Summer 2012

Towards Managing and Understanding the Risk of Underwater Terrorism

Richard J. Gay
Old Dominion University

TOWARDS MANAGING AND UNDERSTANDING THE RISK OF UNDERWATER TERRORISM

by

Richard J. Gay
B.S. January 1997, George Mason University
M.E.M. May 2006, Old Dominion 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
August 2012

Approved by:

Patrick Hester (Director)

Andreas Tolk (Member)

Ariel Pinto (Member)

Joseph DiRenzo (Member)

ABSTRACT

TOWARDS MANAGING AND UNDERSTANDING THE RISK OF UNDERWATER TERRORISM

Richard J. Gay
Old Dominion University, 2012
Director: Dr. Patrick Hester

This dissertation proposes a methodology to manage and understand the risk of underwater terrorism to critical infrastructures utilizing the parameters of the risk equation. Current methods frequently rely on statistical methods, which suffer from a lack of appropriate historical data to produce distributions and do not integrate epistemic uncertainty. Other methods rely on locating subject matter experts who can provide judgment and then undertaking an associated validation of these judgments.

Using experimentation, data from unclassified successful, or near successful, underwater attacks are analyzed and instantiated as a network graph with the key characteristics of the risk of terrorism represented as nodes and the relationship between the key characteristics forming the edges. The values of the key characteristics, instantiated as the length of the edges, are defaulted to absolute uncertainty, the state where there is no information for, or against, a particular causal factor. To facilitate obtaining the value of the nodes, the Malice spectrum is formally defined which provides a dimensionless, methodology independent model to determine the value of any given parameter. The methodology produces a meta-model constructed from the relationships between the parameters of the risk equation, which determines a relative risk value.

This dissertation is dedicated to my God,
"who trains my hands for war, and my fingers for battle"
Psalm 144:1 (Revised Standard Version)

ACKNOWLEDGEMENTS

I extend my sincere thanks to my committee for their patience and understanding over the years. Dr. Pinto's questions provided new areas to explore and his cheerful smile always kept the defenses real. Dr. Tolk provided the tough questions and the right amount of support to keep me going – thanks for saying no at the first proposal. Dr. DiRenzo always provided support: an introduction or open doors when needed. And of course to Dr. Hester – How many times did you have to read variations of this work? Thank you for your support, your praise when needed, and your gentle nudges when I got off course. Your attention to detail of the many drafts always astounded me!

To the whole crew at JAMSS restaurant in Old Saybrook, where I've spent well over 500 hours sitting at the breakfast counter working on this paper – thanks. Thanks for the real estate, the support (and coffee) and for your encouragement. Thanks to Captain Andrea Marcille for allowing me to attend many conferences to present papers or interact with the M&S community. Thanks to Dr. Susan Roberts for the mentoring and who volunteered, despite her very busy schedule, to proof read (twice)! Bill Johnston, who has never failed to ask me about my work over the many years we've been friends. Despite the miles you are a trusted sounding board and one of the folks I have to call with great news. I owe you a beer. (Just one.)

Thanks to my parents who taught me a love of learning – thanks for that library in the basement on Jerry's road. To my two sons, both unique in their own ways and contributing in their own different ways: Mick providing an unbeknownst benchmark - Yes Mickster, I wanted to be done with this before you finished your bachelor's. Okay, I'll take a tie. To Brendan, thanks for giving Dad up almost every Saturday morning for your whole life. It's time to watch some Saturday morning cartoons together buddy. Finally to my wife, and anchor, who supported me in every way possible, allowing me to have so many days and nights off to pursue this work. You read more boring drafts than anyone should ever have to read, and for engaging me in the hard conversations even when you didn't have any interest in fractals. Thanks, Bubbles. I love you. Your turn.

NOMENCLATURE

A	Activity (of an attacker)
AIChE	American Institute of Chemical Engineers
ASG	Abu Sayyaf Group
C	Consequence (of an attack)
Ca	Capability (of an attacker)
CCPS	Center for Chemical Process Safety
CI	Critical infrastructure
COBP	Code of Best Practices
COBPE	Code of Best Practices for Experimentation
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
EPRI	Electric Power Research Institute
I	Intent (of an attacker)
IAEA	International Atomic Energy Agency
JI	Jemaah Islamiyah
LTTE	Liberation Tigers of Tamil Elam
MSRAM	Maritime Security Risk Assessment Model
n	Sample size (for statistical analysis)
NEI	Nuclear Energy Institute
NRC	U.S. Nuclear Regulatory Commission
PLF	Palestine Liberation Front
R	Risk (of an attack)
T	Threat (of an attack)
V	Vulnerability (of an attack)
VAM-CF	Vulnerability Assessment Methodology for Chemical Facilities

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

CHAPTER 1
INTRODUCTION

1.1 Problem statement

The threat of terrorism remains a global concern (Cobain & Karim, 2011; DefenceWire, 2008; Fuard & Kamalendran, 2006; Gendar, Alpert & Parascandola, 2010) that challenges risk managers, in both the government and private sectors, to manage and understand the nature of the risk to minimize the expense of mitigation while holistically addressing the underlying issues. The existing methods of risk analysis for terrorism have inherent weaknesses primarily derived from the emphasis on statistical processes or expert opinion. A terrorist organization conducts extensive planning and is reactive to a defender's actions; therefore the nature of the threat is not random but deterministic (Darby, 2006) and using a stochastic process to model the system is contraindicated. This is exasperated in the underwater domain by the minimal number of attacks, on targets with great diversity, which hamper the ability to create accurate probability distributions (Jenelius, Petersen & Mattson, 2006). In many instances, the application of statistics is prone to the assumption that the probability of attack is, by default, absolutely certain (i.e.: p(attack) = 1.0) (Apostolakis, & Lemon, 2005; Brown, Carlyle, Salmeron, & Wood, 2005; Johnson, Khater, & Kuzak, 2005; Levitin, & Ben-Haim, 2008) a false assumption given the large quantity of critical infrastructure and the extremely low number of attackers. Applicable to any method employed to determine risk is the introduction of bias and errors when quantifying qualitative values (Meehl, 1978; Rao, Kushwaha, Verma, & Srividya, 2007). Another concern is that the assumption is occasionally made that the attack scenario is ergodic. Given the various rationalities of the adversarial organizations involved, their intentions and their capabilities, this assumption is incorrect (Jenelius, Petersen & Mattson, 2006; Macgill & Siu, 2005). Finally, in some risk evaluation methodologies a homogenous viewpoint is employed which constrains the risk equation as a convolution of two or three elements, principally threat, consequence and vulnerability at the end of the solution of the risk equation, ignoring the dependent nature of the three elements (Jenelius, Petersen, & Mattson, 2006; Daneshkhah, 2004; Kaplan, 2002).

1.2 Research objective

The objective of this research is to improve the ability to manage and understand the risk of underwater terrorism by creating a model based on the relationships of the elements in the risk equation. This research inductively examined available data to develop and analyze a list of parameters and relationships, which was used to deductively create a multi-perspective model of the risk equation. This research provides an improved understanding of the intent, capability and actions of adversaries, which may assist in identifying options to defeat them. Haimes (2004) summarized the benefit of this undertaking when he noted that policy involving risks is readily accepted when based on firm scientific foundations and steeped in credible scientific or technological information. Answering four research questions about the nature of the relationships between the adversary and the defender supported achieving the research objective.

1.3 Research questions

The nature of the risk of an underwater terrorist attack can be examined as related parameters with specific values (Gay & Hester, 2010). The following four research questions, derived from the precepts of developing a model from the Code of Best Practices for Experimentation (Alberts & Hayes, 2005), hereafter called the COBPE, mapped a path to holistically create a model of the underwater terrorism related parameters.

1.3.1 Research Question One: What are the parameters of an underwater terrorism incident?

As a starting point for the analysis of the parameters pertinent to this research, a list of the applicable parameters must be developed. The initial research, based on analysis of archived information available in government and other trusted databases; interviews with current practitioners of underwater defense and their Red Teams (opposing forces in simulated underwater attack exercises); and review of factors currently utilized in other terrorism incidents (e.g., surface, aircraft/airport, etc.), will develop a list of the pertinent parameters to be studied. This list, comprised of dependent and independent variables, will be ranked by relevance, based on the number of times the parameters were either available or considered, and their connection to other factors currently employed in risk

analysis. The dimensions of the parameters (e.g., unit of measure, range of values, time when known) will also be examined.

1.3.2 Research Question Two: What are the relationships between the identified parameters?

An understanding of the relationship between the parameters is necessary to truly understand the nature of the problem – and its solution space. In any complex adaptive system, such as a terrorism incident, relationships may indicate causality, including direction of causality (e.g., A→B and B→A). Additional questions, similar to those in research question one include appropriate units of measure and range of values. By mapping the relationships between the various parameters, an understanding of their impact and dependencies will be advanced.

1.3.3 Research Question Three: What is the appropriate method to quantify the qualitative variables pertinent to an underwater terrorism threat incident?

The values of many of the parameters are qualitative in nature (e.g., the intention of an adversary). To facilitate modeling, every parameter must be enumerable; basically the set of the possible elements for the parameter must be countable. Pending analysis of the parameters and relations, quantification may be achieved through several methods (e.g., fuzzy logic, matrix ranking, focus groups) that will ensure transparency and validity of the model.

1.3.4 Research Question Four: What is the measure of risk?

The objective of the research is to manage and understand the risk of an underwater terrorism incident. To better understand the magnitude of any scenario each scenario analyzed must have a final value, of one format or another (numerical, alphanumerical, etc.), potentially with a unit of measure, in order to compare the relative risk between them. The final value must have meaning to both the analyst and the policy maker, although *meaning* may be relative within the solution space and only applicable to the scenarios evaluated vice the total population space.

1.4 Research significance

The importance of ports and waterways cannot be overstated since 1/3 of world's economy and 1/4 of the United States' economy relies on international commerce & trade, most of which is transported over the oceans (Abt, 2003). This dependency illustrates the importance of transportation for moving people to and from places of employment, and cargo, including food, fuel and just-in-time production materials from producer to consumer. Ports and waterways are "a key interest from the point of view of transport systems users" (Jenelius, Petersen & Mattson, 2006, p. 538). As Zimmerman notes: "...infrastructure occupies a central position in the U.S. Economy (contributing about 10% of GDP). Small local terrorism attacks can have large regional and national economic impacts" (2005, p. 5). The Department of Homeland Security (DHS) has been criticized in the media for spending "hundreds of millions of dollars to protect ports since Sept. 11 without sufficiently focusing on those that are most vulnerable, a policy that could compromise the nation's ability to better defend against terrorist attacks" (Lipton, 2005, p. 1). Security measures must strike an appropriate balance between security and freedom to ensure rapid transit for perishable and seasonal goods (Saito, Guthmuller & DeWeert, 2005). Utilizing a method to manage and understand uncertainty of the risk of a terrorist attack may assist a decision-maker in improving security for critical infrastructure.

The research provides three significant contributions to risk analysis in the underwater domain. First, it contributes to the body of knowledge by identifying and relating (i.e., mapping) the critical variables pertinent to the risk analysis for underwater terrorism. Second, this research expands the methodologies for the analysis of underwater terrorism risk. Finally, this research provides areas for future research in the critical path for managing and understanding uncertainty when evaluating the risk of an underwater terrorism attack.

1.5 Key assumptions, limitations and delimitations

1.5.1 Assumptions

This research assumed that:

- the relationship between the risk parameters are linear,

- the parameters demonstrated in an underwater attack conducted by the government were similar to those employed by an adversarial organization,
- the current processes employed by the intelligence community would provide adequate vocabulary for the research,
- the Adversary/Defender model is an open system relationship containing "more variables than we can comprehend at one time, or that some of the variables are subject to influences that we cannot control or predict" (Thompson, 2006, p. 6),
- adversarial organizations use similar methods to recruit and train people regardless of the tactics, techniques or procedures employed,
- an adversary operates under less restrictive norms of rationality than the defender,
- an adversary is motivated by a consequence,
- an adversary searches for vulnerability to achieve the desired consequence,
- if a vulnerability is exploited, it will reasonably incur a consequence, and
- the infrastructure under study is, in fact, critical.

1.5.2 Limitations

The interdependencies between the variables of the risk equation cannot be ignored. However, this research focused on the threat variable from the risk equation, as defined in Section 2.2.1, to reduce the scope of the research. This research did not consider how either vulnerability or consequence was determined. It did employ a multi-perspective view of the relationships between vulnerability and consequence with the threat element of the risk equation.

The model testing, one aspect of confirming validity was fashioned in a less restrictive form "so that it covers a broader range of phenomena and is exposed to more opportunities for falsification" (King, Keohane & Verba, 1994, p. 22). However, to achieve significant internal validity, the model testing had a high degree of control, which, unfortunately, reduced the naturalistic conditions, thereby reducing the external validity (Cook & Campbell, 1983). A balance, based on the data population, was maintained in both developing and testing the models.

1.5.3 Delimitations

To minimize the scope of the research, and provide a focus on analysis of the risk equation, this research did not:

- explore how to measure vulnerabilities of attacked critical infrastructures, except as required for the interdependencies of the risk equation,
- explore how to measure the consequence of a successful attack on critical infrastructure except as required for the interdependencies of the risk equation, and will be limited by considering only the external adversary.

Runkel and McGrath (1972) identified three aspects that must be addressed when considering if research is generalizable. First, can the research methodology produce the same results under different conditions? Section 0 explains the process employed for the selection and analysis of the data. This methodology is generic in nature, fostering generalizability for any man-made threat and facilitating other researchers to change the research environment and observe variability, ensuring this research "covers a broader range of phenomena and is exposed to more opportunities for falsification" (King, Keohane & Verba, 1994, p. 22).

Second, Runkel and McGrath (1972) ask if the research design focused on measurement and not process. This research did not take the initial measurements but used and converted (qualitative to quantitative) existing data. The conversion of the data was conducted in the analysis of the cases and used the Malice spectrum outlined in Section 0. The conversion retained the context of the original data to enable exploration, specifically for research question four, what is the measure of risk, of possible alternative explanations that may exist for the causal relationships observed (Huitt, 1998).

Runkel and McGrath's (1972) third aspect is the composition of the sample for the data analysis. Sample size, n, is vital in determining the confidence interval and confidence coefficient of statistical models and impacted the depth of the analysis (Mendenhall & Sincich, 1995). A larger n provides confidence for the inferences that are made from the data. However, n was limited by the availability of unclassified data and the expectation of utilizing two samples for the research – one as hypothesis testing and one sample for

methodology testing. The total sample size was n=51, but it was disaggregated into two samples, n=26 for Sample A and n=25 for Sample B. Sample A was larger because the statistical power desired was π=0.80 and the expected difference between the means of 0.8 required a sample size of at least n=26. The composition of the two samples was dictated by the data sources and the methodology. Data were collected but not sorted. Once the total sample was documented, the sample was parsed into two samples and then sorted – to wit, the samples were generated randomly.

The research was conducted from the perspective of the United States as the defender entity. The perspective of the research includes, but is not limited to, aspects such as resource allocation, rationality, scope and magnitude of the problem set, and the form of government. The research examines adversarial actions across numerous geographic areas, differing governments and over the 60 year time period that minimizes the impact of the research's perspective on generalizability.

CHAPTER 2
REVIEW OF LITERATURE

An exploration of critical infrastructure protection from underwater (formally termed subsurface) attack begins with understanding the relationship between critical infrastructure and risk. A large part of the concept of risk is uncertainty, which will be explored later in this chapter. Parsing the problem further, there is uncertainty in the risk of maritime terrorism, more specifically, an underwater attack to critical infrastructure. An attack conducted underwater is a unique instance of terrorism with unique challenges including the environment, tactics used, techniques employed and the specialized equipment required. Figure **1** provides a graphical depiction of the alignment of these concepts and forms the basis for this review, illustrating the narrowing of focus from the generalized concerns of risk to specialized issues involved with the uncertainty in the analysis of a terrorist attack in the underwater environment. The following sections discuss each topic depicted in Figure **1,** proceeding from the general to the specific.

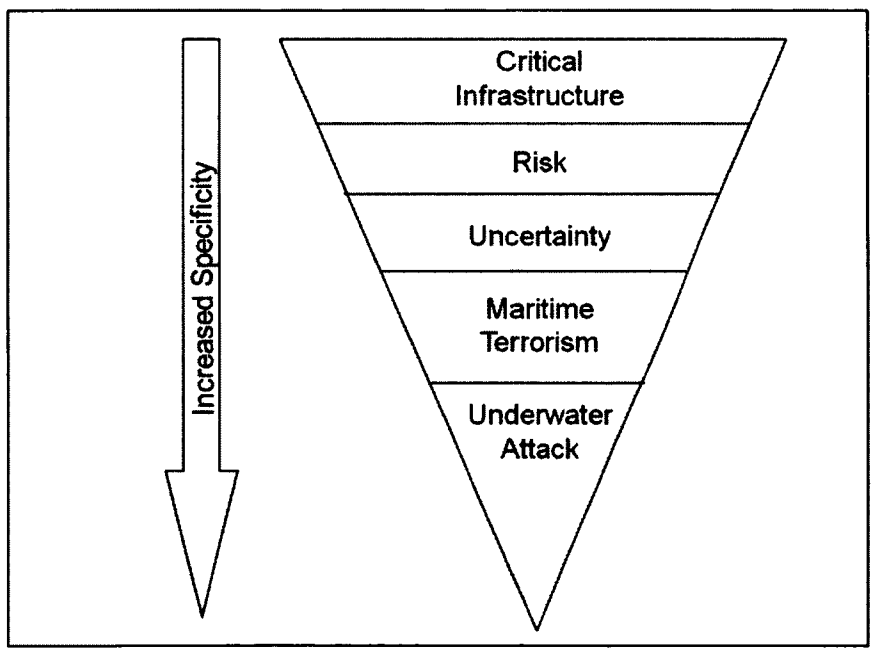

Figure 1: Path of the literature review

The context of this research is managing and understanding the risk of terrorism against critical infrastructure. Most definitions of critical infrastructure (CI) have common variables that point to physical structures that are absolutely necessary for the development and functioning of a society. The intent and spirit of much of the current literature are captured by four definitions: one is provided by the *International Journal for Critical Infrastructures* that defines critical infrastructures as: "...networks for the provision of telecommunication and information services, energy services (electrical power, natural gas, oil and heat), water supply, transportation of people and goods banking and financial services, government services and emergency services" (2004, p. np). This definition incorporates the variables of the basic services (e.g. water, sewer) for society, information and communication services for economic development and the systems that provides for basic government support.

In the second definition, Moteff, Copeland and Fischer (2003) provide a more generalized definition in their report to Congress, which states that critical infrastructures are "infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security" (p. 2). Although this definition includes infrastructure, it leaves the reader with an unclear explanation of the scope of the infrastructure under debate. Is it physical properties, data and information or perhaps other ethereal variables? It does make an interesting distinction that loss of the infrastructure would have an impact on defense, an element only implied in the Journal's definition previously provided.

In both cases, the reader is left to debate the level of impact required to categorize a system as critical vice non-critical. Further, where do environmental consequences fall within the definition? Is loss of public confidence a factor when debating loss of government services or impacting defense or economic security?

The United States government has several key documents that provide an additional definition of critical infrastructure. Presidential Decision Directive 63 (PDD-63), Critical Infrastructure Protection, defines critical infrastructure as variables of the national

infrastructure that are "essential to the minimum operations" (Clinton, 1998, p. 1) for the national and economic security of the United States. The USA PATRIOT Act of 2001 clarified the definition and included virtual systems. It defines critical infrastructures as systems that are "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety" (Critical Infrastructures Protection, 2001, p. 401). The United States' military broadens the definition to include political, military, economic, social, infrastructural and informational (PMESII) elements in a system-of-systems approach to understanding the entire environment (SRI International, 2007).

The definition of critical infrastructure is subjective because it must be scalable, and it depends on the context of the problem being analyzed. Therefore, for this research, critical infrastructure contains the following critical variables: physical structures and not the data or information contained within those structures; these structures must be absolutely necessary for the defense, the society or the economic security of the community served; and loss of the physical infrastructure would have a detrimental effect on the public confidence. Using these variables, the following definition is proposed for this research:

Definition 1: Critical infrastructures are those facilities and their associated components that would cause considerable degradation of political, military, economic, social, infrastructural or informational services, or have a detrimental effect on the environment, in the event of a successful adversarial event.

This definition includes chemical production plants or storage facilities, electric power generation or distribution facilities, transportation nodes or hazardous material nodes such as nuclear power plants or nuclear storage facilities.

This definition contains an ambiguity which can be clarified within the context of the facilities discussed – "considerable degradation". To understand what considerable degradation is, the reader should include appropriate metrics within the context of the conversation. Johnson, Khater and Kuzak (2005) suggest metrics for critical infrastructure include public health and safety such as regulatory requirements, financial

impacts to society and corporations such as business interruptions, loss of public confidence, and environmental consequences.

This definition also remains scalable, capable of being applied internationally, nationally or within a particular community. Scalability remains a vital variable of understanding critical infrastructure. From the perspective of a town planner, the water or electric delivery systems are part of the town's critical infrastructure. However, at the national level, that town's infrastructure may not be considered critical when compared to other facilities such as a transnational oil or gas pipelines or the telecommunications facilities that comprise the Global Information Grid. This research does not debate the merits of either scenario but develops a methodology for managing and understanding uncertainty regardless of how the analyst defines the scope of critical infrastructure.

2.1. Uncertainty

Uncertainty in the risk evaluation environment is a fundamental attribute that is, in a sense, the underlying cause for risk assessment, effectively bounded rationality – decision making without perfect information. Decision Makers distinguish "among three types of uncertainty: inadequate understanding, incomplete information, and undifferentiated alternatives" (Lipshitz & Strauss, 1997, p. 149). Lipshitz and Strauss (1997) document at least 14 different ways that uncertainty is conceptualized including risk, ambiguity or conflict. They propose that "uncertainty in the context of action is a sense of doubt that blocks or delays action" (p. 150). Ayyub (2005), who developed an ignorance hierarchy, utilized a definition that starts with "reality is perceived as a continuum in its composition of objects, concepts and propositions" and builds through knowledge to uncertainty (p. 15).

Other authors approach uncertainty along various stages of an analysis process. For example, Argote (1982) provides a short summary for the beginning of the analysis process when she writes the "concept of [input uncertainty] draws on the work done in the areas of cybernetics and information theory (e.g., Wiener, 1948; Shannon and Weaver, 1949; Miller, 1953; Attneave, 1959) in which uncertainty is expressed as a function of the number of choices or alternatives in a given situation" (p. 422).

Many authors focus on mainly the process of the analysis and its applicable variables, only mentioning uncertainty as an afterthought. However, Macgill and Siu (2005) argue that "knowledge is limited and approximate. In the risk context, this argues for open consideration to be given to uncertainty and in particular how it is dealt with by the various constituencies involved with a risk issue" (p. 1107). They emphasize that certitude, a state of certainty, is a perception or degree of confidence a person has in his/her acquisition of true and valid knowledge, including a magnitude of scientific certainty. The Code of Best Practice for C2 Assessment (COBP) defines uncertainty as "an inability to determine a variable value or system state (nature) or to predict its future evolution" (NATO, 2002, p. 249). The COBP makes an important point that when all the possible outcomes are known, including their associated probabilities, but the outcome of a specific instance is not known, then "there is a risk, in this case a known risk, associated with a particular outcome" (NATO, 2002, p. 249). For this research, the definition of uncertainty will assume a more systems based approach:

Definition 2: Uncertainty is the lack of precise knowledge about a system or a given situation.

2.1.1. Types of uncertainty

The different types of uncertainty have been parsed in multiple ways (e.g., Ayyub, 2005; Lipshitz & Strauss, 1997; Willis et al., 2005). This research will utilize the hierarchy, recreated in Figure **2**, developed by Haimes (2004). It suggests that uncertainty can be broken down into variability and knowledge. It further parses variability into temporal, spatial and individual heterogeneity. Knowledge uncertainty is parsed into model, parameter and decision. The taxonomy appears to align with other taxonomies described in the literature, either directly or through interpretation by the reader. A closer examination of the types of uncertainty follows.

2.1.1.1. Variability

The aleatory uncertainty, labeled variability by Haimes (2004), is about the state of reality and about our knowledge of the state reality. Aleatory uncertainty is frequently used in a natural sense (e.g., earthquakes or points of landfalls for hurricanes) or in a

generic sense like the states of nature that can concern the actions of others (NATO, 2002; Darby, 2006; Woo, 1999). Haimes (2004) clarifies variability when he states "variability occurs when the quantity of concern is not a specific value but rather a population of values" (p. 238). Variability includes the concept of ambiguity or "uncertainty associated with the likelihood of an event" (Darby, 2006, p. 135).

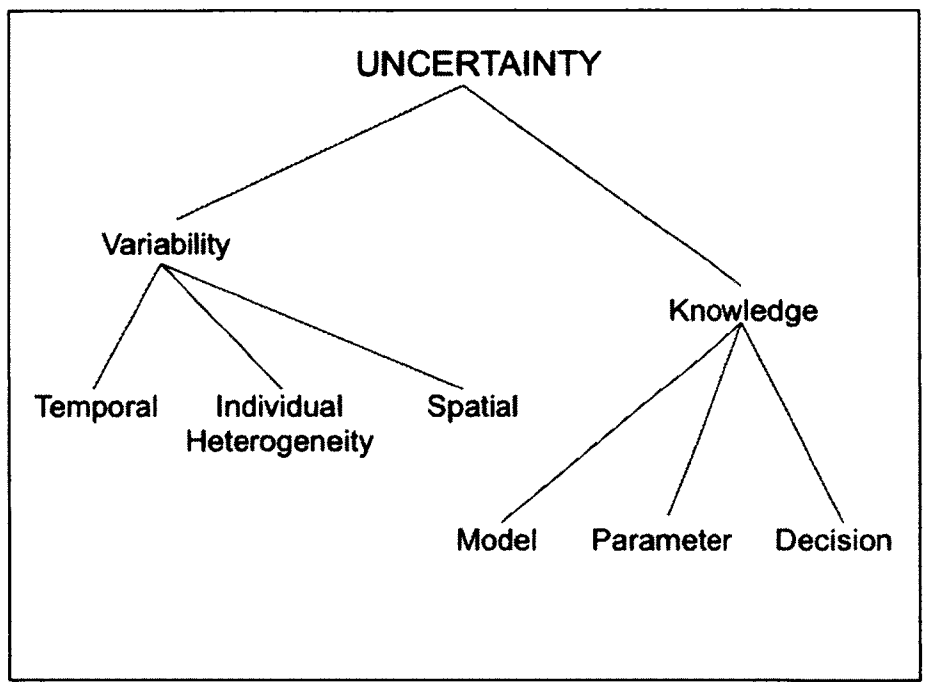

Figure 2: Sources of uncertainty (adapted from Haimes, 2004)

The sub-elements of variability are complimentary but independent. Temporal variability is variability based on the dimension of time. It can be modified by spatial variability which is based on location, specifically geographic location (the reader can consider the case of a hurricane making landfall. The when and where of landfall is a variable that is constricted as the landfall event nears). The final variability factor that was described by Haimes (2004) and included in this research's taxonomy is individual heterogeneity. Similar to Haimes' (2004) application, this research views individual heterogeneity as differences between individual groups (e.g., Al Qaeda, HAMAS, Gama'a al-Islamiyya)

vice individual people and, which is a vital factor when representing populations for making assumptions about uncertainty.

2.1.1.2. Knowledge

In addition to the uncertainty manifest in reality, there is epistemic uncertainty, which is distinguished by decision makers as "inadequate understanding, incomplete information or undifferentiated alternatives" (Lipshitz & Straus, 1997, p. 149). This category of uncertainty, classified as knowledge uncertainty (Haimes, 2004) addresses uncertainty in, or caused by, our model, our parameters and our decision process and is discussed in subsequent paragraphs in this section. Knowledge uncertainty, frequently called epistemic uncertainty, is introduced by humans into the understanding of the event and is solely concerned with our understanding and interpretation of reality (Darby, 2006; Kelly & Smith, 2009). Knowledge uncertainty is related to non-specificity, which cannot be represented by a probability (Darby, 2006). The importance of understanding knowledge uncertainty is highlighted by Woo (2002) when he states: "Whatever the underlying theoretical foundation, given the dependence on the modus operandi of a terrorist organization, any risk calculation inevitably involves a number of subjective probability assignments, variability of which amplifies the epistemic uncertainty" (p. 16).

Humans tend to order the concept of reality into a subconscious structure based on beliefs and feedback loops, commonly referred to as our model. Ordering allows humans to evaluate or manipulate data and to translate real-world observables into information (Kelly & Smith, 2009). The COBP (2002) uses model-based uncertainty and uncertainty of focus to encompass model uncertainty. Model-based uncertainty endeavors to answer if the underlying model is valid and representative of reality. Uncertainty of focus asks if the "assessment covers all the important factors and/or issues" (NATO, 2002, p. 254). Yu and Harris (2009) identify two types of input variables: regressive variables and model parameters. "Regressive variables are those that can be influenced by process design or by a control strategy. With model parameters, there are typically no opportunities to directly influence their variability" (p. 596). Regressive variables are a function of model-based uncertainty and may be caused or exacerbated by the assumptions that engineers or risk analysts invoke (NATO, 2002).

As noted in the previous paragraph, another category of uncertainty is within the parameters of the model created or our understanding of the model parameters and includes imprecision in measurement, censoring or interpretive errors (Haimes, 2004; Kelly & Smith, 2009; Macgill & Siu, 2005). Once a parameter is selected and coded into the model, there are usually limited opportunities to improve the parameter's inconsistency. The COBP (2002) calls this type of uncertainty parameter value uncertainty and introduces the "complexity of uncertain factors (i.e., their dimensionality)—when a sufficiently complex factor (e.g., scenarios or future technology) is uncertain, the team cannot expect to overview the set of all possible true states" (pp. 254-255). Reducing input uncertainty by expressing uncertainty as a function of the number of alternatives has a long history of research in cybernetics and information theory (e.g., Attneave, 1959; Miller, 1953; Shannon & Weaver, 1949; Wiener, 1948). In addition to the uncertainty within the parameter, there exists an "information theory [that suggests], as volume homogeneity increases, input uncertainty increases" (Argote, 1982, p. 426).

Related to parameter uncertainty is the concept of vagueness. Vagueness is a situation where there is uncertainty how to develop the parameter to describe a value within an event. Vagueness is not usually represented by a probability function. Darby (2006) uses an example of a report that is in a box and the box is located in a room. We are certain that the report is in a specific box, and we know exactly where that box is located in the room. However, when asked if the box is in the center of the room there may be several answers: The first answer may be "no" if the box is located in a corner or touching a wall (value = 0). The second answer may be "yes" if the box is directly in the center of the room (value = 1). However, the third answer could be "maybe" if there is some doubt as to the actual center of the room (value $0 < x > 1$) (Darby, 2006, pp. 23-25). Darby (2006) asserts that fuzzy sets address vagueness and differ from crisp sets because they include the concept of partial membership.

The third category of uncertainty related to the interpretation of reality is decision uncertainty that "surrounds the implementation of analytical results into actual decisions and policy" (Haimes, 2004, p. 250) or, as an output of the analytical process, may result

in "undifferentiated alternatives" (Lipshitz & Strauss, 1997, p. 149). Decision uncertainty is post-analysis and will not be examined in this research.

