A RISK ASSESSMENT METHODOLOGY FOR DIVESTING MILITARY CAPABILITIES TO ALLIED NATIONS

THESIS

Jason A. Gastelum, Captain, USAF

AFIT/GOR/ENS/06-09

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GOR/ENS/06-09

A RISK ASSESSMENT METHODOLOGY FOR DIVESTING MILTARY CAPABILITIES TO ALLIED NATIONS

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Research

Jason A. Gastelum, BS

Captain, USAF

March 2006

AFIT/GOR/ENS/06-09

A RISK ASSESSMENT METHODOLOGY FOR DIVESTING MILTARY CAPABILITIES TO ALLIED NATIONS

Jason A. Gastelum, BS
Captain, USAF

Approved:

_____	_____
David R. Denhard, Lt Col, USAF (Chairman)	date
_____	_____
Jeffery D. Weir, Lt Col, USAF (Member)	date

AFIT/GOR/ENS/06-09

Abstract

The United States spent over $400 billion dollars on national defense in 2005. Even with support for the war on terrorism still strong, it is doubtful that the U.S. can sustain such a level of defense investment. One strategy to offset the increasing burden of defense spending is to divest the procurement and/or sustainment of individual defense capabilities to allied nations. The decision to divest any capability, however, introduces risk. This thesis presents a methodology to quantify the risk of the decision to divest a military capability to an allied nation, where risk is defined as the set of risk scenarios, likelihoods and consequences possible under each decision alternative. Risk scenarios are composed of combinations of contingencies that require the capability considered for divestiture. The likelihood of each risk scenario is calculated as the product of the likelihoods of its constituent contingency events. The consequence of each risk scenario is calculated as the sum of the consequences of its constituent contingency events. Once the risk of each decision alternative is quantified this information can be used to rank alternatives and identify the scenarios that contribute most to the risk of each alternative.

Table of Contents

List of Figures

Page

List of Tables

A RISK ASSESSMENT METHODOLOGY FOR DIVESTING MILTARY CAPABILITIES TO ALLIED NATIONS

1 Introduction

1.1 Background

The United States budgeted over $420 billion dollars for national defense in 2005, almost half of its discretionary budget for the year (Department of Defense, 2004). In 2004, the U.S. defense budget exceeded the defense budget of Russia, its nearest competitor, by over $334 billion dollars. In this same year, the U.S defense budget constituted approximately 43% of entire world's military budget (Shah, 2005). Even with support for the war on terrorism still strong, it is doubtful that the U.S. can sustain such a level of defense investment in perpetuity.

One strategy to offset the increasing burden of defense spending is to divest the procurement and/or sustainment of individual defense capabilities to allied nations in order to retain capabilities for use, but without bearing the entire cost burden. Collective security relationships such as this are becoming more common as the costs of national defense escalate. For example, Australia and New Zealand are engaged in an agreement termed Closer Defense Relations in which both nations deliberately seek to avoid duplicating military capabilities in their weapon systems acquisition programs (Quigley, 2005).

Divesting a capability, however, can introduce potential risks. Will the host nation adequately procure and/or sustain the capability elements for which it is responsible? Will the host nation employ the capability when it is required? In order to

choose to divest or retain a military capability it is absolutely critical for senior decision makers to consider the risks associated with the divestiture decision.

1.2 Military Capability Defined

The Department of Defense's focus on capabilities began in earnest in 2001 when the Quadrennial Defense Review directed the Department and Services to replace the service oriented, threat-based approach to defining defense needs with a new, joint oriented, capabilities-based approach called capabilities based planning (CBP) (Department of Defense, 2001: iv-vi). Under this planning paradigm, a capability is defined as "*the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks*" (Crissman, 2002: 23).

This capabilities-based approach is radically different from the former threat-based approach in that it focuses on delivering "capabilities to meet a wide range of security challenges," instead on defeating specific enemies (Joint Defense Capabilities Study, 2003: Chapter 1, 2). In order to realize this capabilities-based paradigm, however, a shared capability lexicon is required.

This common lexicon is provided by the joint capability area framework. Under this hierarchical framework, the highest-level capabilities are partitioned into broad classes called joint capability areas (JCA). JCAs are formally defined in two levels or tiers. The 22 Tier 1 JCAs represent "collections of similar capabilities grouped at a high level in order to support decision making, capability delegation, and analysis." Below these Tier 1 JCAs are 122 Tier 2 JCAs that "capture functional and operational detail that

translates to joint task force level operations/missions." The purpose of the Tier 2 JCAs is to "scope, bound, clarify and better define the intended mission set of the Tier 1 capability category" (Crissman, 2002: 4-5). Tier 1 and 2 JCAs are presented in Figures 1.1 and 1.2.

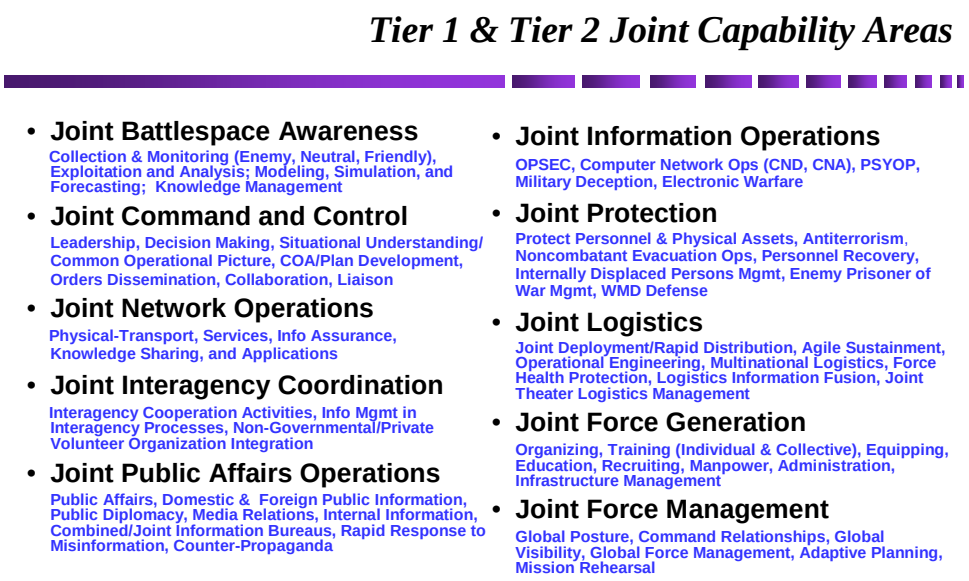

Figure 1.1 Joint Capability Areas (Crissman, 2002: 8)

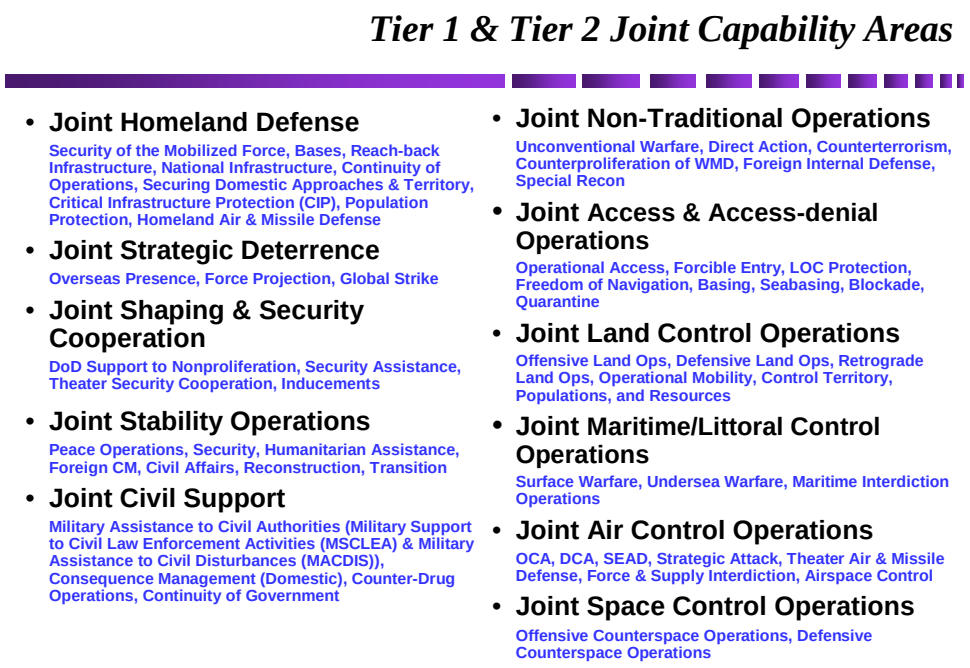

Figure 1.2 Joint Capability Areas (Crissman, 2002: 9)

Tier 2 capabilities can be linked to sets of tasks, grouped into operational templates, defined by the Uniform Joint Task List (UJTL). "The UJTL is a menu of tasks in a common language, which serves as the foundation for capabilities-based planning across the range of military operations" (Department of Defense, 2005). Each task on the UJTL can be further linked to a set of service specific tasks and ultimately, each service level task is linked to individual units. This structure is illustrated graphically in Figure 1.3.

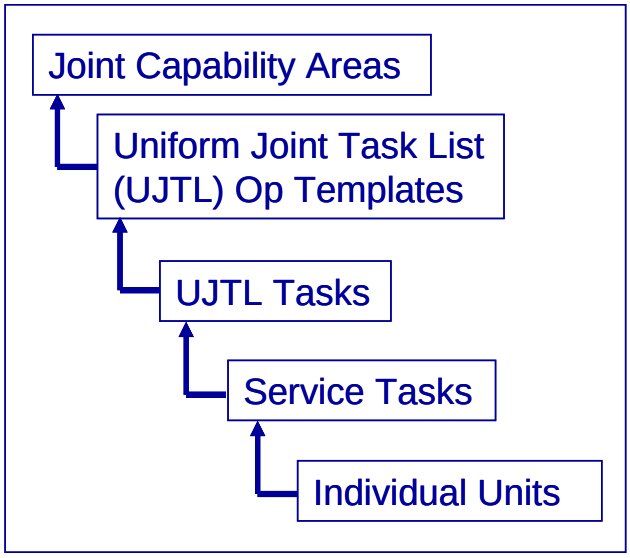

Figure 1.3 Capability Hierarchy

1.3 Quantitative Definition of Risk

In order to quantify the risk of divesting a capability, risk must also be explicitly defined. So what is risk? Risk is the property of an event, in this case a decision alternative, which indicates that the event results in a spectrum of possible consequences. These consequences can be positive or negative; however, it is the negative, or adverse, consequences that are of particular concern to decision makers.

Conventionally, risk is quantified as the answer to the following three questions (Kaplan and Garrick, 1981: 1):

- What event outcomes can happen? (i.e., What can go wrong?)
- How likely is it that a particular event outcome will happen?
- If it does happen, what are the consequences?

The answers to these questions can be presented more compactly in the following triplet.

$$Risk = \{< S_i, L_i, \mathbf{X}_i >\}_c ,$$

where:

- S_i represents the scenario,
- L_i represents the possibility of scenario s_i,
- $\mathbf{X}_i$ represents the consequence of scenario s_i,
- i is the index of the scenario, and
- c denotes that the set is complete.

Since a decision maker will likely be concerned with several different types of consequence, $\mathbf{X}_i$ is presented as a vector, each element of which represents a different type of consequence.

1.4 Problem Statement

The task of this thesis is to develop a risk assessment methodology, drawing from the strengths of current methodologies, to assess the risk associated with the decision to divest a military capability to an allied nation. The methodology presents a tractable procedure to generate the risk scenarios associated with divesting a capability and to determine the likelihood and consequence of each of these scenarios. The product of this methodology is the set of risk scenarios, likelihoods and consequences that define the risk of each decision alternative. This information can be used by decision makers to rank the decision alternatives and highlight the risk scenarios that contribute most to the risk of each alternative.

1.5 Organization

This thesis is divided into five chapters. Chapter 1 introduced the problem and provided a formal definition of capability and risk. Chapter 2 summarizes the principal risk assessment methodologies, including quantitative risk assessment (QRA), anticipatory failure determination (AFD), risk filtering, ranking and management (RFRM), and failure mode and effects analysis (FMEA). Additionally, it critiques several potential measures of risk. Chapter 3 incorporates the strongest parts of each of these methodologies to create a methodology tailored specifically to address the risk of divesting military capabilities. Chapter 4 provides a demonstration of the new methodology using notional data and Chapter 5 presents conclusions and suggests directions for further study. The notional data used in Chapter 4 is presented in the Appendix.

2 Review of the Literature

2.1 Introduction

This chapter accomplishes two tasks. First, it critiques several existing risk assessment methodologies. These include quantitative risk assessment (QRA), anticipatory failure determination (AFD), risk filtering, ranking and management (RFRM), and failure modes and effects analysis (FMEA). Second, it presents the most widely accepted methods to express and measure risk, including variance, expectation and conditional expectation.

2.2 Risk Assessment

There are two fundamental questions with regard to risk that a decision maker may be interested in answering.

- What is the spectrum of consequences, and associated likelihoods, possible under a decision alternative?
- Which scenarios contribute most to the overall risk of that alternative?

Both questions are intimately related and both are relevant to the decision to divest military capabilities. However, each question is motivated by a different decision context.

The context driving the first question is the situation in which the decision maker must choose a decision alternative. This context will be referred to as the traditional decision context. The goal of risk assessment methodologies in this context is to provide the decision maker with the entire spectrum of consequences possible for each alternative

so that this information can be used as a decision parameter, typically along with other attributes such as cost and benefit, to choose the best alternative.

The context motivating the second question is that the initial decision has already been made and the risks associated with that alternative have been assumed. This context will be referred to as the post-decision context. In this context, the task is to determine which of the scenarios of the chosen alternative contribute most to the overall risk of that alternative so that mitigating actions can be implemented. Both questions are important, and both are relevant to the decision to divest a military capability.

While there is a large body of risk assessment literature, it is primarily oriented to specific fields. The focus of this chapter, however, is to review generalized, application independent, methodologies. One consideration is that some of the risk assessment methodologies presented in this chapter only focus on certain parts of the assessment procedure. As such, they are not comprehensive methodologies. It will prove useful, however, to examine these partial methodologies, as the elements that they do address will be important components in a comprehensive risk assessment methodology. Several of the principal methodologies for each context are analyzed. Traditional decision context methodologies include QRA and AFD. Post-decision context methodologies include the RFRM and FMEA.

2.2.1 Quantitative Risk Assessment

Kaplan's QRA methodology presents a framework to quantify the risk of decision alternatives in a traditional decision context. In this context, a decision maker is

interested in quantifying the risk of the decision alternatives so that it may be considered as a one of the parameters on which to base the decision (Kaplan: 1991, 11-39).

