

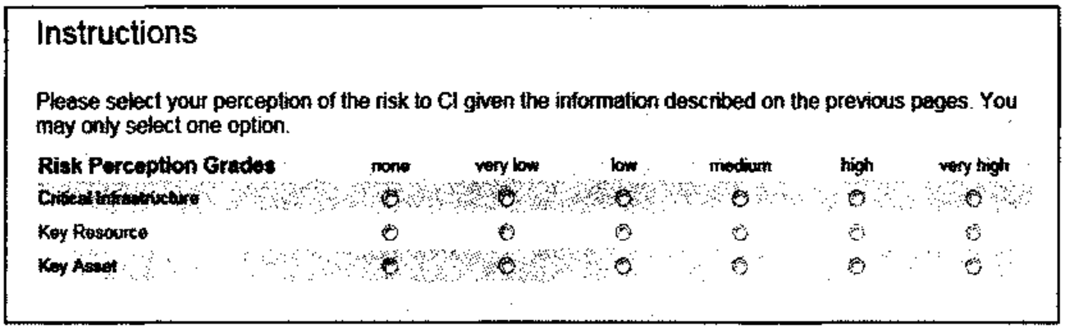
Current Attribute Name: Threat

Grade Definition: This threat scenario poses medium risk to this CI, KR, or KA.

Grade Name:		Belief Degree [0, 1]
None	☐	0
Very Low	☐	0
Low	☐	0
Medium	☑	0.5
High	☑	0.5
Very High	☐	0

Figure D.8. Dialog Box for Data Input

Unlike ER, respondents to the survey are only able to make one selection for each alternative. Since we will be surveying multiple respondents, we intend to use the frequencies of their responses as the belief degrees. If we were to allow users to choose more than one grade, we would end up with inflated frequencies for each grade, meaning that when those frequencies are entered as belief degrees, we could potentially have belief degrees that sum to greater than 1 for each alternative within the perception attribute. To avoid this, we are normalizing the perception data by restricting the survey respondents to only one grade for each alternative within the perception attribute (Figure D.9).



Instructions

Please select your perception of the risk to CI given the information described on the previous pages. You may only select one option.

Risk Perception Grades	none	very low	low	medium	high	very high
Critical Infrastructure	○	○	○	○	○	○
Key Resource	○	○	○	○	○	○
Key Asset	○	○	○	○	○	○

Figure D.9. Grade Selections

This survey was crafted using Inquisite and a version which was converted to plain text is given in APPENDIX E. It would give respondents all of the pertinent background information such as the CIKRKA definitions and examples, the risk scenario, and a means for providing their perceptions. However, upon review, it is easy to see why deploying this survey online might not be advisable. The survey is eight pages and only the last page is the actual questionnaire, the other seven pages include details necessary for respondents to determine their perceptions. In a traditional online deployment of such a survey, the user would not be able to easily refer to the background information, having to navigate back and forth throughout the survey in order to review the information provided.

Therefore, the perception assessment should probably be conducted in the form of a stakeholder meeting. We would be relying on expert elicitation and providing all respondents with a common context is necessary prior to seeking perception data, so it would be prudent to engage the stakeholders in person. This would allow each respondent to review a packet of information and to have that information at their fingertips throughout the perception elicitation process. After reviewing the materials with respondents, the survey could still be provided online for ease of completion and data collection. The data would be collected and the frequencies of the grades selected for the perceptions of CIKRKA would be input into IDS as belief degrees.

The survey would be deployed with a small set of respondents in an informal meeting with volunteer stakeholders. An Informed Consent Document is also provided in APPENDIX F to ensure respondents anonymity, absolving them from any concerns about providing their perceptions of risk to CIKRKA outside the context of their formal, professional risk analysis careers. All respondents would likely have a strong background in homeland defense, homeland security, infrastructure analysis, and risk analysis. While surveying experts would obviously result in perceptions different from those of the layperson, the risk quadruplet model is extensible and adaptable, so future iterations of the model could explore using perceptions from the general public, or even a combination of perceptions from both experts and non-experts.