2.1.1.3. Sources of uncertainty

One source of uncertainty in risk analysis of terrorist attacks is the variability and error in the estimate of threat. The existing foundations for information regarding the parameters that determine what the current terrorist threat is are intelligence estimates, historical analysis, and expert judgment, which are not deterministic in nature and force the model to use approximations to quantify them (Willis, et al., 2005). As an example, using estimates from historical analysis is very difficult since it is very rare for the circumstances surrounding an event to remain the same at all times and the causal connections are not usually fully understood (Jenelius, et al., 2006).

The second source of uncertainty is how the value of consequence is determined. Because of uncertainty, policy analysis may rely on heuristic estimates that may have a low probability of being correct (or, the reciprocal: a high probability of being incorrect). The estimates may provide a concrete estimate of risk but it is not linked to the risk reality (Willis, et al., 2005). Methods for planning under uncertainty currently exist (see Bauer, 2002; Davis, 1994; Lempert, Popper & Bankes, 2003) and can assist with determining risk.

In the previous discussion of risk and uncertainty there is a common thread pertinent to the research questions and eloquently argued by Darby (2006): "A terrorist attack is not a random event; it involves a specific scenario that is selected, planned, and implemented by the adversary" (p. 9). Since the terrorist attack is not a random event there are difficulties in developing a quantitative risk matrix due to the uncertainties involved (Jones, Lyford, Qazi, Solan, & Haimes, 2003). Therefore the use of random modeling and methods of risk analysis based on randomness is flawed. Darby (2006) continues that "terrorist acts are intentional and an evaluation of them involves considerable epistemic uncertainty. Traditional probabilistic risk analysis techniques have difficulty modeling the risk from terrorist's acts due to the inherently large epistemic uncertainty"

(p. 12). Scenarios involving large epistemic uncertainty in the analysis of threat form the keystone for this research.

2.1.2. Uncertainty and reality

If humans were capable of perfect knowledge, then our perception of the world would be equivalent to reality. However, reality is fluid and humans have yet to acquire perfect knowledge, which introduces uncertainty. Figure **3** is an illustration of how an aspect of reality can develop an error cone based on our description of that reality, or our parameters. Furthermore, our working portrayal of reality, essentially our model (either physical, virtual or mental) develops its own potential cone of error. These cones represent the various types of uncertainty that will be discussed in the next few sections and are illustrative of how uncertainty is derived or manifest from reality.

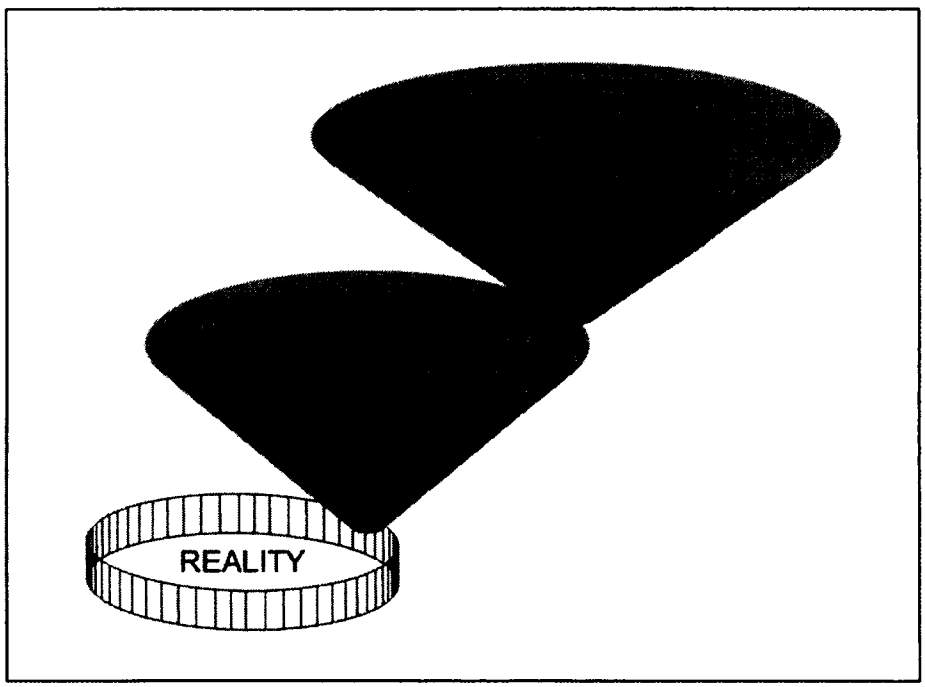

Figure 3: Planes of uncertainty

2.1.3. Dependence

Frequently, uncertainty is driven, or increased by, dependence because of the relationship between the entities or states that can increase the breadth of the fault tree dramatically, and is context-sensitive for each specific scenario. Dependence is context-sensitive and becomes more complicated for specific threats than for random threats. Consider the impact of copycat attacks seen in domestic and international terrorism or the increase in attack frequency around holy days in the Middle East. Consider too, the dependencies which affect vulnerability, for example, Zimmerman (2005) discusses the 1998 water main break in New York city, which caused a street to collapse and a gas line to rupture.

When addressing threat, the analyst or modeler must account for dependence. Darby 2006) incorporates dependence by using a multi-perspective model (Adversary/ Defender) and stresses that dependence is far more complicated for terrorist acts than for random acts (e.g. earthquake or equipment failure) because if one attack scenario is attempted and succeeds in causing a significant consequence then the frequency of the attacks may increase as success encourages more attacks (e.g., road side improvised explosive devices, or IEDs). The frequency of attacks can also increase based on world events as terrorist groups obtain more recruits based on actual or perceived injustices by the United States.

2.2. Risk

Generically, risk is the probability of the occurrence of a specific possible event and is frequently associated with negative outcomes such as the possibility of suffering harm or loss (NATO, 2002) but may also include the possibility of not achieving the objective; an assessment of the probability of failure; an uncertain future scenario; or a perception of consequential pain (NATO, 2002 pp. E-1, E-2). A specific definition of risk has not yet been accepted across disciplines, as noted by Macgill and Siu (2005) who identified 26 different *technical* and *social* definitions of risk, but the concept has evolved to the point of general understanding when discussed among practitioners of risk management. Pertinent to this research, Willis, et al. (2005) assert that "there is not a consistent and shared definition of terrorism risk" (p. vii). They further insist that there is "no existing framework for selecting and combining risk indicators" and lament that the methods for

testing the accuracy and the probability distribution of risk has received little attention (p. vii). An examination of risk definitions reveals a commonality that highlights the core concept of risk; essentially that risk has inherent consequences; and that "risk is an intrinsically dynamic and unstable phenomenon" (Macgill & Siu, 2005, p 1119).

At perhaps the most generic level, risk is defined as "...the uncertainty of outcomes [and] it is best measured in terms of probability distribution functions" (Jorion, 2001, as cited in Samson, Reneke & Wiecek, 2009, p. 559). The context of this definition is financial risk, specifically market volatility. From this definition several points can be ascertained. First, uncertainty exists and must be managed. Second, the financial community is focused on the outcome of the uncertainty – the end result, not the cause or the measures in place to mitigate. A final point is that risk can be measured and quantified as a distribution function, implying there is sufficient historical data to create accurate distributions – a serious concern with underwater terrorism that has less than 100 events on public record.

Shifting from a qualitative perspective to a quantitative discussion, risk is frequently defined as the combination of the probability of an event and the consequences of the event or, mathematically, a convolution of variables (Daneshkhah, 2004; ISO, 2009; Jenelius, Petersen & Mattson, 2006). Kaplan and Garrick advance a two-variable definition when they discuss their risk triplet approach where each scenario has two variables: the probability of the scenario, $p(S_i)$, and the consequence, C, of that scenario (Kaplan & Garrick, 1981). The risk triplet (3-tuple) is $\{S_i, p(S_i), C|S_i\}$, where S_i is the i^{th} scenario, and i is merely the number given to identify a specific scenario (Kaplan, 2002; Kaplan & Garrick, 1981).

Some authors have expanded the concept of the probability of the event to include the threat and vulnerability elements while retaining the consequence (Darby, 2004, 2006; Moteff, 2004). They have utilized mathematical notation to form the following definition:

Equation 1: Risk defined with three probabilities: threat, vulnerability and consequence

Risk (R) = p(Threat (T)) * p(Vulnerability (V)) * p(Consequence (C))
or
R = p(T)*p(V)*p(C)

Where the "*" symbol represent convolution, not multiplication.

Taking the mathematical concept one step further, and providing an avenue for managing the probability distributions in risk, Willis, et al. (2005) proposed a measure of terrorism risk as "the expected consequence of an existent threat, which for a given target, attack mode, and damage type can be expressed as:

Equation 2: Risk defined as expected consequence

Risk = p(attack occurs) *
p(attack results in damage | attack occurs) *
E(damage | attack occurs and results in damage)" (p. 10)

Again, the "*" represent convolution.

Similar to Equation 1, this definition, strongly rooted in probability theory, still harkens back to the basics: probability of an event exists and consequences can be associated with that event – the common theme observed across all disciplines researched.

Using probability functions for underwater terrorism is problematic because the amount of data available to produce a probability distribution is scarce. Recall that probability is used to represent the frequency an event occurs on the state of knowledge. For example, probability as a frequency is defined as the number of successes divided by the number of attempts of a specific trial. In one of the common textbook examples for frequentist probability, the example of a coin toss is given where the probability of getting heads on a fair-coin flip is 50%. However, this measure is dimensionless (it has no specific time duration) and does not provide limits for response to a threat.

When probability is used as a measure of a state of knowledge (known as Bayesian probability), it is measuring the uncertainty inherent in the state of knowledge. When examining the state of knowledge uncertainty can be one of two types: aleatory

uncertainty or epistemic uncertainty. Aleatory uncertainty is due to uncertainty in the problem itself, and is often called random or inherent uncertainty. Epistemic uncertainty comes directly from the state of knowledge the observer or participant has (Darby, 2006).

However, in the current methods of determining probability, each method assumes attacks are ergodic, that is, from observing past events one can accurately predict the future. This approach is flawed because risk evolves over time as adversary's resources and intentions change (e.g., motivational changes, adapting to defenders tactics or law enforcement activity). Jenelius, Petersen and Mattson (2006) emphasize that:

> Estimating the probabilities of extreme events such as natural disasters and terrorist attacks is very difficult. The probabilities are predicted from historical data, which implies that the circumstances around the event remain the same at all times and that all causal connections are known. (p. 540)

Each of the previous definitions contains variables of a widely used definition of risk and is adopted as the definition for this research in the following form: risk is the product of threat, vulnerability and consequence (Darby, 2006; Moteff, 2004; Willis, et al., 2005) or more precisely:

Equation 3: This research's definition of risk

Risk (R) = Threat (T) * Vulnerability (V) * Consequence (C)

or

Definition 3: Risk

R = TVC

The difference between this definition and Equation 1 is the basis on probability. This definition convolutes the values of threat, vulnerability and consequence independent of how the values are determined. Each variable will be discussed in more detail in Sections 0, 0 and 0.

2.2.1. Threat

Threat is the variable that defines the intentions and capabilities of the attacker. In the literature, threat has many different definitions and is addressed in diverse ways. For example, Haimes and Horowitz (2004) define threat as "a potential intent to cause harm or damage to a system by adversely affecting its states" (p. 34). In 2005, Willis, et al., (2005) argue that threats are "external, dynamic forces acting on targets or infrastructure" (p. 51). Note the focus on external forces, thereby eliminating one potential area of threat: internal collaborator or actors. They contend that "threats to a target can be measured as the probability that a specific target is attacked in a specific way during a specified period" (Willis, et al., 2005, p. xvi) and is written as:

Equation 4: Threat as a probability that an attack occurs

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

Interestingly, this measure details a certain type of attack on a specific target, which is an unrealistic constraint on the threat analysis because of the large uncertainty that exists in the terrorist threat environment.

However, Willis et al. (2005) parse threat into intent and capability, something that is agreed upon by more than one author (Moteff, 2004; Roper, 1999; Willis et al., 2005) and the intelligence community, in general. "The key to quantifying the threat (target, weapon, and delivery system) of a terrorist attack is being able to account for varying levels of uncertainty about the likelihood of the threat" (Garrick, et al., 2004, p. 137). Because the intelligence community is focused on detecting and thwarting an attack, they usually view threat in terms of groups of attackers. Willis's (2005) attack-type perspective (p. 6) brings increased utility to analysts and planners because it focuses on what targets are threatened by what type of attack vice being focused on the whom and the why of the attack. This approach is aligned with the engineering communities' practice of risk analysis (see Ayyub, 2005; Pate-Cornell, 2005; von Winterfeldt & Rosoff, 2005).

Other perspectives on the variables contained in the definition of threat include motivation, capability, opportunity and impact (Vidalis, 2004) or the "combination of an

asset, a vulnerability and an attacker" (Bauer, 2002, p. 1). Bauer (2002) asserts an asset is anything the defender wishes to protect and defines attackers, occasionally called "actors", as anyone, to include drug cartels, other government agencies or industrial spies (p. 3).

For this research, the definition of threat will combine several key elements noted above. The intent or desire to do harm will be taken as motivation. The capability of an aggressor must also be considered, for without a means to do harm, there is no threat. However, the intent or the capability may not be completely known even to the aggressor, a fact which does not diminish the actual threat to the facility but merely indicates the level of planning conducted thus far. An important argument not noted in the previous discussion is the damage caused by non-events. The value of a well planned and executed public relations attack (e.g., releasing photographs of aggressors within a nuclear facility without actually damaging that facility) should not be underestimated. The effect would be very similar to a successful physical attack in influencing the government and the associated public. Using these concepts, this research will define threat as:

Definition 4: Threat is the intent and the capability of an external aggressor to adversely affect a target, e.g., a critical infrastructure.

In the previous discussion for threat, a common thread exists that is eloquently argued by Darby (2006): "A terrorist attack is not a random event; it involves a specific scenario that is selected, planned, and implemented by the adversary" (p. 9). Since this statement is taken to be true, then the use of random modeling and methods of risk analysis based on randomness is flawed. He continues that "terrorist acts are intentional and an evaluation of them involves considerable epistemic uncertainty. Traditional probabilistic risk analysis techniques have difficulty modeling the risk from terrorist's acts due to the inherently large epistemic uncertainty" (Darby, 2006, p. 12). Additionally, this research will not assume, similar to Levitin and Ben-Haim's (2008) approach to the evaluation of risk, that an attack will occur, to wit that p(attack occurs) = 1.0.

This theme echoes throughout the current body of literature. Only in the past few years have academia and industry attempted to resolve uncertainty in threat analysis using a systematic and robust methodology (Bernhardt, 2004; Darby, 2006; Steinberg, 2005). The uncertainty gap that exists between the current state and future states is exasperated by the non-ergodic nature of human action and the incomplete knowledge of the analyst or facility operator. Current methods, as outlined in Section 2.3, frequently force the analyst to make epistemic statements about human behavior or attacker capabilities that result in confusion for decision makers or an extraneous commitment of resources to include operationalizing threat assessment to the tactical level (Suzić, 2005).

2.2.2. Vulnerability

The second variable of risk is vulnerability, which is a variable that defines the characteristics of a facility or critical infrastructure. As with threat, a review of the literature indicates there is not a universally accepted definition for vulnerability. Holmgren (2004) defines vulnerability as "sensitivity to threats and hazards" (p. iii). Jenelius, Petersen and Mattson (2006) provide a more specific definition that decomposes vulnerability into two variables: probability of a hazardous event [*threat –ed.*] and what they call "exposure" which contains "the consequences of the event in a certain place" (p. 538). Willis, et al., (2005) provide a measure of vulnerability as "the probability that damages (where damages may involve fatalities, injuries, property damage, or other consequences) occur, given a specific attack type, at a specific time, on a given target, or,

Equation 5: Vulnerability as a probability of damage given an attack

Vulnerability = p(attack results in damage| attack occurs)" (p. 8).

Given the dependence on the occurrence of a specific attack type at a specific time and the uncertainty of risk analysis of a vast array of threats, developing the matrix of vulnerabilities for a critical facility or infrastructure can be bewildering.

For this research, vulnerability will focus on the critical infrastructure's security techniques, tactics and procedures. To wit:

Definition 5: Vulnerability is the set of critical infrastructure-specific opportunities available for an adversary to exploit in conducting operations, including reconnaissance and operational attacks.

Borrowing from theory advanced by Hellström (2007) for cyber systems, the critical infrastructure vulnerability analysis experiences increased complexity because the various systems are usually designed and fielded at different times (a temporal dimension) and in different geographical places (a spatial dimension). Hellström proposes four principles for a vulnerability reduction framework which could be generalized as an aspect of this research: (1) functional interlocking – the systems' functions are dependent on functions of other external systems. (2) Temporal embeddedness – piecemeal additions and improvements introduce vulnerability by building onto or over existing flaws. (3) Critical socio-technical tipping-points – management of a critical system should have a focus on intervention which does not disrupt social functionality (e.g., will the medicine kill the patient?) and (4) dynamic and reversive effects – critical points of large socio-technical systems are dynamic and fluid. (2007).

2.2.3. Consequence

The third variable of risk is frequently called the "so-what" variable: consequence. Interestingly, consequence is frequently assumed to be intuitive – the end result of the attack on the infrastructure would cause substantial impact to society served, and is not given rigorous exploration in the literature. Willis et al. (2005) probably best define consequence as "the magnitude and type of damage resulting, given a successful terrorist attack" (p. 8) and provide a measure for consequence as "the expected magnitude of damage (e.g., deaths, injuries, or property damage to a specific target) or,

Equation 6: Consequence as a probability of damage given an attack occurs

Consequence = p(damage | attack occurs and results in damage)" (p. 9).

This measure is the basis for this research's definition of consequence, accordingly,

Definition 6: Consequence is the total subjective value of damage inflicted as the result of an attack on critical infrastructure.

This definition includes the residual impact from that damage or loss of life such as loss of income or potential future income.

2.2.4. Relationship between risk and uncertainty

The concepts of uncertainty and risk have a tenuous relationship, not just in engineering, but also across many different disciplines. In their review of the different perspectives on uncertainty and risk, Samson, et al., (2009) provide a helpful figure, recreated as Figure 4, which illustrates the relationship between risk and uncertainty currently encapsulated by the body of knowledge. The four leaves in this tree represent significant differences in opinion among authors and have seen numerous papers authored to resolve the conflicts.

Substantial support for the concept that epistemic uncertainty is risk exists across the literature, especially from the economic and finance communities (Samson, et al., 2009). For example, Mehr and Cammack (1961) assert, "...risk is defined as uncertainty" (as cited in Samson, et al., 2009, p. 559). Several authors have used risk and uncertainty interchangeably (e.g., Magee, 1961; Philippe, 2001). However, research efforts outside of the finance community appear to be focused on parsing risk and uncertainty as different concepts.

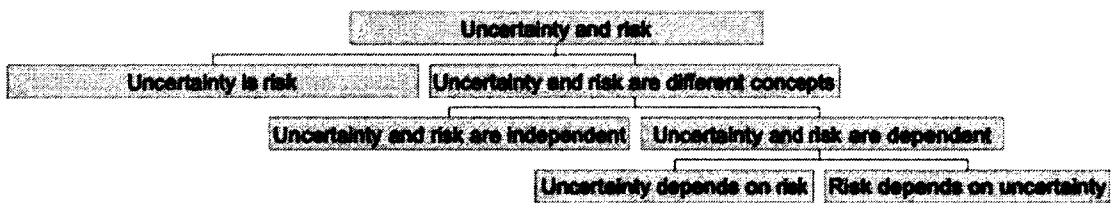

Figure 4: Relationship between uncertainty and risk
(adapted from Samson, et al., 2009, p. 559)

As early as 1901, economists were separating risk and uncertainty, especially Willett, who defined risk as the "objectified uncertainty regarding the occurrence of an undesirable event" (as cited by Samson, et al., 2009, p. 559). He asserted that epistemic

uncertainty of the subjective nature resulted "from the imperfection of man's knowledge" (Samson, et al., 2009, p. 559). Bedford and Cooke (2001) also used uncertainty in their definition of risk explaining that risk is really comprised of two elements: hazards and uncertainty. The division of uncertainty and risk as different concepts requires a further discussion of their dependencies: are risk and uncertainty independent?

The literature has examples that if uncertainty and risk are different concepts, it can also be argued that they are independent. Pfeffer (1956) believed that risk and uncertainty were counterparts of one another and that they differed by how they were measured. He saw risk being measured by objective probability and uncertainty, which he defined as a "state of the mind" being measured by subjective belief (Pfeffer, 1956 as cited in Samson, et al., 2009, p. 560). The focus on the state of the analyst's mind supports the linkage to epistemic uncertainty. Subjective belief is echoed in game theory where risk is defined as an action, which could lead to a specific set of distinct outcomes, but uncertainty's set of outcomes is potentially unknown or meaningless (Luce & Raffia, 1957).

The final two leaves, from the tree shown in Figure **4**, the children branches of the assertion that uncertainty and risk are dependent, have received considerable attention. The first assertion is that uncertainty and risk are dependent and the dependency does not imply that uncertainty depends on risk (Crowe & Horn, 1967), but that risk depends on uncertainty (Macgill & Siu, 2005). This assertion can be seen in articles written for engineering safety (Helton, Johnson, Oberkampf & Sallaberry, 2006; Möller & Hansson, 2008; Rao, Kushwaha, Verma, & Srividya, 2007; Yu & Harris, 2009); terrorism risk analysis (Darby, 2004; Kaplan, 2002; Willis, et al., 2005); human decision analysis (Lipshitz & Strauss, 1997) and transportation (Jenelius, Petersen & Mattsson, 2006). Perhaps the greatest single argument that illustrates that uncertainty gives rise to risk is the concept of removing all epistemic uncertainty – if a researcher had perfect knowledge then there would be no risk because all the variables would be known for a time period. Even without perfect knowledge the relationship between risk and epistemic uncertainty can be explained by Willett (1901) when he asserts that uncertainty is greatest when the degree of probability for risk is equal to one half. The researcher has no indication of

what the outcome will be because the probability of any outcome is equal (Willett, 1901). However, if the researcher can decrease uncertainty, even by the slightest, then the impact on risk would be to either increase or decrease the risk probability (Willett, 1901).

How does one measure what one does not yet know? The concept of measurement as it applies to epistemic uncertainty and risk is relative to the term in question. Epistemic uncertainty is based on what the researcher does not know: it is a state of the mind, not a state of the world (Pfeffer, 1956). However, the units of measure and the upper and lower bounds are either known or can be derived by additional research; albeit, the range may exceed the tolerance of the model in use. Risk, on the other hand, can be measured based on its expected value and the anticipated consequences (Daneshkhah, 2004; Kelly and Smith, 2009). This value may be comprised of parameters which are subject to uncertainty, leaving the value of the risk measurement to be suspect and only as good as the uncertainty analysis which is applied to the parameters.

The ability to quantify epistemic uncertainty and risk is still one of the key areas open for debate. Most authors agree that risk and uncertainty can be quantified (Barker & Haimes, 2008; Daneshkhah, 2004; Darby 2004; Helton, et al., 2006; Kelly & Smith, 2009; Möller & Hanson, 2008; Phillippe, 2001; Rao, et al., 2007; Willis, et al., 2005). However, the quantification of epistemic uncertainty is usually in the form of expert opinion or probabilistic estimates, and it lacks definitive repeatable answers. The use of fuzzy logic, fuzzy sets and other tools intended to articulate and quantify epistemic uncertainty has improved the ability to quantify this type of uncertainty (Darby, 2004). Once quantified, both uncertainty and risk are applied to various methodologies in an attempt to develop probability distributions.

Probability distributions for risk and uncertainty allow researchers to make estimates about the frequency of occurrences for events. Little debate exists in the literature concerning risk distributions. However, distributions related to epistemic uncertainty have some concerns with many authors believing it can be done (Barker & Haimes, 2008; Daneshkhah, 2004; Helton, et al., 2006; Kelly & Smith, 2009; Phillippe, 2001; Rao, et al. 2007; Willis, et al., 2005); and some authors believing it cannot or should not be done

(Darby, 2004, 2006; Möller & Hanson, 2008). Quantifying and distributing rare events are difficult using probability or statistics. By the very nature of probability and statistics, a large population is required in order to have significant confidence in the distribution as a tool for probability. In many cases the use of simulations, including Monte Carlo, can minimize this disparity. However, any quantification or distribution based on a historic analysis must take into account that the values are only truly accurate when all the parameters are the same over a specified time period for both the historic event and the sought-after prediction.

Discussion of the uncertainty distribution curve has a serious detractor – what happens when all the outcomes are not known because of epistemic uncertainty? Darby (2004, 2006) has developed ways to mitigate ambiguity and vagueness. By ambiguity, Darby (2006) attempts to resolve which crisp set (traditional sets in set theory) has the correct answer. Whereas in vagueness, Darby (2004, 2006) is trying to resolve a lack of sharpness for a fuzzy set – in other words – there is epistemic uncertainty in the set membership; and members may have partial set membership.

2.3. Risk management in terrorism scenarios

The presence of risk necessitates risk management for mitigation of the effects that risk may have on a complex system. Risk management in the underwater environment requires processes that can be

> applied to asymmetric warfare, in which elusive, secretive, and decentralized threats engage in loosely coordinated, difficult to detect behaviors. Capturing their behaviors through observation gathered by a diverse collection of sensors is a daunting task fraught with uncertainty. (Costa, Herencia-Zapana & Laskey, 2012, p. 715)

Examinations of the current methods for risk management indicate there are predominantly three approaches employed: first is to essentially reduce the uncertainty that underlies the risk; second is to mitigate the risk; and third is to accept and communicate the nature of the risk (NATO, 2002).

Within the United States government several agencies have responsibilities for maritime terrorism prevention and response. The FBI has authority based in many statues and directives. The Department of Homeland Security, with both the U.S. Customs' and Border Patrol (CBP) and the U.S. Coast Guard, are tasked with preventing terrorists from using cargo containers to smuggle people or weapons of mass destruction into the ports. The Coast Guard is assigned as the lead federal agency responsible for port security (Maritime Transportation Security Act, 2002) and uses a Maritime Security Risk Assessment Model (MSRAM) that utilizes Equation 2, from Section 0, taxonomy and metrics to measure risk at various levels of detail. Additionally, MSRAM is used by the Department of Homeland Security to evaluate maritime counter terrorism grant programs (Edmonson, 2006).

Numerous industry-specific evaluation approaches for protection of critical infrastructure have been fielded by various industry organizations (e.g., NEI or EPRI), the government (e.g., NRC, DOE or DHS) or international associations (e.g., IAEA) for nuclear facilities (Edmonson, 2006; EPRI, 2003; IAEA, 2003; U.S. NRC, 2008). For example, the oil and chemical industry has AIChE/CCPS. Regardless of the industry or the estimating entity, no method adequately addresses the uncertainty in the threat variable, thus reducing the effectiveness of any associated risk management methodology. Furthermore, the various risk management methods can be parsed into categories based upon the metrics used, generally defined as simple indicator, event-based or aggregate (Willis, et al., 2005).

2.3.1. Simple indicator

The simple indicator methodology uses understandable metrics and widely available data to form simple indicators such as population-based indicators that correlate consequence to population and threat to population density. The metrics for simple-indicators are usually well understood by policy makers; however, simple indicators do not adequately reflect the relationships between threat, vulnerability and consequence (Willis, et al, 2005). For example, in 2006, Patterson and Apostolakis presented a methodology that was focused on vulnerability based on stakeholder input but did not address the threat variable. It continued the work of Apostolakis and Lemon (2005) on mean cut sets (mcs) that requires a value to be assigned to them. The process of value assignment requires an

evaluation of the conditional probability that terrorists would successfully attack a given mcs. Because value assignment is extremely difficult to do, many authors separate the vulnerability from the conditional probability of a successful attack.

Darby (2006) developed a model which adequately reflects the relationships between the variables in the risk equation when he applied "non-probabilistic techniques to an overall evaluation of risk from acts of terrorism, including the likelihood of attack" (p. 9) in his Adversary/Defender model. He uses belief/plausibility measures from the Dempster/Schafer theory of evidence to represent uncertainty as a means to capture both epistemic and aleatory uncertainty by using simplistic variables that are reduced to independent probabilities. Darby (2006) built dependence into the model by establishing the Adversary model on the attackers' goal of maximizing consequence and the defenders' goal to minimize risk. He suggests the model could be improved by the probability measures being modified by Bayesian update techniques. Bayes' theorem has been used in methods such as *probabilistic risk analysis* (PRA) and *probabilistic safety analysis* (PSA) (Roland & Moriarity, 1983).

Bayes' theorem can be used to quantify uncertainty by representing all decisions with precise probabilities "since the rational decision-maker always, at least implicitly, assigns a probability value to each potential outcome" (Möller & Hansson, 2008, p. 777). These probability values essentially represent the decision maker's lack of knowledge, one of the categories of uncertainty. Garrick, et al. (2004), assert that in a Bayesian construct "uncertainty refers to the parameters that are used to measure risk and how these parameters represent uncertainties in information and modeling" (p. 141). A serious concern for applying the Bayesian approach is epistemic uncertainty, which by its very nature, may not be reducible to a unique probability. This constraint has contributed to the demand for including non-probabilistic epistemic uncertainty into the analysis (Möller & Hansson, 2008).

In addition to the difficulty in quantifying a decision maker's lack of knowledge, there is also the difficulty in quantifying other qualitative parameters – like target prioritization. Woo (2002) urges invoking Fechner's Law (also called Weber-Fechner's Law or

Weber's Law) "which states that an arithmetic progression in perceptions requires a geometrical progression in their stimuli" (p. 14). Fechner's Law is usually applied in cases where the magnitude of the sensation is not discriminated with near absolute certainty (Shigemoto, 2002). Another theory, that is closely related, is Steven's Power Law, which describes the relationship between the magnitude of a stimulus and its perceived intensity. Steven's Power Law is usually used where the magnitude of the sensation is discriminated with some certainty (Smelser & Baltes, 2001). The application of Steven's Power Law permits a simple indicator understandable metric for decision makers but, in truth, the theory is based on physical stimulus and not societal reactions.

2.3.2. Event-based

Event-based models, like the RMS Terrorism Risk Model employed by the insurance industry, provide a significant improvement in detailed analysis, including sensitivity analysis, and extend across multiple types of events or multiple targets. Frequently the models will include expert judgment, which improves accuracy in describing the details but may force the model to be populated with estimated parameters thereby increasing uncertainty. Event-based methods provide a means of overcoming the arbitrariness of simple indicators of risk, which rely on presumptive correlated relationships (Willis, et al., 2005). As a derivative of the event-based model, Levitin and Ben-Haim (2008) introduce a model that uses a universal generating function with probabilities and probability vectors representing attacker values to focus on damage caused to a complex system by intentional attack.

Koonce, Apostolakis & Cook (2008) propose a methodology based on the MIT Risk Ranking methodology to conduct a systematic development of the ranking of their variables, principally intent, capability and resources, within a bulk power grid for both random acts and deliberate acts, which is based on stakeholder input. They assert "the risk assessment of infrastructures presents additional difficulties due to their diffuse nature" (p. 171) and note that Apostolakis & Lemon's (2005) work "...assumes a 'minor' level of threat to be present" (p. 171) which is an assumption that drives security costs upward regardless of the actual threat (which may, in fact, be non-existent). This assumption is also echoed in Johnson, Khater and Kuzak's (2005) advice to "assume the

facility is a credible target" (p. 8). They suggest one area for additional work is identification and modeling of more specific users groups on the power grid to better establish the consequence on users.