The five steps of the QRA methodology are listed below.

1. defining the risk scenarios via the theory of scenario structuring,
2. defining the consequences for each scenario,
3. calculating the likelihood of each scenario based on Bayes' theorem,
4. aggregating the likelihood and consequence into a probability of exceedance curve, and
5. measuring risk and using the result to make a decision.

The first step in Kaplan's methodology is to identify all the possible risk scenarios. Kaplan emphasizes that generating risk scenarios is more art than science and relies heavily on the analyst's own creativity and experience. Consequently, it is impossible to present an explicit, step-by-step methodology for generating risk scenarios. However, Kaplan does propose a general theory regarding scenario generation that provides a tractable paradigm to facilitate scenario generation. This theory is called the theory of scenario structuring (TSS) and is composed of eight principles: success scenario, initiation, emanation, unending cause and effect, subdivision, pinch point, fault and event trees, and resources (Kaplan et al., 1999: 9-19).

The eight principles of TSS define a framework that yields a logical paradigm from which to generate risk scenarios and that supports the theory's ability to completely enumerate all the risk scenarios. The first principle is the principle of the success scenario. It states that in order for failure scenarios to be understood, the success, or as planned scenario, must be defined first. Typically, the success scenario is thought of as a

trajectory in state space. The principle of initiation is tied closely to this trajectory. It states that any failure is simply a deviation from the success scenario trajectory. Additionally, this deviation must occur at a specific point, which Kaplan calls the initiating event. The principle of emanation says that from each of these initiating events, an entire tree of scenarios can emerge. The deviation points within these trees are called branch points. All of the paths of the scenario trees terminate in end states. A particular path, beginning with the initiating event, through the scenario tree, and terminating at the end state, is the risk scenario. The principle of unending cause-effect states that the cause-effect chain "extends indefinitely in both directions." To make the problems tractable it is necessary to impose a finite scope on this chain. The principle of subdivision says that "every scenario that we can describe with a finite set of words is itself a set of scenarios" which means that "it can be broken down into sub-scenarios" (Kaplan et al, 1999: 13). This principle is important because, as will be discussed later in this chapter, it allows different sets of scenarios to describe the same situation. The pinch point principle says that a scenario may contain pinch points, points at which the downstream tree is independent of the upstream tree. Pinch points are simply points into which multiple paths feed. The principle of fault and event trees is simply the observation that these types of trees can be used to determine the risk scenarios. Fault trees are applicable when end states are given and event trees are applicable when initiating events are given. Additionally, both types of trees can be used when mid-states are given. The last principle is the principle of resources. The term resources denotes "all the substances, fields, configurations, time or space intervals, or other factors present in a situation." The principle states that "if all the resources necessary for an initiating

event are present in a situation, then that event will occur" and conversely, "if at least one of the necessary resources is not present, then that event will not occur" (Kaplan et al, 1999: 15).

The purpose of this set of principles is to establish a framework in which a risk scenario can be defined. In terms of these principles, a risk scenario is a particular path, beginning with the initiating event, through the scenario tree and terminating at the end state. With this definition established, it is clear there are three ways to find risk scenarios. The first is by finding all the possible initiating events and drawing outgoing event trees from each. The second is by finding all of the important end states and drawing incoming fault trees for each. The third is simply a combination of the previous two and begins with mid states from which both fault and event trees are drawn.

One of the critical requirements of a risk assessment is that the set of risk scenarios be complete. If the decision maker has not defined a complete set of scenarios then value of his analysis will be questionable because he has neglected a possible source of damage. Kaplan argues, however, that if followed with sufficiently thorough detail, TSS ensures that the set of scenarios it generates is complete. His argument is based on two of its principles, the principles of initiation an emanation. The initiation principle states that "any risk scenario must begin with an initiating event" (Kaplan: 1991, 24). Since every scenario begins with an initiating event, if the decision maker is careful enough in the process to ensure that every initiating event is generated, he needs only to develop the complete scenario trees for each of these events to account for all of the risk scenarios. Accordingly, if the decision maker is careful enough when he draws the scenario trees, being sure that "the set of branches is complete at each branch point" then

"the set of paths in the tree constitutes a complete and finite set of scenarios emerging from that initiating event" (Kaplan, 1991: 25). This implies strict fulfillment of the principle of emanation as well. If the decision maker has completely defined the set of initiating events and for each of these completely defined the scenario space, then he has completely defined the set of risk scenarios.

One common critique of risk assessment is that any scenario generating methodology cannot possibly generate all the risk scenarios. An often cited example is that if two analysts perform a risk assessment on the same system they will almost assuredly produce non-identical scenario sets. Kaplan rationalizes this inconsistency with the principle of subdivision. This principle states that "any scenario is actually a whole category of scenarios." The example that Kaplan cites is the scenario "pipe springs a leak." "There are an infinite number of kinds, and sizes, and places on the pipe where a leak can occur" (Kaplan, 1991: 24). Essentially, by defining each scenario as a set of scenarios, Kaplan relaxes the requirement that every set of scenarios for a given situation be identical. This principle holds because the risk scenarios generated in each analysis could be different, yet entirely correct, if they are simply defined at different indentures in the scenario set hierarchy. The result is that a scenario generating procedure based on the TSS principles produces a complete set of risk scenarios, even though they may not be unique.

Once the risk scenarios are generated, the next step in the QRA methodology is to determine the consequence of each risk scenario. Kaplan's methodology, however, does not present an explicit methodology to determine these consequences.

The next step is to calculate the likelihoods of the risk scenarios. The method that Kaplan proposes consists of two steps. First, algebraic parameters are assigned to each initiating event and to each branch of their respective event trees. The difficult part of the process is actually quantifying these parameters because it is unlikely that one will actually know the values of the parameters with certainty. Therefore, the parameters are represented using probability distributions. Kaplan suggests incorporating available information from subject matter experts vial Bayes' theorem.

Finally, to obtain the likelihood of each risk scenario, simply multiply the initiating frequency by each of the split fractions along that scenario's path in the scenario tree. If the tree parameters are distributions, which they will likely be, then the "arithmetic of the path equations will have to be carried out as probabilistic arithmetic" (Kaplan, 1991: 27).

Once the risk scenarios, likelihoods and consequences of a decision alternative have been assessed, the risk of the decision alternative is presented as a probability of exceedance curve. This data is then used in a utility model to rank the decision alternatives.

2.2.2 Anticipatory Failure Determination

Anticipatory failure determination is a relatively new tool in the field of risk assessment. It is not a comprehensive risk assessment methodology but focuses instead on the scenario generation step of risk assessment. The goal of AFD is to "identify, and bring to awareness, potential failure modes ("scenarios") in our systems and operations, so that they may be "fixed" before they actually occur" (Kaplan et al., 1999: 5). AFD is

an application of TRIZ, the Russian-developed theory of inventive problem solving, to risk analysis. It provides a systematic, disciplined and exhaustive method to the creative process of scenario generation.

The process AFD suggests is not innovative itself, as it shares the same foundation as the theory of scenario structuring. What AFD adds is a new paradigm in thinking about how to generate risk scenarios. The conventional question driving the search for risk scenarios has been "what can go wrong" (Kaplan and Garrick, 1981: 1). AFD turns the question around and asks "how can I cause this failure" instead. In the terminology of AFD this is called an "inventive problem." The benefit of this new, inverted paradigm is to defeat what Kaplan calls "the phenomenon of denial." This is the tendency of humans to "resist thinking about unpleasant things" (Kaplan et al, 1999: 45). When one is asked what can go wrong with a system, the tendency is to become defensive and deny or minimize the possibility of adverse consequences. If the inverted question is asked instead, the attention is placed on the offensive, proactive and creative capacity of a decision maker. By avoiding the phenomenon of denial, it is much more likely that a complete set of risk scenarios will be developed.

Kaplan partitions AFD into two types. The goal of AFD-1 is to explicitly catalog the chain of causes in a failure that has already occurred. In AFD-2, the goal is to identify all the possible failures that have not yet occurred. "In the language of the theory of scenario structuring, AFD-1 starts with a given end state or mid-state and seeks to determine the actual scenario that led to that end or mid-state. AFD-2 seeks to envision all of the possible end states, mid-states and initiating events, and all the possible scenarios leading to and from these states. Thus we can see AFD-2 incorporates multiple,

repeated applications of AFD-1" (Kaplan et al, 1999: 21). It is exactly the complete enumeration of risk scenarios in AFD-2 that a thorough risk assessment seeks to accomplish. AFD is based on the same principles as TSS and relies on similar methodologies using fault and event trees to generate scenarios so its specific implementation need not be reiterated. The overwhelming contribution of this methodology is not the mechanics of its procedure, but its inventive philosophy to generate risk scenarios under TSS.

2.2.3 Risk Filtering and Ranking Methodology

Risk filtering, ranking, and management is a comprehensive risk assessment and management methodology that "identify(ies) what can go wrong" and generates options to mitigate those risks (Haimes, 2004: 277). This type of risk assessment addresses the post-decision context and seeks to determine the most significant contributors to the risk of a decision alternative.

RFRM consists of eight phases:

1. Scenario Identification
2. Scenario Filtering
3. Bi-criteria Filtering and Ranking
4. Multi-criteria Evaluation
5. Quantitative Ranking
6. Risk Management
7. Safeguarding Against Missing Critical Items
8. Operational Feedback

In step one; Haimes uses his hierarchical holographic modeling (HHM) methodology to generate the set of risk scenarios. It is deemed 'hierarchical' because HHM is geared toward understanding what can possibly go wrong at "many different levels of the system hierarchy" (Haimes, 2004: 90). It is deemed 'holographic' because it is a multidimensional analysis of scenario structuring, rather than a single dimensional analysis akin to conventional photography.

The goal of HHM is to enumerate all the possible sources of risk. This can be quite difficult given the "multiple components, objectives and constraints of a system" not to mention the societal aspects including "functional temporal, geographic, economic, political, legal, environmental, sectoral, institutional, etc" (Haimes, 2004:90). HHM overcomes this obstacle by assessing risk scenarios from many different overlapping perspectives. Fundamental to the methodology is the belief that large-scale manmade systems have more than one single conceptual model. Each of these models is equally correct, and is necessary to adequately describe the system.

In HHM, risk scenarios are developed by decomposing the situation into broad, often overlapping perspectives or visions called head topics, and modeling the system with words according to each of these perspectives. Each subtopic can be thought of in two complimentary ways. Each subtopic is simultaneously a category of risk scenarios and a requirement for the success scenario. Figure 2.1 shows an HHM decomposition of a hypothetical aircraft development project.

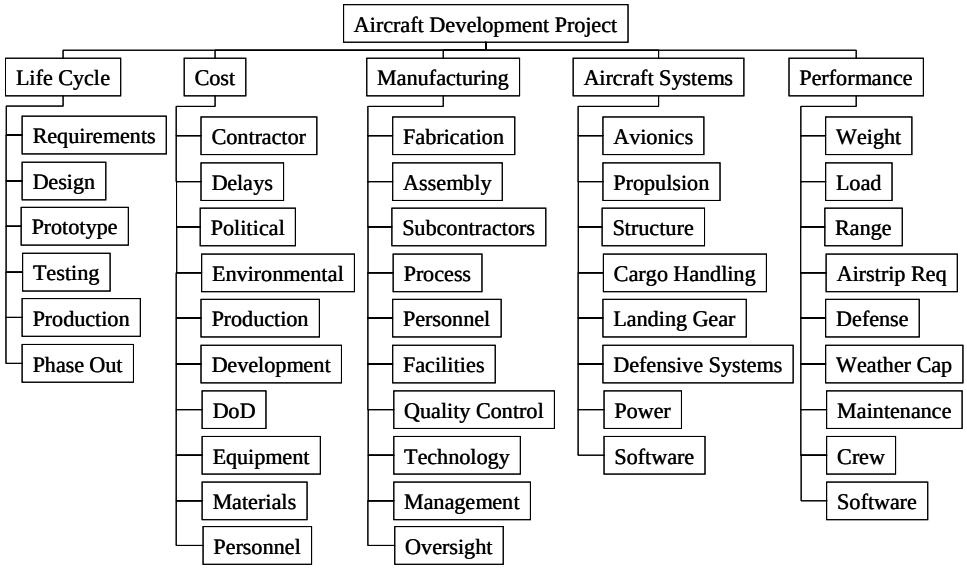

Figure 2.1 Hierarchical Holographic Modeling

The strength of HHM is that it permits multiple modeling perspectives which facilitate a more complete enumeration of the possible risk scenarios. However, since the perspectives may overlap, a risk scenario may appear in multiple decompositions of several head topics. This feature of HHM is one of the major disadvantages of the methodology. "The HHM approach divides the continuum (of risk scenarios) but does not necessarily partition it. In other words, it allows the set of subsets (of risk scenarios) to be overlapping, i.e., non-disjoint" (Haimes, 2004, 94). According to Haimes, this is not a problem if one is not required to quantify the likelihood of the scenarios, but this is what a decision maker seeks to do in a traditional-decision context. It will prove vital, then, to ensure that the risk scenarios are defined such that they are, in fact, disjoint.

Phase two filters scenarios based on scope, temporal domain, and level of decision making. This is the first of several phases that eliminates risk scenarios that are

not the primary contributors of risk. One of the fundamental premises of RFRM is that it is impractical to apply quantitative risk assessment to all of the risk scenarios (Haimes, 2004: 277). In order to create a tractable problem, RFRM filters the set of risk scenarios down to only a few scenarios that are the major contributors of risk. Phase one can generate hundreds, possibly even thousands of risk scenarios, so it is likely that not all of these scenarios will be of immediate concern to all levels of decision making and at all times. "This phase often reduces the number of risk sources from several hundred to around 50" (Haimes, 2004: 281).

Phase three also filters risk scenarios. Filtering is accomplished by plotting a risk scenario on a severity matrix and evaluating its position within the matrix. The location of the risk scenario is based on subjective expert evaluation of consequence and likelihood. Decision makers will be concerned with those risk scenarios that fall in the severe consequence or high frequency regions of the matrix. Risk scenarios that are not in these regions of the matrix are filtered.

Phase four is the final filtering phase. Filtering in this phase is based on "the ability of each scenario to defeat three defensive properties of the underlying system: resilience, robustness, and redundancy" (Haimes, 2004: 283). Haimes defines redundancy as "the ability of extra components of a system to assume the functions of failed components," robustness as "the insensitivity of system performance to external stresses," and resilience as "the ability of a system to recover following an emergency." Additionally, Haimes provides eleven criteria to assess these defensive properties. These are undetectability, uncontrollability, multiple paths to failure, irreversibility, duration of effects, cascading effects, operating environment, wear and tear, hardware, software,

human and organizational interfaces, emergent behaviors and design immaturity (Haimes, 2004: 284). The scenarios that can defeat these criteria are of paramount concern and are retained. Those scenarios that cannot defeat the criteria may be eliminated.