Phase 2. Threat, Vulnerability, and Consequence Assessments Methodology

Complicating the in vivo methodology for the risk quadruplet is the means for leveraging or collecting threat, vulnerability, and consequence data to integrate with the perception data we would collect via survey. These data are not typically collected consistently. Some assessments use risk scores and these are rarely normalized, so comparing a risk score from one study to that from another study could be like comparing apples to oranges. Some assessments may calculate risk where threat is a scenario with an associated threat severity probability distribution, vulnerability is a conditional probability (the probability of a successful attack, given the attack is identified), and consequence is based on some loss function (McGill, et al., 2007). Other assessments use risk words like low, medium, or high, or color coding like red, yellow, or green to describe the severity of a risk (Mallor, et al., 2008).

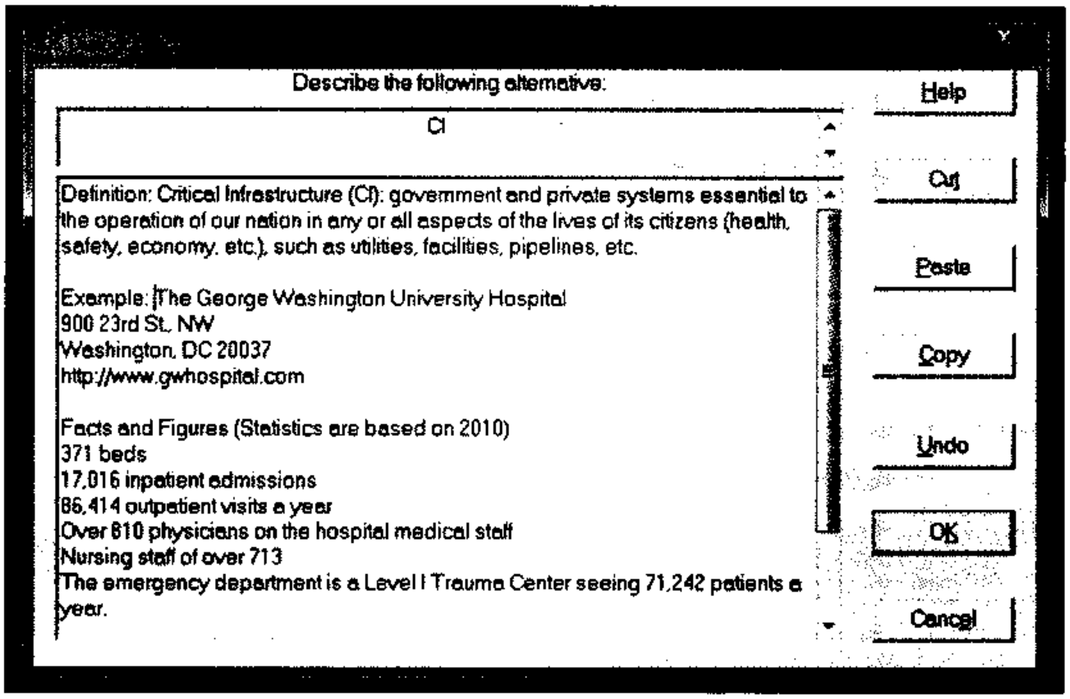
However, IDS can handle mixed data types all within the same ER model, such as stochastic versus deterministic, qualitative versus quantitative, or even incomplete data or data with uncertainties (Xu & Yang, 2001). One option for our in vivo methodology would be to leverage data from threat, vulnerability, and consequence assessments. For example, if the threat under study was flooding, there is historical data available on the impact of flooding to a particular region and its assets. There would be documented information on the consequences such as causalities or cost to repair damages. It might even be possible to determine whether any recommended fortifications provided additional security against flood damage over the years to provide some insight on vulnerabilities.

A taxonomy could be used to identify scenarios specific to CIKRKA (Luiijf & Nieuwenhuijs, 2008). Similarly, the results of an existing vulnerability assessment on a given CIKRKA, such as the Infrastructure Vulnerability Assessment Model (I-VAM) which employs MAUT for its assessment approach (Ezell, 2007), could be incorporated into the overall risk quadruplet model. Or for another example, we could look at a methodology proposed for identifying and ranking infrastructure vulnerabilities due to terrorism (should a terrorist attack be the scenario chosen) (Apostolakis & Lemon, 2005). In order to leverage these assessments, it might make sense to code the results to our common linguistic set (none, very low, low, medium, high, and very high), in order for this data to be normalized across all attributes (threat, vulnerability, and consequence), and thus to be integrated consistently with our perception data. However, the ER model does not require this consistency as it can handle mixed data models, so assessment inputs could be entered independently, or coded to a common and consistent format, if desired.

