VIRGINIA COMMONWEALTH UNIVERSITY

Virginia Commonwealth University
VCU Scholars Compass

Theses and Dissertations

Graduate School

2010

Making decisions about screening cargo containers for nuclear threats using decision analysis and optimization

Jamie Dauberman
Virginia Commonwealth University

Making decisions about screening cargo containers for nuclear threats using decision analysis and optimization

by

Jamie Lynn Dauberman

B.S. Statistical Sciences & Operations Research
Virginia Commonwealth University
2008

M.S. Statistical Sciences & Operations Research
Virginia Commonwealth University
2010

Director: Laura A. McLay
Department of Statistical Sciences & Operations Research
Virginia Commonwealth University

Virginia Commonwealth University
Richmond, Virginia
August, 2010

Acknowledgment

The author wishes to thank several people. I would like to thank Dr. Merrick for his motivating speeches when I felt like giving up, direction when I was lost, help when I was discouraged, and kind words when all else failed. I couldn’t have completed my research or this degree without his motivation and support. He went above and beyond and I can’t thank him enough, especially with my thesis defense preparation. I would also like to thank Dr. McLay for the many opportunities she’s given me. She helped me grow in the field and as a person, constantly challenging me with new research opportunities, exposing me to conferences, encouraging me to give talks and presentations, and most importantly, showing me what it takes to make it in the field as a wife and mother. I would like to thank my husband, Willie, for his love, support and patience. I know I’ve made living with me a challenge at times. I would like to thank my parents, without them, I wouldn’t have ever even had the opportunity to enroll in college. They’ve supported me in every way, encouraged me, and loved me endlessly. I would not be where I am today without them. Last but not least, I would like to thank the rest of my family and my friends for their unending love and support. Each one of you has given me the “pep talks” I needed to continue with my research. I couldn’t have done it without you. So thank you very much!

Table of Contents

List of Figures

List of Tables

Abstract

One of the most pressing concerns in homeland security is the illegal passing of weapons-grade nuclear material through the borders of the United States. If terrorists can gather the materials needed to construct a nuclear bomb or radiological dispersion device (RDD, i.e., dirty bomb) while inside the United States, the consequences would be devastating. Preventing plutonium, highly enriched uranium (HEU), tritium gas or other materials that can be used to construct a nuclear weapon from illegally entering the United States is an area of vital concern.

There are enormous economic consequences when our nation's port security system is compromised. Interdicting nuclear material being smuggled into the United States on cargo containers is an issue of vital national interest, since it is a critical aspect of protecting the United States from nuclear attacks. However, the efforts made to prevent nuclear material from entering the United States via cargo containers have been disjoint, piecemeal, and reactive, not the result of coordinated, systematic planning and analysis. Our economic well-being is intrinsically linked with the success and security of the international trade system. International trade accounts for more than thirty percent of the United States economy (Rooney, 2005). Ninety-five percent of international goods that enter the United States come through one of 361 ports, adding up to more than 11.4 million containers every year (Fritelli, 2005; Rooney, 2005; US DOT, 2007). Port security has emerged as a critically important yet vulnerable component in the homeland security system.

Applying game theoretic methods to counterterrorism provides a structured technique for defenders to analyzing the way adversaries will interact under different circumstances and scenarios. This way of thinking is somewhat counterintuitive, but is an extremely useful tool in analyzing potential strategies for defenders.

Decision analysis can handle very large and complex problems by integrating multiple perspectives and providing a structured process in evaluating preferences and values from the individuals involved. The process can still ensure that the decision still focuses on achieving the fundamental objectives. In the decision analysis process value tradeoffs are evaluated to review alternatives and attitudes to risk can be quantified to help the decision maker understand what aspects of the problem are not under their control. Most of all decision analysis provides insight that may not have been captured or fully understood if decision analysis was not incorporated into the decision making process. All of these factors make decision analysis essentially to making an informed decision.

Game theory and decision analysis both play important roles in counterterrorism efforts. However, they both have their weaknesses. Decision analysis techniques such as probabilistic risk analysis can provide incorrect assessments of risk when modeling intelligent adversaries as uncertain hazards. Game theory analysis also has limitations. For example when analyzing a terrorist or terrorist group using game theory we can only take into consideration one aspect of the problem to optimize at a time. Meaning the analysis is either analyzing the problem from the

defenders perspective or from the attacker's perspective. Parnell et al. (2009) was able to develop a model that simultaneously maximizes the effects of the terrorist and minimizes the consequences for the defender.

The question this thesis aims to answer is whether investing in new detector technology for screening cargo containers is a worthwhile investment for protecting our country from a terrorist attack. This thesis introduces an intelligent adversary risk analysis model for determining whether to use new radiological screening technologies at our nation's ports. This technique provides a more realistic risk assessment of the true situation being modeled and determines whether it is cost effective for our country to invest in new cargo container screening technology. The optimal decision determined by our model is for the United States to invest in a new detector, and for the terrorists to choose agent cobalt-60, shown in Figure 18. This is mainly due to the prominence of false alarms and the high costs associated with screening all of these false alarms, and we assume for every cargo container that sounds an alarm, that container is physically inspected. With the new detector technology the prominence of false alarms decreases and the true alarm rate increases, the cost savings associated with this change in the new technology outweighs the cost of technical success or failure. Since the United States is attempting to minimize their expected cost per container, the optimal choice is to invest in the new detector. Our intelligent adversary risk analysis model can simultaneously determine the best decision for the United States, who is trying to minimize the expected cost, and the terrorist, who is trying to maximize the expected cost to the United States. Simultaneously modeling the decisions of the defender and attacker provides a more accurate picture of reality and could provide important insights to the real situation that may have been missed with other techniques.

The model is extremely sensitive to certain inputs and parameters, even though the values are in line with what is available in the literature, it is important to understand the sensitivities. Two inputs that were found to be particularly important are the expected cost for physically inspecting a cargo container, and the cost of implementing the technology needed for the new screening device. Using this model the decision maker can construct more accurate judgments based on the true situation. This increase in accuracy could save lives with the decisions being made. The model can also help the decision maker understand the interdependencies of the model and visually see how his resource allocations affect the optimal decisions of the defender and the attacker.

Thesis Introduction

This thesis introduces an intelligent adversary risk analysis model for determining whether to use new radiological screening technologies at our nation's ports. This technique provides a more realistic risk assessment of the true situation being modeled and determines whether it is cost effective for our country to invest in new cargo container screening technology. Our intelligent adversary risk analysis model can simultaneously determine the optimal decision for the United States, who is trying to minimize the expected cost, and the terrorist, who is trying to maximize the expected cost to the United States. The decision the United States is whether or not to invest in developing the technology needed for a new radiological screening device. The terrorist is trying to determine which agent to use when they attack the United States. Simultaneously modeling the decisions of the defender and attacker provides a more accurate picture of reality and could provide important insights to the real situation that may have been missed with other techniques. The actions of the defender will affect the actions of the attacker, and this interaction can be accurately captured using the intelligent adversary risk analysis model introduced in this thesis.

1.1 Motivation

The terrorist attacks against the United States highlighted how fragile our nation's security system is. As a direct result of the attacks on September 11, 2001, billions of dollars have been spent on improving aviation security in attempt to minimize the likelihood of another terrorist event. However, aviation security is just one security component, and other measures need to be taken for more comprehensive improvements in homeland security. For example, our nation's ports are a vital component of our nation's security, yet the security efforts thus far have been disjoint and unorganized.

One of the most pressing concerns in homeland security is the illegal passing of weapons-grade nuclear material through the borders of the United States. If terrorists can gather the materials needed to construct a nuclear bomb or radiological dispersion device (RDD, i.e., dirty bomb) while inside the United States, the consequences would be devastating. Preventing plutonium, highly enriched uranium (HEU), tritium gas or other materials that can be used to construct a nuclear weapon from illegally entering the United States is an area of vital concern. Unfortunately, there are places in the world, such as the former Soviet Union, where these materials are not secure. Howard Baker, the former U.S. ambassador to Japan and the former Republican leader of the Senate, testified on Capitol Hill, "It really boggles my mind that there could be 40,000 nuclear weapons, or maybe 80,000 in the former Soviet Union, poorly controlled and poorly stored, and that the world is not in a near-state of hysteria about the danger" (Allison 2004).

In recent years, the security standards in the Soviet Union have begun to improve due to the Second Line of Defense program. However, nuclear materials have been stolen and could potentially be up for sale or already sold. From 1993 to December 2006, there were 332 confirmed incidents which involved the theft or loss of nuclear or other radioactive materials, in sixty-seven percent of these cases, the materials have not been recovered (IAEA, 2006). The International Atomic Energy Agency developed the Illicit Trafficking Database (ITDB) program which requires participating countries to report incidents of illicit distribution and other illegal activities involving nuclear and radioactive materials (IAEA, 2006). The threat of terrorists securing the essential components of a nuclear weapon is a real danger, and implementing security measures to prevent nuclear material from entering the United States has to improve.

It is imperative to be proactive in our security measures in order to protect the United States from a nuclear attack. The terrorists that have attacked the United States in the past did so to ensure mass panic while maximizing the potential economic impact. Because the weapons used on September 11, 2001 were passenger planes full of fuel and innocent people, the impact on the airline industry and the United States economy on September 11, 2001was immediate and overwhelming. New York's economy was arguably hit the hardest, since it was the major target area of the terrorist attacks. From the time the terrorist attack was launched until the end of 2004, the total economic loss to New York is estimated to be between 82.4 and 94.8 billion dollars (Thompson, 2002). In addition to the economy, certain industries suffered greater losses than others, mainly the airline and insurance industries. At the end of 2001, the airlines reported 80,000 layoffs and net losses of more than seven billion dollars (Belobaba, 2006). The federal government quickly came to the aid of the airlines giving five billion dollars in short-term assistance and approximately ten billion in loan guarantees (Makinen, 2002). However, this aid still wasn’t enough; some airlines still had to file bankruptcy.