In phase five, the likelihood of the remaining scenarios is calculated using "Bayes' theorem and all the relevant evidence available" (Haimes, 2004: 285). These likelihoods are then input back into the risk matrix in phase three, and, if necessary, scenarios are filtered again.

Phase six is risk management. Upon completing phase five, the scenarios have been filtered down to a small, more manageable number of risk scenarios that constitute a majority of the risk to the system. In this phase one tries to answer the questions "What can be done, and what options are available?" and "What are the associated tradeoffs in terms of costs, benefits and risks?" (Haimes, 2004: 285). The goal of this phase is to generate a set of options to mitigate the most severe risks.

Phase seven is concerned with safeguarding against missing critical items. In phases two through five, potential risk scenarios were eliminated via filtering. But Haimes' methodology has only suggested options to mitigate those most severe scenarios that have been retained. The potential exists that some of these mitigating options may conflict with one of the eliminated scenarios. This phase "ascertains the extent to which the risk management options developed in phase six affect or are affected by any of the risks scenarios discarded in phases two to five" (Haimes, 2004: 287). If the options conflict with the eliminated scenarios then appropriate revisions to the options generated in phase six must be accomplished.

Finally, phase eight provides operational feedback. As new sources of risk develop, their potential effects should be considered and new mitigation options generated if necessary.

2.2.4 Failure Modes and Effect Analysis

Like RFRM, failure mode and effects analysis addresses the post-decision context and seeks to determine which of the risk scenarios contribute most to the total risk of a decision alternative. The FMEA process is typically used in industry, "during the conceptual and initial design phases of the system in order to assure that all the failure modes have been considered and proper provisions have been made to eliminate these failures" (Rausand, 5: 2004). In this setting, the implied decision context is that the decision to initiate a project has been chosen and the decision maker is now concerned with determining which of the risk scenarios contribute most to the risk of that decision. According to Rausand, the process consists of the following steps:

1. identifying the components of the system,
2. identifying the potential failure modes of the components (risk scenarios),
3. determining the effects the failures have on the system (consequences) and the likelihood of those effects (likelihood), and
4. ranking the scenarios (Rausand, 3: 2004).

The initial step is to determine the components of the system and the functions of each of its components. This step begins by defining the system of interest. Information about the system is gathered, in addition to information pertaining to previous or similar systems. Next, system boundaries are defined, as are the primary mission, functional

requirements and the operational environment. With all of this information in mind, the system can then decomposed into its fundamental components.

This decomposition can be approached in two ways. "The bottom up approach is used when a system concept has been decided. Each component on the lowest level of indenture is studied one-by-one." The top-down approach "is mainly used in an early design phase before the whole system structure is decided" (Rausand, 5: 2004). This approach is function oriented and decomposes the system based on system functions. The decompositions can be functional block diagrams, schematics or other appropriate tools. By decomposing the system into its fundamental units it is possible to enumerate each component or functional unit and describe its proper function. The failure modes of the system, then, are simply the non-fulfillment of the functions of each of the components or functional units.

The next step is to determine these failure modes, or risk scenarios, of the system. This step is called failure analysis and is accomplished by listing each function of each system component. This enables the decision maker to consider the complete set of failure modes of the system. Each of these failure modes is, by the triplet definition of risk, a risk scenario.

For each of these failure modes, FMEA considers three parameters: the frequency of occurrence, O, the severity of the failure, S, and the likelihood that the failure will be detected before the system reaches the customer, D. Each parameter is ranked ordinally, typically on a scale from one to ten.

These parameters are then used to score each failure mode. This is done by using one of several methods. The first involves creating a severity matrix, with axes of

frequency and consequence similar to the method used in RFRM. The scenarios that fall into the catastrophic/frequent regions of the matrix are the focus of mitigation efforts. The other, more common method relies on a figure called the risk priority number (RPN). This measure is similar to unconditional expectation of consequence, but is weighted by the likelihood that the failure will be detected before the system reaches the customer. The RPN can be calculated as either the product or sum of O, S, and D. The state space of the RPN ranges from one to one thousand for a product RPN, or three to thirty for a sum RPN. The RPN is an ordinal ranking in which a higher RPN denotes a more severe risk scenario. In this way, resources can be directed to address the most severe scenarios first.

2.3 Expressing Risk

Once risk has been defined, it is desirable to express it in some meaningful way so that decision alternatives may by ranked. Obviously, one could simply express risk as the set of triplets that define it, but it is difficult to extract a comprehensive understanding of risk in this from, particularly when it is necessary to compare the risk of two decision alternatives.

A more useful graphical representation is a cumulative probability plot which plots the consequence of a decision alternative versus its cumulative likelihood. Typically it is drawn as a probability of exceedance curve which expresses the likelihood that a consequence is equal to or exceeds a specified value. This is an extremely important curve because it completely characterizes the risk of a decision alternative because it displays the entire spectrum of consequences possible under that alternative.

Consequently, the most comprehensive method to rank decisions alternatives is by comparing probability of exceedance curves. A notional probability of exceedance curve is shown in Figure 2.2.

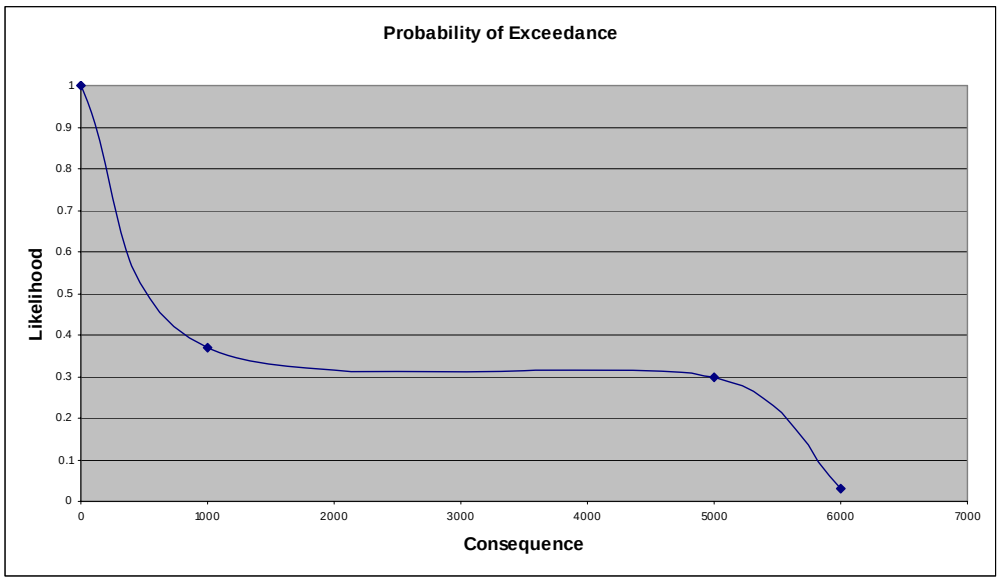

Figure 2.2 Probability of Exceedance Curve

2.4 Measuring Risk

Once the risk of a decision alternative has been quantified it is useful to measure the risk. In order to function as an adequate proxy of risk, however, the measure must be carefully designed to account for the most extreme consequences possible under the decision alternative. The subsequent section summarizes and critiques the principal measures of risk.

2.4.1 Levels of Quantification

One of the fundamental attributes of any measure of risk is the level at which it quantifies consequence and likelihood. The least quantitative measures are easiest to calculate, however, they capture the least amount of information; while the most

quantitative measures capture much more information but are consequently more difficult to calculate. Kaplan partitions the levels as follows (Kaplan et al., 1999: 8):

- verbal,
- ordinal,
- point estimate,
- bounding estimate,
- probabilistic, and
- evidence based.

The first two are qualitative and therefore, the easiest measures to calculate but are consequently the least precise. In a verbal measure of risk, both consequence and likelihood are described with words (i.e. high, medium, and low). An ordinal measure of risk, while it uses numbers instead of words, is only semantically quantitative. Instead of assigning a verbal description of consequence and likelihood, these attributes are assigned a number value. This value represents the rank order of the consequences only. Differences in magnitude of ordinal numbers are undefined.

The next two levels of quantification, point estimates and bounding estimates, are the first levels of measurement that are truly quantitative. Point estimates, unlike ordinal measures, actually represent the underlying magnitude of the system. A bounding estimate is simply a pair of point estimates that, as the name implies, bound the range of the estimate.

The last two levels of quantification, probabilistic and evidence-based, represent the highest levels of fidelity. Instead of estimating consequence and likelihood as single numbers, these parameters are represented with probability distributions. An evidence-

based distribution simply means that Bayes' theorem is used to incorporate all of the prior evidence available into the posterior distributions of consequence and likelihood.

Since the higher levels of quantification capture more information, it is these levels that should be sought to achieve a comprehensive measure of risk. However, it is important to bear in mind that not all situations will provide enough data to characterize consequence or likelihood quantitatively. In these instances it is necessary to resort to qualitative measures.

2.4.2 Qualitative Measure of Risk

If the likelihoods or consequences of a set of risk scenarios are assessed qualitatively, the methods available to measure the risk are limited. Mathematical operations like expectation or variance have no meaning for categorical or ordinal quantities.

This suggests a severity matrix as an appropriate measure of risk. Each risk scenario of a decision alternative is plotted on the severity matrix according to its likelihood and consequence. Regions of the matrix are coded according to the decision maker's values. Regions with high likelihood and high consequences are classified as being the least desirable. The more scenarios that appear in the critical regions of the matrix, the more risky the decision alternative is. A sample severity matrix appears in Figure 2.3.

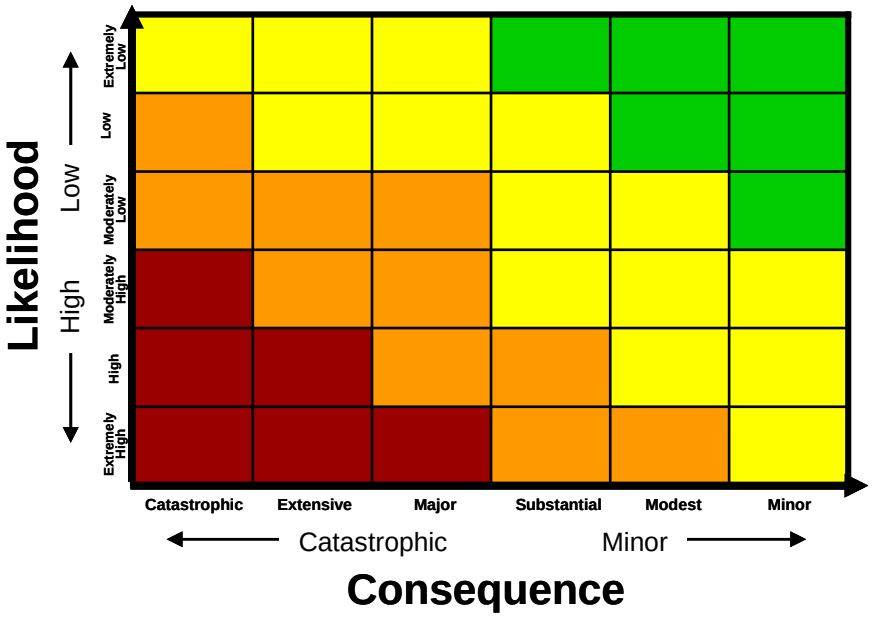

Figure 2.3 Severity Matrix

2.4.3 Quantitative Measures of Risk

One of the primary reasons for conducting a risk assessment is to evaluate a decision alternative based on its risk. While a severity plot gives a much better visualization of risk than the set of triplets alone, it is difficult to make a risk conscious decision based on a graph. One solution is to derive a scalar abstraction of risk; a measure of risk that is easily comparable and facilitates decision making.

In defining this measure it is important to remain cognizant of the distinction between risk itself and a measure of risk. Risk is, per the conventional definition, the entire set of scenarios, likelihoods and consequences. But, by collapsing risk into any measure, a tremendous amount of information is lost. To find a scalar measure that captures enough of the information contained in the set of triplets to make an informed decision is not a trivial task, yet this is precisely the goal of risk assessment procedures.

The ideal measure of risk is one that captures as much information from the triplet as possible but is still simple enough use as a decision parameter.

As there is no single definition of risk common to all applications, there is likewise no single measure of risk common to all applications. Different fields use different measure of risk. Below is a summary of some of the more common measures of risk.

2.4.3.1 Variance as a Measure of Risk

One common measure of the risk of a decision alternative is the variance of its consequence, X, given by $V[X] = E[X^2] - E[X]^2$. Variance is an adequate measure of uncertainty in consequences; however, it is an inadequate measure of the consequences themselves because it neglects the impact magnitude (Sarin, 1993: 137). For instance, consider the following gambles: gamble 1 one has a .5 probability of loosing $50 and a .5 probability of winning $50, gamble 2 one has a .5 probability of winning $1 and a .5 probability of winning $101 dollars. Both gambles have the same variance, but it is intuitive that the first is more risky than the second because some of its consequences are negative, while the second gamble has exclusively positive consequences. It is obvious from this example that some measure of magnitude is also necessary.

2.4.3.2 Expected Value as a measure of Risk

Another common measure of risk is the unconditional expected value of consequence given by $E[X] = \sum_x xp(x)$, where the random variable X represents the consequence. This is also a poor measure of risk because it commensurates low-

likelihood, high-consequence events with high-likelihood, low-consequence events. However, it is the former that most decision makers are primarily concerned with. Because of its simplicity, though, expected consequence is often employed as a measure of risk.

2.4.3.3 Expectation-Variance Measure of Risk

From the discussion above, it is clear that using variance or expected consequence alone as a measure of risk is inadequate. However, a measure using both expectation and variance may be an adequate measure of risk. Pollatsek and Tversky suggest as a measure of risk a linear combination of variance and expectation of consequence using a constant, λ, which represents the decision maker's preference between variance and expectation (Sarin, 1993: 137). The measure is given by the following expression, where the random variable X represents the consequence: $Risk = \lambda V[X] - (1-\lambda)E[X]$.

2.4.3.4 Conditional Expected Value Measure of Risk

Another measure or risk is the conditional expected consequence given by the following equation $E[X \mid P(X) \geq \alpha] = \frac{\sum_{X|P(X)\geq\alpha} x * p(x)}{\sum_{X|P(X)\geq\alpha} p(x)}$, where the random variable X represents the consequence. This expectation is conditioned on the consequence exceeding a specified exceedance probability, α. Haimes uses conditional expectation as a measure of risk in his partitioned multi-objective risk method, PMRM, which "isolates a number of damage ranges and generates conditional expectations of damage, given the damage falls within a particular range" (Haimes, 2004: 304).