Another in vivo option would be to conduct new and independent threat, vulnerability, and consequence assessments. With this approach, we could have more control over the type of data we collect. We could opt to remain consistent with the common linguistic set, or thanks to the flexibility of ER and IDS, we could opt to collect these data distinctly. For example, we may wish to collect threat data as a probability based on historical reports related to the risk scenario. But vulnerability data may not be available quantitatively, so we could collect it qualitatively based on vulnerability reports conducted by the owners and operators of an asset. Consequence data may again be quantitative, but instead of a probability, it could be the number of deaths related to the risk scenario. IDS would also allow us to load the leveraged or collected threat, vulnerability, and consequence data in advance of the perception assessment, such that we could provide overall ranked, integrated assessments of CIKRKA immediately following the perception assessment, which might be valuable if we are already conducting a live stakeholder meeting to assess perceptions, as we could provide feedback instantaneously. If those stakeholders were also decision-makers, this quick turnaround could be very valuable.

Phase 3. Assessment Integration Methodology

The assessment integration approach selected for our in vivo (and in vitro) risk quadruplet methodology was ER, a MCDA approach, and IDS was the software selected to implement ER. Prior to deploying this risk quadruplet model in vivo, it is important to understand the data required for the model. It is also important to understand the ER software available and ensure that it is implemented correctly.



Describe the following alternative:

CI

Definition: Critical Infrastructure (CI): government and private systems essential to the operation of our nation in any or all aspects of the lives of its citizens (health, safety, economy, etc.), such as utilities, facilities, pipelines, etc.

Example: The George Washington University Hospital
900 23rd St. NW
Washington, DC 20037
http://www.gwhospital.com

Facts and Figures (Statistics are based on 2010)
371 beds
17,016 inpatient admissions
86,414 outpatient visits a year
Over 810 physicians on the hospital medical staff
Nursing staff of over 713
The emergency department is a Level I Trauma Center seeing 71,242 patients a year.

Figure D.10. Dialog Box for Description of Alternatives

We previously chose a representative example for each CIKRKA in the National Capitol Region and included pertinent information about the CIKRKA both in IDS (Figure D.10) and Inquisite (Figure D.6). Each of the attributes (threat, vulnerability, consequence, and perception) were defined in IDS as qualitative, so as to grade them using the same linguistic scale. Utilities for the overall or parent attribute (risk) were assigned to these grades (from our linguistic set of none, very low, low, medium, high, and very high) as shown in Table D.8. The utilities were chosen arbitrarily, but it may be worth exploring, during future research, how to assess and incorporate the utilities of those providing inputs for the ER model. These values could easily be revised in future iterations of the model. For our purposes, a risk grade of none would be ideal and thus would receive a Utility of 1. The remaining grades were ranked accordingly. Utilities, unlike probabilities, need not sum to 1.

Table D.8. Grades and Utilities

None	1
Very Low	.9
Low	.7
Medium	.5
High	.3
Very High	.1

To relate parent and child attributes, the following belief degrees were used for each child (threat, vulnerability, consequence, and perception). These values could also be adjusted easily in future iterations of the model. For example, if the child grade of threat is very low, that could relate to a parent grade of none, very low, and low risk with belief degrees of .25, .50, and .25, respectively. However, in the interest of keeping this model simple, belief degrees were assigned using the identity matrix (Table D.9). These belief degrees that relate the parent and child grades are not the same belief degrees that are selected by respondents during data collection when they chose the grade they deem appropriate for a given combination of alternative and attribute.

Table D.9. Belief Degrees for Relating Parent and Child Grades

	1	0	0	0	0	0
	0	1	0	0	0	0
	0	0	1	0	0	0
	0	0	0	1	0	0
	0	0	0	0	1	0
	0	0	0	0	0	1

Weights are then used to relate the child attributes to the parent attribute. This can be done using visual scoring or using a pairwise comparison of attributes. Again, future versions of the model could work with respondents or subject matter experts to complete the pairwise comparison approach provided with the IDS software, which is basically an AHP approach for weighting the child attributes. For this example, we used the visual scoring approach, selected **normalized** to ensure the weights added to 1, and while the weights initially started as equal (.25, .25, .25, and .25), it was decided that perception might not be considered equally important as the other attributes, so it was valued as approximately half as important as the other attributes (where the other attributes were weighted equally) as shown in Figure D.11.