The economic result of September 11, 2001 spanned farther than just the airline industry. The insurance industry had to payout the largest claim in history, approximately forty billion dollars, from loss of life and property damage claims (Insurance Information Institute, 2002; Makinen, 2002). As a direct result of the terrorist attacks, approximately 18,000 small businesses were destroyed, displaced, or disrupted (Makinen, 2002). These effects are long-lasting and are still impacting the airline industry and the overall economy of the United States. Not only did the United States have to pay out billions of dollars in recovery efforts, and other expenses immediately after September 11, 2001, but we are continuing to spend resources that previously would have gone to improvements in product, but are now being spent on improving security measures (Makinen, 2002).

Major counterterrorism research and development efforts have emerged since September 11, 2001. The Department of Homeland Security (DHS) was formed and combined 22 different agencies and approximately 170,000 total federal employees to better and more efficiently manage who and what enters the United States. DHS also is working to prevent the entry of terrorists and the instruments of terrorism while simultaneously ensuring the efficient flow of legitimate traffic.

An area that needs increased protection and advanced security is the 361 U.S. ports. American ports are a fundamental component of the U.S. economy, since nearly all goods entering the

United States enter through one of its ports. Note that not all ports are seaports, and hence, the port system is a diverse system. A port can be defined as an entry to a country, where people or merchandise can lawfully enter. Approximately 1/9 of all cargo containers go to or from the United States (US DOT, 2007). Cargo containers are approximately the size of a truck trailer. A container that is 8 x 8 x 20 feet is commonly abbreviated as a twenty-foot equivalent unit (TEU). Standard sizes of cargo containers are 8 x 8 x 20 feet (one TEU) or 8 x 8 x 40 feet long (two TEUs). Note that not all goods entering the United States are in cargo containers. Some goods, such as timber, may enter the United States on a vessel. This thesis focuses on the screening of goods in cargo containers.

The United States ports are critical gateways to our country for foreign cargo and supplies, most of which are brought to our country on cargo containers. According to the Bureau of Transportation Statistics an average of 50,000 TEUs enter the United States daily. With this magnitude of cargo traffic moving through the U.S. ports, it can be a challenge to maintain efficient flow while also ensuring a satisfactory level of security to prevent potential terrorist attacks (US DOT, 2007). The TEU traffic through the United States seaports is increasing at a rapid rate. Taking into consideration the top ten marine ports in the United States, the percent increase in TEU's between the years of 1995 and 2005 was 94.1. Considering the top port of Los Angeles, CA the percent increase during these years was 163.1 (US DOT, 2007). This increase in cargo traffic poses a challenge for screening cargo containers entering the United States.

There has been more than one occasion where cargo containers were discovered equipped for a terrorist to travel inside the container to North America. One such occasion was reported that a suspected al-Qaeda terrorist was found inside a container traveling to Canada, and he was carrying plans of airports, an aviation mechanic's certificate, and security passes (The Economist, 2002). Obviously, the terrorists have realized the security weaknesses of the world's ports. Improving port security operations is a critical component in preventing and interdicting illicit nuclear material entering the United States.

There are over 15 million containers that are moving around at sea, on land, or standing in yards waiting to be delivered (The Economist, 2002). This magnitude and variety of cargo containers demonstrates that the security measures can not only be taken at our seaports, but also places like land-border crossings, weigh stations for trucks transporting cargo containers, or even at train stations. Each of these places could be security hubs equipped with technology to screen passing cargo containers. At such security hubs, cargo containers could be screened by being scanned by a radiation portal monitor, IID or by being inspected by imaging technologies such as high-energy X-rays or physical inspection. Currently in the United States, it's not uncommon for cargo containers to be delivered to their destination before their very first inspection.

Maritime experts have developed programs to minimize interruptions to the flow of container traffic while simultaneously improving the security measures of United States ports. These proposals implemented to help secure the United States ports were mainly driven by the Maritime Transportation Security Act of 2002, which required the creation of a universal security program to identify and deter threats from entering our ports. Some additional measures have also been implemented in efforts to make our nations ports more secure, for example the expansion of the 24-hour Notice of Arrival (NOA) rule to a 96-hour NOA. The benefit to the 96 hour NOA is that it gives Bureau of Customs and Border Protection (CBP) adequate time to assess the upcoming vessels threat level. The Container Security Initiative (CSI) along with the Customs Trade Partnership Against Terrorism (C-TPAT) are two additional initiatives whose objectives include improving port security operations in the United States. The CSI program pre-screens containers at foreign ports in attempt to eliminate a threat container from ever reaching United States soil. If containers comply with CBP regulations, the C-TPAT agreement allows expedited processing to these containers. Cargo containers that are in compliance with C-TPAT have fewer delays. These initiatives are improving port security, but they are a long way away from improving port security at its optimal level. Through operations research the continuing development of cost an effective security implications, security improvements, and new innovative ideas could have the potential to drastically improve our nation's port security operations.

There are enormous economic consequences when our nation's port security system is compromised. Interdicting nuclear material being smuggled into the United States on cargo containers is an issue of vital national interest, since it is a critical aspect of protecting the United States from nuclear attacks. However, the efforts made to prevent nuclear material from entering the United States via cargo containers have been disjoint, piecemeal, and reactive, not the result of coordinated, systematic planning and analysis. Our economic well-being is intrinsically linked with the success and security of the international trade system. International trade accounts for more than thirty percent of the United States economy (Rooney, 2005). Ninety-five percent of international goods that enter the United States come through one of 361 ports, adding up to more than 11.4M containers every year (Fritelli, 2005; Rooney, 2005; US DOT, 2007). Port security has emerged as a critically important yet vulnerable component in the homeland security system.

Despite the importance of port security to our nation's economy, a small proportion of cargo entering United States ports are inspected for nuclear and radiological material. The Bureau of Customs and Border Protection (CBP) physically inspects approximately five-percent of all cargo containers entering United States ports (Robinson et al., 2005; Ramirez-Marquez, 2008). Screening resources are targeted at high-risk containers, and the Automated Targeting System (ATS) is used to prescreen each cargo container and classify it as high-risk as low-risk (Strohm, 2006). Cargo containers entering the United States at other entry points, such as land border crossings, are extremely unlikely to be physically inspected (Parrish, 2008). Strategies that use radiation detectors to interdict nuclear material on these otherwise uninspected cargo containers have the potential to prevent a nuclear attack.

It is difficult to screen many cargo containers as they enter the United States, particularly those that enter the United States at land border crossings (as opposed to ports) and those that are transported by trains or barges. Cargo containers can be screened at security stations that are not limited to the points of entry to the United States or at foreign ports, where most screening is currently performed. This thesis considers such a scenario, and it focuses on the screening operations within a single station. The methodology used in this thesis can be used as part of a diverse security system to intercept nuclear material with security stations at truck weigh stations along interstates, loading docks, train stations, or at ports. The approach taken in this thesis utilizes the model developed by Parnell et al. (2009) which is discussed in Chapter 4 of this thesis. We modify the model introduced by Parnell et al. (2009) to analyze screening techniques and procedures when considering both the decisions made by the United States and by the terrorists. This model will help determine whether actually investing in new detectors that screen cargo containers entering the United States is a worthwhile investment in the efforts of protecting our country from a terrorist attack.

1.2 The Game Theory Component

At first glance, it may seem that our country's best defense would be to identify the most likely targets and then put forth our maximum efforts to secure and protect those targets. However, by doing this, we show the terrorists where most of our resources have been allocated, thereby inadvertently identifying all formally less attractive targets as weaknesses. As a result the terrorists will then find these (formally) less attractive targets more desirable. This is due to the fact that there is less protection in place and therefore fewer deterrents. Terrorists are thought of as intelligent and rational adversaries who are able to adapt their strategies and/or plans to identify the most attractive targets that have the highest probabilities of a successful attack. Using game theoretic models we can analyze the strategies of terrorists and counterterrorist's. Game theory can be used to determine potential strategies with the highest probabilities of having a favorable outcome. Game theory allows us to take this idea of "move, countermove" into consideration mathematically to aid in quantifying and analyzing security strategies to protect against terrorism.

Applying game theoretic methods to counterterrorism provides a structured technique for defenders to analyzing the way adversaries will interact under different circumstances and scenarios. This way of thinking is somewhat counterintuitive, but is an extremely useful tool in analyzing potential strategies for defenders. To view terrorists as rational thinkers is counterintuitive in itself; however, you have to view their logic from their point of view (Wenzlaff, 2004). They find weaknesses and use them to their advantage, if they have a plan and somehow it gets revealed or compromised, they will most likely adapt and change their plan to something less expected. In this way terrorists are not only rational, they're very intelligent.

Terrorists will do whatever it takes to reduce the chance of discovery by the authorities prior to the completion of their plan. Terrorists strive to maximize their expected utilities (or gains) subject to certain constraints. These constraints include, but are not limited to, such things as budget, resources, expected gains, risk, and time (such as windows of opportunity). The terrorists take all these things into consideration when planning an attack, and therefore they can be thought of as rational thinkers, even if their actions seem irrational to us.

As explained above, game theory can be applied to analyzing terrorism due to the fact that both parties involved are considered to be rational thinkers. Game theory captures the relationship between the two parties and the strategic interactions between the parties. Both parties' decisions influence the sequential decisions or moves of the opposite party, therefore these two parties have to be modeled together since they are interdependent. Game theory can also take into consideration the fact that one or both sides may bluff or lie about their potential actions to try and gain some type of strategic advantage. Also game theory assumes that each player is trying to maximize their own goal subject to some constraints, which as mentioned before, does apply to terrorism.

In counterterrorism situations usually neither the terrorists nor the defender is completely informed, therefore there are uncertainties surrounding the other choices and strategies. These uncertainties can be included in game theory analysis. Usually the values in the game theory payoff tables are uncertain and therefore considered random variables, risk analysis can be used to estimate these values. Because statistics, Bayesian thinking, uncertainties, and other aspects can be modeled using game theory, it makes it an appropriate tool to model terrorism and the interactions between the involved parties.

1.3 The Decision Analysis Component

Decision analysis aims to ease the difficulty of a decision by providing a framework for thinking about the decision, and useful tools for analyzing the decision. The framework provided by decision analysis forces the decision maker to fully understand the problem by clearly stating and representing the decision. Simply by breaking down the decision into smaller components and studying the aspects of the decision, the decision maker may find enough insight to make an informed decision. However, if the decision is still difficult, the decision maker can employ some decision analysis tools, methods, and/or procedures that can further assist in the decision making process.