2.4.3.5 Measuring Scenario Contribution to Risk

In conducting a risk analysis the decision maker may very well be interested in measuring the contribution of an individual scenario instead of the aggregate risk of all the scenarios. Any methodology that seeks to rank risk scenarios implies some measure of this type.

Literature on measures of scenario contributions to risk is scarce, but a logical choice is the scenario-wise component of the unconditional expected consequence. This measure is calculated by simply multiplying the consequence of each risk scenario by the likelihood of that scenario.

2.5 Summary

This chapter presented several of the principal methodologies used to generate the elements of the risk of a decision alternative. Additionally, several conventional measures of risk were presented. In the next chapter, the best of these elements are incorporated into a methodology to generate and measure risk in the context of military capability divestiture.

3 Methodology

3.1 Introduction

This chapter presents a conceptual framework and associated methodology to quantify the risk of the decision to divest a military capability to an allied nation. This requires a methodological procedure to assess the three elements that define the risk of each decision alternative:

- Risk scenarios
- Likelihoods
- Consequences

3.2 Decision Context

The decision of interest is presented as a decision tree in Figure 3.1. The decision alternatives in this context include divesting a single capability to a specific nation or retaining domestic responsibility for the capability.

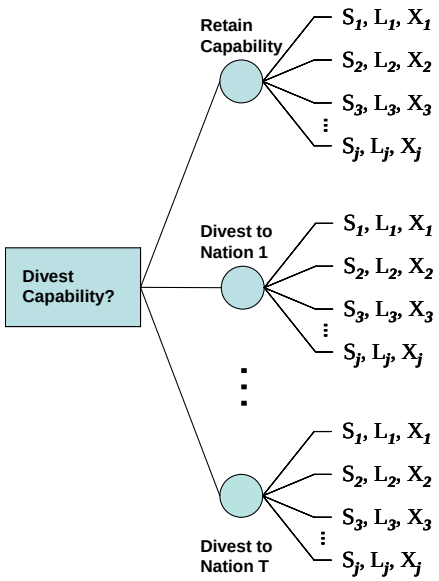

Figure 3.1 Decision Tree

3.3 Quantifying the Risk of a Decision Alternative

According to the conventional definition of risk, the risk of a decision alternative is composed of the set of the following three elements.

- Risk scenario - What can go wrong?
- Likelihood - How likely are the risk scenarios?
- Consequences - What are the consequences of each risk scenario?

The subsequent sections present a methodology to generate each of these elements for the alternatives in the decision to divest a military capability.

3.3.1 Risk Scenarios

The first step in the risk assessment process is to generate the set of risk scenarios possible for each decision alternative. Risk scenarios represent everything that can 'go wrong' with the system in which the decision is made. In other words, risk scenarios

represent the events that initiate consequences. In the context of capability divesture, risk scenarios are the possible combinations of real world contingencies about which decision makers are concerned. Contingencies are defined as events in which the United States is required to use the military capability. Notional contingencies, for example, could include a major regional conflict in Iran, humanitarian assistance in Afghanistan or stability operations in Iraq. Relevant contingencies must be identified by the decision maker or subject matter experts.

In order to generate a formally partitioned set of risk scenarios based on these contingencies, the set of contingencies must be mutually exclusive and collectively exhaustive. These conditions ensure that consequences of the decision alternative are not counted more than once and that all relevant threats are accounted for. Since the contingencies are not dependent on the decision alternative, both decision alternatives (divest or retain) are subject to the same set of risk scenarios; however, the consequence of the risk scenarios will likely be different under each decision alternative.

In order to form a complete set of risk scenarios based on these contingencies, each possible combination of contingencies must be enumerated. With *i* contingencies and two states possible for each contingency (occurrence or non-occurrence), 2^i unique risk scenarios are possible for each decision alternative. A notional set of risk scenarios for each decision alternative, assuming two contingencies, is shown in the decision tree in Figure 3.2; where "1" represents the event that contingency *i* occurs and "0" represents the event that contingency *i* does not occur.

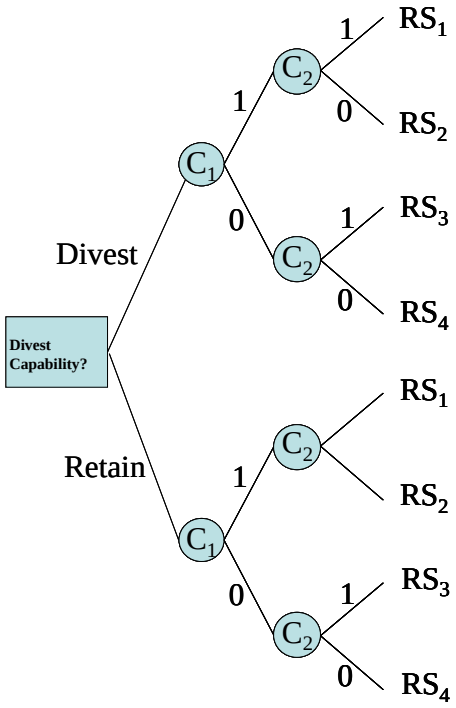

Figure 3.2 Decision Tree with Risk Scenarios

Each risk scenario and the state of every contingency that defines it can be represented more succinctly in tabular form. In Table 3.1, "1" represents the event that contingency *i* occurs and "0" represents the event that contingency *i* does not occur.

Table 3.1 Risk Scenarios and Constituent Contingencies

RS_j	Contingency 1	Contingency 2
RS_1	1	1
RS_2	1	0
RS_3	0	1
RS_4	0	0

3.3.2 Likelihood of a Risk Scenario

Assuming the contingencies are independent and the likelihood of occurrence of each contingency can be estimated by subject matter experts, the likelihood of each risk

scenario can be calculated as the product of the likelihoods of the states of the contingencies that define it. This process is illustrated in the example below for risk scenario one, using the notional data in Table 3.2.

Table 3.2 Contingency Likelihoods

Contingency	L(1)	L(0)
1	**0.10**	**0.90**
2	**0.30**	**0.70**

$$L(RS_1) = L_{C_1}(1) * L_{C_2}(1)$$

$$L(RS_1) = .10 * .30$$

$$L(RS_1) = .03$$

The likelihoods of the remaining scenarios are presented in Table 3.3.

Table 3.3 Risk Scenario Likelihoods

RS_j	Likelihood
RS_1	**0.03**
RS_2	**0.07**
RS_3	**0.27**
RS_4	**0.63**

3.3.3 Consequence of a Risk Scenario

Once the likelihoods for each risk scenario are defined, the consequence of each risk scenario must be determined. Given the compound nature of a risk scenario, however, evaluating its consequences can be problematic. In particular, how can a subject matter expert reasonably evaluate the consequence of a risk scenario composed of dozens of contingencies?

The most basic solution is to assume that the consequence of a risk scenario is additive. Under this assumption, the consequence of a risk scenario can be calculated piecewise as the sum of the consequence of each constituent contingency event. Thus, the consequence of each constituent contingency event must be evaluated. A contingency event is defined as the occurrence event of a particular contingency. The non-occurrence of a contingency is assumed to have no adverse consequence and therefore need not be evaluated. This concept is shown graphically in the Table 3.4 for two notional contingencies. This structure requires that *i* contingency events be evaluated for each decision alternative, where *i* is the number of contingencies.

Table 3.4 Risk Scenario Consequence Structure

RS_j	Contingency 1	Contingency 2	Conseqeunce
RS_1	1	1	Consequence Contingency Event 1 + Consequence Contingency Event 2
RS_2	1	0	Consequence Contingency Event 1 + 0
RS_3	0	1	0 + Consequence Contingency Event 2
RS_4	0	0	0 + 0

Calculating the consequence of even a single contingency event, however, is not a trivial task. Each contingency event itself possesses risk because the consequence of each contingency event is determined not only by the event itself, but also by a "number of external factors" that are "unknown to the decision maker at the time of the decision" (French, 1986: 33). These factors are defined by contingency scenarios, which describe the possible levels of capability required by the contingency event and the possible levels of capability made available by the host nation. Each contingency scenario results in a unique consequence.

Since each contingency event is composed of a set of contingency scenarios, a contingency event possesses a discrete distribution of consequences. It is these distributions that must be added together to calculate the consequence of a risk scenario. Discussion of methods to combine distributions of consequences is postponed until Section 3.5. First, a method to derive the distribution of consequences for a single contingency event is presented.

3.4 Evaluating the Consequence of a Contingency Event

This procedure is analogous to assessing the risk of a decision alternative. First, the scenarios that describe the potential states of nature are generated; second, the likelihood of each scenario is computed; and finally, the consequence of each scenario is estimated.

3.4.1 Generating Contingency Scenarios

Contingency scenarios represent the set of events that can 'go wrong' given a contingency event. The natural partition of contingency scenarios is on the set of actual events that could occur. Partitioned in this way, however, the set of potential scenarios is large and consequently burdensome to generate.

Consider instead partitioning on the possible levels of capability required by the contingency and the possible levels of capability available from the host nation. With respect to the realization of adverse consequences, these factors represent all the pertinent information contained in the actual events because it is the differential between these capability levels that initiates adverse consequences.

Consequently, a contingency scenario is composed of three elements. The level of capability required by the contingency is represented by a requirement scenario. The level of capability available from the host nation is represented jointly by procurement and implementation scenarios. Procurement scenarios represent the level of capability procured and maintained by the host nation. Implementation scenarios represent whether or not the host nation will actually implement the capability it has procured. Each unique combination of requirement, procurement and implementation scenario forms a contingency scenario. Contingency scenarios for a single notional contingency event are shown hierarchically in the event tree in Figure 3.3.

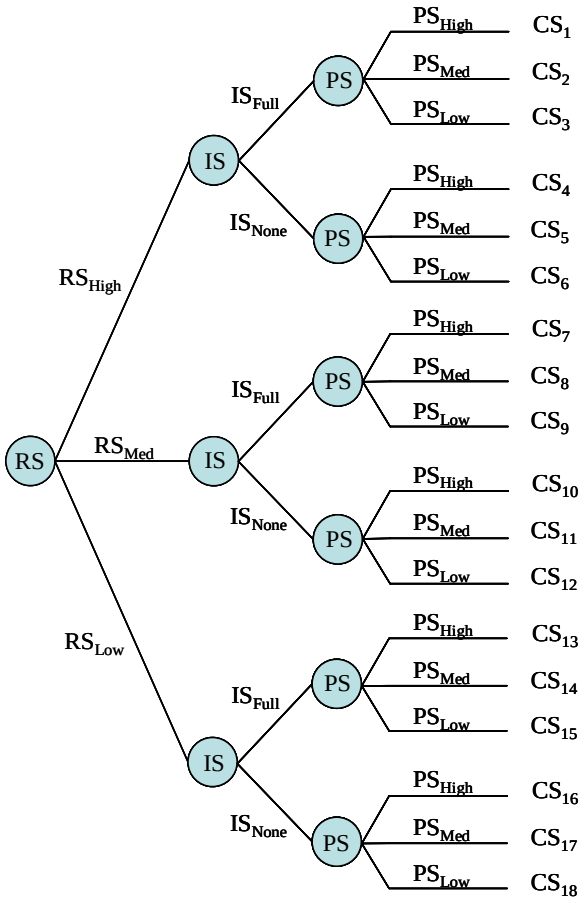

Figure 3.3 Contingency Tree

3.4.1.1 Procurement and Requirement Scenarios

Next, a method to explicitly define the levels of capability through which requirement and procurement scenarios are defined is presented. Conceptually, a capability can be decomposed into a finite set of measurable factors considered in evaluating the efficacy of that capability. A particular realization of the possible states of these measures is termed a capability scenario and corresponds to a particular level of capability.

In order to ensure that capability scenarios are mutually exclusive, each state under a measure is interpreted as the best value that can be achieved under that measure. In order to ensure that the capability state-space is finite, the scale of each measure is partitioned into r_i discrete bins. The thresholds partitioning the bins are determined by subject matter experts and the number of bins is driven by the required fidelity of the assessment. With q measures and r_i states possible under each measure, $\prod_{i=1}^{q} r_i$ capability scenarios are possible. Decomposition of a capability into q measures, each with r_i discrete states is illustrated hierarchically in Figure 3.4.

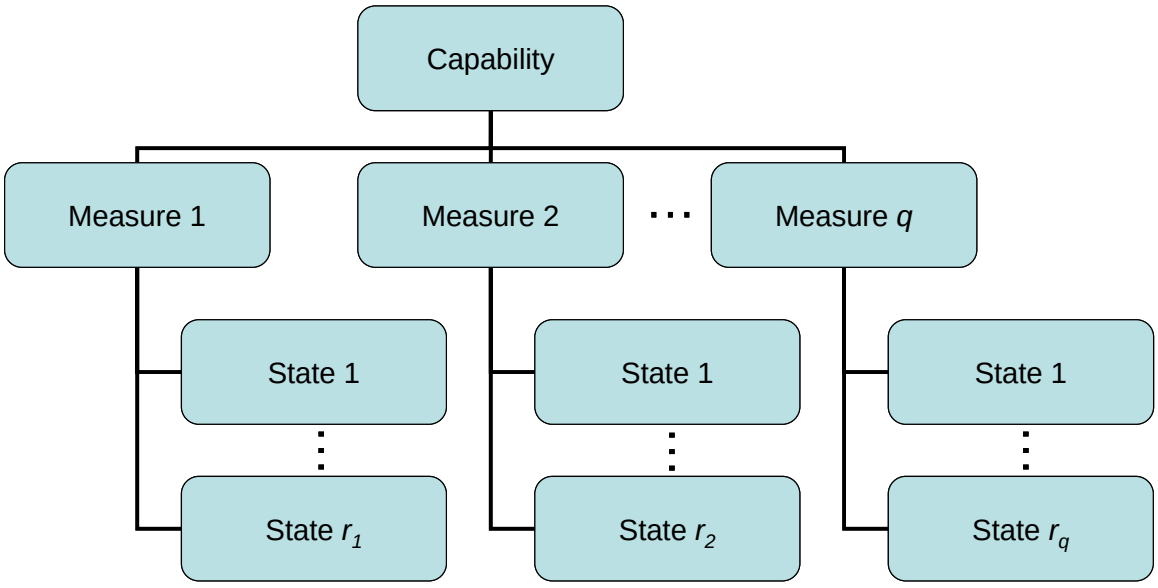

Figure 3.4 Measures of a Capability

A notional set of capability scenarios assuming three measures, each with two states, is presented in Table 3.5. Because the states of the evaluation considerations are mutually exclusive and collectively exhaustive, the capability scenarios cover the entire capability space and represent every possible level of capability.