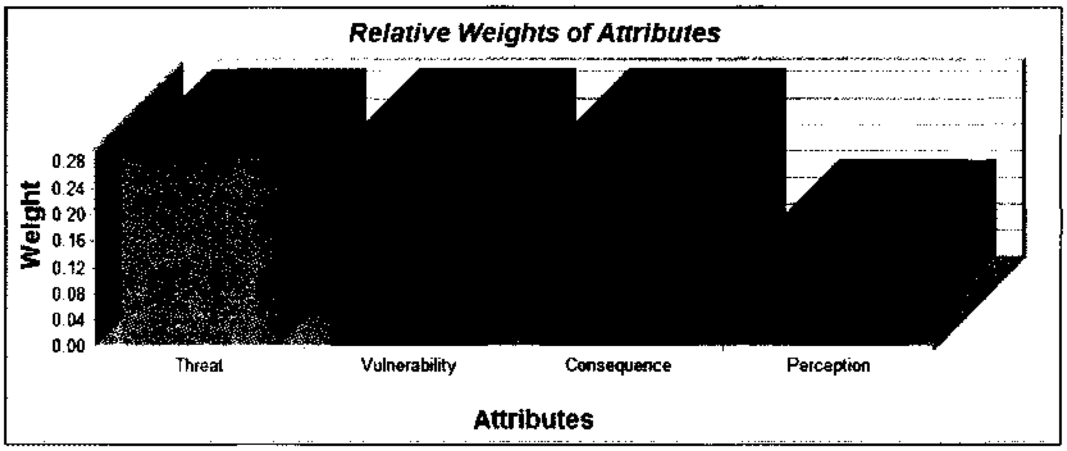


Figure D.11. Attribute Weights Using Visual Scoring

Finally, if this model were to be deployed in vivo, we would provide data for each attribute. For each combination of alternative (asset) and attribute (threat, vulnerability, consequence, and perception), a user would select a grade and a belief degree. The user could select more than one grade, so long as the sum of the belief degrees is less than or equal to 1. IDS would initially value the belief degrees equally across the selections, but the user could override these values (Figure D.11). Instructions provided by IDS would guide the user through the data entry process. The user would have access to the definitions of the alternatives, attributes, and grades from this dialog box. And the user could also provide evidence and comments to explain their selections (these are merely typed responses).

For the perception attribute, this is where we would use the distribution of the frequencies of respondents' Inquisite survey selections (captured during the first phase of the risk quadruplet) as the belief degrees for the grades. Respondents would complete a simple survey to select the grade they feel most adequately reflects their opinion of the risk to each of the CIKRKA alternatives. If 10% of respondents choose a grade of very low for the perception attribute of the first asset, CI, whereas 10% of them chose low, and 80% of them choose medium, then the belief degrees would be assigned to those grades as .1, .1, and .8, respectively. For the threat, vulnerability, and consequence data we would use the data leveraged or collected during the second phase of the in vivo risk quadruplet methodology.

APPENDIX E

INQUISITE RISK QUADRUPLET SURVEY (IN VIVO)

Page 1: Introduction

Please review the following pages which provide definitions and an example for three alternatives:

- Critical Infrastructure – The George Washington University Hospital in Washington, DC
- Key Resource – Motor Gasoline in Virginia
- Key Asset – The Lincoln Memorial in Washington, DC

Next, a scenario will be described:

- Risk Scenario – Tornado

Then, perception and a series of perception grades will also be defined.

Please use all of this information to select the perception grades which you feel most closely reflect your opinion of the risk to each of the alternatives.

Page 2: Alternatives – Critical Infrastructure

Definition: government and private systems essential to the operation of our nation in any or all aspects of the lives of its citizens (health, safety, economy, etc.), such as utilities, facilities, pipelines, etc.

Example: The George Washington University Hospital, 900 23rd St., NW, Washington, DC 20037, http://www.gwhospital.com

Facts and Figure s (2010 Statistics)

- 371 beds
- 17,016 inpatient admissions
- 86,414 outpatient visits a year
- Over 810 physicians on the hospital medical staff
- Nursing staff of over 713
- The emergency department is a Level I Trauma Center seeing 71,242 patients a year.

Additional Information

- Street parking is limited and metered.
- Access via Metro is recommended, if possible.