Clemen and Reilly (2001) state the first step in the decision analysis process is usually for the decision maker to determine the objectives of the decision and to make a flowchart of the decision process. This ensures that the decision maker has a clear understanding of the process and that they have a clear understanding of what they want to achieve out of the decision. Once the objectives and the decision structure are clearly stated, the decision maker then needs to consider alternatives.

The next two steps of the decision analysis process involve breaking down the decision into the smaller more manageable pieces. This step of the process is very important in understanding the total decision and how the pieces will fit together to form a model. By modeling the decision we can create a visual representation of the given decision and provide a better understanding of the inner workings of the decision. While modeling the decision, it becomes clear what factors involved in the decision influence other factors, in other words, the dependencies. Similarly, the uncertainties involved in the problem can also become clear while modeling the decision. Probabilities or probability distributions will be incorporated in any model with uncertainties, and utility functions can be used to represent the decision maker’s attitude to risk.

Using the tools of decision analysis, the model built to represent the decision can be analyzed analytically. This can help the decision maker determine which decision path is best to reach his overall objectives. Since this decision now has a model representation, the model can be tweaked to answer “what if” questions. This question can be answered using sensitivity analysis. Using this tool we can vary some of the probabilities or nearly any parameters of the model by a specified margin and determine whether those changes effect the optimal decision originally determined by the model. Understanding the sensitivities of the model is an important part of determining the validity of the chosen decision solution by the model.

After performing the sensitivity analysis, it's not uncommon to realize the decision process may need some fine-tuning. Clemen and Reilly (2001) use the term "decision-analysis cycle" to describe this entire process, and they explain several repetitions may be needed before a decision that's likely to give the desired result can be made. "In this iterative process, the decision maker's perception of the problem changes, beliefs about the likelihood of various uncertain eventualities may develop and change, and preference for outcomes not previously considered may mature as more time is spent in reflection" (Clemen and Reilly, 2001).

Decision analysis can handle very large and complex problems by integrating multiple perspectives and providing a structured process in evaluating preferences and values from the individuals involved. The process can still ensure that the decision still focuses on achieving the fundamental objectives. In the decision analysis process value tradeoffs are evaluated to review alternatives and attitudes to risk can be quantified to help the decision maker understand what aspects of the problem are not under their control. The process forces the decision maker to be consistent; it is easy to alter our decisions when the pieces are presented to us differently. Performing decision analysis provides consistency though asking plenty of questions and ensuring the decision maker understands what they are saying fully. Most of all decision analysis provides insight that may not have been captured or fully understood if decision analysis was not incorporated into the decision making process. All of these factors make decision analysis essentially to making an informed decision. During deliberations on what new counterterrorism measures should be put in place, decision analysis could aid these policy makers in making more informed, clear, and consistent decisions.

1.4 Combining Game Theory and Decision Analysis

In the past, game theory models were completely separate to decision analysis models. However, it has been discovered that combining the two techniques we could develop a more comprehensive and accurate tool for modeling terrorism. “Early work in using game theory in reliability analysis focused on linking probabilistic risk analysis models with basic game theoretic models to incorporate the effects of strategic interactions into reliability analysis” (Guikema, 2009). Guikema (2009) notes that work by Hausken (2002) provided the first analysis that linked probabilistic risk analysis and game theory into reliability analysis when treating system reliability as a public good. Major (2002) used a zero-sum game with minimax defense strategies to model strategies for defending a potential terrorist target. Zero-sum games assume that both the attacker and defender have exact opposite utility functions and the defense strategy of the defender is to minimize their maximum potential loss. Rios Insua et al. (2009) use adversarial risk analysis to analyze counterterrorism decisions. Adversarial risk analysis (ARA) incorporates intelligent adversaries and uncertain outcomes into the problem by combining game theory and decision analysis methods.

Paté-Cornell and Guikema (2002) created a model for setting priorities among threats and among countermeasures, which combines aspects of probabilistic risk analysis, decision analysis, and game theory. First they needed to develop an *overarching model* which will bring together all the information needed for the model. This information includes the different threat scenarios, the different groups of attackers, the attacker's distinct objectives and the types of potential damage they could achieve given a successful attack scenario. The potential damage is dependent on their individual resources such as people, money, materials, skill, etc. The damage due to an attack also depends greatly on the defenders response and preparedness. Second, there needs to be a detailed analysis on the potential targets and the corresponding weaknesses of that target. Paté-Cornell and Guikema (2002) note that at this second level there needs to be representation of interdependencies among systems, for example the loss of power on operations at a military base in the Middle East. They describe this step as being very important because it can help determine the need for redundancies or other improvements.

The third step in their analysis is to determine the consequences that would be felt by the defender from each attack scenario. This should not only include the immediate and direct consequences such as loss of life or economic effects but also the ripple effects that might be felt after the initial attack. For example, because the weapons used on September 11, 2001 were passenger planes full of fuel and innocent people, the impact on the airline industry was immediate and overwhelming. US airlines had to cut staffing almost immediately. At the close of 2001, the airlines reported 80,000 layoffs and net losses of more than seven billion dollars (Belobaba, 2006). However these effects were not only felt immediately, but they were felt years later. Newman (2003) stated that even two years after September 11, 2001 airlines continuously had to make sacrifices to stay afloat. Many airlines were still implementing pay cuts to pilots and other workers, grounding hundreds of aircraft and eliminating services. In a desperate attempt to avoid company bankruptcy, American Airlines persuaded their employees to give up pay and benefits. Newman also reported, “For the third year running, every major carrier except Southwest will lose money in 2003, with combined losses approaching $7 billion” (Newman, 2003). Newman’s article along with many others proves that the effects of September 11, 2001 are still being felt by the US airlines years after the initial shock.

1.5 Conclusions and Outline of Thesis

By taking aspects of both game theory and decision analysis and incorporating it into a comprehensive model, we can obtain better insight and knowledge for making national security decisions. By incorporating both our objectives as well as the terrorist’s objectives in a single model we may have a more complete perspective on the situation and could perhaps lead us to the best allocation of our resources for defending our country. The following chapters in this thesis take you through a very comprehensive look into both game theory and decision analysis techniques, as well as studies that have combined the two areas. After we build a more advanced understanding of all the areas, we discuss our model and possible contributions of our research.

Chapter 2 takes you through a detailed synopsis of game theory and its usefulness in counterterrorism efforts. In Chapter 3, we describe the area of decision analysis and how it can assist in improving national security. In Chapter 4 we show the benefits of using techniques from both game theory and decision analysis to improve counterterrorism approaches. Chapter 5 is where we introduce our model and explain the potential benefits it could have in aiding decisions made by our government on national security issues. Chapter 6 is a comprehensive look into another technique using optimization that could support improvements to counterterrorism efforts. Finally, in Chapter 7 we discuss our conclusions drawn from our research and the thesis in its entirety.

Game Theory

2.1 Introduction

According to the United States Law Code, *terrorism* means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents (U.S. Code Title 22). In recent years, terrorism has dominated news broadcasts and the new vivid coverage makes for an increase in public awareness. Terrorism is not something that developed recently. Since 1920, the Federal Bureau of Investigation has been investigating terrorism and working to prevent terrorist attacks (Federal Bureau of Investigation). One famous case of terrorism happened in September 1920, known as the Wall Street Bombing. This act of terrorism killed more than 30 people and injured more than 300. The responsible party was never found. The best evidence leads authorities to believe that a small group of Italian Anarchists were behind the attack (Federal Bureau of Investigation). Terrorism, though present, never had a face like it does today. On February 26, 1993, the World Trade Center was attacked by a small band of Middle Eastern terrorists. The intention was to bring down not only the World Trade Center building where they had detonated the bomb, but also to make the twin towers collapse with the debris. It seems that this was a rehearsal for what would one day be known as 9/11.

The acts of terrorism have developed a whole new segment of governmental protection agencies. The National Counterterrorism Center (NCTC) was established in August 2004. The primary mission of the NCTC is to fight terrorism at home and abroad by analyzing threat, sharing information with partner organizations, and to make sure all available resources of national power are used in unity (National Counterterrorism Center). Counterterrorism is a complex system of many dynamic elements that intends to identify potential weaknesses in our countries infrastructure and fix those problems before terrorists can use them to their advantage. A common goal of terrorists is to target an area that will produce widespread terror while simultaneously inflicting maximum economic damage, producing mass casualties, and/or causing widespread panic. An attractive target of terrorists is one that will most likely inflict the most damage and also has the highest corresponding potential success rate.

At first glance, it may seem that our countries best defense would be to identify the most likely targets and then put forth our maximum efforts to secure and protect those targets. However, by doing this, we show the terrorists where most of our resources have been allocated, thereby inadvertently identifying all formally less attractive targets as weaknesses. As a result the terrorists will then find these (formally) less attractive targets more desirable. This is due to the fact that there is less protection in place and therefore fewer deterrents. Terrorists are thought of as intelligent and rational adversaries who are able to adapt their strategies and/or plans to identify the most attractive targets that have the highest probabilities of a successful attack. Using game theoretic models, we can analyze the strategies of terrorists and counterterrorist's. Game theory can be used to determine potential strategies with the highest probabilities of having a favorable outcome. Game theory allows us to take this idea of "move, countermove" into consideration mathematically to aid in quantifying and analyzing security strategies to protect against terrorism.

2.2 Background: Game Theory

2.2.1 Intro and Terminology

In order to describe game theory mathematically, we first need to fully understand what a game is. Each game involves three distinct parts:

1. the participants, players or parties involved,
2. a set of strategies for each player which describes every move that the player will make in every scenario,
3. finally a payoff, which describes the amount each player wins or loses for each scenario throughout the game

The players here will most likely be a country verse an attacker, (i.e. The U.S. versus Al Qaeda) but the players involved in game theory could easily any entities that are able to think rationally and make decisions. To think rationally we imply that the players are trying to optimize their payoffs, whether it is to maximize or minimize their desired outcome of the game. The players are assumed able to make appropriate decisions that they believe will help them reach their optimal outcome. For this paper we are focusing on game theory as applied to counterterrorism, but it should be clear that game theory has many applications and uses.