Table 3.5 Capability Scenarios

Capability Scenario	Measure 1	Measure 2	Measure 3
CBS_1	State 1	State 1	State 1
CBS_2	State 1	State 1	State 0
CBS_3	State 1	State 0	State 1
CBS_4	State 1	State 0	State 0
CBS_5	State 0	State 1	State 1
CBS_6	State 0	State 1	State 0
CBS_7	State 0	State 0	State 1
CBS_8	State 0	State 0	State 0

Since the number capability scenarios increases exponentially with the number of evaluation considerations, the number of scenarios quickly becomes intractable. In order

to decrease the capability state-space to a more reasonable level, the scenarios can be aggregated into classes that provide equivalent levels of capability. The number of classes and assignment to classes is qualitative and is based on the opinion of subject matter experts. A notional partition is shown in Table 3.6.

Table 3.6 Partitioned Capability Scenarios

Capability Scenario	Capability Level
CBS_1	High
CBS_2	Medium
CBS_3	Medium
CBS_4	Low
CBS_5	Medium
CBS_6	Low
CBS_7	Low
CBS_8	Low

The requirement and procurement scenarios are now specified by these classes of capability. For example, consider contingency scenario one (CS_1) in Figure 3.3. RS_{high} denotes that the contingency event requires a high level of capability. Similarly, PS_{high} denotes that the host nation has procured/maintained a high level of capability.

Once the procurement and requirement scenarios are specified, the likelihood of each scenario can be assessed by subject matter experts. Likelihoods for requirement scenarios are dependent on the contingency event and likelihoods for procurement scenarios are dependent on the decision alternative. Notional procurement and requirement scenarios and their likelihoods are presented in Tables 3.7 and 3.8.

Table 3.7 Notional Procurement Scenarios

Procurment Scenario	Capability Level	Likelihood
PS_1	High	0.60
PS_2	Medium	0.20
PS_3	Low	0.20

Table 3.8 Notional Requirement Scenarios

Requirement Scenairo	Capability Level	Likelihood
RS_1	High	0.20
RS_2	Medium	0.45
RS_3	Low	0.35

3.4.1.2 Implementation Scenarios

Even though a nation has procured and maintained a capability adequately, it may not necessarily employ it. Non-implementation may occur because of potential conflicts of interest between the host nation and the nations involved with the contingency or because the host nation is using the capability in another contingency. These events are accounted for by the implementation scenarios. An implementation scenario denotes whether or not the host nation implements its procured capability. At the individual contingency level it is assumed that only two implementation scenarios are possible: full implementation or no implementation.

Likelihoods for each implementation scenario can be assessed by subject matter experts and are dependent on the particular capability, the contingency and the decision alternative. Notional implementation scenarios and their likelihoods are presented in Table 3.9.

Table 3.9 Implementation Scenarios

Implementation Scenario	Description	Likelihood
IS_1	**Implement capability**	**0.6**
IS_2	**Do not implement capability**	**0.4**

3.4.2 Calculating the Likelihood of Contingency Scenarios

The likelihood of a complete contingency scenario is calculated by taking the product of the likelihoods of each scenario that composes it. Since implementation scenarios are dependent on the decision alternative and the contingency, their likelihoods must be conditional on both factors.

3.4.3 Assessing Consequences of Contingency Scenarios

Once the set of contingency scenarios is enumerated, consequences must be assigned to each scenario. Logic dictates that consequences need only be assessed for contingency scenarios in which the required capability level exceeds the available capability level. Conversely, contingency scenarios in which the available capability level exceeds or is equivalent to the required capability level are assumed to have no adverse consequence.

In the context of capability divestiture, multiple risk factors are necessary to completely characterize a decision alternative. Risk factors represent the types of consequence that a risk scenario may produce. As an example, risk factors about which a decision maker may be concerned in the context of capability divestiture are friendly/allied casualties, timeliness of desired effects and post conflict recovery time.

The purpose of this phase of the methodology is to assign a consequence to each risk factor for every contingency scenario. Unfortunately, the consequence of a

contingency scenario in the context of capability divestiture is not explicitly prescribed. Consequently, the assignment of consequences to a risk scenario must be subjective. The decomposition of contingency scenarios into requirement, procurement and implementation scenarios was done intentionally to provide some degree of objectivity to the consequence assessment process. The difference between the required and procured levels of capability for each contingency scenario offers insight into the magnitude of the consequence of the contingency scenario. Ultimately, however, the assignment of consequences is subjective and consequence assessment is based on the judgment of subject matter experts.

The result of this process is a discrete distribution of consequences for each risk factor for a contingency event. These distributions must be added appropriately to compute the consequence of a risk scenario. This process is discussed in the subsequent section.

3.5 Computing the Consequence of a Risk Scenario

The consequence of a risk scenario is computed by summing the consequences of its constituent contingency events. This is problematic, however, since each contingency event possesses a distribution of consequences under each risk factor.

This condition can be handled in two ways. First, the distributions of each constituent contingency event could be convolved to derive a single distribution of consequence. However, this process can easily become overwhelming as the number of contingencies grows.

A less sophisticated but more tractable method is to simply parameterize each distribution of consequence. This can be accomplished by measuring the distribution by taking its conditional expected consequence. The conditional expected consequence is ideal for this purpose because it accounts for the severe consequences about which decision makers are typically concerned. Traditionally, the conditional expected consequence is defined for continuous functions; however, the distribution of consequence for each contingency event is discrete. Consequently, the measure is defined as $E[X \mid P(X) \geq \alpha] = \frac{\sum_{X|P(X)\geq\alpha} x * p(x)}{\sum_{X|P(X)\geq\alpha} p(x)}$, where X represents the discrete random consequence and α represents the desired probability of exceedance. The conditional expected consequence for the notional distribution of consequence in Table 3.10 is presented below.

Table 3.10 Distribution of Consequence for Contingency Event 1

CS	L	X
CS_1	**0.20**	**1000**
CS_2	**0.20**	**900**
CS_3	**0.30**	**500**
CS_4	**0.30**	**100**

$$E[X \mid P(X) \geq \alpha] = \frac{\sum_{X|P(X)\geq\alpha} x * p(x)}{\sum_{X|P(X)\geq\alpha} p(x)}$$

$$E[X \mid P(X) \geq .9] = \frac{\sum_{X|P(X)\geq.9} x * p(x)}{\sum_{X|P(X)\geq.9} p(x)}$$

$$E[X \mid P(X) \geq .9] = \frac{1000 * .20}{.20}$$

$$E[X \mid P(X) \geq .9] = 1000$$

Once the distribution of consequences for each contingency event is transformed into a scalar via measurement under conditional expectation, the consequence of a risk scenario can be computed by simply adding the measures corresponding to the appropriate contingency events. Given the conditional expectations for notional contingencies one and two presented in Table 3.11, the resulting consequence for each risk scenario is presented in table 3.12.

Table 3.11 Conditional Expectations

Contingency	E[X|P(X)>.90]
C_1	1000
C_2	5000

Table 3.12 Risk

Risk Scenario	Contingency 1	Contingency 2	Consequence
RS_1	1	1	1000 + 5000 = 6000
RS_2	1	0	1000 + 0 = 1000
RS_3	0	1	0 + 5000 = 5000
RS_4	0	0	0 + 0 = 0

3.6 Measuring Risk

Once the risk of each decision alternative is quantified it may be useful to measure the risk. The conditional expected consequence can also be used as a measure of risk in this context. In the following example, the conditional expected consequence is calculated for the risk presented in Table 3.12 using the likelihoods presented in Table 3.3.

$$E[X \mid P(X) \geq \alpha] = \frac{\sum_{X|P(X)\geq\alpha} x * p(x)}{\sum_{X|P(X)\geq\alpha} p(x)}$$

$$E[X \mid P(X) \geq .9] = \frac{\sum_{X|P(X)\geq.8} x * p(x)}{\sum_{X|P(X)\geq.8} p(x)}$$

$$E[X \mid P(X) \geq .9] = \frac{6000 * .03}{.03}$$

$$E[X \mid P(X) \geq .9] = 6000$$

3.7 Summary

This chapter provided a methodology to generate the risk of the decision alternatives in the decision to divest a military capability to an allied nation. This was accomplished by defining risk scenarios in terms of contingencies and calculating the consequence of each risk scenario additively as the sum of the consequence of each constituent contingency event.

4 Results and Analysis

4.1 Introduction

This chapter applies the risk assessment methodology presented in Chapter 3 to the decision to divest the Air Force capability *Tactical Surveillance of Mobile Terrestrial Targets* to an allied nation. This example accomplishes three tasks. First, it generates the set of risk scenarios, likelihoods and consequences that define the risk of divesting the capability. Second, it measures the risk of divestiture via the conditional expected consequence operator. Finally, it investigates which scenarios are the most significant contributors of risk and how the risk can be mitigated if these scenarios are managed by the decision maker.

Like any risk assessment methodology, this process is dependent on data provided by subject matter experts. This data includes estimates of the likelihoods and consequences of the risk scenarios and the contingencies of concern. Since subject matter experts were not available for solicitation of data, notional data provided by the author is considered instead. The complete set of notional data used in this chapter is presented in the Appendix.

4.2 Choosing a Capability

This chapter examines the risk of divesting the Air Force service-level capability *Tactical Surveillance of Mobile Terrestrial Targets* (Johnson, 2005:13). Two questions are of immediate concern. First, which specific elements of the capability are considered for divestiture? Second, how does the capability map to the JCA/UJTL framework?

First, the capability must be decomposed further into its constituent elements. According to a study conducted by former Under Secretary of the Air force for Acquisition, Technology and Logistics Pete Aldridge, a capability can be decomposed into seven standard elements: doctrine, organization, training, material, leadership, personnel and facilities (Department of Defense, 2003: Chapter1, 2). In this example, all seven elements of the capability *Tactical Surveillance of Mobile Terrestrial Targets* will be divested. Conceivably, however, any combination of these elements of the capability could be divested. This is directly manifested in the methodology through the subject matter expert's assessment of the consequence of a contingency scenario. For a given contingency scenario, the more elements of a capability that are divested, the greater the consequence may be.

Mapping the capability to the JCA framework is considered next. How does the Air Force service-level capability *Tactical Surveillance of Mobile Terrestrial Targets* impact the hierarchy itself. Because of the structure of the JCA/UJTL framework, a single service-level capability could appear in multiple UJTL tasks. Subsequently, multiple UJTL tasks could appear in multiple operational templates, multiple operational templates could occur in multiple JCAs, multiple JCAs could be required for multiple operations and multiple operations will likely be necessary for a particular contingency. This structure is shown notionally in the Figure 4.1.

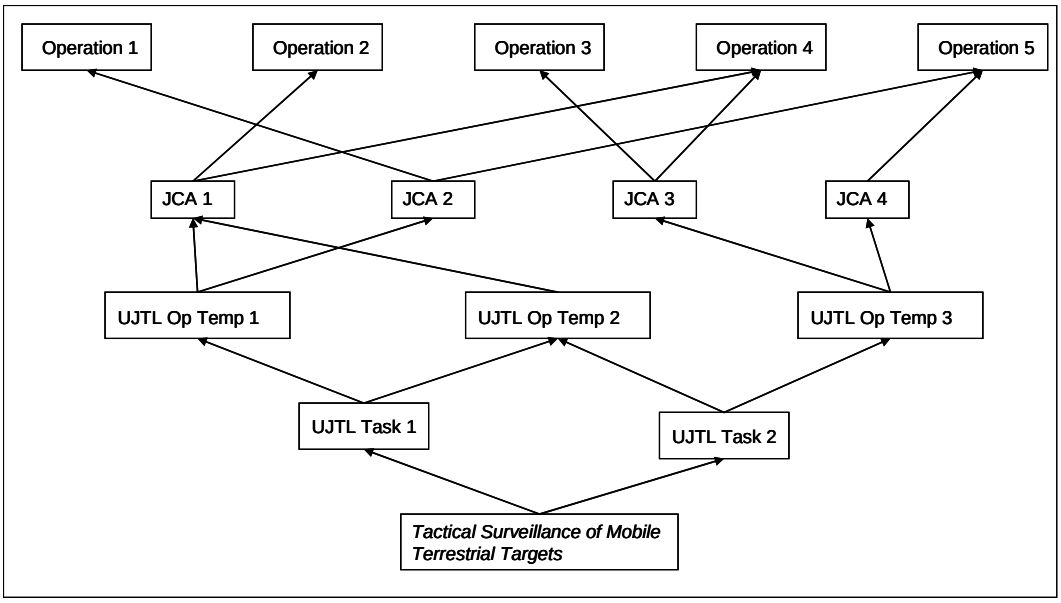

Figure 4.1 JCA/UJTL Structure

The result of this structure is that a single service level capability, like *Tactical Surveillance of Mobile Terrestrial Targets*, can have a cumulative effect through JCA/UJTL hierarchy, appearing multiple times at the operational level. This is precisely why it is critical to evaluate the risk of divesting a military capability.

4.2.1 Focus on Threats

One of the objectives of capabilities based planning (CBP) is to make decisions and plans independent of threats. While this objective can be realized in many areas of planning, in order to formally assess risk, of which consequence and likelihood are fundamental components, threats must be considered. Threats are an integral part of the risk scenario because the consequence and likelihood of a risk scenario are only realized in the context of a specified threat. Since likelihood and consequence are fundamental to

defining risk, threats are a necessary component of a comprehensive risk assessment process.

Consider divesting a capability. What is the consequence? Obviously, this question depends on the threat. If there is no threat then no adverse consequence is realized. Conversely, if the capability required to meet the threat exceeds the available capability then adverse consequences are realized. The consequences cannot be adequately assessed without considering a threat. Certainly one could simply estimate the worst possible consequences of a certain capability scenario, but even this implies an assumed worst-case threat scenario. And even in this case, risk cannot be properly defined because the implied threat does not possess an explicit likelihood. Therefore, the inclusion of threat is absolutely necessary to define the risk of divesting a military capability.

4.3 Contingencies

Contingencies represent events that require the United States to use the Air Force service-level capability *Tactical Surveillance of Mobile Terrestrial Targets*. Six notional contingencies about which decision makers are concerned are listed in Table 4.1, along with their respective likelihoods of occurrence.