2.3.3. Aggregate estimator

The third method, introduced by Willis, et al., (2005) is called the aggregate estimator method and is based on practices from economic forecasting that aggregates information from multiple models or experts. However, Willis, et al.'s (2005) methodology is not the only aggregated methodology currently used. Sandia National Laboratories Vulnerability Assessment Methodology for Chemical Facilities (*VAM-CF*) considers risk as "a function of the severity of consequences of an undesired event, the likelihood of an adversary attack, and the likelihood of adversary success..." (Jaeger, 2002, p. 15). Prior to completing the vulnerability assessments the threat must be described. The VAM-CF uses type of adversary, tactics, and adversary capabilities, which are defined as number of adversaries, weapons, equipment and transportation. Jaeger (2002) then explains that "the potential for attack is determined based on the existence, capability, history/intent and targeting... [as well as] the attractiveness of the potential target" (p. 17).

2.4. Underwater terrorism

This research focuses on the threat of underwater terrorism, itself a subset of maritime terrorism, within the context of critical infrastructure; thus, a clear definition of underwater terrorism is necessary. Defining underwater terrorism is a difficult task since over 100 definitions of terrorism exist that spans over 20 definitional variables (Laqueur, 1999; Schmid & Jongman, 1988). Examining the basic concepts within the United States, the United States Code defines international terrorism as activities that, according to law, would be criminal and involve violent or dangerous actions intended to influence or intimidate the government or its citizens (Crimes & Criminal Procedures, 2006). Inherent in that definition are mass destruction, assassination or kidnapping.

The U.S. Department of Defense states terrorism is the "unlawful use of violence or threat of violence to instill fear and coerce governments or societies...often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that

are usually political" (Joint Doctrine Division, 2010, p. 368). Note that both definitions contain the key point that terrorism is violence intended to influence the government to change its policies.

Lorenz (2007) focuses the definition on maritime terrorism when he proposes maritime terrorism is "the use or threat of violence against a ship (civilian as well as military), its passengers or sailors, cargo, a port facility, or if the purpose is solely a platform for political ends" (p. 4). Lorenz's definition does not address piracy, which can be differentiated from terrorism by its motivation: piracy is criminally motivated and maritime terrorism is politically motivated (Greenberg, et al., 2006). Motivation is the fundamental difference necessary for the definition of maritime terrorism that will be used in this research:

Definition 7: Maritime terrorism is the premeditated use of violence or coercion (such as hijacking a ship and holding hostages without hurting anyone) within the marine environment to influence government behavior for political or ideological gain.

According to the RAND database on terrorism, only 0.37% of the terrorist incidents from January 1968 until March 18, 2008 were maritime related (RAND Worldwide Incident Terrorism Database, 2008). Analysts assume the low number of maritime security incidents can be attributed to the high level of expense, training and complex technical capabilities necessary to successfully conduct a maritime mission (Medalia, 2005; Richardson, 2004). The difficulties specifically include acquiring maritime vehicles or equipment, specialized maritime skills, and waterproof weapons or explosives. Given the value for the dollar, maritime attacks usually have a low ratio of benefit to cost and they are often abandoned in favor of other operations.

Several terrorist groups are considered to have significant maritime capabilities including the Middle Eastern Palestine Liberation Front (PLF), Fattah, Hezbollah, and the South East Asian Liberation Tigers of Tamil Elam (LTTE), the Abu Sayyaf Group (ASG) and Jemaah Islamiyah (JI) (Lorenz, 2007). An example of a successful maritime terrorist attack is the small craft suicide attack on the *USS Cole*, on October 12, 2000. A 35-foot boat, loaded with explosives, pulled alongside the *Cole* while it was refueling in Aden,

Yemen and exploded, killing 17 sailors and injuring 47 more. The attack resulted in $250 million in damages and required 18 months for repairs (GlobalSecurity.org, n.d.).

Although the incidence of maritime terrorism, in relation to other forms of terrorism, is relatively low and the incidence of underwater terrorism is even lower, amounting to a handful of documented incidents; history belies the threat as underwater terrorism is a becoming an attractive alternative to terrorist organizations. One example is Abdul al-Rahim al-Nasheri, sometimes called the Prince of the Sea, who was the chief of operations for al-Qa'ida on the Arabian Peninsula until November 2002. He based his operations on four variables, one of which was possessing underwater demolition teams (Richardson, 2004). The grave consequences associated with successful underwater attacks increase the attractiveness of this method for al-Nasheri and other terrorists. Underwater terrorism also offers other benefits including the ability to operate undetected and the difficulty of defending against attacks. Over the past ten years, advances have been made in underwater sensors, but the underwater environment still remains a difficult area to monitor because of the limited visibility, magnetic anomalies, sea floor debris, harsh operating conditions, extraneous noise and the special equipment needed (Dobkowski, 2007; Sakhuja, 2005).

Although the same conditions that make the underwater theater difficult to defend also impose hardships on the attackers, recent changes to defensive posture and terrorist training have increased the attractiveness of the underwater attack. As traditional, land- and air-based targets become increasingly hardened against attacks, terrorists seek other targets with an increased probability of mission success. Whereas the underwater environment had a lower probability of success because of its harsh environment, it now has a greater probability of success than attacking a hardened target.

Additionally, terrorists are becoming more resourceful and better trained for the marine environment. Abu Sayyaf, a militant Islamic separatist group based in the Philippines, is known to have conducted training for scuba diver strikes, and al-Nasheri claimed al-Qa'ida could use both submersibles and "human torpedoes" (Sakhuja, 2005, np). Sri Lanka's Navy experienced two losses associated to underwater terrorism: In the first

instance a fast attack craft sank after experiencing a blast at 2:30 in the morning. This blast may be attributed to improvised mines or to divers; the Sri Lankan government has not released the details, but the Tamil Tigers took credit for the attack claiming that three of their operatives had engaged the boat (Vasan, 2008a). In the second instance, known to be a suicide diver, the 520 foot logistics support ship, formerly known as the *Invincible*, was attacked and sunk while moored at Ashroff Jetty, Trincomalee (DefenceWire, 2008; Vasan, 2008b). Authorities confirmed a suicide diver conducted this attack because a piece of the diver's torso and diving equipment were recovered (South Asia Terrorism Portal, 2008).

A trained diver would not have to blow himself up to be successful; the use of improvised or stolen mines could be used to temporarily block harbors, destroy shipping or damage land based critical infrastructure (e.g., water intakes to nuclear reactors) in either stand alone attacks or as part of a choreographed attack on a harbor or coastal region (Hasslinger, 2008). Colombo Port was spared an attack because of bad weather and effective security. Eight ships had been targeted and the eight explosive packages with timing devices and magnets, for attaching to the packages to the hulls, were recovered (Fuard & Kamalendran, 2006). Although one of the attackers committed suicide with a cyanide capsule, four others were arrested. Their boats also had frogmen's kits, oxygen cylinders, mobile communication and navigation equipment and National Identity Cards (Fuard & Kamalendran, 2006). Given the grave consequences of a successful water-borne attack, the increased attractiveness to adversaries for an underwater attack, and the demonstrated planning and preparation of adversaries, attention to terrorist threat in the maritime domain is vital.

The business community has been dedicating resources to the research and development of devices to detect and thwart underwater terrorist attacks. The Underwater Inspection Systems (UIS), manufactured by the CodaOctopus group, is a real-time three-dimensional sonar that can be used to image the underwater theater. It can be used proactively to first scan and develop a catalog of known objects in a port area. Then, if a threat is received, a second scan can be conducted and compared with the first to determine anomalies, which can later be investigated by response teams. If an

underwater catalog has not been created, the UIS can still be used to conduct an initial search to assist the response teams in their planning. UIS can be used for bottom scanning, piers and wharfs or examining the bottoms of boats, as necessary. Other devices, similar to the UIS but designed to detect divers, are the Underwater Surveillance System manufactured by Kongsberg Maritime and the Sentinel Intruder Detection Sonar made by Sonardyne. Three different manufacturers with viable products that have successfully come to market and have been purchased by governments and police units around the world indicate a need for underwater inspection and detection devices.

Effective deployment of these devices is a key concept that initiated this research. Financial resources are limited and utilizing these tools represents a significant financial commitment. The U.S. Coast Guard employs several of the devices mentioned above as part of the Underwater Port Security System as an anti-diver tactic. The Coast Guard also conducts an Underwater Terrorism Preparedness Program, which develops actionable preparedness plans in partnership with all port agencies in a geographic area. The program brings responders together before an incident to outline coordination and control tactics, techniques and procedures that will be used at the port facility. The final product is the Underwater Terrorism Prevention Plan for a port area (Branham, 2009).

Another indicator of the importance of a topic is seminars or meetings dedicated to the topic and non-peer reviewed articles published by practitioners of the trade. Although there has not been a dedicated underwater terrorism conference, many conferences have been held related to various topics pertinent to underwater terrorism. For example, the Mine Warfare Association has hosted conferences and proceedings annually dating back to 2001 and five of the 13 themes for this year's Undersea Defense Technology Conference and Symposium (Asia) are underwater terrorism related including Undersea Port and Harbor Security (Underwater Defense Technology, 2010).

Within the literature, several articles have been published that discuss underwater terrorism. In a trade magazine for military and defense industry, Hasslinger (2008) describes a worst case scenario at the beginning of his article and then suggests several actions government planners should consider, including improving the nature and scope

of the United States' vulnerabilities, conducting war games and using the output of the games to study the variables pertinent to the underwater theatre and to assess what systems are required to restore services after an attack. *Popular Mechanics*, a general audience magazine with numerous departments, discussed ways in which the U.S. Navy may counter the threat of underwater terrorism (Pappalardo, 2009). Many user Internet sites with news articles (with robust comments) or blogs exist that are dedicated to the subject.

Unclassified scholarly research into underwater terrorism is minimal but indicates academia is addressing this problem. One article, on asymmetric warfare, has two paragraphs that describe the underwater domain as asymmetric in nature without simulation capabilities (Hill, 2004). Another article is pertinent and discusses countering underwater terrorism through either a sensor-centric approach or a capability-based approach (Kessel, 2007). Both approaches mentioned by Kessel (2007) require the defender to respond once the attacker is already actively attacking the facility.

Other academic material, not previously cited, ranges from the abstract, for example, summarizing or mapping the existing terrorism research domain (see Kushman & Rubin, 2009; Reid & Chen, 2007) to the specific (e.g., effects on the human body of explosions underwater, Almogy & Rivkind, 2007). A plethora of material exists, which may be generalized to this research, that discusses collection of and analyzing data on terrorism (see Gupta, 2005; Jonas & Harper, 2006) through the modeling (see Haimes, 2002) and risk management (see Horowitz & Haimes, 2003; Jha, 2009; Liu, Chen, Gao & Jiang, 2005) processes. One aim of this research is to reduce the gap from the existing material in terrorism to the specific and unique area of underwater terrorism by applying accepted methods in risk management and uncertainty reduction.

2.5. Parameters

Pertinent to the discussion of underwater terrorism, is the discussion of the variables that comprise the risk equation, ergo the parameters. In the intelligence community, threat is first decomposed into the intent (I), capability (Ca) and activity (A) of the adversary such that $R = f[(ICaA)VC]$ (Bodnar, 2005; Chase, Day, Cline, & O'Hagan, 1995). Intent is

comprised of the adversary's ideology, the stated goals of the adversary and the adversary's propaganda history. Capability includes the adversary's tactics, techniques and procedures, operational history and the availability of key resources, specifically people and raw materials. Activity indicate the adversary is actively engaged in attack preparations and includes logistics, movement of people, pre-operational planning, training, pre-operational surveillance, information collection, and testing of the target.

The intent of an adversary, analogous to purpose, is indicated by the adversary's ideology, goals and propaganda. Formally, an adversarial ideology is the ideas and manner of thinking of the adversary, as a group, which oppose the defender, the defender's ideology or the defender's values (Berman, 2008). Very closely related, but distinct from ideology is stated goals, which are the explicitly declared results desired that the adversary is working towards. It would be naïve to consider that the stated goals of an adversary are truly representative of the collective. However, for the purpose of the overall understanding of risk, abstraction of the stated goals to the collective members of the adversarial organization is both suitable and appropriate (Thompson, 2006). Stated goals should not be confused with motivation, which is more personal in nature and tied to individual actors. Propaganda is the spreading of ideas and information for the purpose of helping the adversary's cause or to damage the defender's cause (Propaganda, 2011). It "consists of the planned use of any form of communication designed to affect the minds, emotions, and action of a given group for a specific purpose" (Linebarger, 1954, p. 39).

The capability indicates the adversary's ability or competency to execute an attack and examines past operations and the accumulation of people and material. Critical to assessing the adversary's capabilities is understanding the adversary's tactics, techniques and procedures, usually referred to by its abbreviation, TTP. TTP is comprised of three distinct actions that guide the operation based on the evolving knowledge and experience (U.S. Army, 2011): tactics are the employment of people working in relation to one another; techniques are non-prescriptive methods used employ a tactic and "procedures are the standard, detailed steps that prescribe how to perform specific tasks" (Ibid, p. 6). Experts have some indication that adversarial groups either transfer information or learn

from each other concerning successful TTP (Hedges & Karasik, 2010). As with any organization, an adversary also learns from past successes and mistakes. An adversary's operational history consists of the past operations conducted by the adversary and provides an understanding of what influences, including cultural, social, economic and political forces, impact the organization.

As in any organization, people are the key resource, which form the foundation of this research. Without people, from leadership to front line "soldiers", an adversary would not exist. Terrorist organizations use similar methods to recruit and train people regardless of the tactics, techniques or procedures employed in their attacks (Ozeren, Gunes & Al-Babayneh, 2007). It also appears that terrorist organizations operate under less restrictive norms of rationality (Thompson, 2006).

Vital to any successful attack is the acquisition of materials for the operation, including weapons or explosives, and special equipment for operation in the unsympathetic underwater environment. The acquisition of key resources necessary to conduct operations, either through legal means (purchasing) or illegal means (stealing, black market) may include material necessary to conduct pre-operational requirements, for example, flight manuals (Indiana Intelligence Fusion Center, n.d.).

The final disaggregation of threat includes action, which is the process of performing an act or activity. In any attack, training must occur beforehand to indoctrinate the organization's people on its tactics, techniques and procedures. Training is not the formal training as defined from the discipline of human performance technology. Instead, training implies any intervention meant to teach a person a particular skill or behavior. Training includes providing digital manuals, circulating paper propaganda with a generic vision, mission and instructions to the more formal organized training camps where people prepare physically and mentally to accomplish tasks. To prepare for both the attack and any pertinent training, material must be moved to training areas or attack sites. Moving material is logistics, which is narrowly defined as the movement and maintenance of material (U.S. Army, 1985). An underwater attack requires particular

materials and processes to effectively deploy an attack and this specificity is discretely observable by the defender.

In addition to moving material for training or operational staging, the movement of people must occur. Movement of people is narrowly defined as the change of physical location of people to accomplish tasks, including training, pre-operational surveillance or testing or positioning of people for the planned attack. Conceptually movement of people is more concerned with long distance travel (e.g., transnational flights) vice the daily commuting required for shopping, communications or pre-operational activities. People are also required for pre-operational planning, essentially the process of developing "*tasks*, in a prescribed *order*, that are intended to reach a desired operational *end state*, normally within a given time" (Zhang, et al., 2001, p. 3).

The final three elements of action can be combined into a concept called probing (Gay, 2012). Probing exists when an adversary explores the target through information collection, pre-operational surveillance and testing. Information collection occurs when an adversary attempts to gain information about a place, person or operation pertaining to a target, usually through inquiries including online searches (Indiana Intelligence Fusion Center, n.d.). Pre-operational surveillance involves an adversary observing a target to determine strengths, weaknesses and the number of emergency personnel that may respond to an incident (Indiana Intelligence Fusion Center, n.d). Pre-operational surveillance is different from information collection because surveillance requires people to observe the defender directly and provides an opportunity for defenders to receive indicators of adversarial activity (STRATFOR, 2005). Near the final stages of pre-operational planning, adversaries may conduct testing. Testing is the adversarial actions intend to activate defender response to penetration of security barriers (Indiana Intelligence Fusion Center, n.d.) and is useful in validating the efficacy of the operational plans.

2.6. Ongoing Research

The deficiencies in the theoretical and methodological approaches noted above are being addressed by academia. For example, Guikema (2012) examined the necessary

conditions for intelligent adversary models and partnered with Aven to parse the sources of uncertainty within the analysis practice (Aven & Guikema, 2011). Bristow, Fang and Hipel (2012) suggested utilizing systems of systems methodologies for advancing the risk management of extreme events, a similar concept to this research. At a more methodological level the exploration of game theory has been suggested as a means of adversarial risk analysis that includes the concepts of intelligent adversaries (Rothschild, McLay & Guikema, 2012). Other methods have been advanced even further including decision analytics (Dillion-Merrill, Parnell & Buckshaw, 2009; Parnell, Smith & Moxley, 2010) and Bayesian reasoning (Costa, Herencia-Zapana & Laskey, 2012). The explorations conducted by these authors validates the gaps this research seeks to close in the body of knowledge

CHAPTER 3
RESEARCH METHOD

3.1. Meaning

The purpose of this research is to advance the ability to manage and understand the risk of an underwater terrorist attack. The research contributes to the body of knowledge by analyzing unclassified historic data to articulate the key parameters and their relationships, in the threat element of the risk equation. The research also presents a geometric model of the risk equation which assists decision-making by facilitating an understanding of the relative risk of an underwater terrorist attack given two, or more, scenarios.

3.2. Theoretical Framework

Although the three phases of this research are derived from the Code of Best Practice for Experimentation (Albert & Hayes, 2005), the research employed many layers of abstraction in its design. Figure 5, the Ladder of Abstraction, illustrates those layers graphically. The ladder proceeds from the researcher's worldview, located at the top of the ladder, steadily downward to the conceptual and operational definitions for this research. The following sections articulate the ladder of abstraction.

3.2.1. Researcher's Worldview

The theoretical assumptions of a researcher's ontology and epistemology directly impact the methodology selected by that researcher. The methodology is the mechanism that enables a researcher to develop an understanding of reality. Evolving from the epistemic basis of realism, the research investigates qualitative data by examining the causative factors and variables in the identification of an adversarial threat to underwater critical infrastructure. Furthermore, those causative factors and variables will be used to develop a model to evolutionarily test hypotheses on the creation of a polyhedron risk model in the underwater domain.

Krauss efficiently summarizes Lofland and Lofland's (2005) definition of meaning as the

linguistic categories that make up a participant's view of reality and with which actions are defined. Meanings are also referred to by social analysts as culture, norms, understandings, social reality, and definitions of the situation, typifications, ideology, beliefs, worldview, perspective or stereotypes. (p. 762)

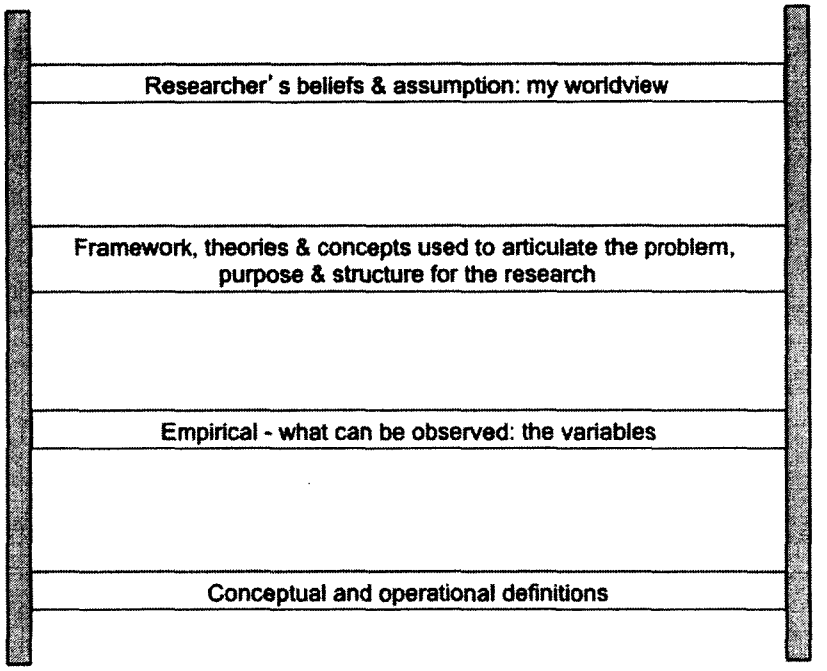

Figure 5: Ladder of abstraction

Given that Western culture and society is fundamentally different from the norms of the perceived adversaries, applying Western contexts and understanding of reality to those of the adversary may provide inaccurate definitions, interpretations or justifications for the adversary's behavior. The researcher is known to be handicapped by the perception barrier and may have unknowingly introduced bias in understanding an adversary's intentions and capabilities.

3.2.1.1. Ontology

Ontology, essentially the philosophy of reality, is the understanding of entities, relationships and interactions at the highest levels of physics and society. The

understanding of the nature of all things is based on either individual or collective conceptualizations – essentially formulating explanations for observed phenomena. The conceptualizations are based on perspective and social influences (e.g., the Galilean argument of the center of the solar system – as being Sun or Earth centric was based on teachings up to that point and challenged by the new information). A researcher's ontological assumptions will influence the choice of methods employed and the resulting conclusions.

The researcher's ontology is generally positivistic – truth is independent of the researcher. However, reality, when considering the nature of the research subject, adversary's intent on doing harm, should be conceptualized as the ultimate goal, not the immediate actions or intentions of the adversary. The researcher suggests this research, even if discovered by the subjects, will not change the nature of reality on the immediate articulation of reality and this truth was discovered empirically by applying both qualitative and quantitative methods.

3.2.1.2. Epistemology

Epistemology is the philosophy of knowledge, an understanding of how we come to know and the relationship between the knower and the known (Krauss, 2005). A researcher's epistemology is the foundation for how the researcher develops knowledge about his/her ontology, in essence, the basis of the researcher's reality.

The researcher's paradigm is more centered on the epistemic continuum – one of realism, which contains elements of both positivism and constructivism (Healy & Perry, 2000). The researcher believes, and approached this research with this conceptualization: that there exist multiple perceptions about a single, mind-independent reality (Healy & Perry, 2000). The researcher believes there are differences between the actual reality and peoples' (whether individual or collective) perceptions of reality. By using empirical methods the researcher endeavored to foster knowledge utilizing a variety of "theoretical reasoning and experimentation" (Outhwaite, 1983, p. 332).

3.2.2. Framework, theories and concepts

This research draws from a diverse foundation for theories and concepts including organizational, systems, risk, and uncertainty theory. Furthermore, the research is based on the language and functions inherent in set theory, graph theory and geometry.

In studying the behavior of the complex adversarial organization, the doctrine of organizational theory was employed. Organizational theory provided a multidisciplinary and systems based strategy to research both the parameters and relations at a macro-level. Applying principles from anthropology, the organizational culture was dissected into quantitative parameters and further studied. Organizational theory provided a plethora of methods including multiple regression, non-parametric statistics, meta-analysis and ANOVA. It also provided philosophy on the study of the rationality of an adversarial organization and its structure, control and technology. It also permitted a systems framework to be applied to interpret the complex dynamic goal-oriented processes demonstrated by the adversarial organizations.

Paramount to this research was application of the tenets of systems theory. Systems thinking provided a framework and techniques to reduce the adversarial organization holistically. The relationship between the adversary and the defender was built upon the concepts of the system-environment boundary, input, output, process, state, information and goal-directedness. The philosophy of the research was based on the whole system concept – essentially that a defender cannot exist in the defending state without the existence of an adversary and that one's actions directly impacts the other, even if knowledge of the action is non-existent. The research also leveraged equifinality across the geometric model to offset the areas of the model with increased uncertainty.

Both Risk and Uncertainty theory provided significant influences in the approach and development of the mathematical model. Applied Risk theory has traditionally been focused on decision-making under probabilistic uncertainty and was influential in approaching the analysis of the parameters and relations. The Risk Index, the Risk Measure, the Uncertainty Measure and the Loss Function inspired the mathematical concepts for the model, providing both the approach and the structure. Additionally, the

malice spectrum for quantifying the parameters is derived from the maximum uncertainty principle.

In both the approach and the implementation of the parametric research, set theory provided language and arithmetic functions. The model's mathematical basis is derived from applying set theory to the parameters and relations described as objects.

Maturing the relationship between the objects collected within the sets, graph theory provided the language and a theoretical background for the development of the mathematical structure used to model the relations between the parameters. Graph theory also provided the theoretical foundation for the development of the matrix, which executes construction of the network diagram, forming the structure of the geometric model.

Finally, geometry provided the language and theoretical basis for the instantiation of the polyhedral model, including the location of the nodes as coordinates and the determination of the volume and the surface area.

3.2.3. Empirical basis

The empirical basis for this research is derived from experimentation that tests the hypothesis concerning the relationship between the parameters observed in samples and the relative risk between the samples. The original data obtained through observation of the samples include (1) if a parameter is observable within a sample and (2) the evaluated magnitude of the parameter in the sample. The data obtained through experimentation are the output of the experiment, a dimensionless value representing a geometric value relative to the specific sample.

Using the definition provided in Section 0, the parameters are both enumerable and capable of being used in mathematical statements, ergo axiomatizable.

Several constraints on empirical purity were noted including the ability to observe the parameters directly and the bias in determining vulnerability and consequence introduced by the data deriving from Western, academic viewpoints as opposed to an adversarial origin. The first constraint was minimized by using trusted sources of data and more than

one source for each sample. The use of multiple data sources and trusted databases elevated the expectation of data integrity by relying on other trained observers following documented procedures and independently verifying those observations. The second constraint, bias, is noted and accepted because the focus of the research is on the threat element and not the vulnerability and consequence.

3.2.4. Definitions

Different nuances in the definitions of terms used across the risk and intelligence domains exist. The definitions were taken from multiple sources, aggregated and then simplified for clarity. Table **1** provides the term, the variable used and the applicable definition.

Table 1: Operational definitions

Concept	Variable	Operational definition
Risk	R	R = Threat * Vulnerability * Consequence
Threat	T	T = Intent * Capability * Activity
Intent	I	I = Propaganda * Stated Intention * Adversarial ideology
Capability	C	C = Tactics, techniques & procedure * Operational history * key resources (people) * key resources (material)
Activity	A	A = Logistics * Movement of people * Surveillance * Information collection * Testing
Propaganda	p	Propagating ideas and/or information for the purpose of assisting the adversary's cause or to damage the defender's cause
Adversarial ideology	i	The beliefs that guide a group in opposition to the Defender's ideology or values
Stated goals	g	The explicitly declared results desired that the adversary is working towards.
Information collection	f	An adversary's attempts to gain information about a target during the pre-operational planning stage.

Table 1. (Continued)

Concept	Variable	Operational definition
Consequence	c	The total subjective value of damage inflicted as the result of an attack on critical infrastructure.
Key resource – people	k	The people directly involved in conducting the attack, including those that build and those that deploy the weapon.
Pre-operational planning	n	The process of developing plans to achieve an operational goal.
Operational history	o	The past operations conducted by the adversary.
Tactics, techniques and procedures	t	People working together in non-prescriptive methods or by following common methodologies.
Pre-operational surveillance	s	Observing a target to determine strengths, weaknesses and forces available.
Key resources – material	m	The acquisition of supplies necessary to conduct operations.
Logistics	l	The movement of material.
Movement of people	b	The change of physical location of people to accomplish tasks.
Training	r	Any intervention meant to teach a person a particular skill or behavior related to adversarial conduct.
Unique environment	u	The setting or conditions in which the attack will be conducted in or access to the Defender through.
Testing	e	Adversarial actions intend to provoke an observable response to an aggressive stimulus.
Vulnerability	v	"The set of critical infrastructure-specific opportunities available for an adversary to exploit in conducting operations, including reconnaissance and operational attacks" (Gay & Hester, 2010, np).

3.3. Rationale for method

This research methodology was chosen because of the degree of the problem formulation, the data available, the environment of the study (to wit, manipulation of the variables *ex post facto*), the methods accepted by the engineering community, and the quantification

of the data for sharing across diverse communities. The problem was strongly defined by inputs (expected parameters), their characteristics and range of conditions and the output (measure of relative risk and an understanding of what influences the value). The data were available in publicly available databases, government sites and open media. The experimentation method is accepted by the engineering community, and using the Code of Best Practice as a guide, enhanced the integrity of the process. Quantification was vital for analyzing the correlation of the parameters and for describing the magnitude of the parameters during the experiment phase. Quantification also supported positivism, which stresses an objective approach based on quantitative analysis and experiments.

Cohen, Lawrence and Morrison (2000) observed that there are four assumptions of science: determinism, empiricism, parsimony and generality. This research, deterministic in origin, researched the casual links for understanding the events driven by factors. In collecting empirical evidence to support a hypothesis, and by robustly validating the model, both empiricism and parsimony were upheld and facilitated generality.

An examination of the precepts of naturalism, qualitative in nature, indicated that it was not well suited as a methodology for this research. Naturalistic research is subjective and traditionally employs case studies and interviews as methodologies, neither of which appear practical for this research. Pure case studies usually produce more detailed information than statistical analysis but are often considered less credible and can be biased by the researcher's intimate knowledge of the case (Hill, 1993; Lueck & Spurlock, 2003). Case studies are also difficult to generalize because they are based on qualitative data that is generalizable to only a particular context (Lee & Baskerville, 2003; Yin, 1994). Another concern is the sensitive nature of any case study – in many instances the case study would be classified and become unusable for this research. The second option, conducting interviews, is not feasible and would be of dubious value since the interview could prejudice the legal proceedings of the interviewed, creating doubt to the integrity of the interview. Given the constraints enumerated and the nature of the problem, model-based experimentation was indicated.

3.4. Research design

The research design followed a traditional waterfall input-process-output model of hypothesis testing. Figure **6** illustrates elements of the research design including the primary inputs and outputs for the research design, which are explained in the following sections.

3.4.1. Input

The research design was impacted by six key inputs, outlined below. The inputs had minimal variability but significant influence on the research design and were outside of the control of the researcher.