You can imagine that if a game is fairly simple with only two players and a small amount of possible steps (moves), the strategy for a player will be straightforward. For example, think of the tick-tack-toe game you played as a child. The standard game consists of a 3x3 matrix of possible choices to insert an ‘X’ or ‘O’ depending on the player making the move. The first player to move has 9 possible choices of where to enter their ‘X’. And for every possible location that the first player puts their ‘X’ the other player has a strategy to place their ‘O’. Before the players even start the game, they have a “game plan” of what moves they will make, given the other players previous move. Most of the time, with small games such as tick-tack-toe, this strategy is developed unconsciously. A set strategy plan that is predetermined for each rivals move is called a pure strategy. Tick-tack-toe is a simple game with a very limited amount of moves and therefore a pure strategy is easily devised. However, once the number of possible moves of a game increases, the strategies of that game, and corresponding payoffs of those strategies becomes ever more complex. Some games become so complex due to the potential moves and strategies, that they cannot be described in a payoff matrix. For the topic of counterterrorism, usually this is the case. However, most papers only consider a snapshot of the real world situation, which then gives them simplified information that they can put into a payoff matrix.

Consider a two player game, where we call the first player A and the second B. Now we will assume that we are playing a two person zero sum game which means that whatever one player wins from a strategy, the other player loses. Player A has strategies i, $i = 1,\dots,n$, and player B has strategies j, $j = 1,\dots,m$, so if Player A gains amount a_{ij} then in a zero sum game player B has to lose amount a_{ij} (Barron 1949). You could easily arrange these strategies in a matrix representing the payoffs to player A which would be called the payoff or game matrix. Here, one would simply arrange all the possible strategies of player A in the rows of the matrix and the corresponding strategies of player B in the columns. For each pure strategy combination there would be a corresponding payoff of a_{ij} for player A and the negative value of this would be the payoff for player B. For example say player A has gained a hundred dollars under a certain play, then player B would lose a hundred dollars for that same play; the opposite holds true as well. Here player A (the row player) is trying to maximize their profit while player B (the column player) is trying to minimize player A's profit.

Since we are discussing a two person zero sum game, we can determine the upper and lower bounds of the games potential payoffs. This means in the worst case scenario player A can at least get the lower value of the game; player B is guaranteed a loss of no more than the upper value of the game. We can determine the values of the upper and lower bounds of the game by first writing the game matrix which contains all the payoffs from each combination of strategies from each player; writing the matrix that contains all a_{ij} values. Then for each row, create an additional column and write the minimum from each corresponding row, and for the columns create an additional row which contains the maximums for each column. The lower value of the game will be the largest minimum of the new column and the upper value of the game will be the smallest maximum of the new row. If the upper value of the game and the lower value of the game are equal then the column with the upper value with a corresponding row with the lower value produce an optimal strategy.

If the lower bound of game is less than the upper bound then there is no optimal strategy that exists. If no optimal strategy exists, how is it possible for a player to strategically play the game? John von Neumann purposed a model mixing strategies and proved that if we allow mixed strategies in a game there will always be a value and optimal strategies in zero sum games. Von Neumann called his new model the minimax theorem (von Neumann, 1928). The minimax theory states that in a zero sum, noncooperative game (the players will not corporate or work together to achieve the maximum profit for each other, but are only out for themselves) a player will try to minimize the rival's maximum payoff (minimax), while simultaneously trying to maximize their own minimum (maximin) payoff (Webster, 1984). This means that all players are trying to maximize their own payoffs while at the same time trying to minimize their losses. If all players use this strategy then the maximum of the minimum (maximin) value will be equal for all the players in the game (Webster, 1984).

To illustrate some of the topics previously discussed, Section 2.2.2 goes through a well known game theory example. There are many examples of how game theory can be used to illustrate the discussed topics, but we'll discuss the prisoner's dilemma. This is a two-player, noncooperative, simultaneous-move, one-time game in which both players has a strictly dominant strategy. A strictly dominant strategy means that the player is looking out for himself, and regardless of the other players adopted strategies, the strictly dominant strategy will always be the best payoff for that particular player.

2.2.2 Prisoner's Dilemma Example

There are two prisoners in custody that have just robbed a store, let’s call them Bob and Sue. There is no definitive evidence that links these prisoners to the crime, thus a confession is vital to the case. The police however can prove that both Bob and Sue have committed a misdemeanor (unrelated to the robbery), which will grant each of them a six month sentence. Bob and Sue were each taken into custody separately and therefore had no chance to discuss a strategy if they were arrested for the robbery. Once in custody they are placed in separate rooms and each is interrogated by the police.

Both Bob and Sue are given the same three options:

1. confess and provide evidence against your partner and you will be sent free with immunity,
2. remain silent and spend six months in jail if your partner remains silent as well,
3. if you remain silent and your partner confesses spend ten years in jail

It’s also known that if both prisoners confess simultaneously then both will spend five years in jail. Below is the payoff table associated with this example. The numbers in parentheses correspond to the time the prisoner will spend in jail. The number before the comma represents the payoff for Bob, and the payoff after the comma represents the payoff for Sue. The entry of (-10, 0) in Table 1, corresponds to Sue confessing and Bob remaining silent; therefore Bob will go to jail for 10 years, which is given a negative sign to reiterate that higher numbers correspond to less desired outcomes, and Sue will walk away with immunity spending no time in jail.

Sue

Table 1: Payoff Table

Bob

	Silent	Confess
Silent	(-½ , -½)	(-10 , 0)
Confess	(0, -10)	(-5, -5)

So what is the best choice for Bob and Sue? The best choice is for both to confess. Although the best known outcome would be for both Bob and Sue to remain silent and only receive six months in jail each, both have a great incentive to double cross the other. Therefore, to remain silent is a gamble, considering each prisoner is assumed to be looking out for themselves. Taking this into consideration, the best strategy is to confess for both Bob and Sue.

In this application it should be obvious that if both Bob and Sue could work together, the most efficient outcome would be (-½, -½), but since the prisoners cannot communicate, the most rational strategy for each prisoner is to confess. By rational strategy, here we mean the prisoners are both trying to minimize their own time spent in jail. Using game theory one assumes that most people are rational thinkers and therefore are optimizing their own payoff. In this case your partner is minimizing their time in jail, so by game theory each player believes the other is going to do what is in their best interest, which is to confess. So each prisoner would confess to optimize their chances of spending the least amount of time in jail as possible.

The strategy to confess is referred to as the "Nash equilibrium" for this example (Webster, 1984). This is because Sue is making the best decision she can, taking into consideration Bob's most likely decision, and Bob is making the best decision he can, taking into consideration Sue's most likely decision. However, illustrated by this example, the Nash equilibrium does not necessarily equal the best payoff for all players involved. For this example the best payoff for both Bob and Sue would be to remain silent and only receive six months in jail, but since they are not able to work together and collaborate, this is not the best choice for them as individuals. This makes sense because you can only think about your own decisions, and you really have no way of knowing what another individual will do if you are unable to communicate. So it is not surprising that the Nash equilibrium for both Bob and Sue is to confess.

2.3 Game Theoretic Methods Applied to Counterterrorism

Applying game theoretic methods to counterterrorism provides a structured technique for defenders to analyzing the way adversaries will interact under different circumstances and scenarios. This way of thinking is somewhat counterintuitive, but is an extremely useful tool in analyzing potential strategies for defenders. To view terrorists as rational thinkers is counterintuitive in itself; however, you have to view their logic from their point of view (Wenzlaff, 2004). They find weaknesses and use them to their advantage, if they have a plan and somehow it gets revealed or compromised, they will most likely adapt and change their plan to something less expected. In this way terrorists are not only rational, they're very intelligent.

For example, in response to some skyjackings an American law was passed and starting in January 1973 all passengers and carry-on baggage boarding American Airlines were required to pass through metal detectors (Federal Aviation Administration). The response from the terrorists was an immediate decrease in skyjackings and increase into other kinds of hostage missions such as kidnappings (Sandler, & Enders, 2004). This is just one example of how terrorists will adapt and choose targets with the path of least resistance. Terrorists proactively choose targets that are less protected and easily accessible which result in the highest probabilities for a successful attack. When the U.S. implemented this new law, it became more difficult for terrorists to successfully skyjack planes, thus they were forced to find a new way of reaching their monetary goals, which became kidnapping. This adaptation to ensure the maximum likelihood of success, demonstrates the fact that terrorists are intelligent adversaries that are capable of changing their tactics and strategies in mid play.

The element of surprise seems to be important in terrorist attacks and to ensure they retain this element they will change their plans. Terrorists will do whatever it takes to reduce the chance of discovery by the authorities prior to the completion of their plan. Terrorists strive to maximize their expected utilities (or gains) subject to certain constraints. These constraints include, but are not limited to, such things as budget, resources, expected gains, risk, and time (such as windows of opportunity). The terrorists take all these things into consideration when planning an attack, and therefore they can be thought of as rational thinkers, even if their actions seem irrational to us.

As explained above, game theory can be applied to analyzing terrorism due to the fact that both parties involved are considered to be rational thinkers. Game theory captures the relationship between the two parties and the strategic interactions between the parties. Both parties' decisions influence the sequential decisions or moves of the opposite party, therefore these two parties have to be modeled together since they are interdependent. Game theory can also take into consideration the fact that one or both sides may bluff or lie about their potential actions to try and gain some type of strategic advantage. Also game theory assumes that each player is trying to maximize their own goal subject to some constraints, which as mentioned before, does apply to terrorism. Game theory notions of bargaining can be applied to terrorism as in hostage negotiations.

In counterterrorism situations usually neither the terrorists nor the defender is completely informed, therefore there are uncertainties surrounding the other choices and strategies. These uncertainties can be included in game theory analysis. Usually the values in the game theory payoff tables are uncertain and therefore considered random variables, risk analysis can be used to estimate these values. Because statistics, Bayesian thinking, uncertainties, and other aspects can be modeled using game theory, it makes it an appropriate tool to model terrorism and the interactions between the involved parties.

2.4 Literature Review: Game Theory and Political Policies

2.4.1 Hostage Situations

The majority of work relating game theory to counterterrorism analyzes political policies of a given country. The analysis determines how the policies deter (or do not deter) terrorists from committing crimes in a given country. The policies analyzed include such things as a country's response to kidnappings or other hostage takings, and how we should develop strategies and policies that minimize the terrorists' utilities. By determining how to minimizing the terrorists' perceived payoff, (or utility) we could potentially make the United States a less attractive target for such terrorist acts. Terrorists are considered to be rational thinkers, therefore making decisions that provide them with the highest utilities, or payoffs.