Table 4.1 Notional Contingencies and Likelihoods

Contingency *i*	Description	L(Occurrence)	L(Non-Occurrence)
1	Major Regional Conflict in Raetia	0.01	0.99
2	Major regional conflict in Noricum	0.05	0.95
3	Humanitarian Assisstance in Dacia	0.20	0.80
4	Small Scale Conflict in Lycia	0.25	0.75
5	Small Scale Conflict in Numidia	0.50	0.50
6	Stability Operations in Baetica	0.10	0.90

4.4 Risk Scenarios and Likelihoods

Risk scenarios are formed by enumerating each possible combination of contingencies. Six contingencies result in 2^6= 64 unique risk scenarios. The likelihood of each risk scenario is calculated as the product of the likelihoods of the contingency events that compose it. The calculation of the likelihood of risk scenario one, in which all six contingencies occur, is shown below. It is calculated as the product of the likelihood of occurrence of each constituent contingency.

$$L(RS_1) = L_{C_1}(1) * L_{C_2}(1) * L_{C_3}(1) * L_{C_4}(1) * L_{C_5}(1) * L_{C_6}(1)$$

$$L(RS_1) = .01 * .05 * .20 * .25 * .50 * .10$$

$$L(RS_1) = 1.25E\text{-}06$$

In Table 4.2, the likelihoods for the remaining risk scenarios are presented. A “1” signifies that contingency *i* occurs and a “0” signifies that contingency *i* does not occur.

Table 4.2 Risk Scenarios

	Contingency						
RS_j	1	2	3	4	5	6	Likelihood
RS_1	1	1	1	1	1	1	0.00000125
RS_2	1	1	1	1	1	0	0.00001125
RS_3	1	1	1	1	0	1	0.00000125
RS_4	1	1	1	1	0	0	0.00001125
RS_5	1	1	1	0	1	1	0.00000375
RS_6	1	1	1	0	1	0	0.00003375
RS_7	1	1	1	0	0	1	0.00000375
RS_8	1	1	1	0	0	0	0.00003375
RS_9	1	1	0	1	1	1	0.000005
RS_{10}	1	1	0	1	1	0	0.000045
RS_{11}	1	1	0	1	0	1	0.000005
RS_{12}	1	1	0	1	0	0	0.000045
RS_{13}	1	1	0	0	1	1	0.000015
RS_{14}	1	1	0	0	1	0	0.000135
RS_{15}	1	1	0	0	0	1	0.000015
RS_{16}	1	1	0	0	0	0	0.000135
RS_{17}	1	0	1	1	1	1	0.00002375
RS_{18}	1	0	1	1	1	0	0.00021375
RS_{19}	1	0	1	1	0	1	0.00002375
RS_{20}	1	0	1	1	0	0	0.00021375
RS_{21}	1	0	1	0	1	1	0.00007125
RS_{22}	1	0	1	0	1	0	0.00064125
RS_{23}	1	0	1	0	0	1	0.00007125
RS_{24}	1	0	1	0	0	0	0.00064125
RS_{25}	1	0	0	1	1	1	0.000095
RS_{26}	1	0	0	1	1	0	0.000855
RS_{27}	1	0	0	1	0	1	0.000095
RS_{28}	1	0	0	1	0	0	0.000855
RS_{29}	1	0	0	0	1	1	0.000285
RS_{30}	1	0	0	0	1	0	0.002565
RS_{31}	1	0	0	0	0	1	0.000285
RS_{32}	1	0	0	0	0	0	0.002565

	Contingency						
RS_j	1	2	3	4	5	6	Likelihood
RS_{33}	0	1	1	1	1	1	0.00012375
RS_{34}	0	1	1	1	1	0	0.00111375
RS_{35}	0	1	1	1	0	1	0.00012375
RS_{36}	0	1	1	1	0	0	0.00111375
RS_{37}	0	1	1	0	1	1	0.00037125
RS_{38}	0	1	1	0	1	0	0.00334125
RS_{39}	0	1	1	0	0	1	0.00037125
RS_{40}	0	1	1	0	0	0	0.00334125
RS_{41}	0	1	0	1	1	1	0.000495
RS_{42}	0	1	0	1	1	0	0.004455
RS_{43}	0	1	0	1	0	1	0.000495
RS_{44}	0	1	0	1	0	0	0.004455
RS_{45}	0	1	0	0	1	1	0.001485
RS_{46}	0	1	0	0	1	0	0.013365
RS_{47}	0	1	0	0	0	1	0.001485
RS_{48}	0	1	0	0	0	0	0.013365
RS_{49}	0	0	1	1	1	1	0.00235125
RS_{50}	0	0	1	1	1	0	0.02116125
RS_{51}	0	0	1	1	0	1	0.00235125
RS_{52}	0	0	1	1	0	0	0.02116125
RS_{53}	0	0	1	0	1	1	0.00705375
RS_{54}	0	0	1	0	1	0	0.06348375
RS_{55}	0	0	1	0	0	1	0.00705375
RS_{56}	0	0	1	0	0	0	0.06348375
RS_{57}	0	0	0	1	1	1	0.009405
RS_{58}	0	0	0	1	1	0	0.084645
RS_{59}	0	0	0	1	0	1	0.009405
RS_{60}	0	0	0	1	0	0	0.084645
RS_{61}	0	0	0	0	1	1	0.028215
RS_{62}	0	0	0	0	1	0	0.253935
RS_{63}	0	0	0	0	0	1	0.028215
RS_{64}	0	0	0	0	0	0	0.253935

4.5 Defining Capability Levels

The levels of capability used to characterize procurement and requirement scenarios must be explicitly defined in order to assess consequence. This requires a subject matter expert to define a comprehensive set of measures for *Tactical Surveillance of Mobile Terrestrial Targets*. A notional set of measures and the states possible under each measure is presented in Figure 4.2 (Johnson, 2005: 13).

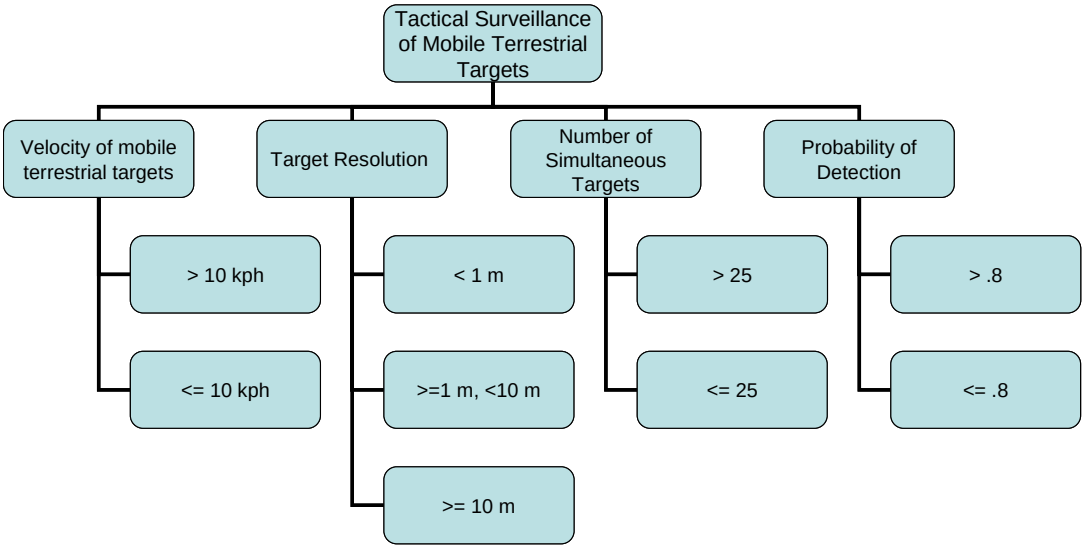

Figure 4.2 Capability Measures

All possible combinations of the states of the measure are enumerated to generate capability scenarios which define the possible levels of capability. These scenarios are shown in the Table 4.3 where the number under each measure represents the state of the capability under that measure.

Table 4.3 Capability Scenarios

Capability Scenario	Measure 1	Measure 2	Measure 3	Measure 4
CBS_1	1	1	1	1
CBS_2	1	1	1	2
CBS_3	1	1	2	1
CBS_4	1	1	2	2
CBS_5	2	1	1	1
CBS_6	2	1	1	2
CBS_7	2	1	2	1
CBS_8	2	1	2	2
CBS_9	1	2	1	1
CBS_{10}	1	2	1	2
CBS_{11}	1	2	2	1
CBS_{12}	1	2	2	2
CBS_{13}	2	2	1	1
CBS_{14}	2	2	1	2
CBS_{15}	2	2	2	1
CBS_{16}	2	2	2	2
CBS_{17}	1	3	1	1
CBS_{18}	1	3	1	2
CBS_{19}	1	3	2	1
CBS_{20}	1	3	2	2
CBS_{21}	2	3	1	1
CBS_{22}	2	3	1	2
CBS_{23}	2	3	2	1
CBS_{24}	2	3	2	2

Next, subject matter experts group capability scenarios into classes with roughly equivalent levels of capability. In this example, capability scenarios are partitioned into three classes of capability: high, medium and low. A notional partition is shown in the Table 4.4.

Table 4.4 Partition of Capability Scenarios

Capability Level	Capability Scenario	Measure 1	Measure 2	Measure 3	Measure 4
High	CBS_1	1	1	1	1
	CBS_2	1	1	1	2
	CBS_3	1	1	2	1
	CBS_5	2	1	1	1
	CBS_9	1	2	1	1
Med	CBS_4	1	1	2	2
	CBS_6	2	1	1	2
	CBS_7	2	1	2	1
	CBS_{10}	1	2	1	2
	CBS_{11}	1	2	2	1
	CBS_{13}	2	2	1	1
	CBS_{15}	2	2	2	1
	CBS_{17}	1	3	1	1
	CBS_{18}	1	3	1	2
	CBS_{19}	1	3	2	1
	CBS_{21}	2	3	1	1
Low	CBS_8	2	1	2	2
	CBS_{12}	1	2	2	2
	CBS_{14}	2	2	1	2
	CBS_{16}	2	2	2	2
	CBS_{20}	1	3	2	2
	CBS_{22}	2	3	1	2
	CBS_{23}	2	3	2	1
	CBS_{24}	2	3	2	2

4.6 Evaluating a Contingency Event

Next, the risk of each contingency event is assessed. Evaluation of a contingency event requires substantial input from subject matter experts. In particular, subject matter experts must specify the likelihood of each possible requirement, implementation and procurement scenario, along with the consequence of each contingency scenario that they compose. Notional data for a single contingency event is presented in Tables 4.5 and 4.6.

Table 4.5 Notional Likelihoods

IS	Likelihood
IS_{full}	0.90
IS_{none}	0.10

PS	Likelihood
PS_{high}	0.80
PS_{med}	0.10
PS_{low}	0.10

RS	Likelihood
RS_{high}	0.20
RS_{med}	0.20
RS_{low}	0.60

Table 4.6 Notional Contingency Scenarios

CS_j	IS	RS	PS	Likelihood	Consequence
CS_1	IS_{full}	RS_{high}	PS_{high}	0.1440	0
CS_2	IS_{full}	RS_{high}	PS_{med}	0.0180	5
CS_3	IS_{full}	RS_{high}	PS_{low}	0.0180	6
CS_4	IS_{none}	RS_{high}	PS_{high}	0.0160	10
CS_5	IS_{none}	RS_{high}	PS_{med}	0.0020	10
CS_6	IS_{none}	RS_{high}	PS_{low}	0.0020	10
CS_7	IS_{full}	RS_{med}	PS_{high}	0.1440	0
CS_8	IS_{full}	RS_{med}	PS_{med}	0.0180	0
CS_9	IS_{full}	RS_{med}	PS_{low}	0.0180	5
CS_{10}	IS_{none}	RS_{med}	PS_{high}	0.0160	8
CS_{11}	IS_{none}	RS_{med}	PS_{med}	0.0020	8
CS_{12}	IS_{none}	RS_{med}	PS_{low}	0.0020	8
CS_{13}	IS_{full}	RS_{low}	PS_{high}	0.4320	0
CS_{14}	IS_{full}	RS_{low}	PS_{med}	0.0540	0
CS_{15}	IS_{full}	RS_{low}	PS_{low}	0.0540	0
CS_{16}	IS_{none}	RS_{low}	PS_{high}	0.0480	3
CS_{17}	IS_{none}	RS_{low}	PS_{med}	0.0060	3
CS_{18}	IS_{none}	RS_{low}	PS_{low}	0.0060	3

4.7 Measuring the Consequences of Each Contingency Event

Once the distribution of consequences for each contingency event is generated, it is measured by taking its conditional expected consequence. The following example computes the conditional expected consequence of the data presented in Table 4.6. In this example, the specified condition is that the cumulative likelihood of the consequence exceeds .9. The conditional expectations of the remaining contingency scenarios are presented in the Table 4.7.

$$E[X \mid P(X) \geq \alpha] = \frac{\sum_{X|P(X)\geq\alpha} x * p(x)}{\sum_{X|P(X)\geq\alpha} p(x)}$$

$$E[X \mid P(X) \geq .9] = \frac{\sum_{X|P(X)\geq.9} x * p(x)}{\sum_{X|P(X)\geq.9} p(x)}$$

$$E[X \mid P(X) \geq .9] = \frac{10 * .02 + 8 * .02 + 6 * .018 + 5 * .036 + 3 * .006}{.02 + .02 + .018 + .036 + .006}$$

$$E[X \mid P(X) \geq .9] = \frac{.666}{.10}$$

$$E[X \mid P(X) \geq .9] = 6.66$$

Table 4.7 Contingency Consequences

Contingency *i*	Description	E[X|P(X)>=.9]
1	Major Regional Conflict in Raetia	444
2	Major regional conflict in Noricum	1000
3	Humanitarian Assisstance in Dacia	7
4	Small Scale Conflict in Lycia	100
5	Small Scale Conflict in Numidia	150
6	Stability Operations in Baetica	25

4.8 Resulting Data

Next, the consequence of a risk scenario is computed as the sum of the consequences of the appropriate contingency events. The consequence of risk scenario one is computed below. In this scenario all of the contingency events occur. Consequences for the remaining scenarios are shown in the Table 4.8.