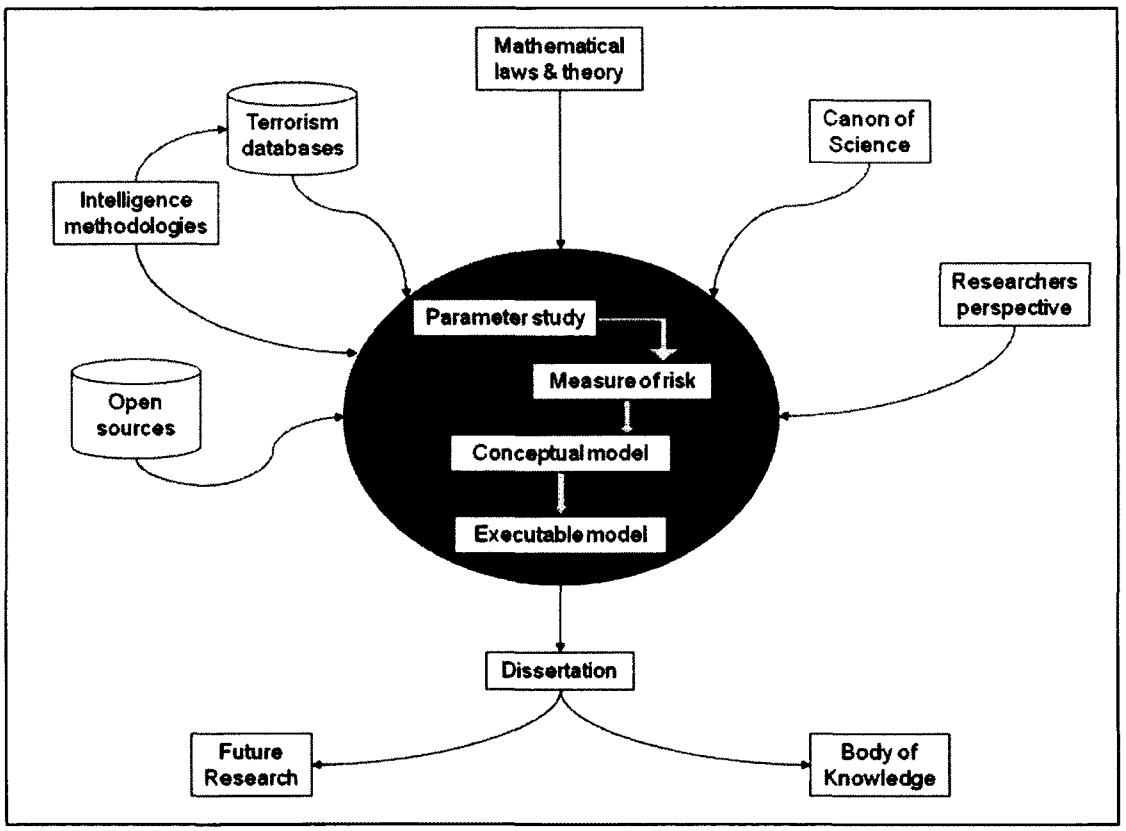

Figure 6: Research design

3.4.1.1. Open sources

Data were acquired utilizing publically available information including government, academic, and news media sources. Open source information provides a basis for

understanding the minimal data available from the government or academic terrorism databases. The information contained in open sources must be viewed in context and examined for the source of the information when seeking collaboration. Three, four or even more similar versions of the same fact may be propagated by one news company and modified by local authors – indicating no collaboration of fact. The open source news media provided an archive of analog material that was not available digitally, except as a photograph or scanned image.

3.4.1.2. Intelligence Community's methodologies

The perspective of both the researcher and the literature reviewed has been forged from a defensive viewpoint, which has been influenced by the methodologies employed by the intelligence community, which provided the initial categorization of data and heavily influenced the reliability of those data.

3.4.1.3. Terrorism Databases

The primary data for this research were obtained from unclassified governmental and academic databases. Each database was selected for academic excellence and robustness. However, the databases were representative of the defender perspective and limited in scope by the designer of the database. The databases available did not contain standardized parameters or entries, requiring extensive cross-referencing and additional data derived from open sources.

3.4.1.4. Databases used

Three databases were used for the primary search for data. The databases were administered by either government or educational institutions that are Centers of Excellence for terrorism research. The databases, shown in Table **2**, did not include the requisite data to conduct a robust analysis of the parameters but represent the initial source of information that provided the foundation of this research.

Table 2: Databases used in this research

Database Name	Parent Organization	Comments
RAND Database of Worldwide Terrorism Incidents (RDWTI)	RAND Corporation	A compilation of terrorism data from 1972 through 2009
Global Terrorism Database (GTD)	The National Consortium for the Study of Terrorism and Responses to Terrorism (START) located at the University of Maryland	An open-source database including information on terrorist events around the world from 1970 through 2010
Worldwide Incidents Tracking Systems (WITS)	National Counter Terrorism Center (NCTC)	The U.S. Government's database on acts of terrorism compiled from open source data from 2005 to 2010.

3.4.1.5. Mathematical laws and theories

Mathematical laws and theories provided influence by introducing some of the language and theories for this research.

3.4.1.6. Canon of science

The Canon of Science provided a standardized basis for comparison of all research on a common ground through four criterions, commonly identified as Truth Value, Applicability, Consistency, and Neutrality. Truth Value, or internal validity, is a tenet of research design that includes such aspects as study rigor (the method used, care in measurement and understanding of what wasn't measured) and considering what possible alternative explanations may exist for the causal relationships observed (Huitt, 1998). Applicability, also called external validity or generalizability, ensures the research can be used more broadly and adds value to the research process. Consistency, sometimes called reliability or replicability, allows for other researchers to validate or verify the findings of the research both as a means of confirming the findings and as a basis for advancing future research. The final criterion, Neutrality, focuses on the objectivity of the research. Together, the Canon provides a framework upon which research the research will be advanced.

3.4.2. Research phases

Using the COBPE (Alberts & Hayes, 2005) as a guide, the research was parsed into three phases: pre-experiment, experiment and post-experiment, which are shown in Figure 7. During the pre-experiment phase the first three research questions were explored in detail and the conceptual model, a mathematical construct, was developed. Data were obtained from numerous sources, as noted in Section 0, and a multivariate analysis was conducted to determine the relationships between the parameters.

Phase	Pre-experiment				Experiment	Post experiment
Activity						
Analyze Sample for parameters	Analyze Sample for values of the parameters	Analyze *binary matrix* for relationships	Create network diagram, evaluate *binary matrix* and diagram. Code file.	Test	Run Samples	Analyze results
Product						
Binary matrix	*Malice matrix*	multivariate analysis	Network diagram List of relationships Model	Test results	output of model	Analysis
Research question						
Question 1	Question 3	Question 2			Question 4	
Section						
3.5.1 3.5.2 4.3.1 4.5.1	3.5.1.1 3.5.2	3.5.2 4.3.2 4.5.2	3.5.3	3.5.5 4.3.3 4.5.3	3.6 4.5.4	3.7 4.4

Figure 7: Research phases

Using the information obtained from the analysis and the mathematical model, a network diagram was constructed to examine the model in a multi-perspective approach. The network diagram facilitated examining the nature of the model (verification of the nature of the relationships, open or closed construct, number of surfaces, etc.) prior to construction of the executable model. Finally, the executable model was constructed and

tested. At this point, the fourth research question, *what is the measure of risk*, remained unanswered. Upon completion of the testing of the executable model, per Section 3.5.5, the pre-experiment phase was completed.

Testing of the executable model found it to be valid, allowing testing of the null hypothesis to commence. Using the same samples from the pre-experiment phase, the research entered the second phase, the experimentation phase. During the experimentation phase, the values of each sample's parameters were run through the model to determine the relative risk across the sample space. The first sample, n=26, called Sample A, included output of both the surface area of the geometric shape and the sum of the edges which comprise the geometric shape. The results from Sample A demonstrated that calculating the surface area was contraindicated, therefore the second sample, n=25, only had output for the sum of the edges of the geometric shape.

In the third phase, post experiment, an analysis of the strengths and weaknesses of the sampling process, the impact of the hypothesis testing, and improvements to the modeling process were completed. Details of this phase can be found in Section 3.7. The results of the analysis from Sample A were used to improve the methodology for Sample B.

External validity was facilitated by using the intelligence community's variables as a basis and by conducting a robust analysis of the causal effects to derive the relationships. Given the researcher's prior experience in this area, care was taken to validate both the existence, and the value, of the parameter to mitigate the effects of the Rosenthal effect (Rosenthal, 2002). To corroborate the parameters deduced from the analysis of the samples, expert opinion was solicited from a group of risk and intelligence professionals. To further generalization, mitigation of the situation—specific parameter "underwater environment" was not used. Instead, the parameter "unique environment" was substituted. However, given that only cases of underwater terrorism were drawn as samples, the constrained data sample remains a potential barrier to external validity.

3.5. Process

The actual experiment, although guided by the empirical process of hypothesis testing, was an adaptive experiment intended to build and validate a model that facilitates managing and understanding of the epistemic risk of an underwater attack. Although described in serial fashion, the design evoked a reiterative nature, as shown in Figure 8, which is based on the principles for conducting a model-based experiment from the COBPE (Alberts & Hayes, 2005). Readers familiar with the COBPE should note that the COBPE exists to support experimentation that answers questions about another area under research whereas with this research, the area under research *is* the focus of the experimental design.

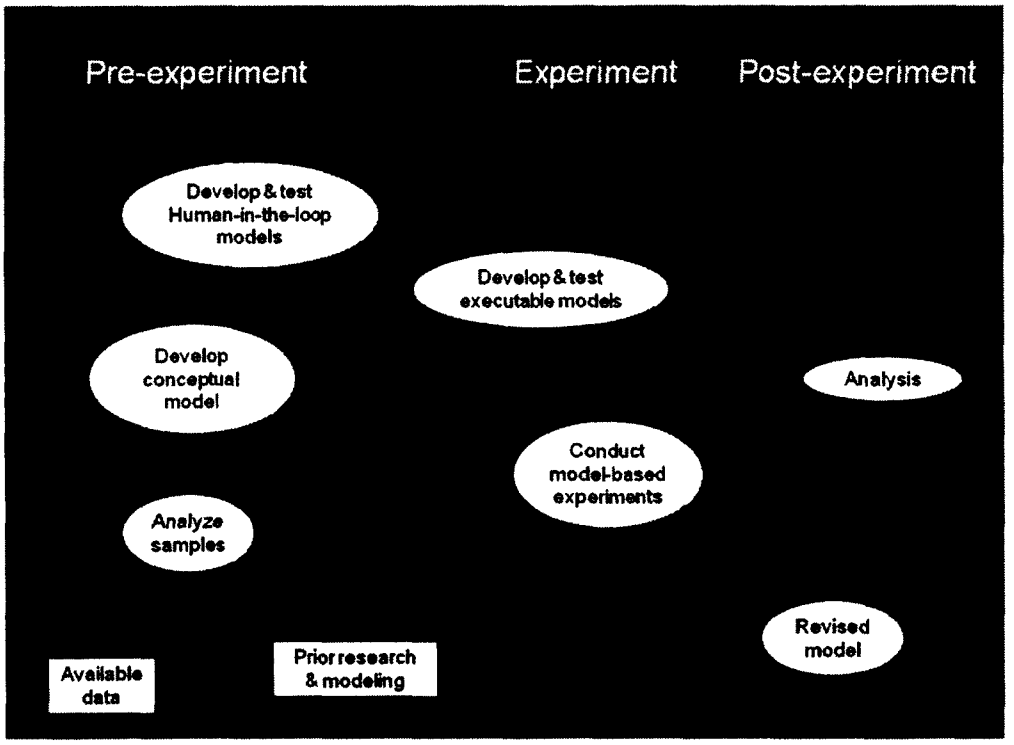

Figure 8: Research process

3.5.1. Phase 1: Pre-experiment

The pre-experiment phase focused on data collection and creation of the Human-in-the loop model. The Data Collection Plan, Appendix A, documented the process used to collect, protect and archive samples collected. A literature review was conducted to

determine the appropriate process to quantify the qualitative data, as noted in Section 0. Section 0 explains the data collection in more detail. Following data collection, a multivariate analysis was conducted and critically reviewed. A detailed discussion of the analysis process is described in Section 0. The results of the analysis were used to create the conceptual model. The conceptual model, mathematical in nature, facilitated understanding of the quantitative parameters involved, the nature of the experiment, and potential barriers to model validity.

The conceptual model and network graph enabled development and testing of the human-in-the-loop (HIL) model. The HIL model demonstrated the interactions and limits of the executable model and assisted in the testing design, Section 3.5.5. The HIL model evolved into the executable model and provided rapid analysis of functionality that influenced the hypothesis testing and anomaly-handling precepts. The completion of the executable model's validation and verification testing marked the transition to the experiment phase.

3.5.1.1. Quantifying qualitative variables

Since there exist numerous methods to quantify qualitative data (e.g., Chi, 1997; Darby, 2004; Dey, 1993; Shemmings, 2006) a literature review was conducted to determine the most appropriate method which could be easily applied to the epistemic uncertainty inherent in underwater terrorism. The literature review included products from the National Intelligence Community (see publications from the Central Intelligence Agency's Center for the Study of Intelligence) and academic research pertaining to information in the news media (e.g. Dunn, Moore & Nosek, 2005).

3.5.1.2. Data collection

The research employed a deductive empirical cycle initially examining parameters from previous research for a maritime risk analysis tool (Gay, 2006). Entering the databases noted in Section 0, a keyword search was performed using the words listed in Table 3. A review of the results of the key word search was conducted and relevant entries were extracted and created the basis of the sample's population. An example of the data collection log worksheet is given in Appendix B. Using the initial data set drawn from

the databases, additional research was conducted with open source material (law enforcement briefs, scholarly journals and open source media) to continue to develop the attack's profile. Profiles of each scenario were examined utilizing multiple perspectives, including the intelligence community's threat analysis, organizational theory prepositions, precepts of cyber terrorism studies and dive planning.

Table 3: Keywords used in database search

Underwater	Undersea	Submerged	Submarine	Marine
Maritime	Aquatic	Diver	Limpet	UWIED

Although there were many sources of information, a case was only accepted if it had at least two trusted (defined as government or academic center of excellence) references. No classified material was reviewed. However, open source (media or educational institution) material was used to better understand the total scenario.

As the sample's profile was developed, data were examined for originality, fact, and supposition and then compared against known organizations. For example, the profiles of various terrorist groups are well documented and openly available (e.g., LTTE). This information augmented the sample's profile, providing background for the sample where the original sources may have omitted details. As data were examined, each sample's data tested the null hypothesis – that the parameters indicated encompassed the domain of knowledge about a particular sample.

Each sample was also specifically researched through the databases after the initial key word search. As the samples were examined, the databases indicated additional cross-references that were pursued as separate data points. The samples were cross-referenced to ensure each sample indicated one, and only one, separate incident.

The output of the data collection was two matrices. The first matrix, called the Binary matrix, was composed of the indicator variables, utilizing the number *one* to indicate the parameters were noted in the specific case, or a *zero*, representing no indication of the

parameter was observed. The second matrix, called the Malice matrix, was composed on the value, determined by using the Malice Spectrum, for each parameter in the model. The Malice Spectrum presented in detail in Section 4.2, maps representative qualitative judgments to quantitative values. Where the specific case provided no indication of the value of the parameters, the value 0.5 (absolute uncertainty) was entered.

As a means to determine the importance and the ease of collecting the parameters used in this research, expert opinion was solicited based on a survey-like tool. The instrument was sent via email to a select group of known experts with a list of 21 parameters. Each expert was asked to evaluate the 21 parameters for importance in determining the overall risk and for ease in obtaining the value of the parameter. A Likert scale of one to five was employed. For importance, five represented critically important. For ease, five represented very difficult to obtain.

Four experts were selected to represent a cross section of maritime intelligence and critical infrastructure risk analysis. The experts came from academia, the Department of Homeland Security and from the Coast Guard's intelligence community. In addition to asking the experts to evaluate the parameters, each expert was asked for his/her experience in the field and formal training or education in the discipline. An expert was defined utilizing two criteria – education in the domain and experience. The minimum requirement for education was at least 160 hours of classroom instruction, or 20 classroom days, which is comparable to 10 credit hours of study. This criterion ensured a basis for understanding of the vocabulary and methodologies available. The second criterion, experience, was based on the emergent property of communities of practice. The criteria of having accomplished at least 10,000 hours of practical experience within the domain (Gladwell, 2008) equates to about five years of full time employment in the domain. The domains were homeland security risk and homeland security threat analysis. The results of the solicitation were plotted on a scatter plot based on the average value of the opinions provided.

3.5.1.3. Dummy variable definitions

In soliciting the expert opinion, seventeen of the parameters on the instrument were the ones used in this research. The other four parameters, called dummy parameters, were inserted as a control and to determine their value in the overall risk picture. The four dummy parameters were selected because they are currently used in intelligence or risk studies. Two parameters, population index and criticality are considered part of the consequence element. Leadership was selected as a distracter since the leaders of an organization are always important, but in the current distributed leadership model employed by adversarial groups it may not be known. The final dummy parameter, finance, is obviously vital to conducting any activity but does not directly relate to the threat element. Finance relates to threat because it supports acquiring material, moving people and material and enabling training. The specific definitions, as provided to the experts are articulated below.

Leadership (a) is the "process of social influence in which one person can enlist the aid and support of others in the accomplishment of a common task" (Chemers, 1997, p. 1) through overall direction and strategy. Depending on the structure and primary influence to the adversarial group, leadership may be a person or a group of people who guide or direct the adversarial organization. Leadership can be viewed as the organizational construct of command and control or the personalities of the leaders actually in specific roles.

Finance (d) is the activity that includes the origination, marketing, and management of cash and money surrogates through a variety of fund raising, capital accounts, and investments created for supporting and entertaining the adversarial organization or to pay for protection and asylum.

Directly linked to consequence, but frequently considered separately, is the population index (x) of an area. Essentially, it is a measure of all of the people inhabiting a specified area, including transients (e.g. commuters versus resident). Population index is occasionally measured as density, ergo, the number of people living per unit of an area

(e.g. per square mile) or the number of people relative to the space occupied by those people.

One parameter, which has been treated as part of consequence or as an independent variable, is criticality (y). Criticality accounts for the severity of the consequences for the entity. Criticality is directly related to the importance of the facility to a system and its environment when considering a specific event and the impact of the loss of that facility.

3.5.2. Sample analysis

Utilizing the Binary matrix a multivariate analysis was conducted. The samples were drawn from numerous databases and augmented by open source documents; thus the variables were discrete random variables demonstrating a range of possible, but countable, values, ergo a discrete random variable. This characteristic is attributed to the origin of the samples, primarily the trusted databases and open source documents generated by numerous authors for varying purposes. Utilizing the Binary matrix, two analyses were conducted, covariance and correlation of coefficient, to evaluate the latent structure contained within the set of variables from the sample. The covariance provided the behavior between the parameters – whether similar or dissimilar. The correlation coefficient provided the linear dependence. These analysis were run on both Sample A, n=26, and Sample B, n=25, independently. The threshold ranges accepted for the Pearson's correlation was -1.0 to -0.5 and 0.5 to 1.0.

The results of the multivariate analysis were compared with the results of the critical analysis and where there were differences, further analysis occurred. The additional analysis included further research on the parameters of the sample and questioning the validity of the parameters indicated in the initial sample. The additional research was focused on questioning the efficacy of the process used to evaluate the sample, not on adjusting the process to sample to the expected results.

3.5.3. Network graph

The network graph was generated using MATLAB© software. A 17 X 17 matrix was created using ones to indicate where relationships exist, as indicated by of correlation coefficient. Utilizing the biograph function a network graph was created, and visually

analyzed. This analysis consisted of comparing the displayed nodes and edges with the 17 X 17 matrix to ensure equivalence and then comparing the network to the output matrix of the multivariate analysis. Although the analysis of the table of parameters indicated the existence of super-nodes (nodes connected to every other node), the network graph indicated concerns with using volume or surface area of the resulting geometric shapes – that the geometric shapes would be pulled apart by dissimilar values of the edges. This concern was instrumental in creation of the error handling for the Human-in-the-Loop and executable models. The length of the edges in the network were determined by the MATLAB© biograph function and do not represent any particular value. They exist only to visually indicate relationships.

3.5.4. Human-in-the-Loop (HIL) model

The HIL model was created in MATLAB© using the conceptual model produced from the relationships noted in the correlation of coefficients and network graph and using Heron's formula to determine the surface area of the triangles by using the value of the edges. Heron's formula first determines the semi-perimeter, *sp*, using:

$$sp = \frac{(a + b + c)}{2}$$

where: a = length of edge x_1
b = length of edge x_2
c = length of edge x_3

and then computes the surface area of the triangle using the formula:

$$Surface\ Area = \sqrt{sp(sp - a)(sp - b)(sp - c)}$$

For Sample A, the edge lengths were computed by adding the value of the two end nodes for each edge of the side of every triangle in the geometric shape. Because a side of one triangle may also be the side of another triangle, a strong potential for duplicate values being included in the computation exists. Additional code was added to the model to compute only the edge lengths of the network diagram by summing the value of the nodes for each edge across the network diagram.

In testing Sample A's algorithm 48.6% of the test cases returned errors, shown in Figure **15** and Figure **16**. Hypothesis testing for Sample A indicated 14% of the actual cases evoked errors, as noted in Section 0. Therefore the process for Sample B only included examining the sum of the edge lengths across the network by adding the value of the two applicable nodes for each edge.

The sum of the individual surface area and the sum of the edge lengths, across the network diagram were used as the final result of the model for Sample A. Code was inserted to monitor when the triangle was incalculable because either it was opened by stretching or so compressed that it had no surface area. In this instance, the value of zero was returned to the summating equation and the error was counted. The error code was used as numerable indicator to flag those instances where the value of the parameters stressed the relationships inherent in the model. It provided an opportunity to visually examine potential cause and effect relationships. The sum of the edge lengths across the network diagram was used as the final result of the model for Sample B.

Testing of the HIL model was conducted per Section 3.5.5. Initial testing indicated that calculations for surface area had an unacceptable number of errors. Given this concern, the function for computing the volume of a polyhedron was not computed. The complexity of the solution space prohibited a test of the entire solution space by increasing the value of each parameter from zero for increments of 0.05. The estimated time to determine the surface area solution space, using the computing resources available, exceeded one century.

3.5.5. Testing

The test plan, based on a white-box, waterfall philosophy, was developed to test all of the functional, application performance and use requirements for academic testing of the hypothesis(s) supporting this research. Specific error handling was minimally incorporated in the MATLABe code and testing was not focused on user friendliness. Testing of the MATLABe environment was considered outside the scope of the test plan. The primary purpose of the test plan was to ensure the application met the requirements for supporting the determination if a relationship exists between the parameters of the

risk equation and the geometric properties of the instantiation of the risk equation. The application was not designed to be a simulation, but instead, to assist in understanding and managing the risk of an underwater terrorism event. The secondary purpose of the testing was to identify and expose all issues and associated risks with the hypothesis evaluation, and to ensure they are appropriately resolved. Performance was not considered in the testing methodology. The requirements are given in Table 4, the requirements traceability matrix.

Table 4: Requirements traceability matrix

Requirement	Function	Test case
1.0 Determine the geometric characteristics from a matrix.	Network creation	Submit matrix to create network of connections with: Nodes Edges 2 1 3 2 3 3 4 3 4 4 4 5 4 6
2.0 Given a matrix of values that correspond to a pre-coded polyhedron, determine the surface area of all faces.	Heron's formula	Test using vectors: 0, 0, 0 0 ,x, 0 0, 0, x x, 0, x x, x, x Determine surface area with x equal to .5 each and 1.0 each. Then test: 1, .7 .7

Table 4: (Continued)

Requirement	Function	Test case
3.0 Given a matrix of values that correspond to a pre-coded polyhedron, determine the sum of the edge lengths.	Sum of the relations	Test using vectors: 0, 0, 0 0 ,x, 0 0, 0, x x, 0, x x, x, x Determine surface area with x equal to .5 each and 1.0 each. Then test: 1, .7 .7
4.0 Determine the values for 2.0 and 3.0 above for the following cases:		
All values set at the state of complete uncertainty.		All parameters = 0.5
All values set at the state of complete favorability to the defender.		All parameters = 0.0
All values set at the state of complete favorability to the adversary		All parameters = 1.0
Values of key parameters set high and low		High parameters = 1.0. Low parameters = 0.1 Other parameters = 0.5

3.5.6. Executable model

The executable model did not differ from the human-in-the-loop model substantially. The only difference was how data were provided to the functions. In the human-in-the-loop model, data were provided by a human and checked against the expected results after each scenario. In the executable model data were submitted to the functions via a script file.

3.6. Phase 2: Experiment

Upon successful completion of the model's functional testing, script files were created from the samples, which called the model's functions and returned both graphic and numeric results. For Sample A, the results included data on the surface area and the sum of the edges. After the post experiment analysis of Sample A, it was verified that the surface area calculations contained too many errors. Therefore, the model was modified for Sample B's experiment to return only data on the sum of the edges of the network. After the modification the experiment continued the testing of the null hypothesis to wit, that it is not possible to develop a model that facilitates understanding the risk scenario based on the parameters observed from prior underwater terrorism incidents.

3.7. Phase 3: Post-experiment

The third phase of the research was the post-experiment phase, which analyzed the output of the model and identified revisions to the process and functionality. The analysis phase consisted of evaluating the network diagram, the overall range of possible values, the range of returned values, the standard deviation of the sampled values, and the proportionality of the returned results. The expectation was that an improved understanding of the nature of the relative risk among the samples would be evident. The analysis also sought to identify the strengths and weaknesses of the sampling process, the hypothesis testing, the model and any potential study bias to determine potential improvements to the methodology.

CHAPTER 4
RESEARCH FINDINGS

The research findings start with items common to all the samples – the basis of the parameter research and how to quantify qualitative variables. The section then progress through Sample A and Sample B presenting the findings on the parameters, the relationships between the parameters, test data for the model, the output from the experiment and a brief analysis of the experiments data. Discussions of the impacts of the analysis are included in Section 0.

4.1. Expert opinion of parameters

The expert opinion solicitation conducted to evaluate the efficacy of the analytical research conducted with Samples A and B are shown in Figure 9. The four experts collectively represent 31 years of experience with a minimum experience base of 6 years and an average of 7.75 years. For education, the respondents had an average of 1.4 years of education with a maximum of 3.0 years and a minimum of 230.4 hours of classroom time.

Figure 9 shows the importance on the Y-axis and Ease on the x-axis. For importance, a five represents that the parameter is considered very important in determining risk or threat while a value of one represent the parameter is not very important in determining risk or threat. For ease, five represents the value of the parameter is very difficult to obtain while one represents the value of the parameter is very easy to obtain. The parameter key resource—people (k) and the dummy parameter finance (d) were indicated as most important but difficult to obtain while the parameter unique environment (u) and the dummy parameter population index (x) were indicated as least important although the population index was noted as easily obtainable. All of the parameters derived from answering Research Question One were rated at least a 2.5 on the 5.0 Likert scale validating that the parameters utilized in the research have importance within the domains of homeland security risk and homeland security threat analysis.

4.2. How to quantify qualitative variables

In answering Research Questions One and Two the parameter was both indicated and related to another, or it was not. The research questions did not address the magnitude or

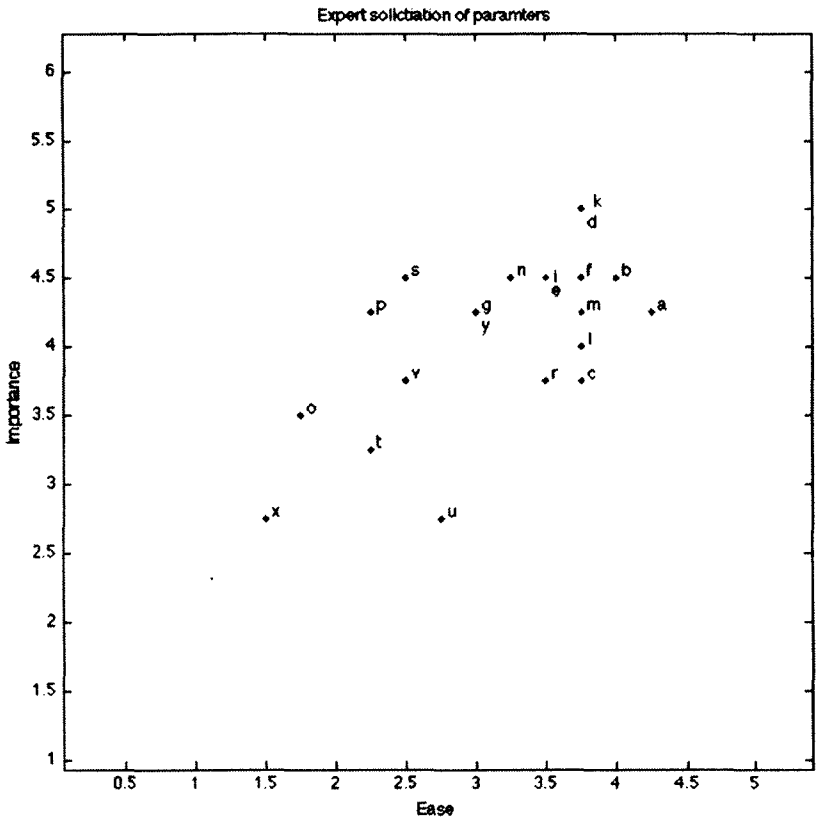

Figure 9: Expert opinion of parameter importance and ease

value of the parameters. The concern is how to assign a quantitative value from a qualitative estimate that may range across extreme values. Darby (2004) provided a basis for the approach to solving this problem by using possibility theory, including a discussion on fuzzy measures, which can range in value from 0 to 1.0. Willet (1901), in discussing uncertainty as a probability, asserted that uncertainty is greatest when the degree of probability for risk is equal to one half, or expressed as a decimal = 0.5. Essentially, if there is absolutely no information about a given parameter either for or against and adversarial position, the parameter is in its greatest state of uncertainty or

valued at 0.5. If, however, information about the parameter indicates an absolute end state, then the value is equal to 1.0, representing a 100 probability of occurrence, or 0.0, representing no probability of occurrence.

However, as noted in the introduction, probability is not an acceptable means for quantifying the qualitative data in many instances. Since each parameter is analyzed under varying degrees of epistemic uncertainty and can range across a continuum of uncertainty (from known to completely unknown) a spectrum is appropriate. Spectrums are used in many domains (e.g., light, electromagnetic) and unify the end states. Consider that each parameter is comprised of a large number of characteristics that are n-dimensional. Algebraic theory has two theories to address the representation of an n-dimensional object. In linear algebra, the spectral theorem for symmetric matrices allows for diagonalization of a matrix that meets certain conditions. In algebraic topology, the generalized cohomology theory facilitates studying the topology based upon its group including n-dimensional closed cells. Both of these theories support using a spectrum as a means to mathematically instantiate a parameter from a vector or matrix of characteristics but do not provide a methodology to map the qualitative value to a quantitative result.

The intelligence community, drawing upon research on words of estimative probability (see Kent, 1964, Kesselman, 2008, or Wheaton & Chido, 2008), uses the Estimative language continuum, Figure **10**, to map the qualitative judgments of their analysts to a continuum. It avoids precise numerical ratings but reflects the intelligence community's estimate of probability (National Intelligence Estimate, 2007).

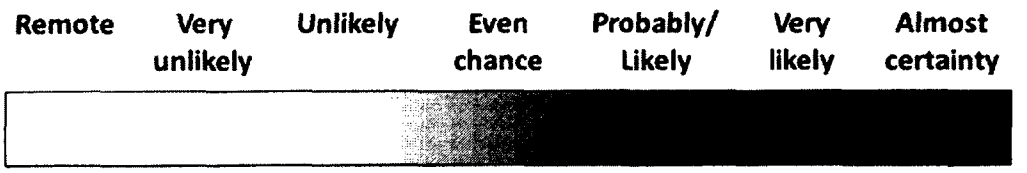

Figure 10: Estimative language continuum
(from National Intelligence Estimate, 2007)

Applying Darby's (2004) application of fuzzy measures to Willet's (1901) description of uncertainty yields a scale from zero to one that can then be placed over the Intelligence community's estimative language continuum. With minor modification of the words on the continuum, to encompass the vocabulary of uncertainty, a new spectrum, the Malice Spectrum, is created. The Malice Spectrum, shown in Figure **11**, allows analysts or facility managers to map representative qualitative judgments to quantitative values. Using the perspective of the defender, information from any source, permits the analyst or facilities manager to develop a comparable estimate across diverse qualitative fields.

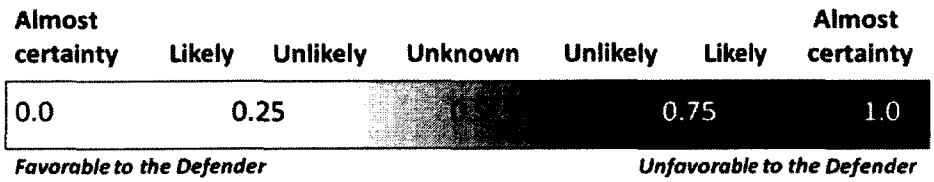

Figure 11: Malice spectrum

The Malice Spectrum permits descriptive precision in evaluating parameters while limiting the value of the parameters from the range zero to one, inclusive.