Game theory has been applied to hostage-taking terrorists in the past. This research was done on the basis that American does not negotiate with terrorists (U.S. Department of State) and game theorist wanted to see whether the logic that is behind this policy really works. The logic behind the theory is that countries, including the U.S., that have a zero tolerance for negotiating with terrorists will deter terrorists from taking hostages from these countries, since the countries will not negotiate or meet their demands. "The U.S. Government will make no concessions to terrorists holding official or private U.S. citizens hostage. It will not pay ransom, release prisoners, change its policies, or agree to other acts that might encourage additional terrorism. At the same time, the United States will use every appropriate resource to gain the safe return of American citizens who are held hostage by terrorists" (U.S. Department of State). In theory, the logic behind this policy makes sense. However in practice, depending on the individual taken, or on the situation at hand, even countries that have a no-negotiation policy sometimes end up negotiating. This results in the overall policy being compromised and the logic behind the policy is desecrated.

In May 1974, Israel, a country with a no-negotiation policy similar to the United States, was faced with a terrorist hostage situation involving 102 school children. The terrorists barricaded themselves in the school and demanded the government release some prisoners they were holding in exchange for the lives of the children. Israel decided to negotiate for the children and told the terrorists they needed more time. The terrorists denied the request for more time, and ultimately shot and killed 22 students, and wounded over 50. Even though the negotiation never took place, by agreeing and preparing to do so, Israel completely reneged on its no-negotiation policy. Terrorists see instances like this, and realize that even if a country has a no-negotiation policy; it's possible they will decide to negotiate if the hostages are of enough value (Sandler and Arce, 2003).

There have been multiple studies done to model the hostage taking strategy of terrorists with governments with the no-negotiation policy. One study decided that first the government would have to choose its level of deterrence which will correspond to the success level of a terrorist hostage attack (Sandler and Arce, 2003). If a terrorist believes they have a positive expected payoff, the terrorist will attack (Lapan and Sandler, 1988). The conclusions of the study indicate that the effectiveness of the no-negotiation strategy is directly tied to the government's ability to stand behind the policy, that each party has complete information (meaning the government and the terrorists know all payoff information), the terrorists' payoff being tied only to the negotiation success (meaning the terrorist is not going to benefit from just advertising their cause or committing the crime itself), and spending a significant amount to eliminate logistical success (Lapan and Sandler, 1988).

2.4.2 Allocation of Resources

Many times there are limited resources that are needed at multiple locations. Determining where these resources should go to result in the highest overall benefit, is strategically allocating resources. Game theory has also been applied to terrorism in the way a government should allocate resources. In one such study, the researchers take a collection of locations in which the government must try to protect and the terrorist must choose a location to attack (Bier et al., 2005). Their study gives the first move to the defender; the defender is aware of the fact that once they make a move the attacker observes this move and strategically designs their attack. They find that it is important for the defender to publicly announce their allocation of resources so they can strategically protect more valuable targets while leaving others unprotected. Leaving certain targets unprotected, or with less protection, could make them more attractive to terrorists. Thereby the defender can actually play a part in the attacker's behavior by influencing which targets are the most attractive. They find a number of useful results. First they find that, "the defender may optimally leave some locations undefended, even if they are subject to a positive probability of attack, and even if the defender would prefer (holding the attacker's behavior fixed) to reduce the success probabilities of attacks at those locations" (Bier et al., 2005). Another interesting result is that when the collection of locations grows too large, the optimal result is to do nothing at all. This only changes when a subset of locations can be bounded and considered valuable while others are considered unimportant.

Chen et al. (2009) demonstrates another way game theory has been applied to the allocation of resources. The study models how an urban location can allocate limited resources in response to a terrorist attack. The study considers not only a primary target the terrorist attacks, but also a diversionary attack as well. For instance, the terrorists may create diversionary attacks to preoccupy the authorities while clearing the path for the actual primary location giving the attack a higher probability of causing mass causalities. The study developed a model to determine the interaction of the commander in charge of the security resources and the terrorist. This first model of the study was done as a non-cooperative finite and zero-sum game. Non-cooperative means exactly as it sounds; both sides are operating in secret therefore not cooperating or sharing information with one another. A zero-sum game is when the one party's gain is the exact opposite as the opposing party. What the security commander gains the terrorist loses, or vice versa. The first part of this model is designed to determine the probability a target is actually the terrorist's primary target, not simply the diversionary one. The second model uses the probabilities determined from the first model and uses them to create a reallocated set of the security resources.

2.4.3 New Security Options

Heal and Kunreuther (2005) applies game theory to terrorism through modeling interdependent security (IDS) as a technique to determine the affects of individual choices about security options in interdependent systems. This study looks at the airline industry and how security upgrades to checked baggage can affect the profits of that particular company but also the overall system. The checked baggage is an interdependent system due to the fact that one airline can invest in extensive screening techniques for its own checked baggage but then at a connection other airlines checked baggage that has not undergone the same screening techniques can be combined with the first airlines. This is because once a checked bag has been stored on the plane it rarely goes through another screening process. With the minimal amount of time allotted for connections, screening checked baggage is virtually impossible. Game theory was applied to this problem to determine how airline A's policy would affect airline B and vice versa. Game theory matrices and tactics were used in the analysis to develop a simulation model. It was found that some airlines (the larger ones) could be used to tip the scales as to whether the new screening practices should be put into place. This means that small set of airlines could potentially be used to tip the overall equilibrium of no investment in the new security measures to a new equilibrium of full investment. This would happen when the small set of airlines holds enough weight to influence the remaining set of airlines to follow their investment decision. This may happen if this small set of airlines actually accounts for the majority of passengers and they decide to implement the new security measures and publically declare that they will not share connections with airlines that do not participate in the new security measures. This could obviously scare the smaller airlines into implementing the security measures just to avoid losing future customers.

2.4.4 Applied to Bioterrorism

Game theory has not only been applied to the political policies regarding the response to a terrorist act, but it has also been suggested as a tool to analyze the decisions about protecting and preventing a terrorist attack. Bioterrorism is an emerging form of terrorism which game theory has modeled. "Biotechnology is powerful, relatively inexpensive, and increasingly accessible to U.S. adversaries, from nation-states, to nonstate actors including terrorists, to deranged individuals" (DHS Bioterrorism Risk Assessment, 2008). Biological agents tend to be fairly easy to conceal and very hard to track. "The anthrax mailings of 2001 increased public and governmental awareness of the threat of terrorism using biological weapons" (BioWatch Program, 2003). The Homeland Security Act of 2002 created the Department of Homeland

Security to help combat the rising threat of terrorism (Public Law No. 107-296). The Department of Homeland Security (DHS) was formed and combined 22 different agencies and approximately 170,000 total workers to better and more efficiently manage who and what enters the United States. The mission of the DHS is to protect the United States from any terrorist attack, which of course includes bioterrorism.

Weapons of mass destruction have been a topic of concern and debate for many years now. Weapons of mass destruction can include chemical, radiological/nuclear, or biological agents (Federal Bureau of Investigation). The Weapons of Mass Destruction Commission stated their concern, "that terrorist groups may be developing biological weapons and may be willing to use them. Even more worrisome, in the near future, the biotechnology revolution will make even more potent and sophisticated weapons available to small or relatively unsophisticated groups. In response to this mounting threat, the Intelligence Community's performance has been disappointing" (WMD Commission, 2005). The United States government is being urged to do more to protect its citizens of this threat and put regulations and policies in place to protect, respond, and act to a bioterrorism threat.

The United States has and continues to take steps to protect its citizens from a bioterrorism attack. The DHA has also developed the BioWatch Program to provide early detection and warnings of an airborne pathogen release (BioWatch Program, 2003). The bioWatch program has detectors attached to the Environmental Portection Air quality monitors. The monitors catch particles that are then sent to a laboratory for testing. The particles are tested and analyzed in a timely manner. It's believed that if a large scale pathogen release was to occur, the implementation of these monitors will drastically reduce the amount of time until the release is detected and therefore reduce the time for appropriate response and action by government agencies. This reduction in response time will result in a reduced amount of causalities or infected persons.

In 2006 the first DHA Bioterrorism Risk Assessment (BTRA) was published. The BTRA was intended to provide a thorough assessment of bioterrorism, including the associated risks and threats, in the hopes that this assessment could aid in developing strategic planning and response tactics for the U.S. government. Using the assessment as a detective tool, various government agencies could identify potential gaps in our bioterrorism defenses. By identifying these gaps priorities could be set for the U.S. to eliminate the key vulnerabilities.

The BTRA is under constant revision. One of the suggested revisions called for an improvement in modeling intelligent adversaries who seek to maximize their probably of a successful attack. "BTRA probabilities are conditioned on past events and are retrospective, whereas the terrorist is prospective, constantly adjusting tactics to exploit any evident weakness in U.S. defenses" (DHS Bioterrorism Risk Assessment, 2008). Therefore one of the suggestions to improve the BTRA is to apply game theoretic models and techniques to capture the adversaries' potential actions. The BTRA can develop, "a game-theoretic model of the adversaries that randomizes expected consequences to capture the variability of outcomes. These are not mere theoretical tools, but rather substantive suggestions drawn from extensive research and experience in the military and in the private sector" (DHS Bioterrorism Risk Assessment, 2008). By implementing the use of game theory as well as other modeling techniques the BTRA can improve its ability to provide an accurate representation of the real world situation.

In spring of 2002 United States was faced with determining a defense strategy to a bioterrorism attack involving smallpox. Game theory was not used in this official study, but a later study was done to analyze the same problem using a combination of risk analysis and game theory to develop an optimal defense strategy (Banks and Anderson, 2006). For this example, the U.S. concentrated on three attack scenarios which include the terrorist attack doesn’t happen, a singular terrorist attack happens in one area, or lastly multiple simultaneous terrorist attacks happen in populated areas. They also looked at only four possible defense scenarios such as the government could stockpile a vaccine, develop a stock pile and start biosurveillance, stockpile the vaccine and start biosurveillance and inoculate certain personnel, or finally provide mass vaccination to citizens (Banks and Anderson, 2006). The payoff matrix to this would consist of a 4x3 matrix with each corresponding payoff, or cost in this case, listed. The costs in this scenario would probably include a combination of the following: dollars, economic impacts, lives lost or affected, time, or any other resources used following the attack.