Page 3: Alternatives – Key Resource

Definition: public or private resources essential to the operation of our nation's government and economy, such as fuel or goods.

Example: Motor Gasoline in Virginia, Energy Information Administration

Reserves & Supply (September 2011)

- Motor Gasoline Stocks (Excludes Pipelines): 266K barrels (US Share: 0.7 %)

Distribution & Marketing (2008)

- Fueling Stations: 4,140 (US Share: 2.6%)

Consumption (2009)

- Motor Gasoline Consumed: 94.5M barrels (US Share: 2.9 %)

Environment (2008/2009)

- Alternative-Fueled Vehicles in Use: 21,505 (US Share: 2.8 %)
- Ethanol Consumed: 8,616K barrels (US Share: 3.3 %)
- Ethanol Plants: 0

Page 4: Alternatives – Key Assets

Definition: those buildings, geographic regions, monuments, or icons, whose destruction would cause a crushing blow to our nation's ego, morale, and identity, but which are not essential to the operation of our nation, such as the Washington Monument or the Statue of Liberty.

Example: Lincoln Memorial

Facts and Figure s (2011)

- Located on the National Mall in Washington, DC
- Surrounded on three sides by water
- Approximately 6M people visit annually
- Open to the public 24 hours a day
- Free to visit

Additional Information

- The memorial was built to honor Abraham Lincoln, but it has become a symbol of the American Civil Rights movement as it is also the site of Martin Luther King, Jr.'s famous "I Have a Dream" speech.

Page 5: Risk Scenario – Tornado

Definition: natural or man-made occurrence, hazard, individual, entity, or action that has or indicates the potential to damage an asset.

Example: Tornado, National Oceanic and Atmospheric Administration (NOAA), National Climatic Data Center (NCDC)

- F0 (<73mph): Some damage to chimneys; branches broken off trees; shallow-rooted trees pushed over; sign boards damaged.
- F1 (74-112mph): Peels surface off roofs; mobile homes pushed off foundations or overturned; moving autos blown off roads.
- F2 (113-157mph): Roofs torn off frame houses; mobile homes demolished; boxcars overturned; large trees snapped or uprooted; light-object missiles generated; cars lifted off ground.
- F3 (158-206mph): Roofs and some walls torn off well-constructed houses; trains overturned; most trees in forest uprooted; heavy cars lifted off the ground and thrown.
- F4 (207-260mph): Well-constructed houses leveled; structures with weak foundations blown away some distance; cars thrown and large missiles generated.
- F5 (261-318mph): Strong frame houses leveled off foundations and swept away; automobile-sized missiles fly through the air in excess of 100 meters (109 yds); trees debarked; incredible phenomena will occur.

NOAA NCDC Data (4/30/1950 - 9/30/2011)

- Magnitude: Count, Deaths, Injuries, Property Damage
- F0: 20, 0, 0, $2,653,000
- F1: 44, 0, 5, $3,468,000
- F2: 14, 0, 3, $1,628,000
- F3: 5, 2, 53, $300,000
- F4: 0
- F5: 0
- Totals: 83, 2, 61, $8,049,000

Page 6: Attribute – Perception

Definition: subjective judgment about the severity of a risk scenario to an asset; may be driven by sense, emotion, or personal experience; generally measured qualitatively; referred to merely as perception throughout this research.

Page 7: Grades

Below are the perception grade choices and examples.

- None: "I perceive this CI, KR, or KA to have no risk from this risk scenario."
- Very Low: "I perceive this CI, KR, or KA to have very low risk from this risk scenario."
- Low: "I perceive this CI, KR, or KA to have low risk from this risk scenario."
- Medium: "I perceive this CI, KR, or KA to have medium risk from this risk scenario."
- High: "I perceive this CI, KR, or KA to have high risk from this risk scenario."
- Very High: "I perceive this CI, KR, or KA to have very high risk from this risk scenario."

Page 8: Instructions – Perception Grades

Please select your perception of the risk to each asset given the information described on the previous pages. You may only select one option.