4.3. Sample A

In conducting this research, 51 cases were selected based on the integrity of the sources and the availability of multiple data sources as discussed in Sections 0 and 0. The cases were randomly mixed and the first sample, called Sample A was drawn, consisting of 26 cases.

4.3.1. Parameters

Observing the first sample, Figure **12** graphically shows the descending progression of percentage that each parameter was observed. Recall, the parameters were treated as indicator random variables; therefore the mean represents the percentage that each parameter was observed across the sample. Additionally, as indicator random variables, the standard deviation for the parameters would be meaningless.

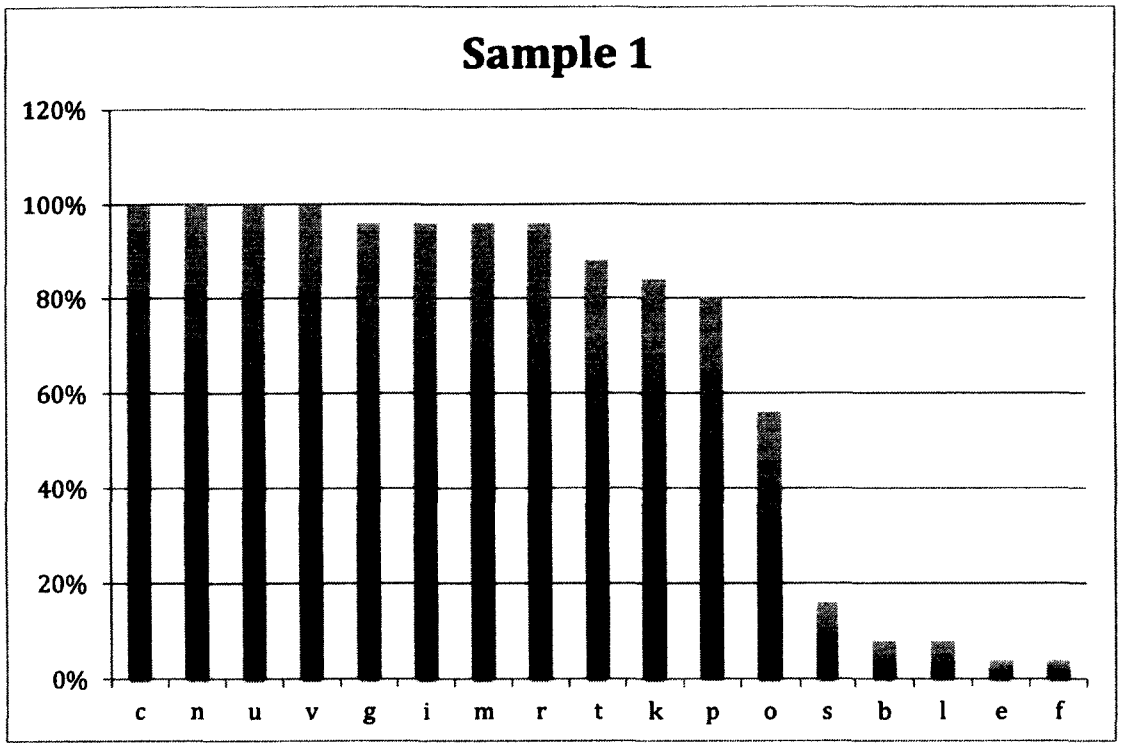

Figure 12: Each parameter's occurrence in Sample A by percent

The first 11 parameters, consequence © through propaganda (p) are evident at least 80% of the time. The parameters consequence ©, operational planning (n), unique environment (u) and vulnerability (v) were observed 100% of the time. Parameter operational history (o) is also strong, being observed 56% of the time. Although parameters surveillance (s), movement of people (b), logistics (l), testing (e) and information collection (f) are not significantly evident, parameters surveillance (s), testing (e) and information collection (f) could be grouped together as probing. Parameters movement of people (b) and logistics (l) were not directly observed or reported significantly, with 8% observance for each.

4.3.2. Relationships

The results of the covariance tests, sorted according to parameter occurrence rate, are provided in Table 5.

Table 5: Covariance results for Sample A

	c	n	u	v	g	i	m	r	t	k	p	o	s	b	l	e	f
c		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
u	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0
v	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0
g	0	0	0	0		.04	0	0	0	-.01	.03	-.02	-.03	-.04	-.04	0	-.04
i	0	0	0	0	.04		0	0	0	-.01	.03	-.02	-.03	-.04	-.04	0	-.04
m	0	0	0	0	0	0		0	.04	.03	-.01	.02	.01	0	0	0	0
r	0	0	0	0	0	0	0		.04	.03	-.01	.02	.01	0	0	0	0
t	0	0	0	0	0	0	.04	.04		.06	.02	.07	.02	.01	.01	0	0
k	0	0	0	0	-.01	-.01	.03	.03	.06		-.03	.09	.03	.01	.01	.01	.01
p	0	0	0	0	.03	.03	-.01	-.01	.02	.03		.03	-.01	-.06	-.02	-.03	-.03
o	0	0	0	0	-.02	-.02	.02	.02	.07	.09	.03		.07	.04	.04	.02	.02
s	0	0	0	0	-.03	-.03	.01	.01	.02	.03	-.01	.07		.03	.03	-.01	.03
b	0	0	0	0	-.04	-.04	0	0	.01	.01	-.06	.04	.03		.03	.04	.04
l	0	0	0	0	-.04	-.04	0	0	.01	.01	-.02	.04	.03	.03		0	.04
e	0	0	0	0	0	0	0	0	0	.01	-.03	.02	-.01	.04	0		0
f	0	0	0	0	-.04	-.04	0	0	0	.01	-.03	.02	.03	.04	.04	0	

Of the 272 possible covariance results, 158 (58%) are zero, 72 (26%) are positive and 42 (15%) are negative. Table 6 shows the matched pairs for the positive values from the covariance analysis. In all cases, the relationship was bi-directional – either positive or negative in both directions.

Table 6: Positive values from covariance for Sample A

o:	ob	oe	of	ok	ol	om	op	or	os	ot
k:	kb	ke	kf	kl	km	kr	ks	kt		
s:	sb	sf	sl	sm	sr	st				
t:	tb	tl	tm	tp	tr					
b:	be	bf	bl							
p:	pg	pi								
f:	fl									
g:	gi									

Table 7 shows the matched pairs for the negative values from the covariance analysis.

Table 7: Negative values from covariance for Sample A

g:	gb	gf	gk	gl	go	gs		
i:	ib	if	ik	il	io	is		
p:	pb	pe	pf	pk	pl	pm	pr	ps
e:	es							

By itself, given the parameters were treated as indicator random variables and the information came from unclassified sources, which may not have all the pertinent information known about the incident, this information provides no insight into the nature of the relationships between the variables directly.

The Pearson's product-moment correlation of coefficients, presented by parameter occurrence rate, for Sample A is shown in Table **8**. The asterisks given for the values of parameters consequence (c), pre-operational planning (n), unique environment (u) and vulnerability (v) represent that they were observed in all instances and have a direct linear relationship. Other than consequence, pre-operational planning, unique environment and vulnerability, only three relationships have an absolute value greater than 0.7, explicitly fg, fi, and gi, forming a triangular relationship. If the pairs with an absolute value of 0.69 were included (be, bf, bg, and bi) only the parameters movement of people (b) and testing

(e) remain to be considered. By including absolute values equal to or greater than 0.5 the pairs bp, ko, kt, tm, tr, li, lg, and lf are under consideration. Having no other contrary indications and given the data was drawn from imprecise sources, the heuristic that absolute value of $r \geq 0.5$ indicated a substantially strong linear relationship was accepted for this research. Using $r \geq 0.5$, all of the parameters are under consideration for the network graph.

Table 8: Results of correlation of covariance for Sample A

	c	n	u	v	g	i	m	r	t	k	p	o	s	b	l	e	f
c		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
n			*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
u				*	*	*	*	*	*	*	*	*	*	*	*	*	*
v					*	*	*	*	*	*	*	*	*	*	*	*	*
g						1.0	-.04	-.04	-.08	-.09	.41	-.18	-.47	-.69	-.69	.04	-1.0
i							-.04	-.04	-.08	-.09	.41	-.18	-.47	-.69	-.69	.04	-1.0
m								-.04	.55	.47	-.10	.23	.09	.06	.06	.04	.04
r									.55	.47	-.10	.23	.09	.06	.06	.04	.04
t										.51	.12	.42	.16	.11	.11	.08	.08
k											-.22	.49	.19	.13	.13	.09	.09
p												.16	-.05	-.59	-.22	-.41	-.41
o													.39	.26	.26	.18	.18
s														.27	.27	-.09	.47
b															.46	.69	.69
l																.04	.69
e																	-.04
f																	

Notwithstanding the parameters consequence (c), operational planning (n), unique environment (u) and vulnerability (v), which were observed in each case, 15 linear relationships were observed between the 12 parameters that form 72 one-to-one relationships between the parameters, and form 136 distinct triangles. A network graph, per Section 0, was created to facilitate understanding of the nature of the relationships and is shown in Figure **13**. Each node represents a parameter. The edges indicate a relationship between the parameters, although the length of the edge has no meaning – it was determined by the software used to generate the figure.

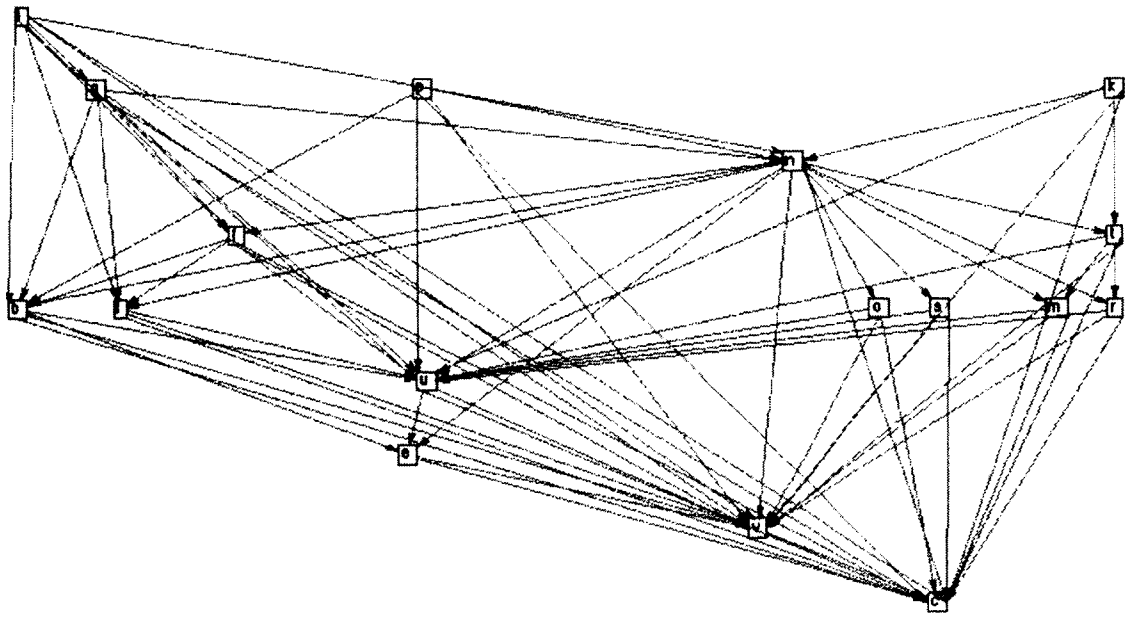

Figure 13: Complete network graph for Sample A

Because of the parameters consequence (c), pre-operational planning (n), unique environment (u) and vulnerability (v) having a one to one relationship with all the other parameters, Figure **13** is difficult to observe the unique relationships. Therefore, Figure **14** is provided, which clearly indicates the smaller number of relationships without consequence (c), pre-operational planning (n), unique environment (u) or vulnerability (v) as super-nodes.

Using both the correlation of coefficients analysis and the network graph, a mathematical model for the surface area of Sample A was created. Essentially, the surface area is the sum of three individual summations: the triangles formed by seven unique relationships; the sum of the triangles formed by pairs of the parameters consequence (c), pre-operational planning (n), unique environment (u) and vulnerability (v); and the sum of the triangles formed by parameters c, n, u and v with the other parameters. This model can be written as:

$$(big+bif+bgf+igf+igl+gfl+ifl)$$

$$+$$

$$\sum_{i=x}^{X} \sum_{i=y}^{Y} (xyc) \qquad x = (p, i, g, k, o, t, f, s, m, l, b, r, e)$$
$$y = (n, u, v)$$

$$+$$

$$\sum_{i=a}^{A} \left[\sum_{i=zx}^{ZX} abzx + \sum_{i=zy}^{ZY} abzy + \sum_{i=zz}^{ZZ} abzz + apb + atr \right] \qquad a = (c, n, u, v)$$
$$zx = (e, f, g, i)$$
$$zy = (f, i, l)$$
$$zz = (i, l)$$

Using this equation, Heron's formula can be applied to determine the surface area of the triangles or the sum of the edges can be computed by adding the value of the parameters, instantiated as nodes. Coding this equation into MATLAB ©, per Section 0, a human in the loop model can be created.

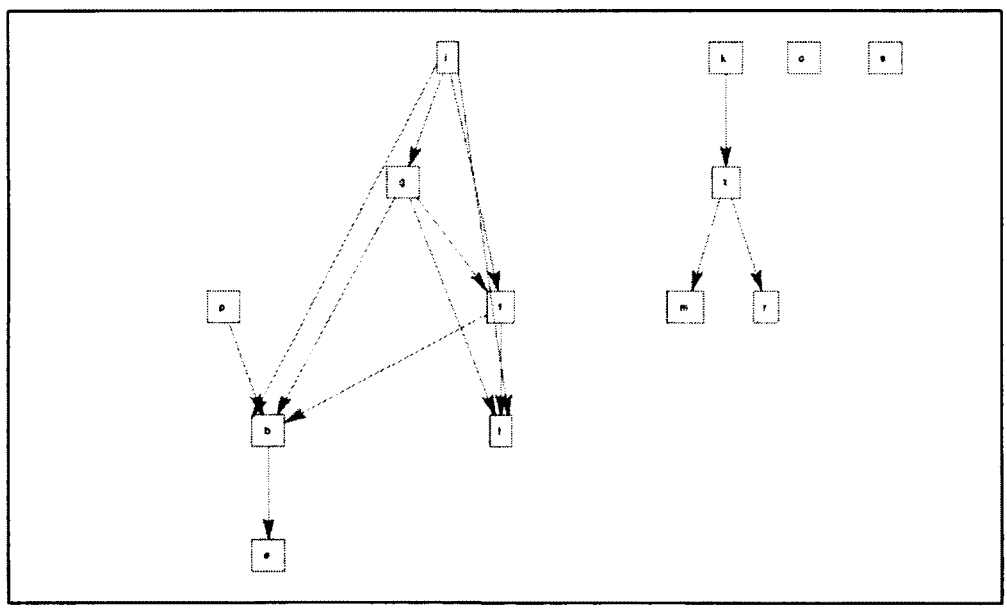

Figure 14: Network graph of the unique relationships from Sample A

4.3.3. Sample A test results

Utilizing the test criteria given in Section 3.5.5, testing was satisfactorily conducted and the results are shown in Table **9**, Table **10**, and because of its size, Appendix D.

Table 9: Test requirement 1.0, create geometric characteristic from a matrix results

Test Protocol	Expected		Actual		Remarks
	Nodes	Edges	Nodes	Edges	
1.0	2	1	2	1	Satisfactory
	3	2	3	2	Satisfactory
	3	3	3	3	Satisfactory
	4	3	4	3	Satisfactory
	4	4	4	4	Satisfactory
	4	5	4	5	Satisfactory
	4	6	4	6	Satisfactory

Table 10: Test requirement 2.0 and 3.0, given a matrix determine surface area and sum of the edge lengths results

Test Protocol		
2.0 Surface Area		
	Surface Area Expected	Surface Area Computed
0, 0, 0	Error – no triangle formed	Error
0, .5, 0	Error – no triangle formed	Error
0, 0, .5	Error – no triangle formed	Error
.5, 0, .5	Error – no triangle formed	Error
.5, .5, .5	.1083	.1083
0, 1, 0	Error – no triangle formed	Error
0, 0, 1	Error – no triangle formed	Error
1, 0, 1	Error – no triangle formed	Error
1, 1, 1	.4330	.4330
1, .7, .7	.2449	.2449
3.0 Sum of Edges		
	Sum expected	Sum returned
0, 0, 0	0	0
0, .5, 0	.5	.5
0, 0, .5	.5	.5
.5, 0, .5	1.0	1.0
.5, .5, .5	1.5	1.5
0, 1, 0	1.0	1.0
0, 0, 1	1.0	1.0
1, 0, 1	2.0	2.0
1, 1, 1	3.0	3.0
1, .7, .7	2.4	2.4

A graphic display of the results of the test conducted on Sample A, Figure **15**, illustrates the results for the surface area and edge length computations using the edges of the triangles as the basis for the computations. Note that a scalar of 0.5 was used on the sum of the edges and on the errors. The scalar was then applied again for the product of the surface area and the sum of the edges. The scalar was used to facilitate study of the relationships on one graph.

After the initial test of Sample A, the code was updated to compute the sum of the edges based on the network diagram. The results of the update are shown in Figure **16**. Note that a different scalar has been used to offset the sum of the edges with the surface area for ease of comparison.

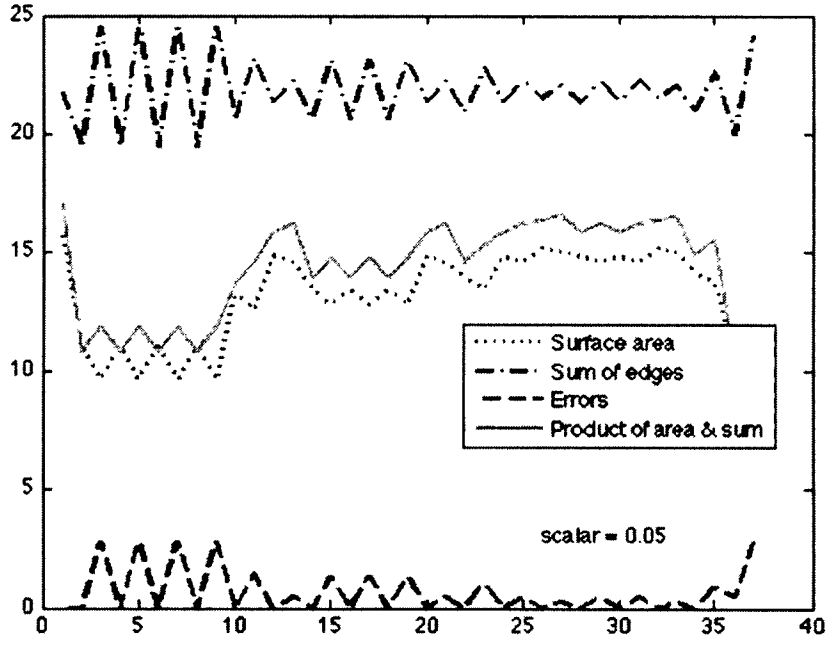

Figure 15: Test results from Sample A – sum of the edges computed using triangles formed.

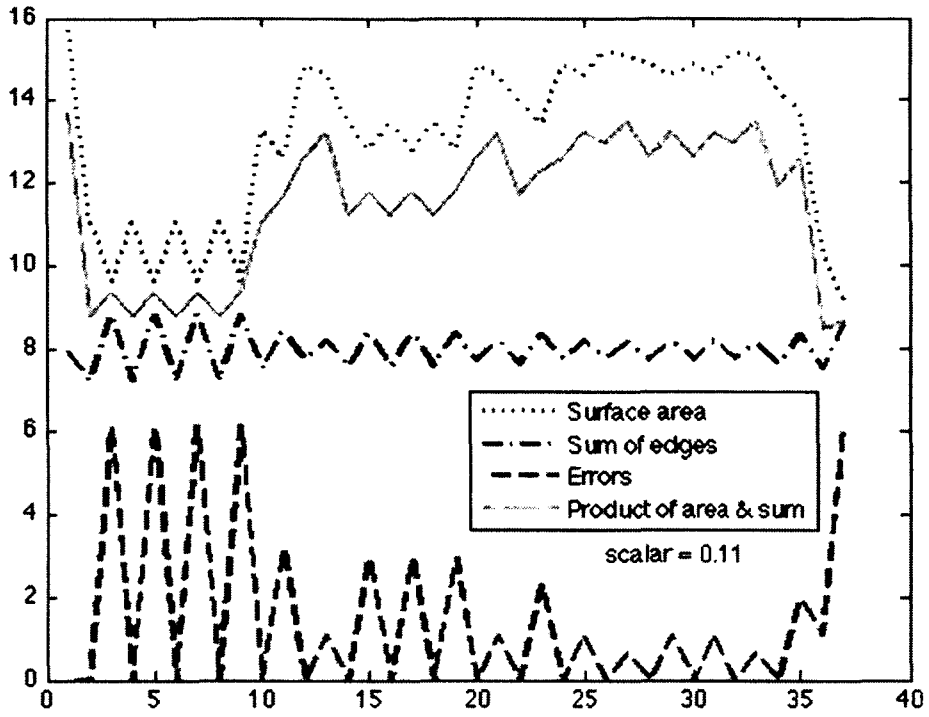

Figure 16: Test results from Sample A - sum of the edges computed from network diagram.

4.4. Results of experiment for Sample A

Sample A, consisting of 26 cases of underwater terrorism, was submitted to the geometric structure generated by the parameters observed within the cases and the relationships between those parameters are indicated by a correlation of coefficients analysis. Figure 17 shows the surface area and the sum of the edges for Sample A. A scalar of 0.05 was applied to the results of the sum of the edges to facilitate plotting the surface area and the sum of the edges on the same graph. The total number of errors generated by the surface area calculations for this sample was 537 out of 3,770 calculations (14%). The least number of errors for the surface area calculation for any one case in Sample A was 3 (2%) with a maximum number of errors for two different cases of 47 (32%). In each case in Sample A, there were errors in computing surface area.

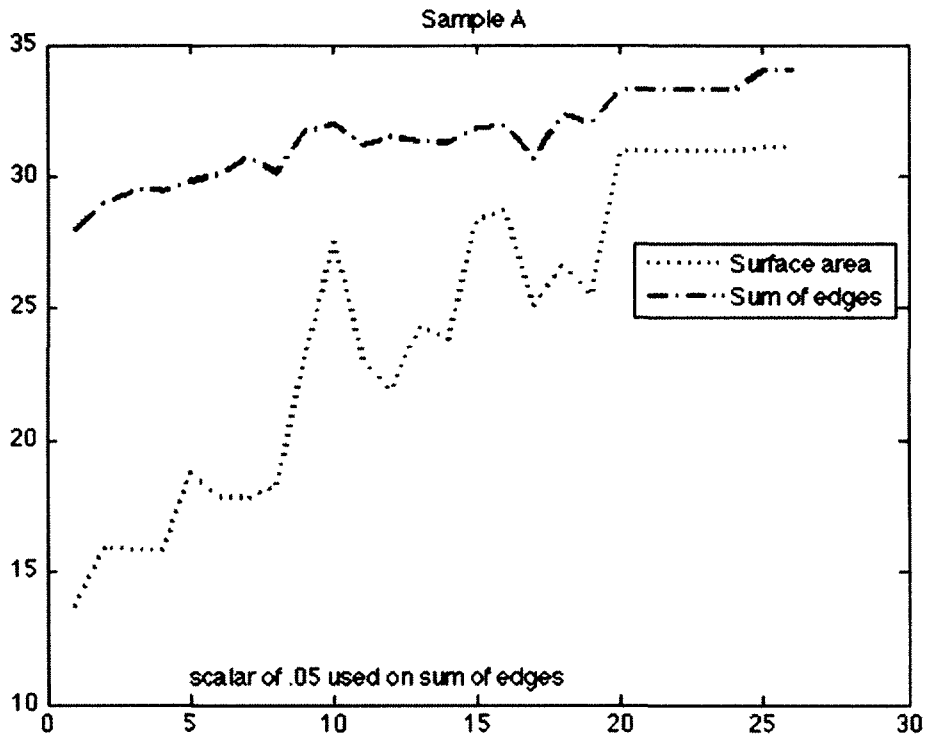

Figure 17: Sample A's surface area and sum of the edges results using the edges of the triangles formed for computations.

Despite the known errors in the calculations using the triangle method, the surface area and the sum of the edges illustrate a relationship for both sums of the edges. The relationship can be seen in the scatter plot that maps the surface area to the X-axis and the sum of the edges to the Y-axis, shown in Figure **18** and in Figure **19** that suggest a positive correlation. Given the high incident of errors, this correlation was not researched further.

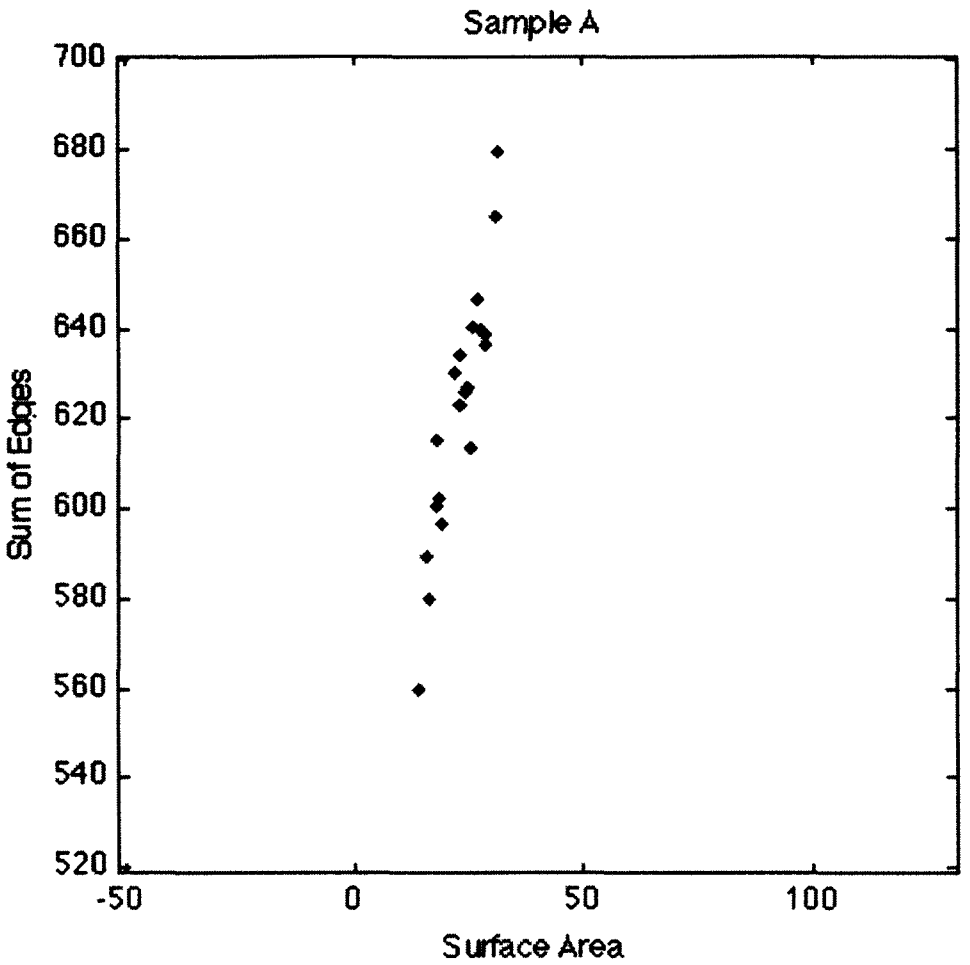

Figure 18: Sample A's sum of the edges and surface area using the triangles formed method

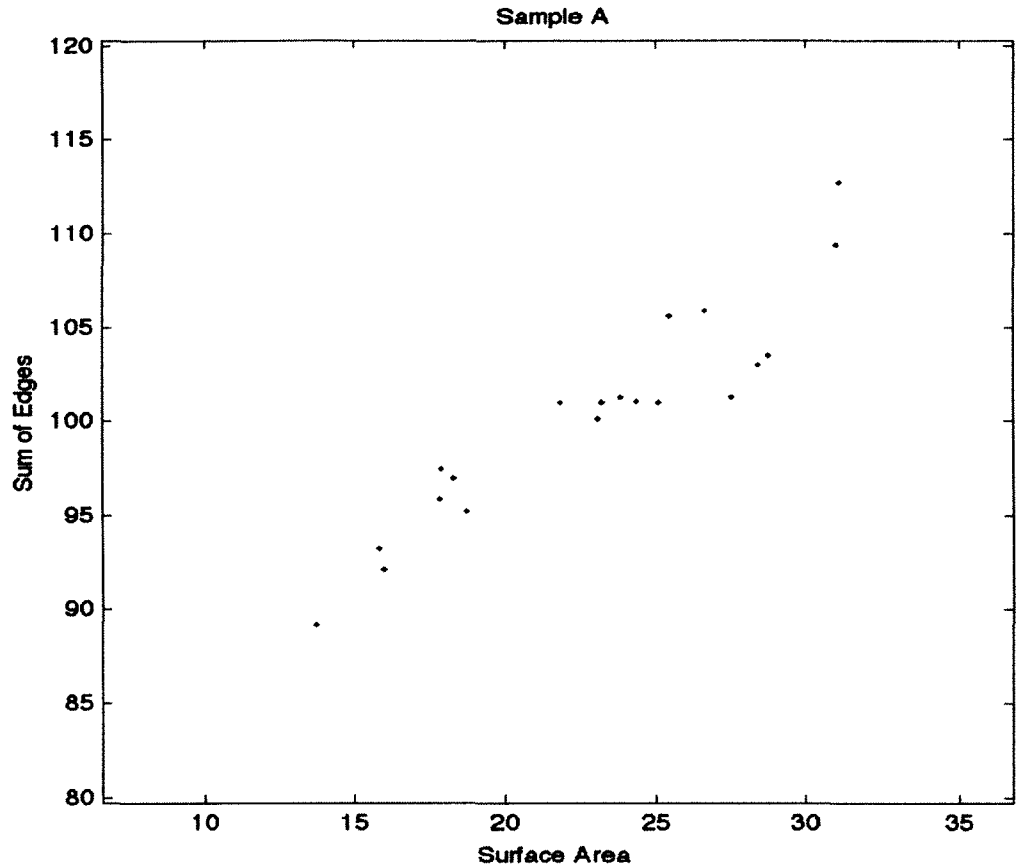

Figure 19: Sample A's surface area and sum of edges using the network method

For the sum of the edges in Sample A, the data did not exhibit integrity errors. Recall that the range of the sum of the edges for the sample space ranges from 0 to a maximum of 870 with absolute uncertainty at 435. The sample, n=26, had a maximum value of 679.8 and a minimum value of 560. The mean for the sample was 629.8 with a standard deviation of 32.1. The results of Sample A's experiment are shown in Figure **20**. The difference from absolute uncertainty to the minimum value noted in Sample A is 125 and the difference from the maximum value for any case in Sample A to the computed maximum for Sample A was 190.2. The values for any case in Sample A are in a band with width 119.8. 11 of the 26 (42%) of the cases were outside of the standard deviation with seven below and four above.