$$Con(RS_1) = Con_{C_1}(1) + Con_{C_2}(1) + Con_{C_3}(1) + Con_{C_4}(1) + Con_{C_5}(1) + Con_{C_6}(1)$$

$$Con(RS_1) = 444 + 1000 + 7 + 100 + 150 + 25$$

$$Con(RS_1) = 1726$$

Table 4.8 Risk

RS_j	Likelihood	Conseqeunce
RS_1	0.00000125	1726
RS_2	0.00001125	1701
RS_3	0.00000125	1576
RS_4	0.00001125	1551
RS_5	0.00000375	1626
RS_6	0.00003375	1601
RS_7	0.00000375	1476
RS_8	0.00003375	1451
RS_9	0.000005	1719
RS_{10}	0.000045	1694
RS_{11}	0.000005	1569
RS_{12}	0.000045	1544
RS_{13}	0.000015	1619
RS_{14}	0.000135	1594
RS_{15}	0.000015	1469
RS_{16}	0.000135	1444
RS_{17}	0.00002375	726
RS_{18}	0.00021375	701
RS_{19}	0.00002375	576
RS_{20}	0.00021375	551
RS_{21}	0.00007125	626
RS_{22}	0.00064125	601
RS_{23}	0.00007125	476
RS_{24}	0.00064125	451
RS_{25}	0.000095	719
RS_{26}	0.000855	694
RS_{27}	0.000095	569
RS_{28}	0.000855	544
RS_{29}	0.000285	619
RS_{30}	0.002565	594
RS_{31}	0.000285	469
RS_{32}	0.002565	444

RS_j	Likelihood	Conseqeunce
RS_{33}	0.00012375	1281
RS_{34}	0.00111375	1257
RS_{35}	0.00012375	1131
RS_{36}	0.00111375	1107
RS_{37}	0.00037125	1181
RS_{38}	0.00334125	1157
RS_{39}	0.00037125	1031
RS_{40}	0.00334125	1007
RS_{41}	0.000495	1275
RS_{42}	0.004455	1250
RS_{43}	0.000495	1125
RS_{44}	0.004455	1100
RS_{45}	0.001485	1175
RS_{46}	0.013365	1150
RS_{47}	0.001485	1025
RS_{48}	0.013365	1000
RS_{49}	0.00235125	281
RS_{50}	0.02116125	257
RS_{51}	0.00235125	131
RS_{52}	0.02116125	107
RS_{53}	0.00705375	181
RS_{54}	0.06348375	157
RS_{55}	0.00705375	31
RS_{56}	0.06348375	7
RS_{57}	0.009405	275
RS_{58}	0.084645	250
RS_{59}	0.009405	125
RS_{60}	0.084645	100
RS_{61}	0.028215	175
RS_{62}	0.253935	150
RS_{63}	0.028215	25
RS_{64}	0.253935	0

4.9 Analysis

The methodology provides the distribution of consequences possible from divesting a military capability to an allied nation. The next logical question is how this information might be employed by a decision maker.

4.9.1 Traditional Decision Context

First, in order to make a decision, a decision maker could compare the probability of exceedance curves of each decision alternative. A probability of exceedance curve shows the cumulative likelihood that a consequence will exceed a specified value. The exceedance curve for the alternative to divest *Tactical Surveillance of Mobile Terrestrial Targets* is shown in Figure 4.3.

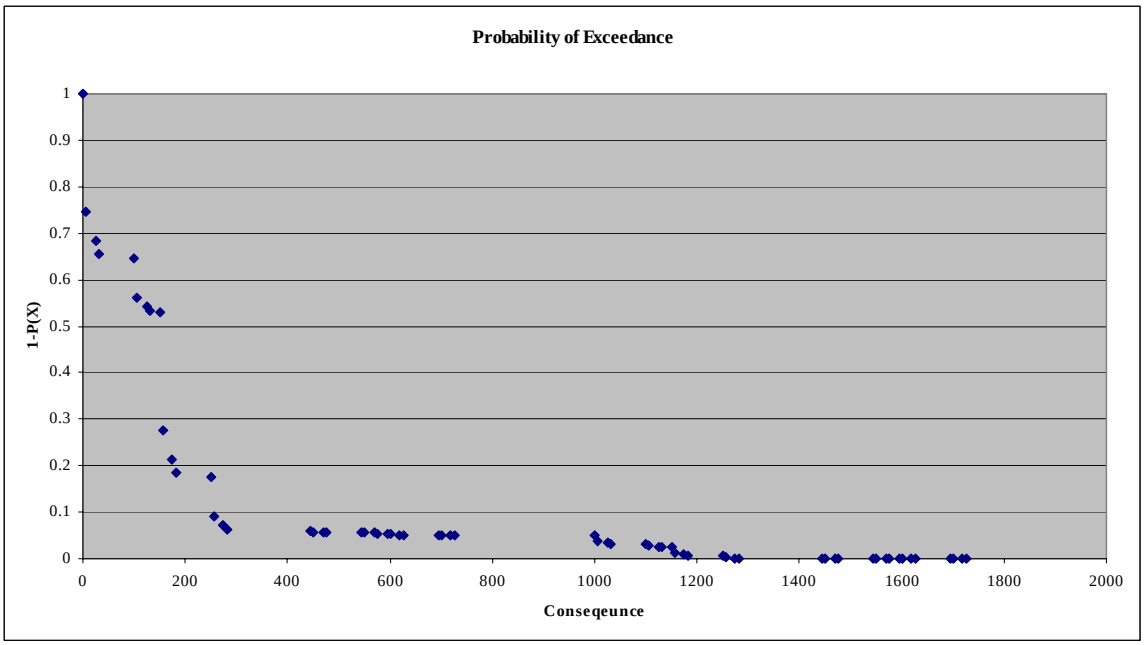

Figure 4.3 Probability of Exceedance Curve

If the cumulative likelihood of every consequence of a particular decision alternative is less or equally likely than every consequence of another alternative, then the first alternative is said to be stochastically dominant over the second. If a decision alternative is dominant over another alternative then the dominating alternative is preferred. If the conditions for dominance are violated then other methods for ranking the decision alternatives are necessary, in this case, evaluation under a utility model. Additionally, if multiple risk factors are considered, a multi-attribute utility model is necessary to rank the alternatives

A second technique for ranking alternatives is to compare risk measures. For this application, risk can be measured using the conditional expected consequence presented in Section 4.7 or using the other measures as outlined in Section 2.4.3. Conditional expected consequence is often considered an adequate measure of risk because it accounts for the most extreme events possible in a distribution. The expectation and two conditional expectations for the data in Table 4.8 are presented in Table 4.9.

Table 4.9 Unmitigated Measures of Risk

E[X]	**158**
E[X|P(X) >=.75]	**455**
E[X|P(X) >=.90]	**750**

4.10 Post Decision Analysis

Once a decision maker has chosen a decision alternative, he may be interested in reducing the risk associated with that alternative. Because of the structure of the methodology, the relevant question is not which risk scenarios are of most concern but which contingency events are of most concern.

Upon examining the likelihoods and consequences of the contingency events, two stand out: Contingency 2, which has the highest conditional expected consequence, and Contingency 5, which has the highest likelihood. These contingencies are presented in the following table.

Table 4.10 Contingencies of Concern

Contingency *i*	Description	L(Occurrence)	L(Non-Occurrence)	E[X|P(X) >=.9]
1	Major Regional Conflict in Raetia	0.01	0.99	444
2	Major regional conflict in Noricum	0.05	0.95	1000
3	Humanitarian Assisstance in Dacia	0.20	0.80	7
4	Small Scale Conflict in Lycia	0.25	0.75	100
5	Small Scale Conflict in Numidia	0.50	0.50	150
6	Stability Operations in Baetica	0.10	0.90	25

Contingency 2 is examined first. Why does Contingency 2 produce such severe consequences? To answer this question it is necessary to examine its constituent contingency scenarios. The largest consequences under Contingency 2 result from the scenarios in which the capability is not implemented. These scenarios are presented below.

Table 4.11 Contingency Events of Concern

CS_j	IS	RS	PS	Likelihood	Consequence
CS_1	IS_{full}	RS_{high}	PS_{high}	0.5120	0
CS_2	IS_{full}	RS_{high}	PS_{med}	0.0640	150
CS_3	IS_{full}	RS_{high}	PS_{low}	0.0640	400
CS_4	IS_{none}	RS_{high}	PS_{high}	0.1280	1000
CS_5	IS_{none}	RS_{high}	PS_{med}	0.0160	1000
CS_6	IS_{none}	RS_{high}	PS_{low}	0.0160	1000
CS_7	IS_{full}	RS_{med}	PS_{high}	0.0640	0
CS_8	IS_{full}	RS_{med}	PS_{med}	0.0080	0
CS_9	IS_{full}	RS_{med}	PS_{low}	0.0080	200
CS_{10}	IS_{none}	RS_{med}	PS_{high}	0.0160	600
CS_{11}	IS_{none}	RS_{med}	PS_{med}	0.0020	600
CS_{12}	IS_{none}	RS_{med}	PS_{low}	0.0020	600
CS_{13}	IS_{full}	RS_{low}	PS_{high}	0.0640	0
CS_{14}	IS_{full}	RS_{low}	PS_{med}	0.0080	0
CS_{15}	IS_{full}	RS_{low}	PS_{low}	0.0080	0
CS_{16}	IS_{none}	RS_{low}	PS_{high}	0.0160	100
CS_{17}	IS_{none}	RS_{low}	PS_{med}	0.0020	100
CS_{18}	IS_{none}	RS_{low}	PS_{low}	0.0020	100

In this context, risk can be mitigated if the decision maker can ensure that the host nation will implement its capability if Contingency 2 occurs. Assuming this can be guaranteed (which implies the likelihood of full implementation equals one), the measure of risk for Contingency 2 falls from 1000 to 378. The resulting overall measures of risk are presented in Table 4.12. All three measures of risk have decreased significantly, particularly the conditional expectations.

Table 4.12 Mitigation Option 1

E[X]	**127**
E[X|P(X) >=.75]	**309**
E[X|P(X) >=.90]	**413**

Next, consider Contingency 5. Recall, Contingency 5 is of concern because of its high likelihood of occurrence. The decision maker may be interested in the effect on the risk of divestiture if the contingency could be avoided entirely. Assuming the U.S. can take actions that result in the likelihood of Contingency 5 being negligible (i.e., its likelihood of occurrence equals .01); the resulting measures of risk are presented in Table 4.13.

Table 4.13 Mitigation Option 2

E[X]	85
E[X|P(X) >=.75]	487
E[X|P(X) >=.90]	660

Both mitigation options are presented along with the no mitigation option in the following table.

Table 4.14 Results

Mit Optn	Description	E[X]	E[X|P(X) >=.75]	E[X|P(X) >=.90]
0	No Mitigation	158	455	750
1	Ensuring Implementation in Contingency 2	127	309	413
2	Avoiding Contingency 5	85	487	660

4.11 Summary

This chapter applied the risk assessment methodology presented Chapter 3 to the decision to divest the Air Force capability *Tactical Surveillance of Mobile Terrestrial Targets* to an allied nation. First, it generated the set of risk scenarios, likelihoods and consequences that define the risk of divesting the capability. Second, it measured the risk of divestiture via the conditional expected consequence operator. Finally, it investigated which scenarios were the most significant contributors of risk and conducted a sensitivity

analysis to evaluate how the measures of risk change if these scenarios can be managed by the decision maker.

5 Conclusion

5.1 Summary

This thesis provided a tractable methodology to identify the three elements (i.e., risk scenarios, likelihoods and consequences) that define the risk of each decision alternative in the decision to divest a military capability to an allied nation.

In this methodology, risk scenarios are defined as combinations of contingencies that require the capability considered for divestiture. The likelihood of each risk scenario is calculated as the product of the likelihood of the contingency events that compose it.

The consequence of each risk scenario is defined as the sum of the consequences of the contingency events that compose it. Each contingency event, however, possesses a distribution of consequences. To facilitate assessment of the distribution of consequences, each contingency event is decomposed into a set of contingency scenarios. Each contingency scenario is defined by an available and required capability level. Levels of capability are defined by the states a capability can possibly take on under a set of measures defined by subject matter experts. Each contingency scenario produces a unique consequence that can be estimated by subject matter experts based on the differential in the required and available capability levels.

In order to construct the consequence of each risk scenario, the consequence of each contingency event must be combined. This requires collapsing the distribution of consequences of each contingency event into a representative measure for which addition is defined. This measure should be chosen carefully so that the most extreme consequences are accounted for. An appropriate measure for this task is the conditional

expected consequence. This measure calculates the expected consequence given that the consequence exceeds a specified threshold.

Once the distribution of each contingency event has been measured, the measures are added appropriately to construct the consequence of each risk scenario. This process results in a complete set of risk scenarios, likelihoods and consequences for each decision alternative.

Next, this information is applied to the decision process. If a decision maker has not yet made a decision, the risk of each decision alternative can provide input to the decision process via several mechanisms. First, exceedance curves for alternatives can be compared; second, the distributions of consequence can be evaluated in a utility model; finally, the risk can be used as a decision attribute. The conditional expected consequence was proposed as an adequate measure of risk in this context. If the decision maker has already chosen a decision alternative, sensitivity analysis on the risk calculations can be used to determine the most significant contributors to risk. This knowledge then drives risk mitigation options that can be evaluated under the proposed methodology.

5.2 Methodology Improvements

There are several aspects of the methodology that could be improved by further study. First, methods to combine expert opinion and available information to produce more accurate assessments of likelihood and consequence should be explored. Second, alternative decompositions of contingency events should be examined to determine the optimal level of resolution necessary to elicit accurate assessments of consequence.

5.2.1 Objectivity of Inputs

Every risk assessment methodology is dependent on the accuracy of its inputs. In the context of capability divestiture, these inputs are highly subjective because many of the risk scenarios have never before been realized. Consequently, frequency data cannot be used to estimate the likelihoods of risk scenarios nor can historical data be used to directly assess the consequences of risk scenarios.

Ideally, however, the inputs to a risk assessment should be objective. In order to obtain a more robust estimate of the likelihood of a risk scenario, several authors have suggested methods based on Bayes' theorem to fuse all available information and produce more accurate assessments of both likelihood and consequence. Incorporation of this technique into the methodology could produce more accurate assessments of risk.

5.2.2 Decomposition of Contingency Events

Alternative decompositions of contingency events should also be explored. Conceptually, an inverse relationship exists between the tractability of a risk assessment methodology and its accuracy. A methodology that facilitates the most accurate assessments of consequence necessarily requires the most specific risk scenarios, and is consequently less practical to construct. Conversely, a tractable methodology is tractable precisely because the resolution of its risk scenarios is low.

The intent of this thesis was to decompose a contingency event generically, so that the decomposition is not dependent on the specific capability, yet in a manner that still provides enough resolution to a potential subject matter expert to facilitate an accurate assessment of consequence. However, in practice this partition is likely too

coarse for a subject matter expert to accurately assess consequences. Decompositions using Haimes' HHM or Kaplan's TSS may result in more detailed contingency scenarios that facilitate more accurate assessment of consequence.