The cell values of the cost matrix are each random variables since the total cost in each cell is not a known value. These individual values are not independent; therefore it’s appropriate to view the entire game theory table as a multivariate random variable with a complex joint distribution (Banks and Anderson, 2006). Taking into consideration that these values are of unknown quantities, risk analysis was used to help determine an appropriate estimate for each cost associated with the attack/defense combinations. The values were determined by risk analysis through expert elicitation, which means experts in the topic of consideration were questioned to gain insight on the probabilities and related costs of each smallpox defense/attack scenario. Any assumptions and all values that were found in this study through risk analysis were intended to represent the real world problem as accurately as possible. The results from the expert elicitation determined the random payoff matrices that were used in the study.

Once the payoff tables were determined, simulation was then used to generate random tables from their joint distribution. Then for each table they can determine which strategy is optimal using von Neumann's minimax criterion. By repeating this process many times, they could then determine which optimal strategies appear the most and ultimately determine an ideal strategy. It may not be adequate to merely count the number of times a strategy appears, but also determine some type of weight that takes into account the costs of each strategy and how far the resulting cost of suboptimal strategies are from the optimal.

Although we did not go into the fact that this example combined the techniques of game theory as well as some techniques from decision analysis such as expert opinion, it should be noted that the authors stated that combining these two approaches "captures facets of the problem that are not amenable to either game theory or risk analysis on their own" (Banks and Anderson, 2006). In the next section we will discuss this combination approach in detail.

2.4.5 Game Theory and Reliability Methods

It has been suggested that security and counterterrorism can benefit from the combination of game theory and risk and reliability models (Bier, 2005). Reliability methods have proved useful in engineering or other fields when trying to protect against failures (or events) which are usually both rare and extreme (Bier et al., 1999). Because these events are rare, data is scarce. Reliability methods take a complex system and decompose the system down to its basic elements. By doing this they can then analyze these elements as separate entities. These entities may have more data to provide insight to such things as individual failure rates.

In 1975, the Nuclear Regulatory Commission (NRC) conducted a study to evaluate the accident risks in the U.S. commercial nuclear power plant facilities. The NRC was among the first to use modern risk assessment methods which were built on the techniques of reliability methods (Bier, 2005). This analysis of risk enabled the NRC to evaluate the impacts of nuclear power plants on safety, while simultaneously evaluating functionality. The NRC stated "in risk assessment... data and results using random variable and probabilistic approaches, can be usefully employed" (NRC Reactor Study, 1975). Since the information being evaluated had little data, the NRC determined that risk analysis was an appropriate tool to use for the analysis. Risk analysis not only relies on the data that is available, Bayesian methods, and as mentioned in the smallpox example, expert elicitation.

As useful and dynamic as risk and reliability analysis is, it is not appropriate to analyze counterterrorism by itself. Generally risk and reliability analysis evaluate failures or potentials for accidents, but these are fixed problems. However, as we've determined throughout this paper, terrorists are able to change their paths or strategies throughout the game. Therefore, the problem of terrorism is far from fixed. This is where the combination of game theory and risk and reliability analysis comes to light. If we could combine risk and reliability analysis with game theory, we could not only evaluate the probabilities of risks and the reliabilities of new security measures, we could also evaluate how terrorists would potential adapt to those new security measures. This would provide valuable insights to personnel developing the security measures. This combination of techniques could provide information about how accurate and effective the new measures would be once in place at deterring terrorists, or whether the new measures would simply deflect terrorists to another similar route.

A clear example of how only considering risk and reliability analysis fails to capture the entire picture is the anthrax attacks in 2001. The U.S. Postal Service considered putting sterilization equipment in every post office in the country (Cleaves et al., 2003 and Bier, 2005). If the postal service would have considered this proposal and evaluated it using the combination of reliability analysis and game theory, they would have thoroughly gone through and determined the possible outcomes of this proposal. By doing this, they would have realized that the terrorists would most certainly adapt their current strategy and eliminate mailing the packages through the U.S. Postal Service. Instead, the terrorists could use an array of other options including UPS, FedEx, or another form of transportation for the packages. Obviously, the cost of the U.S. Postal Service implementing this proposal would have far outweighed any potential benefit. The postal service did not even take this risk deflection into consideration when evaluating this proposal (Cleaves et al., 2003 and Bier, 2005).

Risk and reliability models, as mentioned before, decompose a system to get a closer and more detailed look of its elements. However, by doing this, risk and reliability models cannot take into consideration how, by investing in a new security feature, the adversary will react. Therefore, risk and reliability modeling in the security or counterterrorism field can at times "vastly overstate both the effectiveness and the cost-effectiveness of those investments" (Bier, 2005). It is obvious risk and reliability models need to include game theory techniques to accurately represent a real world situation. It should also be clear that game theory techniques could benefit from the addition of risk and reliability analysis when applied to counterterrorism. This is due to the fact that "most current applications of game theory to security deal with individual components or assets in isolation, and hence could benefit from the use of reliability analysis tools and methods to more fully model the risks to complex networked systems such as computer system, electricity transmission systems, or transportation systems" (Bier, 2005).

2.4.6 Game Theory and Last Line of Defense

As mentioned in above statements and uses of game theory, it has been applicable to counterterrorism policies, reallocation or resources, airline baggage, or other security measures to prevent terrorism. Wein and Atkinson (2007) use game theory and other analytical tools to model what they call a "last line of defense" scenario. In this instances the materials to perform an act of terrorism are already smuggled into the country and the materials are successfully assembled into a nuclear bomb either using plutonium or uranium. Wein and Atkinson (2007) model a last line of defense scenario where a terrorist driving an assembled nuclear bomb towards the center of a city. While driving the terrorists has to pass a series of radiation sensors that surround the city’s center. There is a fleet of security vehicles that stop and search vehicles that set off these sensors. In this study, the government chooses how many radiation sensors surround the city as well as how many security vehicles make up the fleet. The decisions made by the government are meant to minimize the likelihood that a terrorist would make it to the center of the city which minimizes the damage caused by a bomb detonation. There are budgetary constraints associated with each of these decisions.

Wein and Atkinson (2007) view the government as the leader, or the party that will make the first move in the game, and the terrorist as the follower, or the second party to make a move. The first move of the government is to determine the number of sensors vehicles will have to drive past in order to reach the center of the city. The second choice of the government is to determine the number of security vehicles will be in the fleet. The government also has to determine a threshold for the sensors as to how much radiation they have to detect in order to set off the alarm. All of these decisions are made with the goal of minimizing the damage by a bomb detonation. The terrorist observes the government’s decisions and then decides to try and carry the bomb to the city’s center.

Stochastic dynamic programming is used to model the terrorist that is moving through the system towards the target. At any given time the terrorist has a binary decision to make, either to detonate the bomb or to continue towards the primary target. Bayesian updating is used to update the terrorists assumed probabilities while moving through the system. The terrorist does not know the exact threshold of the sensors and therefore does not know whether he is setting off the alarm or not. Queuing theory is also used in this study to account for the potential congestion of vehicles traveling through the system that need to be stopped by the security fleet. If terrorist drives past the sensors, triggers an alarm, and gets stopped by a security vehicle, then it is assumed that the attack is spoiled and the terrorist has failed.

Both plutonium and uranium bombs were considered in four scenarios. The combination of small and large networks (how steps make up the system from the time the terrorist enters the area under surveillance by the police to the center of the city.) N = 5 or N = 50 and the probability that the bomb will be detonated when stopped by authorities, q = 0.5 and q = 0.9. It is determined that the terrorist cannot be deterred from continuing directly to the city center in all but one scenario. Since plutonium has a fairly high detection rate with a low false positive rate, it is found that the optimal solution would be to only have one sensor. A system that only has one sensor and ten to twenty security vehicles can minimize the damage made by a plutonium weapon, even if the weapon is lightly shielded. However, uranium has a detection rate approximately equal to its false alarm rate, and it is found that the system has virtually no effect on this type of weapon (Wein and Atkinson, 2007).

2.5 Conclusions

Using decision analysis techniques such as expert elicitation, data mining, and others, it may be possible to provide accurate estimates for payoff matrices involving the defender and terrorists. These matrices when combined with game theoretic models would be priceless tools for combating terrorism. It is believed that sectors of decision analysis such as risk and reliability analysis need to be considered to accurately model terrorism using game theory. This is because, as mentioned before, they can provide more accurate estimates of the perceived terrorist payoffs. The values found in the payoff matrices need to be as accurate as possible to provide usefulness to the agencies using them. The strategies with the highest utilities for the terrorists and/or defenders may change drastically depending on the payoff matrices values. Risk and reliability analysis by itself does not prove to be sufficient for modeling terrorism. This is because neither risk nor reliability analysis can take the attackers responses to reliability or security improvements into account. Thus there has to be a combination of risk and reliability techniques as well as game theoretic models for the application and applicability of game theory to terrorism.

There are limitations of game theory when it comes to terrorism. For instance, game theory relies on the payoff matrix to determine the most attractive choices for the defender and attacker. However, many times by one party choosing a path to follow or making a certain choice, could bring multiple choices that look attractive to the opposing player. This cannot be modeled through the matrix and is therefore a shortcoming of game theory analysis. Pure decision analysis seems like a reliable tool to be able to somehow combine this shortcoming of game theory analysis into a terrorist model. However game theory is still needed when using decision analysis because as shown in pervious sections, decision analysis does not take into account the reactions of the opposing parties.