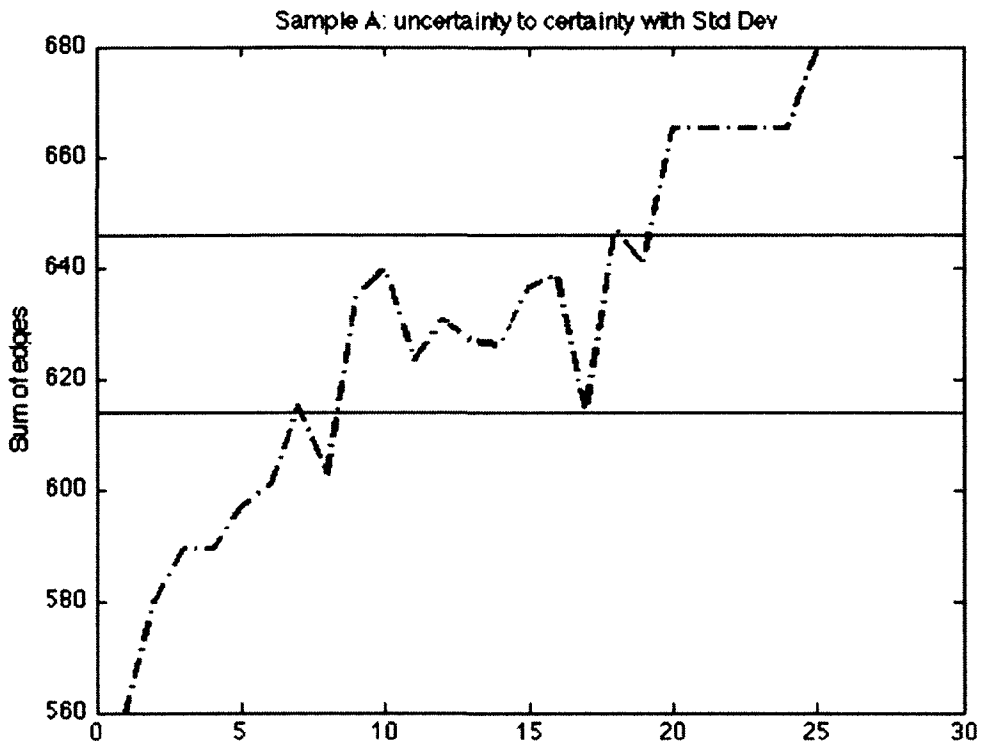

Figure 20: Sample A's sum of edges from the experiment

Figure 21 shows the sum of the edges using the network diagram. It also shows the standard deviation of 6.6, the mean of 102.0 and is limited on the Y-axis by the point of absolute uncertainty (all values set to 0.5) of 72 and the maximum value for the network of 144. This sample had a minimum value of 89.2 and a maximum value of 112.7.

A discussion of Sample A can be found in Section 0.

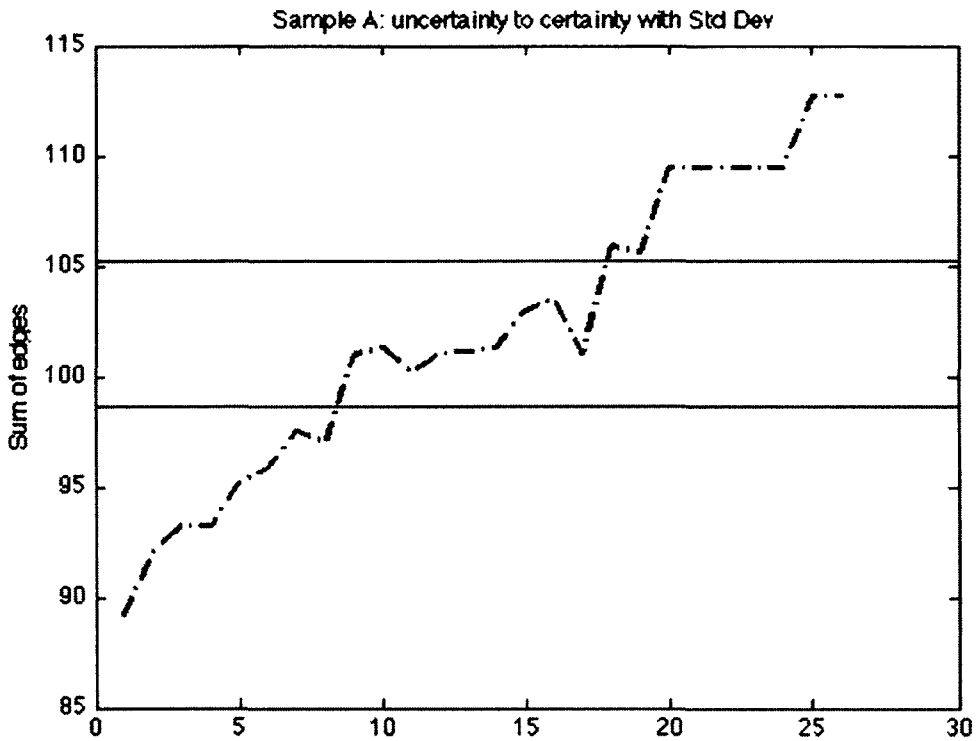

Figure 21: Sample A's sum of the edges using the network diagram

4.5. Sample B

Sample B, the remaining 25 cases (see Section 0) of the original 51 accepted, was analyzed and processed after making some changes to the methodology as previously noted. The most important change was eliminating the calculations of the surface area and using only the edges of the network diagram for the computation.

4.5.1. Parameters

Observing the second sample, Figure **22** graphically shows the descending progression of percentage that each parameter was observed. Again, the parameters were treated as indicator random variables; therefore the mean represents the percentage that each parameter was observed across the sample. Additionally, as indicator random variables, the standard deviation for the parameters would be meaningless.

The first 10 parameters, unique environment (u) through key resources—people (k) are evident at least 80% of the time. Only the parameter unique environment (u) is observed 100% of the time. The parameters operational history (o) and propaganda (p) are also strong, being observed 72 % and 56% of the time, respectively. Again, the parameters

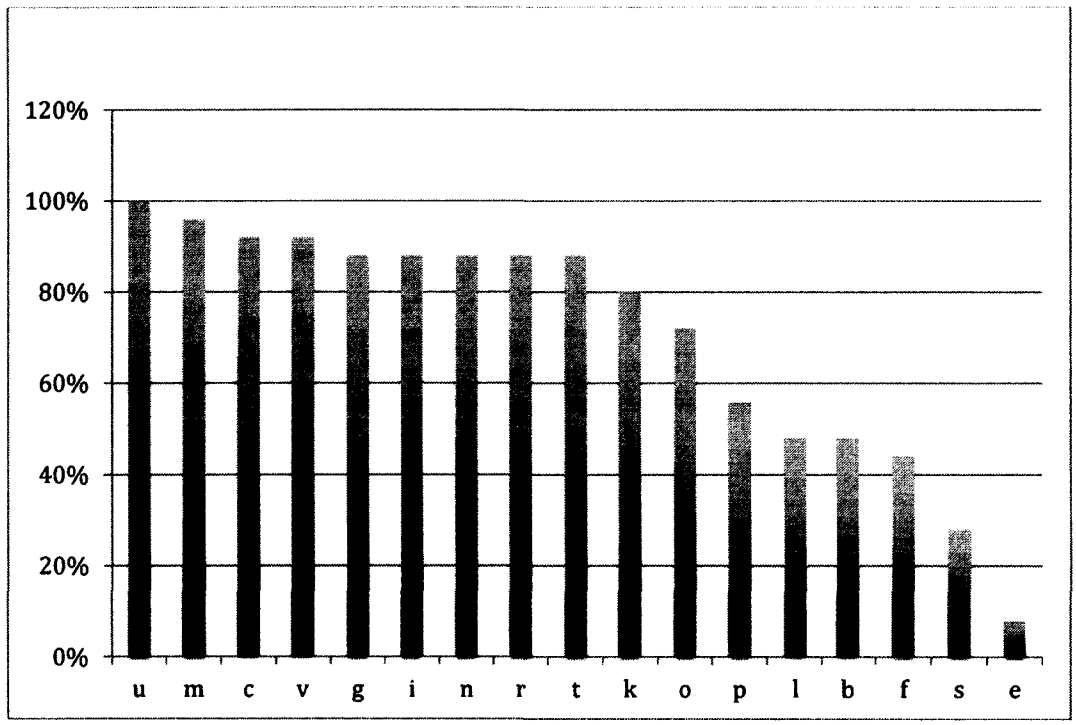

Figure 22: Each parameter's occurrence in Sample B by percent

information collection (f), surveillance (s) and testing (e), which can be grouped together as probing, have the lowest number of observations.

4.5.2. Relationships

The results of the covariance tests, sorted according to parameter occurrence rate, are provided in Table **11**. Of the 272 possible covariance results, 214 (79%) are positive, 50 (18%) are zero and 8 (3%) are negative. Table **12** shows the matched pairs for the positive values from the covariance analysis. In all cases, the relationship was bi-directional – either positive or negative in both directions.

Table 11: Covariance results for Sample B

	u	m	c	v	g	i	n	r	t	k	o	p	l	b	f	s	E
u		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
m	0		.04	.04	.04	.04	.04	0	.04	.03	.03	.02	.02	.02	.02	.01	0
c	0	.04		.07	.03	.03	.03	.03	.07	.02	.02	0	0	.04	.04	.02	.01
v	0	.04	.07		.03	.03	.03	.03	.07	.02	.02	0	0	.04	.04	.02	.01
g	0	.04	.03	.03		.11	.11	.03	.07	.1	.09	.07	.06	.06	.05	.03	.01
i	0	.04	.03	.03	.11		.11	.03	.07	.1	.09	.07	.06	.06	.05	.03	.01
n	0	.04	.03	.03	.11	.11		.03	.07	.1	.09	.07	.06	.06	.05	.03	.01
r	0	0	.03	.03	.03	.03	.03		.07	.06	.05	.03	.02	.06	.05	.03	.01
t	0	.04	.07	.07	.07	.07	.07	.07		.06	.05	.03	.02	.06	.05	.03	.01
k	0	.03	.02	.02	.1	.1	.1	.06	.06		.14	.07	.06	.1	.05	.02	-.02
o	0	.03	.02	.02	.09	.09	.09	.05	.05	.14		.12	.05	.09	.04	0	-.02
p	0	.02	0	0	.07	.07	.07	.03	.03	.07	.12		.09	-.03	.11	.08	0
l	0	.02	0	0	.06	.06	.06	.02	.02	.06	.05	.09		.09	.11	.03	.04
b	0	.02	.04	.04	.06	.06	.06	.06	.06	.1	.09	-.03	.09		.07	-.01	0
f	0	.02	.04	.04	.05	.05	.05	.05	.05	.05	.04	.11	.11	.07		.12	.04
s	0	.01	.02	.02	.03	.03	.03	.03	.03	.02	0	.08	.03	-.01	.12		.02
e	0	0	.01	.01	.01	.01	.01	.01	.01	-.02	-.02	0	.04	0	.04	.02	

Table 12: Positive values from covariance for Sample B

m:	mc	mv	mg	mi	mn	mt	mk	mo	mp	ml	mb	mf	ms
c:	cv	cg	ci	cn	cr	ct	ck	co	cb	cf	cs	ce	
v:	vg	vi	vn	vr	vt	vk	vo	vb	vf	vs	ve		
g:	gi	gn	gr	gt	gk	go	gp	gl	gb	gf	gs	ge	
i:	in	ir	it	ik	io	ip	il	ib	if	is	ie		
n:	nr	nt	nk	no	np	nl	nb	nf	ns	ne			
r:	rt	rk	ro	rp	rl	rb	rf	rs	re				
t:	tk	to	tp	tl	tb	tf	ts	te					
k:	ko	kp	kl	kb	kf	ks							
o:	op	ol	ob	of									
p:	pl	pf	ps										
l:	lb	lf	ls	le									
f:	fs	fe	bf										
s:	se												

The matched pairs for the negative values from the covariance analysis are ke, oe, pb, and bs.

By itself, given the parameters were treated as indicator random variables and that the information came from unclassified sources, which may not have all the pertinent

information known about the incident; this information provides no insight into the nature of the relationships between the variables directly.

The Pearson's product-moment correlation of coefficients, presented by parameter occurrence rate, for Sample B is given in Table 13.

The asterisks given for the values of the parameter unique environment (u) represent that it was observed in all instances and has a direct linear relationship. Four of the pairs, ig, in, gn and vc have a linear relationship with a value of 1.0. 6 additional relationships have an r value of greater than 0.7: ki, kg, kn, ko, tv and tc, tending to a strong correlation with the parameter key resource – people (k). The correlation between tactics, techniques and procedures (t) continues into the correlation band of an r value greater than 0.6, with ti, tg, tn, tr, mv and mc. The least valued accepted relationships,

Table 13: Correlation of coefficients for Sample B

	u	m	c	v	g	i	n	r	T	k	o	p	l	b	f	s	e
u		*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
m			.69	.69	.55	.55	.55	-.08	.55	.41	.33	.23	.2	.2	.18	.13	.06
c				1.0	.34	.34	.34	.34	.8	.22	.14	.04	-.01	.28	.26	.18	.09
v					.34	.34	.34	.34	.8	.22	.14	.04	-.01	.28	.26	.18	.09
g						1.0	1.0	.24	.62	.74	.59	.42	.35	.35	.33	.23	.11
i							1.0	.24	.62	.74	.59	.42	.35	.35	.33	.23	.11
n								.24	.62	.74	.59	.42	.35	.35	.33	.23	.11
r									.62	.43	.32	.17	.11	.35	.33	.23	.11
t										.43	.32	.17	.11	.35	.33	.23	.11
k											.8	.36	.28	.48	.24	.09	-.22
o												.52	.24	.42	.19	-.01	-.14
p													.37	-.12	.46	.37	-.04
l														.36	.44	.11	.31
b															.28	-.06	.01
f																.52	.33
s																	.14
e																	

those greater than 0.5, include op, oi, og, on, mi, mg, mn, mt, and fs. All correlations above 0.5 total 25 pair-wise relationships focused on the parameters c, f, g, i, k, m, n, o, p, r, s, t, u, and v.

Sample B had 25 linear relationships between the parameters, not including unique environment (u) that formed 23 unique triangles and one two-node spur. If unique environment is added, an additional 25 triangles and two spurs are added to the geometric shape – a total of 48 faces and 3 spurs. A network graph is shown in

Figure 23 that illustrates the network with all the parameters included. Figure **24** is a network graph with the parameter unique environment (u) omitted.

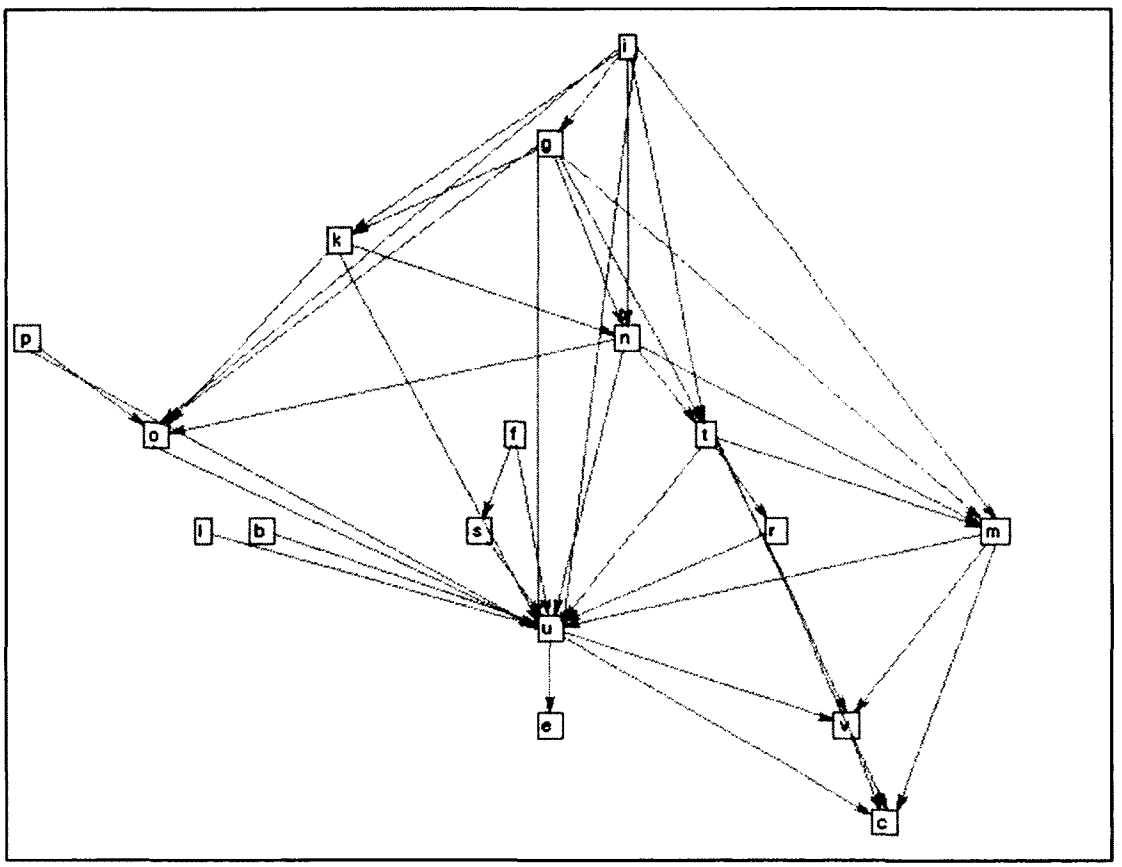

Figure 23: Sample B network graph - all parameters

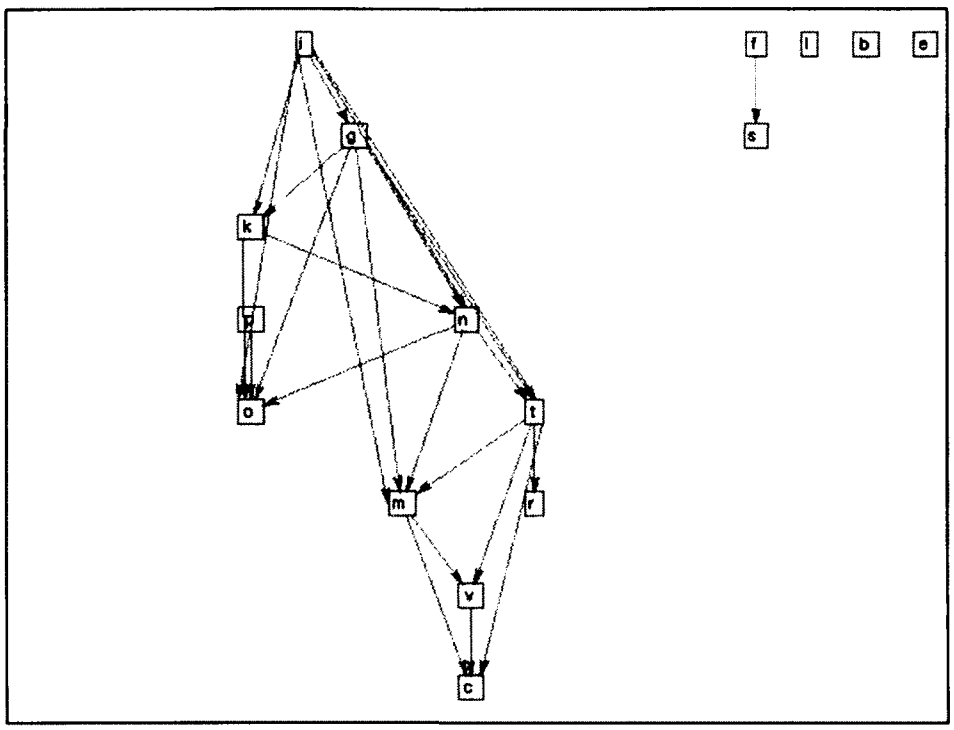

Figure 24: Sample B network graph without the parameter unique environment (u)

4.5.3. Sample B test results

Without the surface area calculations as part of the function, the test parameters were very similar, but omitted the requirement for surface area and surface area errors. Utilizing the test criteria given in Section 3.5.5, except as noted, testing was satisfactorily conducted and the results are shown in Table **14**, Table **15** and Table **16**.

Table 14: Test requirement 1.0, create geometric characteristic from a matrix results

Test Protocol	Expected		Actual		Remarks
	Nodes	Edges	Nodes	Edges	
1.0	2	1	2	1	Satisfactory
	3	2	3	2	Satisfactory
	3	3	3	3	Satisfactory
	4	3	4	3	Satisfactory
	4	4	4	4	Satisfactory
	4	5	4	5	Satisfactory
	4	6	4	6	Satisfactory

Table 15: Test requirement 3.0, given a matrix determine the sum of the edge lengths

Test Protocol 3.0		
	Sum expected	Sum returned
0, 0, 0	0	0
0, 0.5, 0	0.5	0.5
0, 0, 0.5	.5	0.5
0.5, 0, 0.5	1.0	1.0
0.5, 0.5, 0.5	1.5	1.5
0, 1, 0	1.0	1.0
0, 0, 1	1.0	1.0
1, 0, 1	2.0	2.0
1, 1, 1	3.0	3.0
1, .7, .7	2.4	2.4

Table 16: Test requirements 4.0, using special cases for the test protocol given in 3.0, determine the sum of the edges results

Test protocol: Sum of the edges	Triangle method		Network method	
	Expected	Actual	Expected	Actual
Low value test. All parameters set to zero	0	0	0	0
High value test. All parameters set to 1.0	294.0	294.0	82.0	82.0
Mid-range test. All parameters set to 0.5	147.0	147.0	41.0	41.0
Anchor test – u low. All parameters set to 0.5 except $u = 0.1$	125.8	125.8	34.6	34.6
Anchor test –u high. All parameters set to 0.5 except $u = 1.0$	173.5	173.5	49.0	49.0
Unique test – l low. All parameters set to 0.5 except $l = 0.1$	146.6	146.6	40.6	40.6
Unique test – l high. All parameters set to 0.5 except $l = 1.0$	147.5	147.5	41.5	41.5
Unique test – f low. All parameters set to 0.5 except $f = 0.1$	146.2	146.2	40.2	40.2

Table 16: (Continued)

Test protocol: Sum of the edges	Triangle method		Network method	
	Expected	Actual	Expected	Actual
Unique test – *f* high. All parameters set to 0.5 except *f* = 1.0	148.0	148.0	42.0	42.0
Unique test – *t* low. All parameters set to 0.5 except *f* = 0.1	134.2	134.2	37.8	37.8
Unique test – *t* high. All parameters set to 0.5 except *t* = 1.0	163.0	163.0	45.0	45.0
Test anchor & unique – low. All parameters set to 0.5 except *t* = 0.1 and *b* =1.0	134.7	134.7	38.3	38.3
Test anchor & unique – high. All parameters set to 0.5 except *t* = 1.0 and *b* =0.1	162.6	162.6	44.6	44.6

A graphic display of the results of the test conducted on Sample B is shown in Figure **25**. Since surface area was not computed, no scalar was used in this graph.

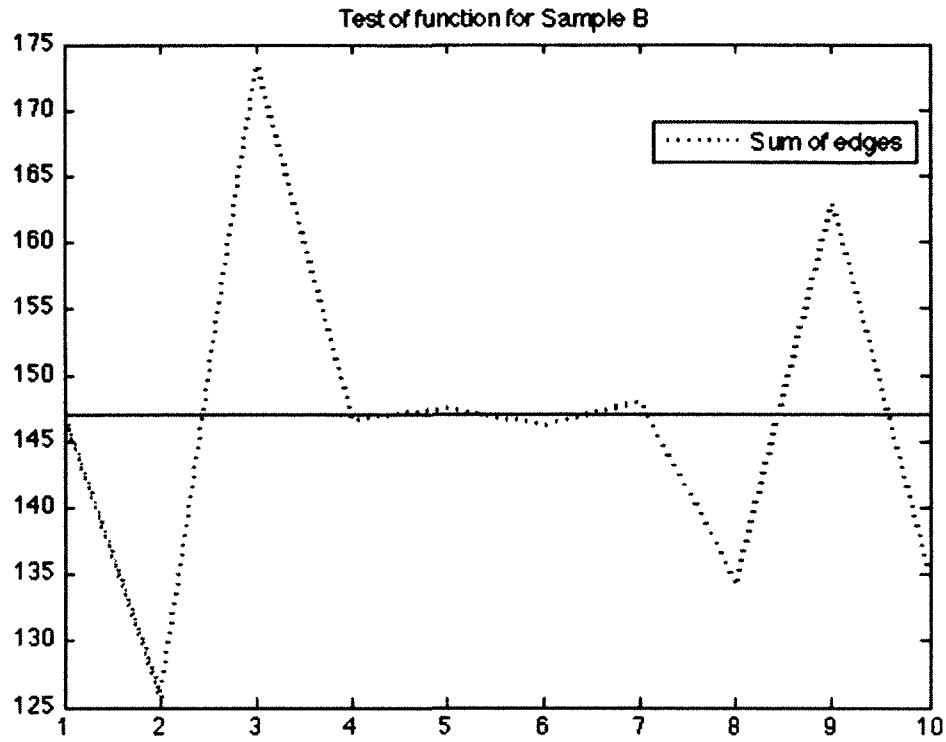

Figure 25: Test results from Sample B – triangle method

4.5.4. Results of experiment for Sample B

Sample B, consisting of 25 new cases of underwater terrorism, was submitted to the geometric structure generated by the parameters observed within the cases and the relationships between those parameters as indicated by a correlation of coefficients analysis. Figure **26** shows the sum of the edges using the triangle edge method for Sample B and Figure **27** shows the sum of the edges using the network method.

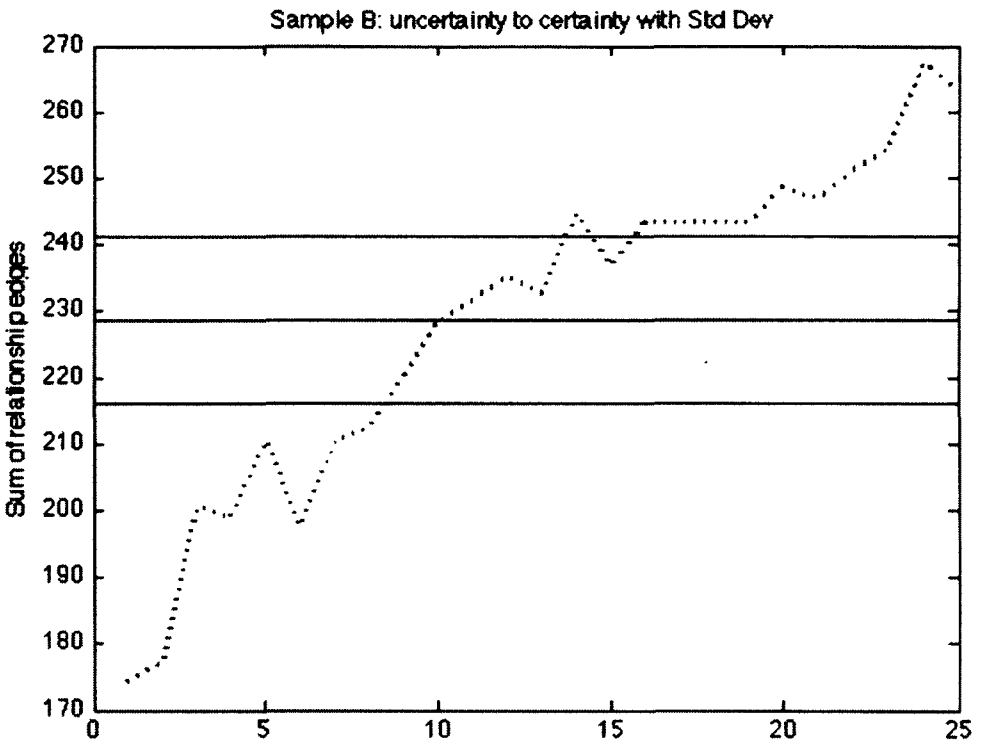

Figure 26: Sample B experimentation results - sum of edges using triangle edge method

For the sum of the edges in Sample B, the data did not exhibit integrity errors. Recall that the range of the sum of the edges for the sample space ranges from 0 to a maximum of 294 with absolute uncertainty at 147. The sample, n=25, had a maximum value of 267.5 and a minimum value of 174.3. The mean for the sample was 228.7 with a standard deviation of 25.0. The difference from absolute uncertainty to the minimum value noted in Sample B is 27.3 and the difference from the maximum value for any case in Sample B to the computed maximum for Sample B was 26.5. The values for any case in Sample B are in a band with width 93.2. Nineteen of the 25 (76%) of the cases were outside of the standard deviation with eight below and 11 above.

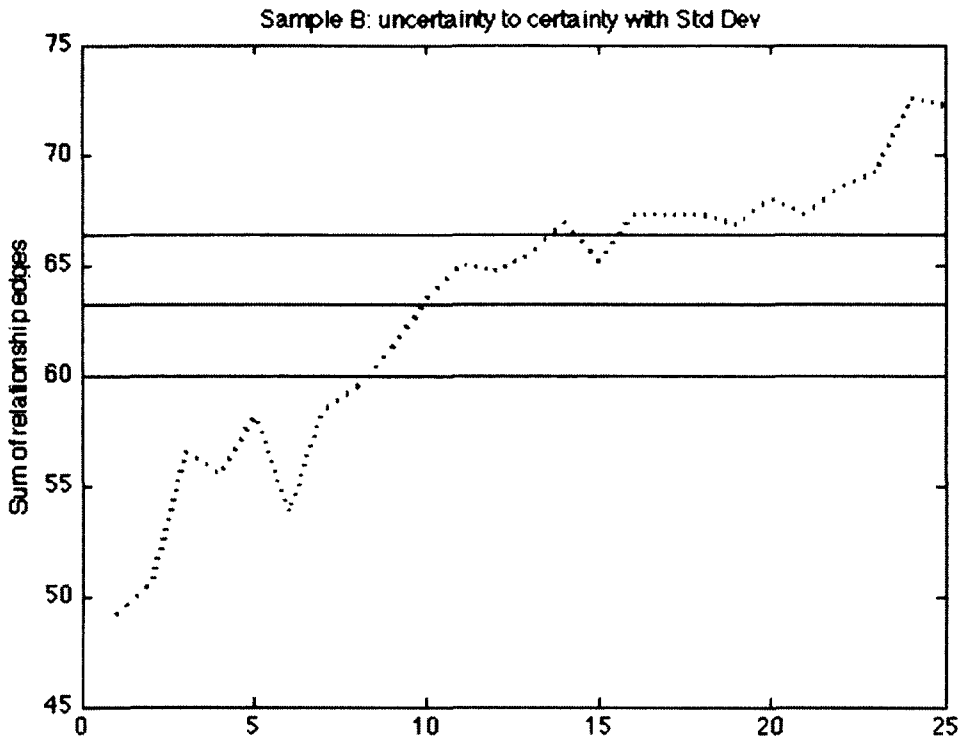

Figure 27: Sample B's experimental results - sum of edges using network method

For the sum of the edges in Sample B, the data did not exhibit integrity errors. Recall that the range of the sum of the edges for the sample space ranges from 0 to a maximum of 82 with absolute uncertainty at 41. The sample, n=25, had a maximum value of 72.5 and a minimum value of 49.2. The mean for the sample was 63.2 with a standard deviation of 6.4. The difference from absolute uncertainty to the minimum value noted in Sample B is 8.2 and the difference from the maximum value for any case in Sample B to the computed maximum for Sample B was 9.5. The values for any case in Sample B are in a band with width 23.3. Nineteen of the 25 (76%) cases were outside of the standard deviation with eight below and 11 above. A discussion of Sample B can be found in Section 0.