Critical Infrastructure (GWU Hospital) (Choose one)

○ none
○ very low
○ low
○ medium
○ high
○ very high

Key Resource (Motor Gasoline in VA) (Choose one)

○ none
○ very low
○ low
○ medium
○ high
○ very high

Key Asset (Lincoln Memorial) (Choose one)

○ none
○ very low
○ low
○ medium
○ high
○ very high

APPENDIX F

INFORMED CONSENT DOCUMENT (IN VIVO)

Informed Consent Document

Dr. Gheorghe and Kara Norman Hill are studying models to integrate assessments of risk, vulnerability, consequence, and perception for improved ranking of critical infrastructure, key resources, and key assets. This study will present examples of critical infrastructure, key resources, and key assets, as well as a hypothetical risk scenario, then ask participants to provide grades, based on their perceptions of the risk to the critical infrastructure, key resource, and key asset. The goal is to test the viability of the risk quadruplet methodology for integrating this subjective, qualitative perception data with objective quantitative and qualitative data from threat, vulnerability, and consequence assessments.

You are invited to participate in this study by providing your risk perception opinions after reviewing an information packet describing examples of critical infrastructure, key resources, and key assets, as well as the hypothetical risk scenario. The research project is anticipated to continue for no more than one year from the date of data collection.

There are no potential risks to respondents completing this survey. All scenarios are hypothetical and only personal opinions are being solicited and the respondents will remain effectively anonymous insomuch as the data will not be associated with any personally identifiable information. Similarly, there are no immediate benefits to participation, however, participants are encouraged to contact the researchers for additional information on the risk quadruplet model should they be interested.

The researchers will keep a record of your informed consent document in order to ensure compliance with the policies of the Institutional Review Board. Your perception data will not be connected to any personally identifiable information and will be stored in a separate database. Only the researchers will know the identity of study participants and that information will not be published as part of the research, although the research will indicate that the participants are subject matter experts and will cite the agencies and/or universities represented in the sample of survey participants.

Your signature on this form means that you understand the information presented, and that you wish to participate in the study. You understand that participation is voluntary, and you may withdraw from the study at any time.

_________________________________ _______________

Signature of Participant *Date*

Dr. Adrian Gheorghe
agheorgh@odu.edu
757-683-6801

Kara Norman Hill
kteeln@gmail.com
703-615-6998

APPENDIX G

DATA SIMULATION (IN VITRO)

Phase 1. Perception Data Simulation

If we had been able to deploy the in vivo risk quadruplet methodology using a survey to collect risk perception data, respondents would have selected a single grade for the CI, KR, and KA, based on their perceptions of the risk to that asset (as shown in the survey provided in APPENDIX E). Then the respondents' selections would be used to calculate the belief degrees. For the in vitro approach to the risk quadruplet, we simulated this data.

Generating perception data from a uniform distribution would be similar to respondents providing an equal number of responses for each of the grades, insinuating that their perceptions are completely random (with a response of none as equally likely as very high), without any pattern. Any model results using that kind of data would be meaningless as the impact of the perception attribute would be washed out in the risk quadruplet. However, it is assumed that a group of respondents, when analyzing risk to CIKRKA, would provide similar perception grades. We see evidence for comparable subject matter expert behavior when exploring the risk perception comparison of experts in the 2012 WEF Global Risks Report (Figure C.19). Subject matter experts tended to provide comparable estimates (collected with a risk perception survey) on the likelihood and impact of risks across almost all of the different risk categories ("Global Risks," 2012). Therefore, we must explore another means of generating perception data.

First we created a set of 100 respondents who were programmed to randomly choose a value between one and six, based on the Triangular Distribution. In probability theory and statistics, the triangular distribution is a continuous probability distribution with a lower limit represented by ***a***, an upper limit of ***b***, and a mode given by ***c*** ("Triangular Distribution," 2012). Given a random variable ***U*** drawn from the uniform distribution along the interval (0, 1), the following random variable, ***X***, can be used to generate random numbers from a triangular distribution ("Triangular Distribution," 2012).

$$\begin{cases} X = a + \sqrt{U(b-a)(c-a)}\ for\ 0 < U < F(c) \\ X = b - \sqrt{(1-U)(b-a)(b-c)}\ for\ F(c) \le U < 1 \end{cases}$$

Equation G.1. Generating Triangular-Distributed Random Variables

For our simulation, ***a*** corresponds to 1 (which, in turn, corresponds to a grade of none), and ***b*** corresponds to 6 (which relates to a grade of very high). In order to simulate the effects of respondents working from similar background information, such as a common risk scenario and contextual information regarding the CIKRKA we adjusted the mode of the triangular distribution depending on the asset for which the simulated respondent was providing their perception (Table 4.3). By varying the mode across the CIKRKA, we will be able to better see how the perception attribute affects the overall risk score.