Parnell et al. (2009) decided to take aspects of game theory and decision analysis to model an arbitrary bioterrorism attack on the United States. They broke the model down into six essential components. These components are: "the initial actions of the defender to acquire defensive capabilities, the attacker's uncertain acquisition of the agents (e.g., A, B, and C), the attacker's target selection and method of attack(s) given agent acquisition, the defender's risk mitigation actions given attack detection, the uncertain consequences, and the cost of the defender actions" (Parnell et al., 2009). They refer to their game as the defender-attacker-defender decision analysis model. The defender first has two decisions, the first decision is whether to add a city to the Bio Watch plan, and the second is whether to buy a stockpile of a given vaccine. After these decisions the attacker then has to decide on a target and a method of attack, and then the last decision in the model is whether to deploy the vaccine stockpile. The acquisition of the agent by the terrorist is a probability, meaning it's not a known quantity, and the consequences of an attack are also unknown; however, the costs associated with this model are assumed to be known. The unique and tricky concept of modeling a terrorist plot in this way is that the objectives of defenders and attackers are entirely conflicting. Obviously the United States would like to minimize its risk of a terrorist attack and any consequences given a terrorist attack and the terrorists' goal is to maximize that risk. The authors simultaneously model both objectives and determine a decision tree and influence diagram to represent their model. This is a successful representation of a system and using some game theory methodology along with aspects of decision analysis, Parnell et al. (2009) was able to have a true representative system.

Of course with any type of mathematical method of analyzing human behavior there are going to be errors. People do not always act rationally, even though they may know what course of action will secure them the highest expected utility, it doesn't necessarily mean that they will choose that path. Therefore game theory is a useful and appropriate tool for analyzing some aspects of human interactions, and can potentially provide valuable information to combating terrorism; however, it’s far from a perfect science.

Information provided through the tool of game theory and decision analysis could be used to better understand the rationale behind a terrorist attack. This thorough understanding could in turn be used to uncover and destroy a terrorist operation. Game theory coupled with decision analysis could provide a more timely, accurate, and efficient way of analyzing the movements and potential strategies of our adversaries. Through the use of combination of game theory and decision analysis as applied to terrorists, we could potentially uncover cells and plans that we would have otherwise never been aware of until it was too late. As a result, we could save countless lives of innocent victims.

Decision Analysis

3.1 Intro and Terminology

Everyone has been faced with a difficult decision in their lives, but how each individual handles these situations can be the difference between making an informed, or ill-informed decision. Decision analysis aims to ease the difficulty of a decision by providing a framework for thinking about the decision, and useful tools for analyzing the decision. The framework provided by decision analysis forces the decision maker to fully understand the problem by clearly stating and representing the decision. Simply by breaking down the decision into smaller components and studying the aspects of the decision, the decision maker may find enough insight to make an informed decision. However, if the decision is still difficult, the decision maker can employ some decision analysis tools, methods, and/or procedures that can further assist in the decision making process.

Clemen and Reilly (2001) state the first step in the decision analysis process is usually for the decision maker to determine the objectives of the decision and to make a flowchart of the decision process. This will ensure that the decision maker has a clear understanding of the process and that they have a clear understanding of what they want to achieve out of the decision. Once the objectives and the decision structure are clearly stated, the decision maker then needs to consider alternatives. Clemen and Reilly state that it is often the case that when the decision maker defines the decision situation and clearly outlines the objectives, alternatives appear that were not obvious at the beginning of the decision process.

The next two steps of the decision analysis process involve breaking down the decision into the smaller more manageable pieces. Clemen and Reilly (2001) state, "decomposition by the decision maker may entail careful consideration of elements of uncertainty in different parts of the problem or careful thought about different aspects of the objectives". Obviously, this step of the process is very important in understanding the total decision and how the pieces will fit together to form a model. By modeling the decision, we create a visual representation of the given decision and provide a better understanding of the inner workings of the decision. There are many techniques that can be used to model the decision process, for example, flow charts, influence diagrams, or decision trees are very common and widely recognized as vital elements of the decision analysis process. While modeling the decision it will come clear as to what elements of the decision influence other aspects, therefore dependencies and uncertainties can be determined. Probabilities or probability distributions will be incorporated in any model with uncertainties, and utility functions can be used to represent the decision maker's attitude to risk.

Using the tools of decision analysis, the model built to represent the decision can be analyzed analytically. This can help the decision maker determine which decision path is best to reach his overall objectives. Since this decision now has a model representation, the model can be tweaked to answer "what if" questions. What if some of the probabilities used in the model are far from the true values? For example, if the model under the basic scenario tells the decision maker to choose decision A, how much variation in the specified probability would make the model change from the decision from A to B? This question can be answered using a tool called sensitivity analysis. Using this tool we can vary some of the probabilities or nearly any parameters of the model by a specified margin and determine whether those changes effect the optimal decision originally determined by the model. Consider a model that tells the decision maker to choose decision A but when a probability in the model is varied from 0.2 to 0.21 and the ideal decision changes from A to B, the decision maker may want to put in more research to determining the closest possible value for that probability as in the real world scenario the model is trying to represent. This research could prove critical to making an informed decision. However if that same decision maker varies that same probability from 0.2 to 0.9 and the ideal decision stays at decision A, that decision maker can feel fairly confident that the decision A is the best decision to make. This would also tell the decision maker that spending a lot of time researching this probability may not be necessary since the model is not sensitive to it. Understanding the sensitivities of the model is an important part of determining the validity of the chosen decision solution by the model.

After performing the sensitivity analysis, it’s not uncommon to realize the decision process may need some fine-tuning. For example, new alternatives may be found during the decision modeling process, the objectives may need to be varied, or the uncertainties may need to be further researched before continuing. Clemen and Reilly (2001) use the term “decision-analysis cycle” to describe this entire process, and they explain several repetitions may be needed before a decision that’s likely to give the desired result can be made. They state that, “In this iterative process, the decision maker’s perception of the problem changes, beliefs about the likelihood of various uncertain eventualities may develop and change, and preference for outcomes not previously considered may mature as more time is spent in reflection".

3.2 Basic Decision Tree Example

A basic example of how decision analysis can aid in making hard decisions is a case involving a 10 year old girl's decision on whether or not to attend the funeral of her friend, which is also their family pastor. Barbara, Mhairi, and Roger Mullin created a case study of this difficult decision. After hours of agonizing over the decision of whether or not to attend her pastors funeral, her dad finally sat her down and offered to help her draw out her decision. He thought visualizing the decision might help her decide what was best for her.

Her decision is first, whether to attend the funeral. Her dad drew the beginning of a decision tree diagram. The first node is a decision node represented by the square. A decision node represents decisions among alternatives (Kim and Bridges, 2006). This is followed by two branches to represent the two choices that Mhairi can choose from, either to go to the funeral or to stay at home. This is shown in Figure 1.

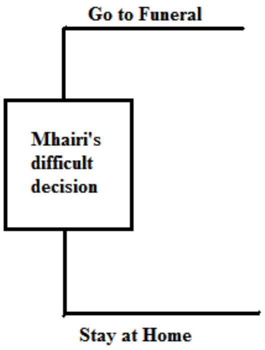


Figure 1: Mhairi's decision (Mullin et al. 2008)

The second step in this decision tree is to determine the outcomes of each path. For instance if Mhairi decides to go to the funeral, what might happen? First Mhairi says she could either go to the funeral and she'd be able to go and be composed and say goodbye to her friend, or she'd go and get too upset and have to leave early, embarrassed, and not get to say goodbye. Her father placed a circle at the end of the branch indicating the chance of these two outcomes. The chance nodes represent random events. See Figure 2.

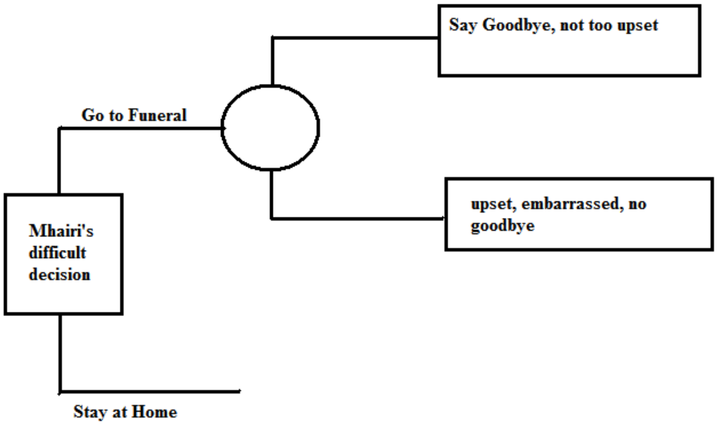

Say Goodbye, not too upset
Go to Funeral
upset, embarrassed, no goodbye
Mhairi's difficult decision
Stay at Home

Figure 2: Adding the first Chance node (Mullin et al. 2008)

Mhairi's dad now tells her she needs to fill in the last branch of the tree. She needs to figure out the possible outcomes if she decides to stay at home. Mhairi decides that two things could happen 1) she'd stay at home and she'd be very upset that she didn't get to say goodbye to her friend in the proper way, 2) she'd stay at home and be ok with the fact that she didn't get to say goodbye to him at the funeral. She filled in the tree according to Figure 3.

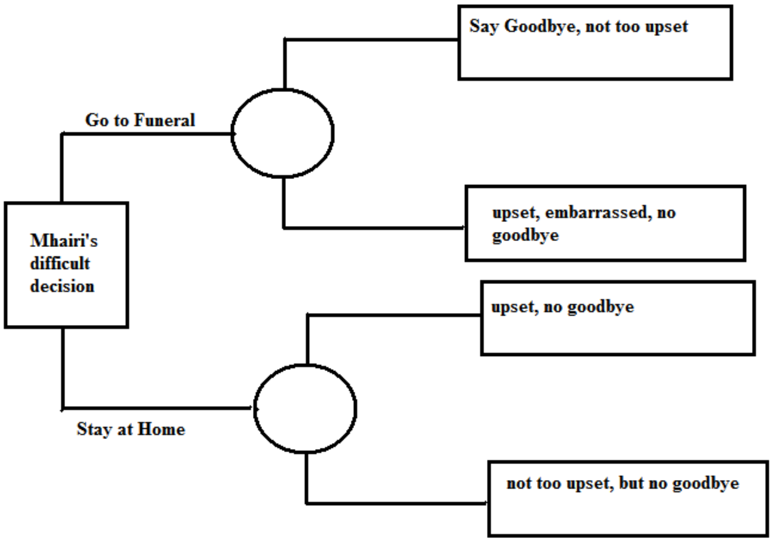

Say Goodbye, not too upset
Go to Funeral
upset, embarrassed, no goodbye
Mhairi's difficult decision
upset, no goodbye
Stay at Home
not too upset, but no goodbye

Figure 3: Adding the final branch of Chance (Mullin et al. 2008)

Mhairi now has a more clear understanding of her decision and it has helped her to see it drawn out on paper. She never thought about the consequences of staying home or going to the funeral. But she still can't decide what to do. Now her dad explains what probabilities are and how she needs to assign those values to the different branches of the decision tree. First he asks her to assign probabilities (or likelihoods) of what she thinks will happen given the decision she makes. For example, if she decides to go to the funeral what is the chance she'll get to say goodbye, and not be too upset. She assigns the below probabilities to each branch as indicated in Figure 4.