CHAPTER 5
CONCLUSION

This Chapter provides a discussion of the research findings following the order of the research questions. It then discusses a comparison of the two samples and examines their relationship based on the hypothesis testing. It concludes with suggestions for future research.

5.1. Discussion

This research contributed to a better understanding and management of several key areas to the risk of underwater terrorism. First, it substantiated that the current parameters used by many practitioners in the risk and intelligence community are applicable. It demonstrated that conceptually the relationship between the parameters can be determined through analytics. It established the Malice Spectrum as a tool to instantiate the values of the parameters independent from the process of the value-determination. Finally, it demonstrated the proof of concept that risk can be better understood and managed – potentially even simulated – using the geometric characteristics of the network graph of the R=TVC equation. Weaknesses in this research that directly contribute to the applicability of this research exist – specifically the use of unclassified data may have reduced the granularity of the samples potentially impacting the robust analysis of the final geometric structure based on the relationships of the risk equation. Each of these points is articulated in detail, below.

5.1.1. Parameters

The research indicates that the parameters utilized for this study, those currently used by many facets of both the risk and the intelligence communities, are pertinent and appropriate for understanding the risk equation. Given that the equation, R=TVC was only parsed for the threat element; and that each case obtained for this data samples was intentionally an underwater incident; and that each case was, at least, a small success from the adversaries point of view, withdrawing vulnerability, consequence and unique environment from the discussion is warranted. The research design was biased towards those parameters. What was intriguing is that Sample B did not have a 100% correlation

with vulnerability and consequence, although they were noted in each case. Given that the purpose of an adversary is to exploit vulnerability to cause consequence, this lack of correlation remains unexplained.

Both samples had the same parameters in the set of strongly evident parameters. In this context, evident is defined as the number of cases in which the parameter was observed across the sample. For both samples, the set of strongly evident parameters included stated goals, adversarial ideology, key resource – material and pre-operational planning. For parameters key resource – material and pre-operational planning, the strong correlation was driven by the uniqueness of the underwater environment. The special planning and movement of trained people to operate in the environment was often noted in either the databases or in the media. For the parameters stated goals and adversarial ideology, since each case was after the fact either a complete success or a partial success, the goals were known – usually by statement from the adversaries and the actual adversary, with the applicable ideology, was known. In a pre-event risk analysis, this information may be more difficult to discover.

For the weakly evident parameters, again, both samples had a similar set that included movement of people, testing, information collection and logistics. The parameters testing, information collection and surveillance can be (and has been done so by the intelligence or risk communities) grouped together as probing. The lack of probing noted within the cases does not indicate that probing did not occur but can be accounted for because either it was not recorded in the databases explicitly, it was not exciting enough to be included in the media or, if noticed, may have thwarted the attack and would therefore not have allowed the event to occur. The potential to thwart an attack by knowledge of the attack is especially true of testing. The data do not clarify if testing is being actively conducted by adversaries or if the testing that was conducted resulted in the adversaries being thwarted by law enforcement or the defender. The parameters movement of people and logistics were not usually discussed in the databases or the media sources. Several reasons may account for the omission of movement of people or logistics, ranging from the information was not available to the authors or database

managers; the information may not make exciting reading; or the information may be of such a classified nature that it was not revealed in the open sources available.

The expert solicitation validated that observing only unclassified information may have skewed the results. Specifically, finance (d) was considered to be one of the two most important variables. In discussing finance with the experts, they agreed that without finance, the adversarial organization would be unsuccessful. However, obtaining unclassified information about finance was, at best, difficult and there was not enough information available to ensure the data collected were accurate. The other dummy parameters, population index (x), criticality (y) and leadership (a) were within the expected areas on the scatter plot. Essentially, population index and criticality are element of the consequence parameter and should be evaluated in future research. Leadership, for any rational organization, is a significant parameter for analyzing the organization but frequently does not indicate the overall risk. Both leadership and finance are leading measures that impact other parameters. Leadership impacts ideology, stated goals and propaganda. Finance impacts key resource material, movement of people, logistics and potential key resource – people. The unclassified data did not provide granularity to evaluate these parameters in this research.

One parameter that was added and did not appear to be important to the experts is the unique environment. The underwater environment, although mentioned, has not received significant treatment in the literature. This environment is a difficult area to attack in or defend because of the limited visibility, magnetic anomalies, sea floor debris, harsh operating conditions, extraneous noise and the special training and equipment needed (Dobkowski, 2007; Sakhuja, 2005). The analysis, biased as it was towards the unique environment, validates to veracity that the unique environment, when it exists, must be considered. The necessity to protect material and people from water, salty or otherwise, incurs a liability on the defender to protect critical infrastructure and a liability on the adversary to mount a successful attack because of the special preparations and opportunity for detection as material, probing and training is conducted. To this point, the unique environment has been a favorable factor for the defender. However, given the hardening of other targets, this benefit may become a liability.

5.1.2. Relationships

The research demonstrated that the relationships of the risk equation can be determined through analytics. Examining the parameters with the highest number of correlations, Sample A's set was pre-operational planning, unique environment, vulnerability, consequence, movement of people, information collection, stated goals and adversarial ideology. Sample B's set was unique environment, stated goals, adversarial ideology, key resources – material, pre-operational planning and tactics, techniques and procedures. The parameter unique environment is inherent in the data since the data collection was biased towards only those cases in the underwater environment. Parameters stated goals, adversarial ideology and pre-operational planning are common to the sets and explained by the same effect as unique environment. Key resources – material is an intriguing parameter. For Sample A it had a low number of correlations and in Sample B it was correlated seven times – one of the highest number of correlations. A review of the specific cases indicates the disparity in correlations may be caused by the actual location where each case occurred. In the first sample, most of the cases occurred in ports where the adversaries lived or operated. For Sample B, most of the attacks took place where the adversaries had to move to.

The parameters with the lowest number of correlations for Sample A were testing, key resources—people, key resources – material, operational history, propaganda, training and surveillance. For Sample B, they were movement of people, testing, information collection, logistics, propaganda, training and surveillance. The parameters testing, propaganda, surveillance and training are common to both samples. Interestingly parameters movement of people, information collection and key resource – people are in the lowest number of correlations for one sample, but the highest number of correlations for the other sample. The disparity in correlation is attributed to the small sample sizes. It's expected that an aggregated analysis of the samples would resolve this disparity. The low correlation for both testing and surveillance is not surprising, for the same reason noted in Section 0. The low number of correlations for propaganda is contraindicated. Propaganda did not appear to follow ideology and goals as strongly correlated. The contradiction is a weakness in the research design – the data for ideology and goals were recorded in the databases or the media, but the source of that information (propaganda?

Intelligence?) was not available. The low number of correlations for training is not expected. Training was noted in a majority of the cases and is inherent in an attack in any unique environment. Training was assumed to have a linear relationship with the other parameters, specifically supporting exploiting a vulnerability to obtain a consequence. This exception to what was expected indicates the potential utility for this research – training was related to tactics, techniques and procedures for both samples. It verifies the veracity of the parameter relationships; in this case, that training can be used to indicate what tactics, techniques or procedures that an adversary may be planning to use.

Although Sample A had a larger sample size and larger diversity in cases, Sample B, which included a number of cases with Shayetet 13 or the Sea Shepherd Society as the adversary, had a more robust basis of verifiable information available. Potentially, Sample B is a better representation of what can be known about an organization.

Using the specific information from the analysis and applying critical thinking based upon studying each case, the known perpetrators and the tactics used, relationships are apparent that may not directly correlate to the analysis. Propaganda appears to assert an adversarial ideology and clarify the stated goals of the organization. Indications that propaganda history provides *support* for the accumulations of both key resources: people and material were observed. An adversarial ideology *elicits* tactical stated goals and indicates a desire for strategic consequence, whereas the stated goals *pursue* tactical consequences as a means to obtain strategic objectives.

People are vital to any organization. In an adversarial organization, people *enable* the employment of tactics, techniques and procedures and *utilize* the other key resource, materials, to *exploit* vulnerabilities. They are also required to conduct pre-operational planning. Pre-operational planning *determines or modifies* the tactics, techniques and procedures used. It also *determines* the required training, *coordinates* movement and logistics, and *acquires* the material key resources. Training, of course, *prepares* people for the operation.

As with any organization, an adversary learns from their past successes and mistakes through their operational history. An adversary's operational history *enables* effective propaganda and *informs* their pre-operational planning. Operational history can also be used as an *indicator* of tactics, techniques and procedures and *informs* the information collections efforts of the adversary. The key to understanding the operational history of an adversary is understanding the adversary's tactics, techniques and procedures (TTP). TTP *exploits* vulnerabilities to *accomplish* the organization's stated goals.

Reviewing the cases, there were incidents where only one form of probing was evident. Without explicitly looking for one of the three element of probing – information collection, surveillance or testing, the signs may be lost, or the relationship each has with other parameters may be understated. This research suggests that each parameter should be viewed independently. Information collection *seeks* consequences be determining, vulnerabilities and *informing the* pre-operational planning. Surveillance *modifies* an adversary's pre-operational planning by influencing the design of testing and confirming the expected vulnerabilities. Testing, which usually occurs later in the planning cycle, *reconciles* the pre-operational planning and *validates* vulnerabilities that exist for the adversary to exploit.

A successful attack cannot occur without the materials used in the attack (e.g. special equipment for underwater operations, explosives). Materials are what *enable* tactics, techniques and procedures, *act upon* the vulnerabilities of the defender and are *used for* training the people. The materials must be moved for training, assembly or for the attack via logistics. Besides moving the material, the people involved in the attack must be moved. Movement *positions* people for training, surveillance, and testing.

The unique environment of underwater operations introduces complexities with must be managed and accounted for. For this research, the unique environment accounted for the setting or conditions in which the attack was conducted. The underwater environment is unlike anything else on Earth and changes drastically from target location to target location. Operating within the confines of a heavily trafficked, cold, noisy harbor (Boston) is dramatically different from a low traffic, warm water, quiet approach to

remote infrastructure (the Florida Keys). The unique environment *requires* special training *and* materials. Because of the interaction with the environment (water flow), this unique environment *increases* the consequence of the attack. Given the restricted visibility and difficulty in securing undersea boundaries, the unique environment *impacts* vulnerability, the ability to conduct pre-operational surveillance and the ability to execute testing. The unique environment parameter can be generalized beyond the underwater environment paradigm to include other unique environment like polar operations, non-pressurized airborne attacks or sub terrarium attacks.

5.1.3. Malice spectrum

This research established the basis of the malice spectrum which instantiates the values for the parameters independent of the methods utilized to obtain those values (see Gay & Hester, 2012). Utilizing the malice spectrum provides a common scale for diverse parameters and eliminates the units of measure. Although the accuracy of determining the value of any parameter is minimal, the malice spectrum provides a level of precision that permits discrimination between cases. The analyst can add another digit to any number to increase the value over similar cases. For example, if an analyst believes three organizations have strong but similar adversarial ideologies, the analyst can assign all three a value of 0.7 or discriminate by assigning 0.7, 0.71 and 0.72 if there was some compelling reason to elevate one over another. Another strength of the malice spectrum is the ability to assign a value to a parameter that is independent of the method used to determine the parameter's score. The malice spectrum directly addresses one of the concerns noted in the introduction – that current methods force the analyst to use either statistical methods or expert opinion. Using the malice spectrum permits any method to be used and the results to be applied directly. The malice spectrum is also already aligned with the linguistic ambiguity inherent in the risk equation and is very similar to a model that is widely accepted by the intelligence community.

Conversely, the malice spectrum has two detractors. First, the malice spectrum is a subjective, vice objective, knowledge system. Instantiating the number may be influenced by personal interpretations or prejudice. The first detractor leads to the second detractor, the ability to obtain repeatability across diverse analysts. The lack of

repeatability may be mitigated by the use of job aids or training when used in a practical setting. However, enhancing repeatability through job aids or training may hamper the effectiveness of the malice spectrum, reducing the ability for the analyst to apply critical thinking in an individual, subjective evaluation.

5.1.4. Measure of risk

Research Question Four was "What is the measure of risk?" to ensure the final value had meaning to the analyst and the policy maker. The original research indicated risk would be a measure of either volume or surface area. However, the final results indicate that risk can be measured as a sum of the edges between the nodes in the geometric representation of the risk equation, essentially acting as a proxy for the volume or surface area. By using the malice spectrum, the number derived from the computations became dimensionless – regardless of the geometric formula used. The final result of any comparison between cases was just a number based on length of every individual edge that ranged in size from zero to two. In describing the final result, the use of the term *relative risk* is appropriate since the final comparison between any two, or more, cases is just comparison of a series of numbers that indicate the greater likelihood of an unfavorable occurrence.

5.2. Objective utility

Can the risk of an underwater terrorism event be understood and managed using this process? Unequivocally yes. With known cases entered according to ascending order of known values of the parameters, the output demonstrated an expected increase in value based on the relationships of the parameters. More importantly, an understanding of the nature and critical path of the risk equation is emerging from this unclassified, open source, sampling.

Using the surface area or the volume of the geometric shape to determine the final values of the relative risk of each case was not demonstrated, and in fact, was shown to be contraindicated because the triangles which form the surface areas tend to collapse or tear apart as the values of the parameters change from complete uncertainty. However, the value of the sum of the edges from the geometric shape created in a network diagram was

shown to be an effective calculation at least twice. In both samples the sum of the edges were shown to occupy a band well into the unfavorable solution space and the band was at least 18% into the unfavorable area. The band does not represent an absolute threshold of a pending event, but does indicate that a potential threshold could be calculated based on data from unsuccessful cases.

The variations in the output, the spikes and dips when the input was provide in ascending order, frequently occur where the value of the input is consistent, as shown in Figure **28**. The variations are caused by the interaction of the parameters across the relationships and provide a suggestion for a critical path to reduce overall risk through investment. If knowledge of the variations actually reduces the risk, or just reduces the numerical calculation, can only be determined by experts in the risk field.

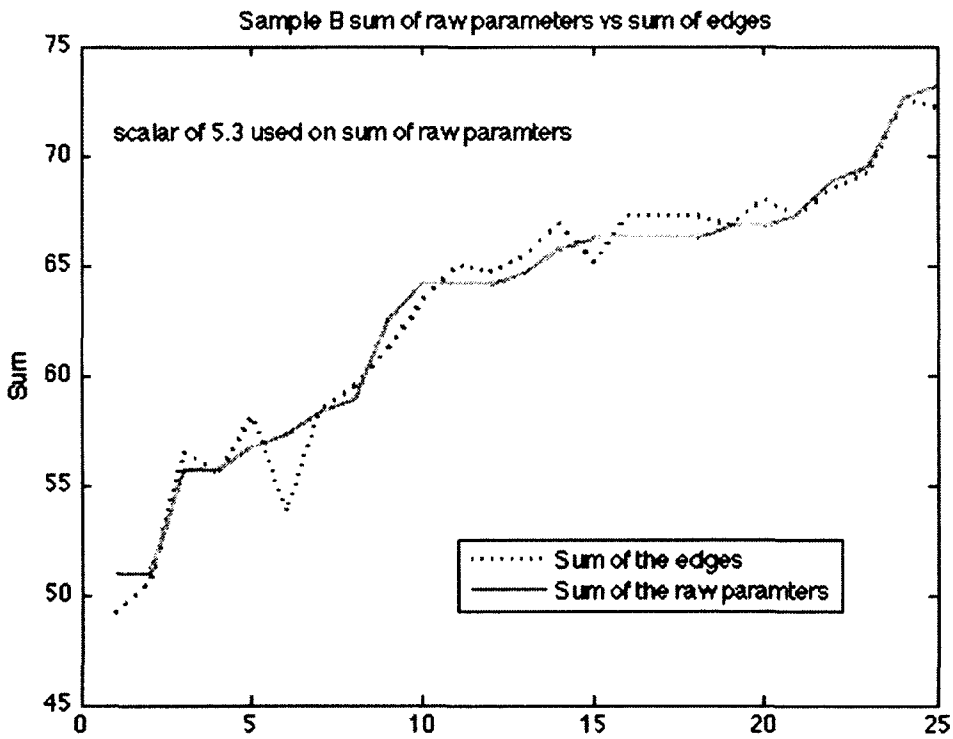

Figure 28: Comparison of Sample B's raw data to calculated relative risk

In the post analysis the data looked similar but was from two different models. Would the output from one sample on another sample's model be similar? Although not part of the original analysis, the research would not be complete without answering that question. Therefore the data for Sample B were submitted to the model created by Sample A for the sum of the edges computed by the edges of the triangles and by the edges from the network diagram. The data for Sample B were then plotted against the output from the Sample B model and is shown in Figure 29. Although the values from the Sample A model had to be scaled to plot with the results of the Sample B model, the similarity, despite the differing model and method is plainly evident. That different networks give the same relative risk solution is not surprising, since the data were linear. It does, however, indicate the processes are comparable and that the least complex solution space – the sum of the edges from the network diagram – is value added.

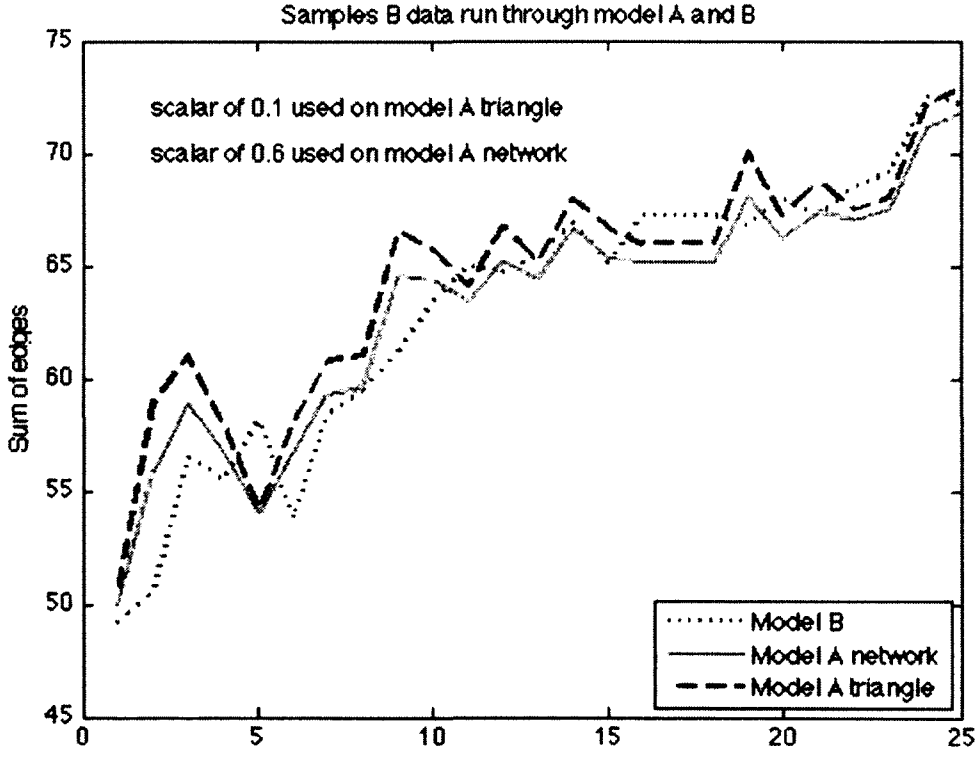

Figure 29: Sample B data through both models

5.3. Future research

Several areas for future research exist, mostly focused around the limitations already noted throughout this paper. Although obtaining declassified abstracts of classified databases may answer many of the concerns noted, true research with classified data is required to create the most comprehensive analysis of the parameters and their relationships and to establish a true threshold of concern for an event horizon. The classified data may also provide insight into the temporal relationships between the parameters and facilitate development of more robust predictive tools. Once the temporal relationships are mapped, an analysis of how the values of the parameters changed over time may indicate a better measure of risk as in incorporates the temporal dimension of the risk equation, which heretofore has been ignored.

Another area for research is consideration of combining information collection, pre-operational surveillance and testing into one parameter, perhaps called "probing". What would aggregation of these parameters do to the analysis of overall risk? Would aggregation impact intelligence analysis, risk analysis or have no impact?

The standardization of the process to determine the values of each parameter will require cross discipline research between the intelligence, security and insurance communities to develop a linguistic-based membership set which appropriately corresponds the qualitative values from the respective communities to the malice spectrum. Another concern is math doesn't take into account the linguistic spin of an evaluation. Can the integration of the mathematical analysis of the parameters with a linguistic analysis be improved? Finally, with the parameters, should any parameter be weighted?

The original vision of this research was that risk was a complex calculation similar to the volume of an icosidodecahedron, also called a Hoberman sphere, increasing as the distance between the nodes increased. Although the ability to maintain this complex concept was lost to the inability to determine an accurate geometric area, the question and vision remain. Perhaps the surface area should be based on the sum of multiple spheres with the radius of each sphere equal to one or more nodes?

The creation of a new model for each sample drawn, although relatively equivocal, does not facilitate communication across risk communities. Therefore, a detailed analysis of the combined analytics and linguistics to develop one model that will be used across the domains is required.

As Tolk (2012) noted, successful modeling and simulation requires the model to be conceptually valid, technically mature and applicable to the user; to wit, operationally applicable. This methodology, including the Malice Spectrum, has been demonstrated within this thesis to be conceptually valid and operationally applicable. However, there are several areas of technical immaturity which must be researched before utilizing the methodology in a real-time engagement. This includes connectivity to intelligence fusion networks for the collection of formatted data, integration of a data warehousing process to provide a continuous confidence level of the data and development of the process to nest (link together) various scenarios. The development of an automated algorithm to implement the Malice Spectrum that combines new input from intelligence Fusion Centers with historic trends, and expert opinion previously stored would reduce the processing time and provide a means for immediately evaluating the impact of adversarial actions on the current measured risk level. Further research into a what-if module would fully implement the system as a usable decision support system, comparable to the requirements enumerated and motivated in Tolk (2009) and will continue to improve the ability to manage and understand the risk of underwater terrorism.

5.4. Contribution

This research sought to improve the ability to manage and understand the risk of underwater terrorism by creating a model based on the relationships of the parameters in the risk equation. The research inductively examined available data to develop and analyze a list of parameters and relationships, which was used to deductively create a multi-perspective model of the risk equation. It identified parameters that provide a multi-perspective view of the underwater terrorism incident and identified the relationships between those parameters. The research developed and tested a method to quantify the qualitative variables pertinent to the underwater terrorism threat and

successfully evaluated 51 cases of underwater terrorism, developing a relative risk picture across two samples.

It explored the feasibility of using the geometric shape generated by the network graph to determine the surface area as a measure of relative risk and found that to be unrealistic because of the numerous errors in the calculations as the parameters of the risk equation changed.

This research introduced the malice spectrum as a tool to remove dimensions and disaggregate the determination process from the final value used to instantiate the values of the nodes in the network diagram.

The research explored the concept of using the surface area or the volume of the geometric shape to determine the relative risk between cases but was unable to determine an appropriate method to keep the edges from pulling apart or collapsing on itself when treating the risk equation as a geometric face. It then determined the sum of the edges of the network diagram to determine relative risk between 51 cases across two samples. It showed that this method was an effective way to understand the underlying structure of the risk of underwater terrorism and provided a framework to manage that risk.

BIBLIOGRAPHY

Abt, C. (2003). *The economic impact of nuclear terrorist attacks on freight transport systems in an age of seaport vulnerability*. Cambridge, MA: Abt Associates, Inc.

Alberts, D. S., & Hayes, R. E. (2005). *Code of best practice for experimentation*. CCRP Publication Series, Defense Technical Information Center (DTIC).

Almogy, G., & Rivkind, A. (2007, August). Terror in the 21st century: Milestones and prospects – Part I. *Current Problems in Surgery, 44*(8), 496-554.

Apostolakis, G., & Lemon, D. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Analysis, 25*, 361-376.

Argote, L. (1982, September). Input uncertainty and organizational coordination in hospital emergency units. *Administrative Science Quarterly, 27*(3), 420-434.

Attneave, F. (1959). *Applications of information theory to psychology*. New York: Holt, Rinehart & Winston.

Aven, T., & Guikema, S. (2011). Whose uncertainty assessments (probability distributions) does a risk assessment report: the analysts' or the experts'? *Reliability Engineering & Systems Safety, 96*, 1257-1262.

Ayyub, B. (2005). *Risk analysis for critical infrastructure and key asset protection: methods and challenges*. Retrieved from http://www.usc.edu/dept/create/events/2004_11_18/Risk_Analysis_for_Critical_Infrastructure_and_Key_Asset_Protection.pdf.

Barker, K., & Haimes, Y. (2008). Assessing uncertainty in extreme events: Applications to risk-based decision making in interdependent infrastructure sectors. *Reliability Engineering & System Safety, 94,* 819-829.

Bauer, M. (2002). Paranoid penguin: Practical threat analysis and risk management. *Linux Journal, 93*, 9.

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

Berman, R. (2008). *Anti-Americanism and the pursuit of politics.* Retrieved from www.princeton.edu/~ppns/papers/ berman.pdf.

Bernhardt, W. (2004, May). Bridging the uncertainty gap in intelligence analysis: a framework for systematic risk and threat assessment. *Strategic Review for Southern Africa, 26*(1), 61-92.

Bodnar, J.W. (2005, May). Making sense of massive data by hypothesis testing. In *Proceedings of 2005 International Conference on Intelligence Analysis.* McLean, VA.

Branham, Steve. (2009, May). Addressing risk in the underwater battle space – A Coast Guard perspective. *Conference proceedings of the Mine Warfare Association,* Panama City Beach, FL. Retrieved from http://www.minwara.org/ Meetings/2009_05/Presentations/wedpdf/Branham%20Mine%20Warfare%20Conference.pdf.

Bristow, M., Fang, L., & Hipel, K. W. (2012). System of systems engineering and risk management of extreme events: concepts and case study. *Risk Analysis,* in press. Epub ahead of print retrieved from http://onlinelibrary.wiley.com/ journal/10.1111/(ISSN)1539-6924/earlyview.

Brown, G., Carlyle, M., Salmeron, J., & Wood, K. (2005, November). Analyzing the vulnerability of critical infrastructure to attack and planning defenses. *Tutorials in Operations Research,* 102-123.

Chase, R. H., Day, J. A., Cline, D. D., & O'Hagan, J.G. (1995, May). *Reconnaissance, surveillance, and target acquisition collection planning--embedded within the MEF intelligence and operations cycle.* Written in fulfillment of a requirement for the Marine Corps Command and Staff College. Retrieved from http://www.fas.org/irp/eprint/dereschk.htm.

Chemers, M. (1997). *An integrative theory of leadership.* Mahwah, NJ: Erlbaum.

Chi, M. (1997). Quantifying qualitative analysis of verbal data: A practical guide. *The Journal of Learning Sciences, 6*(3), 271-315.

Clinton, W. (1998). *Presidential decision directive/NSC-63.* Washington: The White House. Retrieved from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

Cobain, I., & Karim, F. (2011, January 17). *UK linked to notorious Bangladesh torture center.* Guardian, Retrieved from http://www.guardian.co.uk/world/2011/jan/17/uk-link-bangladesh-torture-centre.

Cohen, L., Lawrence, M., & Morrison, K. (2000). *Research Methods in Education* (5th ed.). London: Routledge.

Cook, T. D., & Campbell, D. T. (1983). The design and conduct of Quasi-Experiments and true experiments in field settings. In M. Dunnette (Ed.) *Handbook of Industrial and Organizational Psychology.* New York: Wiley.

Costa, P., Herencia-Zapana, H., & Laskey, K. (2012). Uncertainty representation and reasoning for combat models. In A. Tolk (Ed.), *Engineering Principles of Combat Modeling and Distributed Simulation (*pp. 715-745). Hoboken, NJ: Wiley.

Crimes and Criminal Procedures, 18 U.S.C. 2331(1) (2006).

Critical Infrastructures Protection, 42 U.S.C. 5195c(e) (2001).

Crowe, R., & Horn, R. (1967). The meaning of risk. *Journal Risk Insurance, 34*(3): 459-74.

Daneshkhah, A. (2004). *Uncertainty in probabilistic risk assessment: A review.* Retrieved from http://www.shef.ac.uk/content/1/c6/03/09/33/risk.pdf

Darby, J. (2004). *Estimating terrorist risk with possibility theory* (LA-14179). Los Alamos, NM: Los Alamos National Laboratories.

Darby, J. (2006). *Evaluation of risk from acts of terrorism: The adversary/defender model using belief and fuzzy sets* (SAND2006-5777). Albuquerque, NM: Sandia National Laboratories.

Davis, P. (1994). Institutionalizing planning for adaptiveness. In P. Davis (Ed.), *New Challenges for Defense Planning: Rethinking How Much is Enough* (pp.73-100). Santa Monica, CA: RAND.

DefenceWire (2008). *MV Invincible/A-520 sunk.* Retrieved from http://defencewire.blogspot.com/mv-invinciblea-520-sunk.html.

Dey, I. (1993). *Qualitative data analysis: A user-friendly guide for social scientists.* New York: Routledge.

Dillion-Merrill, R., Parnell, G., & Buckshaw, D. (2009). Logic trees: Fault, success, attack, event, probability and decision trees (pp 1-22). In *Wiley Handbook of Science and Technology for Homeland Security*. Hoboken, NJ: Wiley.

Dobkowski, J. (2007, November). Using magnetic barriers to detect an underwater terrorist threat. *Sea Technology*. Retrieved from http://findarticles.com/p/articles/mi_qa5367/is_200711/ai_n21299662.

Dunn, E., Moore, M., & Nosek, B. (2007). The war of the words: how linguistic differences in reporting shape perceptions of terrorism. *Analysis of Social Issues and Public Policy*, 5(1), 67-86.

Edmonson, R. (2006, October 27). Coast Guard: Risk-Assessment Tools Aid Consistency. *Pacific Shipper*.

Fuard, A., & Kamalendran, C. (2006). *Deadly plan to blast Colombo port*. The Sunday Times. June 18. Retrieved from http://www.sundaytimes.lk/060618/news/1.html.

Garrick, B., Hall, J., Kilger, M., McDonald, J.C., O'Toole, T., Probst, P., et al. (2004). Confronting the risks of terrorism: making the right decisions. *Reliability Engineering & System Safety, 86*, 129-176.

Gay, R. J. (2006). *Quantifier risk analysis project in Excel®*. Unpublished Masters project for the U.S. Coast Guard Atlantic Area Office of Intelligence, Old Dominion University, Norfolk, VA.

Gay, R. J., & Hester, P.T. (2010). Modeling risk – it's not a probability, it's a polyhedron. *Proceedings of Huntsville Simulation Conference 2010*, Huntsville, AL, October 26-28.

Gay, R. J., & Hester, P.T. (2012). Modeling risk as a polyhedron. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 1-8*, pps (in press).

Gay, R. J. (2012). Key factors in managing and understanding the risk of underwater terrorism. *Proceedings of SpringSim 2012; Emerging Applications of M&S in Industry and Academia*, Orlando, FL, March 26-28.

Gendar, A., Alpert, L., & Parascandola, R. (2010). Terrorist threat on United States still real, warns Attorney General Eric Holder. *New York Daily News*, December 22.

Retrieved from http://www. nydailynews. com/news/national/2010/ 12/22/2010-12-22_terrorist_threat_on_united_ state_still_real_warns_attorney_general_eric_holder.html.

Gladwell, M. (2008). *Outliers: The story of success*. New York: Little, Brown & Co.

GlobalSecurity.org. (n.d.). *USS Cole Bombing*. Retrieved March 18, 2008, from http://www.globalsecurity.org/security/profiles/uss_cole_bombing.htm.