Appendix

The notional data used in Chapter 4 is presented in the Appendix. Baseline likelihoods and consequences are presented in Tables A.1 and A.2. The revised risk for mitigation option one is presented in table A.3. The revised risk for mitigation option two is presented in table A.4

Table A.1 Baseline Scenario Likelihoods

Contingency 1

RS	Likelihood
RS_{high}	0.70
RS_{med}	0.20
RS_{low}	0.10

IS	Likelihood
IS_{full}	0.90
IS_{none}	0.10

PS	Likelihood
PS_{high}	0.80
PS_{med}	0.10
PS_{low}	0.10

Contingency 2

RS	Likelihood
RS_{high}	0.80
RS_{med}	0.10
RS_{low}	0.10

IS	Likelihood
IS_{full}	0.80
IS_{none}	0.20

PS	Likelihood
PS_{high}	0.80
PS_{med}	0.10
PS_{low}	0.10

Contingency 3

RS	Likelihood
RS_{high}	0.20
RS_{med}	0.20
RS_{low}	0.60

IS	Likelihood
IS_{full}	0.90
IS_{none}	0.10

PS	Likelihood
PS_{high}	0.80
PS_{med}	0.10
PS_{low}	0.10

Contingency 4

RS	Likelihood
RS_{high}	0.70
RS_{med}	0.20
RS_{low}	0.10

IS	Likelihood
IS_{full}	0.85
IS_{none}	0.15

PS	Likelihood
PS_{high}	0.80
PS_{med}	0.10
PS_{low}	0.10

Contingency 5

RS	Likelihood
RS_{high}	0.55
RS_{med}	0.30
RS_{low}	0.15

IS	Likelihood
IS_{full}	0.70
IS_{none}	0.30

PS	Likelihood
PS_{high}	0.80
PS_{med}	0.10
PS_{low}	0.10

Contingency 6

RS	Likelihood
RS_{high}	0.50
RS_{med}	0.20
RS_{low}	0.30

IS	Likelihood
IS_{full}	0.82
IS_{none}	0.18

PS	Likelihood
PS_{high}	0.80
PS_{med}	0.10
PS_{low}	0.10

Table A.2 Contingency Consequences

Contingency 1

CS_j	L_j	X_j
CS_1	0.504	0
CS_2	0.063	120
CS_3	0.063	200
CS_4	0.056	500
CS_5	0.007	500
CS_6	0.007	500
CS_7	0.144	0
CS_8	0.018	0
CS_9	0.018	150
CS_{10}	0.016	250
CS_{11}	0.002	250
CS_{12}	0.002	250
CS_{13}	0.072	0
CS_{14}	0.009	0
CS_{15}	0.009	0
CS_{16}	0.008	100
CS_{17}	0.001	100
CS_{18}	0.001	100

Contingency 2

CS_j	L_j	X_j
CS_1	0.512	0
CS_2	0.064	150
CS_3	0.064	400
CS_4	0.128	1000
CS_5	0.016	1000
CS_6	0.016	1000
CS_7	0.064	0
CS_8	0.008	0
CS_9	0.008	200
CS_{10}	0.016	600
CS_{11}	0.002	600
CS_{12}	0.002	600
CS_{13}	0.064	0
CS_{14}	0.008	0
CS_{15}	0.008	0
CS_{16}	0.016	100
CS_{17}	0.002	100
CS_{18}	0.002	100

Contingency 3

CS_j	L_j	X_j
CS_1	0.144	0
CS_2	0.018	5
CS_3	0.018	6
CS_4	0.016	10
CS_5	0.002	10
CS_6	0.002	10
CS_7	0.144	0
CS_8	0.018	0
CS_9	0.018	5
CS_{10}	0.016	8
CS_{11}	0.002	8
CS_{12}	0.002	8
CS_{13}	0.432	0
CS_{14}	0.054	0
CS_{15}	0.054	0
CS_{16}	0.048	3
CS_{17}	0.006	3
CS_{18}	0.006	3

Contingency 4

CS_j	L_j	X_j
CS_1	0.476	0
CS_2	0.0595	15
CS_3	0.0595	30
CS_4	0.084	100
CS_5	0.0105	100
CS_6	0.0105	100
CS_7	0.136	0
CS_8	0.017	0
CS_9	0.017	20
CS_{10}	0.024	20
CS_{11}	0.003	20
CS_{12}	0.003	20
CS_{13}	0.068	0
CS_{14}	0.0085	0
CS_{15}	0.0085	0
CS_{16}	0.012	15
CS_{17}	0.0015	15
CS_{18}	0.0015	15

Contingency 5

CS_j	L_j	X_j
CS_1	0.308	0
CS_2	0.0385	50
CS_3	0.0385	75
CS_4	0.132	150
CS_5	0.0165	150
CS_6	0.0165	150
CS_7	0.168	0
CS_8	0.021	0
CS_9	0.021	50
CS_{10}	0.072	100
CS_{11}	0.009	100
CS_{12}	0.009	100
CS_{13}	0.084	0
CS_{14}	0.0105	0
CS_{15}	0.0105	0
CS_{16}	0.036	40
CS_{17}	0.0045	40
CS_{18}	0.0045	40

Contingency 6

CS_j	L_j	X_j
CS_1	0.328	0
CS_2	0.041	15
CS_3	0.041	20
CS_4	0.072	25
CS_5	0.009	25
CS_6	0.009	25
CS_7	0.1312	0
CS_8	0.0164	0
CS_9	0.0164	15
CS_{10}	0.0288	20
CS_{11}	0.0036	20
CS_{12}	0.0036	20
CS_{13}	0.1968	0
CS_{14}	0.0246	0
CS_{15}	0.0246	0
CS_{16}	0.0432	10
CS_{17}	0.0054	10
CS_{18}	0.0054	10

Table A.3 Mitigation Option 1 Risk

RS_j	L_j	X_j
RS_1	1.25E-06	1104
RS_2	1.13E-05	1079
RS_3	1.25E-06	954
RS_4	1.13E-05	929
RS_5	3.75E-06	1004
RS_6	3.38E-05	979
RS_7	3.75E-06	854
RS_8	3.38E-05	829
RS_9	0.000005	1097
RS_{10}	0.000045	1072
RS_{11}	0.000005	947
RS_{12}	0.000045	922
RS_{13}	0.000015	997
RS_{14}	0.000135	972
RS_{15}	0.000015	847
RS_{16}	0.000135	822
RS_{17}	2.38E-05	726
RS_{18}	0.000214	701
RS_{19}	2.38E-05	576
RS_{20}	0.000214	551
RS_{21}	7.13E-05	626
RS_{22}	0.000641	601
RS_{23}	7.13E-05	476
RS_{24}	0.000641	451
RS_{25}	0.000095	719
RS_{26}	0.000855	694
RS_{27}	0.000095	569
RS_{28}	0.000855	544
RS_{29}	0.000285	619
RS_{30}	0.002565	594
RS_{31}	0.000285	469
RS_{32}	0.002565	444

RS_j	L_j	X_j
RS_{33}	0.000124	659
RS_{34}	0.001114	635
RS_{35}	0.000124	509
RS_{36}	0.001114	485
RS_{37}	0.000371	559
RS_{38}	0.003341	535
RS_{39}	0.000371	409
RS_{40}	0.003341	385
RS_{41}	0.000495	653
RS_{42}	0.004455	628
RS_{43}	0.000495	503
RS_{44}	0.004455	478
RS_{45}	0.001485	553
RS_{46}	0.013365	528
RS_{47}	0.001485	403
RS_{48}	0.013365	378
RS_{49}	0.002351	281
RS_{50}	0.021161	257
RS_{51}	0.002351	131
RS_{52}	0.021161	107
RS_{53}	0.007054	181
RS_{54}	0.063484	157
RS_{55}	0.007054	31
RS_{56}	0.063484	7
RS_{57}	0.009405	275
RS_{58}	0.084645	250
RS_{59}	0.009405	125
RS_{60}	0.084645	100
RS_{61}	0.028215	175
RS_{62}	0.253935	150
RS_{63}	0.028215	25
RS_{64}	0.253935	0

Table A.4 Mitigation Option 2 Risk

RS_j	L_j	X_j
RS_1	2.5E-08	1726
RS_2	2.25E-07	1701
RS_3	2.48E-06	1576
RS_4	2.23E-05	1551
RS_5	7.5E-08	1626
RS_6	6.75E-07	1601
RS_7	7.43E-06	1476
RS_8	6.68E-05	1451
RS_9	1E-07	1719
RS_{10}	9E-07	1694
RS_{11}	9.9E-06	1569
RS_{12}	8.91E-05	1544
RS_{13}	3E-07	1619
RS_{14}	2.7E-06	1594
RS_{15}	2.97E-05	1469
RS_{16}	0.000267	1444
RS_{17}	4.75E-07	726
RS_{18}	4.28E-06	701
RS_{19}	4.7E-05	576
RS_{20}	0.000423	551
RS_{21}	1.43E-06	626
RS_{22}	1.28E-05	601
RS_{23}	0.000141	476
RS_{24}	0.00127	451
RS_{25}	1.9E-06	719
RS_{26}	1.71E-05	694
RS_{27}	0.000188	569
RS_{28}	0.001693	544
RS_{29}	5.7E-06	619
RS_{30}	5.13E-05	594
RS_{31}	0.000564	469
RS_{32}	0.005079	444

RS_j	L_j	X_j
RS_{33}	2.48E-06	1281
RS_{34}	2.23E-05	1257
RS_{35}	0.000245	1131
RS_{36}	0.002205	1107
RS_{37}	7.43E-06	1181
RS_{38}	6.68E-05	1157
RS_{39}	0.000735	1031
RS_{40}	0.006616	1007
RS_{41}	9.9E-06	1275
RS_{42}	8.91E-05	1250
RS_{43}	0.00098	1125
RS_{44}	0.008821	1100
RS_{45}	2.97E-05	1175
RS_{46}	0.000267	1150
RS_{47}	0.00294	1025
RS_{48}	0.026463	1000
RS_{49}	4.7E-05	281
RS_{50}	0.000423	257
RS_{51}	0.004655	131
RS_{52}	0.041899	107
RS_{53}	0.000141	181
RS_{54}	0.00127	157
RS_{55}	0.013966	31
RS_{56}	0.125698	7
RS_{57}	0.000188	275
RS_{58}	0.001693	250
RS_{59}	0.018622	125
RS_{60}	0.167597	100
RS_{61}	0.000564	175
RS_{62}	0.005079	150
RS_{63}	0.055866	25
RS_{64}	0.502791	0

Bibliography

Crissman, D. Joint Capability Areas. Briefing. Apr 2002.

Department of Defense. Universal Joint Task List. Presentation. 11 Mar 2005.

-----. *Fiscal 2005 Department of Defense Budget Release*. Article. n. pag. 2 Feb 04. 1 Jan 06 http://www.defenselink.mil/releases/2004/nr20040202-0301.html.

-----. *Joint Defense Capabilities Study: Final Report*. Report. Dec 2003. 1 Jan 06 http://www.paxriver.org/files/ACF1223%2Epdf

-----. *Quadrennial Defense Review*. Quadrennial Report. 30 Sept 2001. 9 Jan 2006 http://www.defenselink.mil/pubs/qdr2001.pdf.

French, S. Decision *Theory: An Introduction to the Mathematics of Rationality*. New York: John Wiley & Sons, 1986.

Haimes, Y. *Risk Modeling, Assessment and Management*. New Jersey: John Wiley & Sons, 2004.

Johnson, D. Air Force Capabilities Based Planning and the CRRA. Briefing. 25 Aug 05.

Kaplan, S. "On the Method of Discrete Probability Distributions in Risk and Reliability Calculations-Application to Seismic Risk Assessment," *Risk Analysis*, 1: 189-196 (August 1981).

Kaplan, S. "The *general theory of quantitative risk assessment*," in Risk based decision making in water resources V, 11-39. Eds. Haimes, D.A. Moser, and E.Z. Stakhiv. New York: American Society of Civil Engineers, 1991.

Kaplan, S. and Garrick J. "On the Quantitative Definition of Risk," *Risk Analysis*, 1: 11-27 (1981).

Kaplan, S. Visnepolschi, S. Zlotin, B. Zusman, A. *New Tools for Failure and Risk Analysis.* Southfield, MI: Ideation International, 1999.

Kiefer, Todd. "Capabilities Based Planning and Concepts." Presentation. 22 Sept 2004.

Miles, R. "Risk-Adjusted Mission Value: Trading Off Mission Risk for Mission Value," *Risk Analysis* 24: 415-424 (2004).

Quigley, D. *Review of the lease of F-16 Aircraft for the Royal New Zealand Air Force*. Report. n. pag. 30 Nov 05. http://www.executive.govt.nz/f16/index.html.

Rausand, M. and Hoyland A. *System Reliability Theory*. New Jersey: John Wiley & Sons, 2004.

Sarin, R. and Weber, M. "Risk-value Models," *European Journal of Operations Research*, 70: 135-149 (January 1993).

Shah, Anup. "In Context: U.S. Military Spending Versus Rest of the World." Webpage. n. pag. 1 Jun 2005. 2 Jan 06 http://www.globalissues.org/Geopolitics/ArmsTrade/Spending.asp#InContextUSMilitarySpendingVersusRestoftheWorld.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
23-03-2006	**Master's Thesis**	Sep 2004 - Mar 2006

4. TITLE AND SUBTITLE
A RISK ASSESSMENT METHODOLOGY FOR DIVESTING MILITARY CAPABILITY TO ALLIED NATIONS

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Gastelum, Jason, A., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Street, Building 642
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GOR/ENS/06-09

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
OSD/PA&E
Attn: Maj Paul McAree
Wilson Blvd, Suite 300 DSN: 426-9380
Arlington, VA 22209-2306 e-mail: paul.mcaree@osd.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The United States spent over $400 billion dollars on national defense in 2005. Even with support for the war on terrorism still strong, it is doubtful that the U.S. can sustain such a level of defense investment. One strategy to offset the increasing burden of defense spending is to divest the procurement and/or sustainment of individual defense capabilities to allied nations. The decision to divest any capability, however, introduces risk. This thesis presents a methodology to quantify the risk of the decision to divest a military capability to an allied nation, where risk is defined as the set of risk scenarios, likelihoods and consequences possible under each decision alternative. Risk scenarios are composed of combinations of contingencies that require the capability considered for divestiture. The likelihood of each risk scenario is calculated as the product of the likelihoods of its constituent contingency events. The consequence of each risk scenario is calculated as the sum of the consequences of its constituent contingency events. Once the risk of each decision alternative is quantified this information can be used to rank alternatives and identify the scenarios that contribute most to the risk of each alternative.

15. SUBJECT TERMS
Risk, Risk Analysis, Risk Management, Military Capabilities

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			David R. Denhard, LtCol, USAF (ENS)
U	U	U	UU	90	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 3325; e-mail: David.Denhard@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18