Our ER model, which must ultimately integrate this perception data with threat, vulnerability, and consequence data consists of alternatives (CIKRKA assets) and attributes (risk, threat, vulnerability, consequence, and perception). For the threat, vulnerability, and consequence attributes, this produces a limited number of combinations of CIKRKA and attributes. There would only be one observation for each combination of asset with the threat, vulnerability, and consequence (which would be the resulting scores from those assessments). However, there could be multiple observations for each combination of asset with the perception attribute as the perceptions would be collected from multiple respondents for the in vivo risk quadruplet methodology; for the in vitro viability testing, the perceptions would be collected from our 100 pseudo respondents. We used the proportion of respondents who chose each grade (from our linguistic set of none, very low, low, medium, high, and very high). The simulated respondent choices (the random values between one and six generated from the Triangular Distribution) corresponded to those six grades. The belief degrees for each grade were then calculated as the proportion of respondents who selected that grade within a given alternative.

Phase 2. Threat, Vulnerability, and Consequence Data Simulation

Similarly, in the in vivo risk quadruplet methodology the threat, vulnerability, and consequence data would have been leveraged or collected. However, those data are not readily available due to the sensitive nature of such information. Therefore, attempting to access historical assessments to test the viability of the risk quadruplet is not a practical option for this research. It is assumed that the data for threat, vulnerability, and consequence assessments could be leveraged or collected to fit our in vivo model in the future. However, it was decided, for the purposes of this research, that this data could be simulated for an in vitro test of the viability of the risk quadruplet methodology.

It seemed appropriate to simulate the data as qualitative, using the same linguistic set as the one used for the simulated risk perception data (which would have also been the same set used in the in vivo Inquisite survey). In IDS, a user would select a grade and a belief degree for each attribute. The user can select more than one grade, so long as the sum of the belief degrees is less than or equal to 1. IDS would initially value the belief degrees equally across the selections, but the user can override these values (Figure D.5).

If we had leveraged or conducted actual threat, vulnerability, and consequence assessments, then we would have assigned a grade and belief degree based on those assessments to the different alternatives (CI, KR, and KA) in our IDS model. For the simulated data, though, we opted for generating belief degrees from a uniform distribution. For each belief degree within each attribute (threat, vulnerability, and consequence), as well as across each of the nine alternatives (CIKRKA), we chose a random number between 0 and 1, then constrained those values such that the sum of the belief degrees added to 1 for each attribute. The resulting pseudo-random values were used as belief degrees for each grade within each alternative (Table 4.4).

VITA

Kara Norman Hill

Engineering Management and Systems Engineering Department

Norfolk, VA 23529

Education

1. Ph.D., Engineering Management, Department of Engineering Management and Systems Engineering, Old Dominion University (ODU), Norfolk, VA, May 2012
2. M.S., Statistics, Department of Statistics, The George Washington University (GWU), Washington, DC, December 2006
3. B.S., Mathematics, Department of Mathematics and Applied Mathematics, Virginia Commonwealth University (VCU), Richmond, VA, May 2002

Positions

1. Associate, Booz Allen Hamilton, Norfolk, VA, January 2008 - Present
2. Mathematical Statistician, Department of Energy, Energy Information Administration, Washington, DC, May 2003 - January 2008

Experience

- Over 4 years of academic research experience focused on a doctoral dissertation in the fields of engineering management, systems engineering, risk analysis, risk perception, homeland security, and homeland defense, "Risk Quadruplet: Integrating Assessments of Threat, Vulnerability, Consequence, and Perception for Homeland Security and Homeland Defense"
- Over four years of consulting experience for the military and federal government, emphasizing skills in decision analysis, applied mathematics, statistics, experimental design, operations research, systems engineering, engineering management, survey design, stakeholder analysis, metrics analysis, and metrics visualization, while leveraging expertise in homeland security, homeland defense, as well as emergency preparedness, response, and recovery
- Over five years of analytical experience for the federal government in the field of energy, utilizing skills in mathematics, statistics, operations research, survey design, and survey management to ensure statistical soundness and effectiveness of nationwide energy surveys, the data collected from which were used in crucial national level estimates and predictions of energy production, generation, and reserves