Greenberg, M., Chalk, P., Willis, H., Khilko, I., & Ortiz, D. (2006). *Maritime terrorism: Risk and liability*. Santa Monica, CA: RAND Center for Terrorism Risk Management Policy.

Guikema, S. (2012). Modeling intelligent adversaries for terrorism risk assessment: some necessary conditions for adversary models. *Risk Analysis, 32*:7, 1117-1121.

Gupta, D. (2005, September). Toward an integrated behavioral framework for analyzing terrorism: individual motivations to group dynamics. *Democracy and Security.*

Haimes, Y., & Horowitz, B. (2004). Modeling interdependent infrastructures for sustainable counterterrorism. *Journal of Infrastructure Systems, 10*(2), 33-41.

Haimes, Y. (2002). Roadmap for modeling risks of terrorism to the homeland. *Journal of Infrastructure Systems, 8*(2), 35-41.

Haimes, Y. (2004). *Risk modeling, assessment, and management* (2nd ed.). Hoboken, NJ: Wiley.

Hasslinger, K. (2008, March). Undersea warfare: The hidden threat. *Armed Forces Journal*. Retrieved from http://www.afji.com/2008/03/3463927.

Healy, M., & Perry, C. (2000). Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. *Qualitative Market Research – An International Journal, 3*(3), 118-126.

Hedges, M., & Karasik, T. (2010). *Evolving terrorist tactics, techniques and procedures (TTP) migration across South Asia, Caucasus and the Middle East*. INEGMA Special Report No. 7. Institute of Near East and Gulf Military Analysis (INEGMA).

Hellström, T. (2007). Critical infrastructure and systemic vulnerability: Towards a planning framework. *Safety Science, 45*, 415-430.

Helton, J., Johnson, J., Oberkampf, W., & Salaberry, C. (2006). Sensitivity analysis in conjunction with evidence theory representations of epistemic uncertainty. *Reliability Engineering & System Safety, 91*, 1414-1434.

Hill, F. (1993). Research methodology and the management disciplines: The need for heterogeneity. *Irish Journal of Management, 14*(2), 46-57.

Hill, F. (2004). Attacking Asymmetrical Warfare Simulation Issues. *Conference proceedings from the 2004 Spring Simulation Interoperability Workshop (SIW). Simulation Interoperability Standards Organization.* Arlington, VA. Retrieved from http://www.sisostds.org/index.php?tg=articles&idx=More&article=126&topics=58.

Holmgren A. (2004). *Vulnerability analysis of electrical power delivery networks,* (TRITA-LWR LIC 2020). Stockholm: Department of Land and Water Resources Engineering.

Horowitz, B., & Haimes, Y. (2003). Risk-based methodology for scenario tracking, intelligence gathering, and analysis for countering terrorism. *System Engineering, 6*(3): 152-169.

Huitt, W. (1998). Critical thinking: An overview. *Educational Psychology Interactive.* Valdosta, GA: Valdosta State University. Retrieved from http://chiron.valdosta.edu/whuitt/col/cogsys/critthnk.html.

IAEA (2003). *Security of radioactive sources, interim guidance for comment.* Vienna: Radiation Safety Section, IAEA.

ISO Guide 73:2009 (2009). *Risk management vocabulary.* Geneva: International Organization for Standardization.

Indiana Intelligence Fusion Center. (n.d.). *8 signs of terrorism.* Retrieved from http://in.gov/iifc/2331.htm.

International Journal of Critical Infrastructures (2004). IJCIS Leaflet. Retrieved from https://www.inderscience.com/www/IJCIS_leaflet.pdf.

Jaeger, C. (2002, November/December). Vulnerability assessment methodology for chemical facilities (VAM-CF). *Chemical Health & Safety*, 15-19.

Jenelius E., Petersen T., & Mattson, L-G. (2006). Importance and exposure in road network vulnerability analysis. *Transportation Research, 40*(7), 537-560.

Jha, M. (2009, March). Dynamic Bayesian network for predicting the likelihood of a terrorist attack at critical transportation infrastructure facilities. *Journal of Infrastructure Systems, 15*:1(31), 31-39.

Johnson, J., Khater, M., & Kuzak, D. (2005). Critical facility terrorist risk assessment and estimates of nation-wide terrorism risk, *Symposium on Terrorism Risk Analysis,* Los Angeles, CA: University of Southern California. Retrieved from http://www.usc.edu/dept/create/events/2004_11_18/Critical_Facility_Terrorist_Risk_Assesment_and_Estimatess_of_Nationwide_Terrorism_Risk.pdf.

Joint Doctrine Division. (2010, as amended through May 15, 2011). *DOD dictionary of military and associated terms* (JP 1-02). Defense Technical Information Center. Retrieved from: http://www.dtic.mil/doctrine/new_pubs /jp1_02.pdf/.

Jonas, J., & Harper, J. (2006, December 11). Effective counterterrorism and the limited role of predictive data mining. *Policy Analysis (584).* CATO Institute.

Jones, E., Lyford, J., Qazi, M., Solan, N., & Haimes, Y. (2003). Virginia's critical infrastructure protection study. In M. Jones, B. Tawney, & K. White Jr. (Eds.) *Proceedings of the 2003 Systems and Information Engineering Design Symposium* (pp. 177-182). Blacksburg, VA. Retrieved from http://www.sys.virginia.edu/sieds03/proceed2003/proceedings/B303.pdf.

Jorion, P. (2001). *Value at risk: The new benchmark for managing financial risk.* New York: McGraw-Hill Professional.

Kaplan, S. (2002). Applying the general theory of Quantitative Risk Assessment (QRA) to terrorism risk. In *Risk-Based Decision Making in Water Resources* (pp. 77-81). American Society of Engineers.

Kaplan, S., & Garrick, B. (1981). On the quantitative definition of risk. *Risk Analysis, 1*(1). 11-27.

Kelly, D., & Smith, C. (2009). Bayesian inference in probabilistic risk assessment – The current state of the art. *Reliability Engineering & System Safety, 94,* 628-43.

Kent, S. (1964). Words of estimative probability (unclassified 22 Feb 1993). *Studies in Intelligence,* Fall, 49-65. Retrieved from https://198.81.129.141/library/center-for-the-study-of-intelligence/kent-csi/vol8no4/pdf/v08i4a06p.pdf.

Kessel, R. (2007, June 5-7). Protection in ports: Countering underwater intruders. *UDT Europe, Undersea Defence Technology Europe,* Naples, Italy. Reprinted in NURC-PR-2007-005.

Kesselman, R. (2008). Verbal probability expressions in National Intelligence Estimates: A comprehensive analysis of trends from the 1950's to Post 9/11. *International Studies Assoc 49th Annual Convention: Bridging Multiple Divides*, San Francisco. March 26, 2008.

King, G., Keohane, R., & Verba, S. (1994). *Designing social inquiry: Scientific inference in qualitative research.* Princeton: Princeton University Press.

Koonce A., Apostolakis, G., & Cook, B. (2008). Bulk power grid risk analysis: Ranking infrastructure variable according to their risk significance. *International Journal of Electric Power & Energy Systems, 30*(3), 169-183.

Krauss, Steven E. (2005). Research paradigms and meaning making: a primer. *The Qualitative Report, 10*(4), 758-770

Kushma, J., & Rubin, C. (2009). Focal points in homeland security/emergency management research and practice. *Journal of Homeland Security & Emergency Management, 6*(1): art 30.

Laqueur, W. (1999). *The new terrorism: Fanaticism and the arms of mass destruction.* New York: Oxford University Press.

Lee, A., & Baskerville, R. (2003). Generalizing generalizability in information systems research. *Information System Research, 14*(3), 221-243.

Lempert R., Popper, S., & Bankes, S. (2003). *Shaping the next one hundred years: New methods for quantitative, long-term policy analysis* (MR-1626-CR). Santa Monica, CA: RAND Corporation.

Levitin, G., & Ben-Haim, H. (2008). Importance of protections against intentional attacks. *Reliability Engineering & System Safety, 93*, 639-46.

Linebarger, P. (1954). *Psychological warfare.* Washington, D.C.: Combat Forces Press.

Lipshitz, R., & Strauss, O. (1997). Coping with uncertainty: A naturalistic decision-making analysis. *Organizational Behavior and Human Decision Processes, 69*(2), 149-163.

Lipton, E. (2005, February 20). *Audit Faults US for its spending on port defense.* (correction appended). New York Times. Retrieved from http://www.nytimes.com /2005/02/20/politics/20secure.html.

Liu, Y-Q., Chen, Y-W., Gao, F., & Jiang, G-P. (2005). Risk evaluation using evidence reasoning theory. *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics.* Guangzhou, 2855-2860. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01527429.

Lorenz, A. (2007). *Al Qaeda's maritime threat.* Intelligence and Terrorism Information Center at the Israel Intelligence Heritage & Commemoration Center. Retrieved from http://www.ict.org.il/apage/11847.phpApril15,2007.

Luce, R., & Raffia, H. (1957). *Games and decisions.* New York: Wiley.

Lueck, G. A., & Spurlock, D. (2003). Research methods in engineering management: Approaches to studying people. *ASEM 24th National Conference Proceedings.* St. Louis, 458-462. Retrieved from http://www.gbv.de/dms/tib-ub-hannover/379932199.pdf.

Macgill, S., & Siu, Y. (2005). A new paradigm for risk analysis. *Futures, 37,* 1105-1131.

Magee, J. (1961). *General insurance* (6th ed.) Homewood, Illinois: Richard D. Irwin.

Maritime Transportation Security Act of 2002 (MSTA). (2002). US Public Law 107-295, Nov. 25, 2002.

Medalia, J. (2005). *Terrorist nuclear attacks on seaports: Threat and response* (Congressional Report No. RS21293) Updated January 24, 2005. Washington DC: Library of Congress Congressional Research Service.

Meehl, P. (1978). Theoretical risks and tabular asterisks: Sir Karl, Sir Ronald and the slow progress of soft psychology. *Journal of Consulting & Clinical Psychology, 46,* 806-834.

Mendenhall, W., & Sincich, T. (1995). *Statistics for Engineering and the Sciences* (4th ed.). Upper Saddle River, NJ: Prentice Hall.

Miller, G. (1953). What is information measurement? *American Psychologist, 8,* 3-11.

Möller, N., & Hansson, S. (2008). Principles of engineering safety: Risk and uncertainty reduction. *Reliability Engineering System Safety, 93,* 776-83.

Moteff, J. (2004). *Risk management and critical infrastructure protection: Integrating and managing threats, vulnerabilities and consequences* Congressional Report No. RL32561). Washington, DC: Library of Congress Congressional Research Service.

Moteff, J., Copeland C., & Fischer J. (2003). *Critical infrastructures: What makes an infrastructure critical?* Report to Congress. Washington, D.C.

NATO SAS-026,039. (2002). *NATO code of best practice for C2 assessment.* CCRP Publication Series, Defense Technical Information Center (DTIC).

National Intelligence Estimate (July, 2007). The terrorist threat to the US Homeland. *National Intelligence Council*, Washington, DC.

Outhwaite, W. (1983). *Concept formation in social science*. London: Routledge.

Ozeren, S.; Gunes, I., & Al-Babayneh, D. M., (Eds.) (2007). Understanding terrorism: Analysis of sociological and psychological aspects. *Proceedings of the NATO Advanced Research Workshop on Sociological and Psychological Aspects of Terrorism*, Washington, D.C., 8-9 September 2006. Netherlands: IOS Press.

Pappalardo, Joe (2009, October). 3 new ways the U.S. Navy will fight underwater terrorism. *Popular Mechanics*. Retrieved from http://www. popularmechanics.com/technology/military/4249315.

Parnell, G., Smith, C., & Moxley, F. (2010). Intelligent adversary risk analysis: A bioterrorism risk management model. *Risk Analysis, 30*(1), 32-48.

Pate-Cornell, E. M. (2005). Risks of terrorist attacks: Probabilistic assessment and use of intelligence information. *Symposium on Terrorism Risk Analysis, University of Southern California*. Los Angeles, CA.

Patterson S., & Apostolakis G. (2006). Identification of critical locations across multiple infrastructures for terrorist actions. *Reliability Engineering & System Safety, 92*, 1183-1203.

Pfeffer, I. (1956). *Insurance and economic theory*. Homewood, Illinois: Richard D. Irwin.

Philippe, J. (2001). *Value at risk: The new benchmark for managing financial risk.* New York: McGraw-Hill.

Propaganda. (2011). In *Merriam-Webster.com*. Retrieved from http://www.merriam-webster.com/dictionary/propaganda.

RAND Worldwide Terrorism Incident Database (RWTID). Retrieved from http://rand.org/ise/projects/terrorismdatabase/ .

Rao, K., Kushwaha, H., Verma, A., & Srividya, A. (2007). Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies. *Reliability Engineering & System Safety, 92*, 947-56.

Reid, E. F., & Chen, H. (2007). Mapping the contemporary terrorism research domain. *International. Journal of. Human-Computer Studies, 65*, 42-56.

Richardson, M. (2004). *A time bomb for global trade: Maritime-related terrorism in an age of weapons of mass destruction.* Singapore: Institute of Southeast Asian Studies.

Roland, H., & Moriarty, B. (1983). *System safety and engineering management*. New York: Wiley.

Roper, C. (1999). *Risk management for security professionals*. London: Butterworth-Heinemann.

Rosenthal, R. (2002). The Pygmalion effect and its mediating mechanisms. In J. Aronson (Ed.). *Improving Academic Achievement, Impact of Psychological Factors on Education* (pp. 25-36). San Diego: Elsevier.

Rothschild, C., McLay, L., & Guikema, S. (2012). Adversarial risk analysis with incomplete information: A level-k approach. *Risk Analysis, 32*(7), 1219-1231.

Runkel, P., & McGrath, E. J. (1972). *Research on human behavior: A systematic guide to method.* New York: Holt, Rinehart & Winston.

Saito, T., Guthmuller H., & DeWeert, M. (2005, April). Port and Harbor Security, (UCRL-JRNL-208854). *OE Magazine*, 15-17.

Sakhuja, V. (2005). Terrorist's underwater strategy. *Institute of Peace and Conflict Studies, art 1679*. Retrieved from http://www.ipcs.org/Terrorism_kashmirLevel2.jsp?action=showView&kValue=1692&subCatID=1014&status=article&mod=g.

Samson, S., Reneke, J., & Wiecek, M. (2009). A review of different perspectives on uncertainty and risk and an alternative modeling paradigm. *Reliability Engineering & System Safety, 94*, 558-567.

Schmid, A., & Jongman, A. (1988). *Political terrorism: A new guide to actors, authors, concepts, databases, theories, and literature* (2nd ed.). New Brunswick, NJ: Transaction.

Shannon, C., & Weaver, W. (1949). *The mathematical theory of communication.* Urbana, IL: University of Illinois Press.

Shemmings, D. (2006). Quantifying qualitative data: An illustrative example of the use of Q methodology in psychosocial research. *Qualitative Research in Psychology, 3*(2), 147-165.

Shigemoto, K. (2002). Weber-Fechner's Law and demand function. *Tezukayama Academic Review, 9*, 41-46.

Smelser, N. J. & Baltes, P. B. (2001). *International encyclopedia of the social and behavioral sciences.* Amsterdam; New York: Elsevier, 15105-15106.

SRI International (2007). *PRIME: A PMESII (political, military, economic, social, infrastructural and informational) model development environment. AFRL-RI-RS-TR-2007-281.* Rome, New York: US Air Force Research Laboratory.

Steinberg, A. (2005). Threat assessment technology development. In A. Dey, B. Kokinov, D. Leake & R. Turner (Eds.), *Modeling and using context* (pp. 490-500). Berlin: Springer.

South Asia Terrorism Portal (2010). *Suicide attacks by the LTTE.* Retrieved from http://www.satp.org/satporgtp/countries/shrilanka/database/data_suicide_killings.htm.

STRATFOR (2005, September 29). *Vulnerabilities in the terrorist attack cycle.* Retrieved from http://www.stratfor.com/vulnerabilities_terrorsit_attack_cycle.

Suzić, R. (2005). A generic model of tactical plan recognition for threat assessment. In V. Dasarathy, (Ed.), *Proceedings of SPIE, 5813, Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications,* Orlando, FL (pp. 105-116). Bellingham: SPIE.

Thompson, J. D. (2006). *Organizations in action: Social science bases of administrative theory.* 4th printing. New Brunswick, NJ: Transaction Publishers.

Tolk, A. (2009). Using simulation systems for decision support. In A. T. & El Sheikh (Eds.), *Handbook of Research on Discrete Event Simulation Environments: Technologies and Applications* (pp. 317-336). Hershey, PA:IGI Global.

Tolk, A. (2012). Challenges of combat modeling and distributed simulation. In A. Tolk (Ed.), *Engineering Principles of Combat Modeling and Distributed Simulation* (in press). New York:Wiley.

Underwater Defence Technology (2010). *UDT Asia Conference and Exhibit, Singapore, Conference themes.* Retrieved from http://www.udt-asia.com/page.cfm/Link=41/t=m/goSection=3.

U.S. Army (1985). *Field Manual 700-80, Logistics.* Department of the Army.

U.S. Army (2011). *Field Manual 3-0, change 1, Operations.* Department of the Army.

U.S. Nuclear Regulatory Commission (NRC) (2008). *Threat assessment.* Retrieved from http://www.nrc .gov/security/domestic/phys-protect/threat.html.

Vasan, R. S. (2008a). *Incident Analysis: sinking of SLN Dvora craft on 22nd March 2008.* South Asia Analysis Group.

Vasan, R. S. (2008b). *SRI LANKA: Sinking of a 520/MV Invincible in Trincomalee.* South Asia Analysis Group.

Vidalis, S. (2004). *A critical discussion of risk and threat analysis methods and methodologies* (CS-04-03). Wales, UK: School of Computing, University of Glamorgan.

Von Winterfeldt, D., & Rosoff, H. (2005). Using project risk analysis to counter terrorism. *Symposium on Terrorism Risk Analysis*, Los Angeles CA: University of Southern California. Retrieved from http://www.usc.edu/dept/create/assets/002/51845.pdf.

Wheaton, K. & Chido, D. (2008). Words of Estimative Probability. *Competitive Intelligence Magazine*, 11(5). Retrieved from http://www.scip.org/Publications/CIMArticleDetail.cfm?ItemNumber=5813.

Wiener, N. (1948). *Cybernetics.* New York: Wiley.

Willett, A. (1901). *The economic theory of risk and insurance*, (1951 printing). Philadelphia, University of Pennsylvania Press.

Willis, H., Morral, A., Kelly, T., & Medby J. (2005). *Estimating terrorism risk*. Santa Monica, CA: RAND Center for Terrorism Risk Management Policy.

Woo, G. (1999). *The mathematics of natural catastrophes*. London: Imperial College Press.

Woo, G. (2002). Quantitative Terrorism Risk Assessment. *Journal of Risk Finance, 4*(1), 7-14.

Yin, R. (1994). *Case study research: Design and methods* (2nd ed.). Thousand Oaks, CA: Sage.

Yu, W., & Harris, T. (2009). Parameter uncertainty effects on variance-based sensitivity analysis. *Reliability Engineering & System Safety, 94*, 596-603.

Zhang, L., Mitchell, B., Falzon, L., Davies, M., Kristensen, L., & Billington, J. (2001). Model-based operational planning using coloured petri nets. *6th International Command and Control Research and Technology Symposium*. Annapolis, MD. Retrieved from http://www.dodccrp.org/events/6th_ICCRTS/Tracks/Papers/Track3/054_tr3.pdf.

Zimmerman, R. (2005). Outside of the box: Indicator-based assessments for terrorist attacks against critical infrastructure. *Terrorism Risk Analysis*, Los Angeles, CA: University of Southern California. Retrieved from http://www.usc.edu/dept/create/events/2004_11_18/Outside_of_the_box_indicators_based_assessments_for_terrorist_attacks_against_critical_infrastrucutre.pdf

APPENDIX A

OPERATIONAL DEFINITIONS

Concept	Variable	Operational definition
Risk	R	R = Threat * Vulnerability * Consequence
Threat	T	T = Intent * Capability * Activity
Intent	I	I = Propaganda * Stated Intention * Adversarial ideology
Capability	C	C = Tactics, techniques & procedure * Operational history * key resources (people) * key resources (material)
Activity	A	A = Logistics * Movement of people * Surveillance * Information collection * Testing
Propaganda	p	Propagating ideas and/or information for the purpose of assisting the adversary's cause or to damage the defender's cause
Adversarial ideology	i	The beliefs that guide a group in opposition to the Defender's ideology or values
Stated goals	g	The explicitly declared results desired that the adversary is working towards.
Key resource – people	k	The people directly involved in conducting the attack, including those that build and those that deploy the weapon.
Pre-operational planning	n	The process of developing plans to achieve an operational goal.
Operational history	o	The past operations conducted by the adversary.
Tactics, techniques and procedures	t	People working together in non-prescriptive methods or by following common methodologies.
Pre-operational surveillance	s	Observing a target to determine strengths, weaknesses and forces available.
Key resources – material	m	The acquisition of supplies necessary to conduct operations.
Logistics	l	The movement of material.
Movement of people	b	The change of physical location of people to accomplish tasks.

Training	r	Any intervention meant to teach a person a particular skill or behavior related to adversarial conduct.
Unique environment	u	The setting or conditions in which the attack will be conducted in or access to the Defender through.
Testing	e	Adversarial actions intend to provoke an observable response to an aggressive stimulus.
Information collection	f	Collecting information on a person or facility to assist in pre-operational planning.
Vulnerability	v	"The set of critical infrastructure-specific opportunities available for an adversary to exploit in conducting operations, including reconnaissance and operational attacks" (Gay & Hester, 2010).
Consequence	c	"The total subjective value of damage inflicted as the result of an attack on critical infrastructure" (Gay & Hester, 2010)

APPENDIX B
DATA COLLECTION PLAN

Justification

The purpose of this data collection is to determine what the parameters of an underwater terrorism incident are as an initial effort to manage and understand the risk of underwater terrorism. At the end of this collection process the answer to the first research question (*What are the parameters of an underwater terrorism incident?*) should be answered.

Data Collection Process

Initial data will be obtained, utilizing keywords, from unclassified government or educational databases available on the internet. That data will form a basis for collecting additional open source data from the internet. Open source data will require at least two independent sources to be considered valid. Additional details may require the use of interviews with analysts having access to classified data to obtain unclassified amplifying information.

Key words:

underwater	undersea	submerged	submarine
marine	maritime	aquatic	diver
limpet	UWIED		

Detailed procedure for database search:

- Identify trusted data source.
- Using individual key words, search data base.
- Download obtained data, preferably in Excel format, to home directory.
- Each successful search will be documented with the database name, date searched and key words used.
- Each successful search will be saved as a separate file using the naming convention: *databasename_keyword(date).xls.*

- Note information in the Data Collection Log.
- Copies of the files will be stored at two different locations (personal and work computers).

Detailed procedure for open source search:

- Using the initial parameters collected above, search for applicable open source records.
- Identify trusted data sources from the returned search items.
- Save applicable files to the home directory. Save in .pdf format using the author's last name as the file name.
- Note information in the Data Collection Log.
- Copies of the files will be stored at two different locations (personal and work computers).

Privacy Protection

Not applicable. No personally protected or classified data is expected to be collected.

Records Management

As noted above.

Storage & Destruction

All the data files will be saved to a CD and filed with the dissertation at Old Dominion University.

APPENDIX C

DATA COLLECTION LOG EXAMPLE

Source Name: Worldwide Incident Tracking System (WITS)
Source Type: Open source & unclassified; 2004 – 2009; Domestic & international
Date Searched: Aug 12, 2011 @ 1600

Search Term	Total hits	Usable hits	
Underwater	0		
Undersea	0		
Submerged	0		
Submarine	0		
Marine	0		
Maritime	6	0	
Aquatic	0		
Diver	1787		Exported, suspect nothing relative in collected.
Limpet	0		
UWIED	7	0	All appeared to be IED not UWIED

Files created: One spreadsheet made: WITS_Diver_AUG12.

APPENDIX D

TEST RESULTS FROM SAMPLE A

Test Protocol	Expected			Actual			Remarks
	Surface Area	Edge Length by Triangle	Network Edge Length	Surface Area	Edge Length	Network Edge Length	
Low value test. All parameters set to zero	0	0	0	0	0	0	Expected 145 calls to surfarea(), 145 surface errors returned, as expected.
High value test. All parameters set to 1.0			144	62.7868	870	144	
Mid-range test. All parameters set to 0.5			72	15.6967	435	72	
Anchor test – *n* low. All parameters set to 0.5 except *n* = 0.1			65.6	11.0275	390.2	65.6	n = u = v = c
Anchor test – *n* high. All parameters set to 0.5 except *n* = 1.0			80.0	9.6345	491.0	80.0	Area decreases because the triangle gets smaller as n increases until the two 0.5 sides are compressed against the third side.

Test Protocol	Expected			Actual			Remarks
	Surface Area	Edge Length by Triangle	Network Edge Length	Surface Area	Edge Length	Network Edge Length	
Anchor test – *u* low. All parameters set to 0.5 except *u* = 0.1			65.0	11.0275	390.2	65.0	n = u = v = c
Anchor test –*u* high. All parameters set to 0.5 except *u* = 1.0			80.0	9.6345	491.0	80.0	Area decreases because the triangle gets smaller as n increases until the two 0.5 sides are compressed against the third side.
Anchor test – *v* low. All parameters set to 0.5 except *v* = 0.1			65.6	11.0275	390.2	65.6	n = u = v = c
Anchor test – *v* high. All parameters set to 0.5 except *v* = 1.0			80.0	9.6345	491.0	80.0	Area decreases because the triangle gets smaller as n increases until the two 0.5 sides are compressed against the third side.

Test Protocol	Expected			Actual			
	Surface Area	Edge Length by Triangle	Network Edge Length	Surface Area	Edge Length	Network Edge Length	Remarks
Anchor test – *c* low. All parameters set to 0.5 except *c* = 0.1			65.6	11.0275	390.2	65.6	n = u = v = c
Anchor test – *c* high. All parameters set to 0.5 except *c* = 1.0			80.0	9.6345	491.0	80.0	Area decreases because the triangle gets smaller as n increases until the two 0.5 sides are compressed against the third side.
Unique test – *b* low. All parameters set to 0.5 except *b* = 0.1			68.4	13.2787	411.8	68.4	Unique.
Unique test – *b* high. All parameters set to 0.5 except *b* = 1.0			76.5	12.5574	464.0	76.5	29 surface errors.

Test Protocol	Expected			Actual			Remarks
	Surface Area	Edge Length by Triangle	Network Edge Length	Surface Area	Edge Length	Network Edge Length	
Unique test – *e* low. All parameters set to 0.5 except *e* = 0.1			70.0	14.8629	427	70.0	e = k = m = p = r
Unique test – *e* high. All parameters set to 0.5 except *e* = 1.0			74.5	14.6142	445	74.5	10 surface errors.
Unique test – *f* low. All parameters set to 0.5 except *f* = 0.1			68.8	13.4455	413.4	68.8	f = g = i
Unique test – *f* high. All parameters set to 0.5 except *f* = 1.0			76.0	12.7739	462.0	76.0	27 surface errors.
Unique test – *g* low. All parameters set to 0.5 except *g* = 0.1			68.8	13.4455	413.4	68.8	f = g = i

Test Protocol	Expected			Actual			
	Surface Area	Edge Length by Triangle	Network Edge Length	Surface Area	Edge Length	Network Edge Length	Remarks
Unique test – *g* high. All parameters set to 0.5 except *g* = 1.0			76.0	12.7739	462.0	76.0	27 surface errors.
Unique test – *i* low. All parameters set to 0.5 except *i* = 0.1			68.8	13.4455	413.4	68.8	f = g = i
Unique test – *i* high. All parameters set to 0.5 except *i* = 1.0			76.0	12.7739	462.0	76.0	27 surface errors.
Unique test – *k* low. All parameters set to 0.5 except *k* = 0.1			70.0	14.8629	427	70.0	e = k = m = p = r
Unique test – *k* high. All parameters set to 0.5 except *k* = 1.0			74.5	14.6142	445	74.5	10 surface errors.

Test Protocol	Expected			Actual			
	Surface Area	Edge Length by Triangle	Network Edge Length	Surface Area	Edge Length	Network Edge Length	Remarks
Unique test – *l* low. All parameters set to 0.5 except *l* = 0.1			69.2	13.9458	418.2	69.2	Unique.
Unique test – *l* high. All parameters set to 0.5 except *l* = 1.0			75.5	13.4234	456.0	75.5	21 surface errors.
Unique test – *m* low. All parameters set to 0.5 except *m* = 0.1			70.0	14.8629	427	70.0	e = k = m = p = r
Unique test – *m* high. All parameters set to 0.5 except *m* = 1.0			74.5	14.6142	445	74.5	10 surface errors.
Unique test – *o* low. All parameters set to 0.5 except *o* = 0.1			70.4	15.1964	430.2	70.4	o = s

Test Protocol	Expected			Actual			
	Surface Area	Edge Length by Triangle	Network Edge Length	Surface Area	Edge Length	Network Edge Length	Remarks
Unique test – *o* high. All parameters set to 0.5 except *o* = 1.0			74.0	15.0472	441.0	74.0	6 surface errors.
Unique test – *p* low. All parameters set to 0.5 except *p* = 0.1			70.0	14.8629	427	70.0	e = k = m = p = r
Unique test – *p* high. All parameters set to 0.5 except *p* = 1.0			74.5	14.6142	445	74.5	10 surface errors.
Unique test – *r* low. All parameters set to 0.5 except *r* = 0.1			70.0	14.8629	427	70.0	e = k = m = p = r
Unique test – *r* high. All parameters set to 0.5 except *r* = 1.0			74.5	14.6142	445	74.5	10 surface errors.

Test Protocol	Expected			Actual			
	Surface Area	Edge Length by Triangle	Network Edge Length	Surface Area	Edge Length	Network Edge Length	Remarks
Unique test – *s* low. All parameters set to 0.5 except *s* = 0.1			70.4	15.1964	430.2	70.4	o = s
Unique test – *s* high. All parameters set to 0.5 except *s* = 1.0			74.0	15.0472	441.0	74.0	6 surface errors.
Unique test – *t* low. All parameters set to 0.5 except *t* = 0.1			69.2	14.1959	420.6	69.2	Unique.
Unique test – *t* high. All parameters set to 0.5 except *t* = 1.0			75.5	13.7482	453.0	75.5	18 surface errors.
Test anchor & unique – low. All parameters set to 0.5 except *n* = 0.1 and *p* =1.0			68.1	10.2785	400.2	68.1	10 surface errors.

Test Protocol	Expected			Actual			Remarks
	Surface Area	Edge Length by Triangle	Network Edge Length	Surface Area	Edge Length	Network Edge Length	
Test anchor & unique – high. All parameters set to 0.5 except $n = 1.0$ and $p = 0.1$			78.0	9.1343	483.0	78.0	56 surface errors.
Vector too long test. Send vector of length 18. All parameters set to 0.5	MATLAB internal error handling.		As expected.				
Vector too short test. Send vector of length 16. All parameters set to 0.5	MATLAB internal error handling.		As expected.				

VITA

RICHARD J. GAY is a Commander with the United States Coast Guard serving as the Deputy Director of the Leadership Development Center at the Coast Guard Academy in New London Connecticut. He received his B.S. is Computer Engineering (1997) from George Mason University and his M.S. in Engineering Management (2006) from Old Dominion University. His research focuses on the domain of risk and celestial navigation.