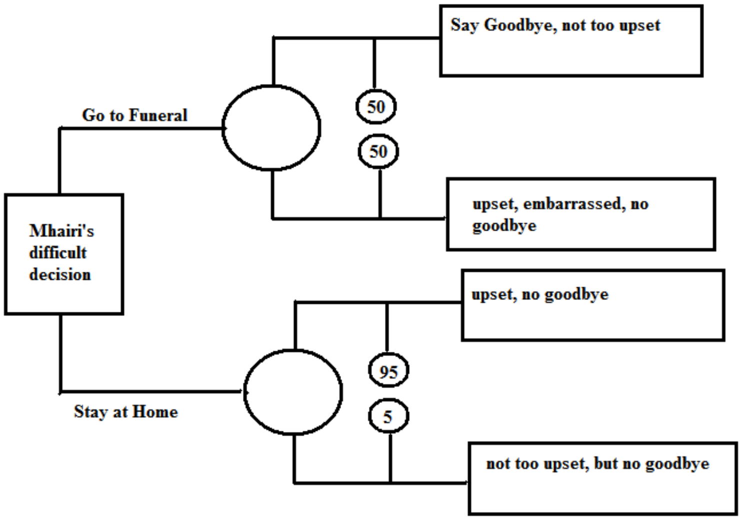

Say Goodbye, not too upset
Go to Funeral
50
50
upset, embarrassed, no goodbye
Mhairi's difficult decision
upset, no goodbye
95
5
Stay at Home
not too upset, but no goodbye

Figure 4: Assigning Probabilities (Mullin et al. 2008)

Now Mhairi’s dad asks her to assign values to each outcome. He explains that these values need to be represented on some type of scale. To make this scaling process clear, he makes her choose the worst outcome of all possible outcomes. She determines the worst outcome to be if she went to the funeral and go too embarrassed and had to leave early without saying goodbye. Since this is the worst possible outcome they decide to give this the value of 0. This 0 is show by “upset, embarrassed, no goodbye (0). Next he makes her decide which the best outcome of all the outcomes is. Here she decides that if she gets to go to the funeral and say goodbye without getting too upset, that would be the best possible outcome. He suggests that she give this outcome a value of 100, that way they can have a 0 to 100 scale to measure the other outcomes. This 100 value is shown in “say goodbye, not too upset (100). In most decision trees you will see this same technique done, but the values range from 0 to 1 instead of 0 to 100. These values represent the person’s preferences in respect to each objective. Now that she has a range to judge what values each objective should have, she can determine numbers for the other outcomes that are possible in this decision. For option "upset, no goodbye" she determines that to be about a 20 on the 1 to 100 scale. The option "not too upset but no goodbye" she thinks is about a 50 value on the scale. The values of the outcomes are represented in Figure 5.

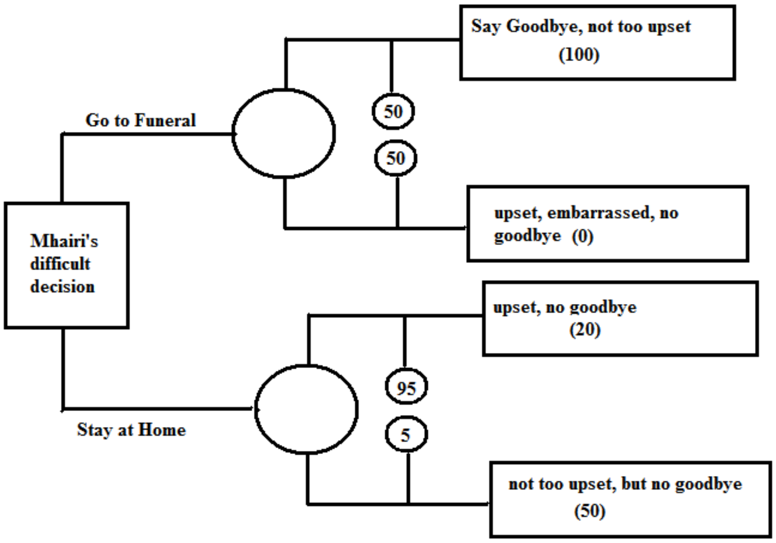

Say Goodbye, not too upset
(100)
Go to Funeral
50
50
upset, embarrassed, no goodbye (0)
Mhairi's difficult decision
upset, no goodbye
(20)
95
5
Stay at Home
not too upset, but no goodbye
(50)

Figure 5: Defining Values (Mullin et al. 2008)

Next Mhairi's dad has to explain how to insert the utility values onto her tree. He explains that the utility of something is just the combination of chance and the value she placed on those outcomes. The utilities need to reflect the decision maker's priorities among the objectives. He explains that if she decides to go to the funeral she has a 50% chance of obtaining an outcome she values at 100, so 0.50*100 is 50. But she also has a 50% chance of obtaining an outcome she values at 0, 0*100 is 0. The combination of these is 50, so that's her utility if she goes to the funeral. He goes through the same process for if she decides not to go to the funeral and comes up with the utility of 21.5. The expected value of Mhairi's tree would be 50 if she decides to go to the funeral and 21.5 if she decides not to go. These expected utilities are show in Figure 6.

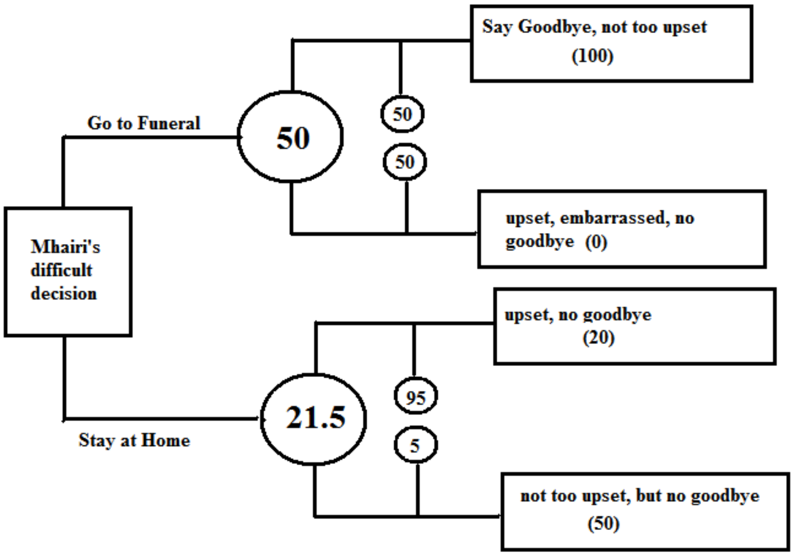

Say Goodbye, not too upset
(100)
Go to Funeral
50
50
50
upset, embarrassed, no goodbye (0)
Mhairi's difficult decision
upset, no goodbye
(20)
21.5
95
5
Stay at Home
not too upset, but no goodbye
(50)

Figure 6: Adding Utilities (Mullin et al. 2008)

Mhairi's father starts to explain that even though this decision of whether or not to attend the funeral is very difficult, it's clear what decision she should make. Her utility for going to the funeral of 50 is much higher than the utility of 21.5 to stay home. This step is often referenced as rolling back the decision tree. By calculating the decision branch with the highest expected utility value, the decision maker can understand the expected outcome depending on their selected path.

By this decision tree, Mhairi should go to her pastor's funeral. Even though if she goes to the funeral she has an equal chance of getting either her most desired outcome valued at 100, or her very worst outcome valued at 0, she should still go to the funeral. This is because if she decides to stay home, even though she is now guaranteed not to get her worst outcome, she only has a 5% chance of getting just an OK outcome valued at 50, but a very high chance of getting a not so good outcome valued at 20. So even though she'll be taking a chance by going to the funeral she has a better chance at a desired outcome.

Mhairi attended the funeral with her family and made it through the entire service. Roger Mullin, Mhairi's father, observed, "She not only coped, she understood her decision by participating in a decision analysis and found comfort in seeing things laid out logically." This example not only shows the basics of decision analysis and how simple the formulation of the trees can actually be, but it also shows that emotions can play big roles in these decisions. The calculations placed in decision trees, or other methods of decision analysis do not have to be just cold hard facts or numbers, they can be emotional values and justifications.

3.3 Basic Influence Diagram Example

The Mhairi example demonstrates the importance and uses of a decision tree yet, did not use an influence diagram. Obviously, not all decision analysis examples will include every aspect of decision analysis. It is possible to use different sets of tools specified for that particular problem. Since influence diagrams are such an important and widely used tool of decision analysis it's important to explain what they are and how they can be applied in practice.

It's important to understand that decision trees and influence diagrams are extremely different tools. Although in most cases you will see both in use, it is not because they have to be used together. This is shown by the Mhairi example. But when they are both used together they could possibly provide an even deeper understanding of the decision at hand. Influence diagrams show more dependencies within the aspects of the decision without getting cluttered with too many details. Influence diagrams are more of a big picture overview where decision trees get more caught up in the details of the decision. Influence diagrams can be very important in developing a snap shot of the decision and what factors may or may not influence the overall objective. They are often a cleaner visual aid than a decision tree.

Campos et al. 2004 note that influence diagrams usually have 3 or 4 distinct types of nodes. They have at least one decision node which most instances drawn as a rectangle (such as *Take Umbrella* in Figure 7). This rectangle represents the variables that are under the control of the decision maker and the alternatives available. For example with the *Take Umbrella* decision, there are two alternatives, either to take the umbrella or don't take the umbrella. An influence diagram also includes chance nodes which are denoted as circles and represent probabilities or uncertainties for variables that are not under the decision maker's control, such as *Forecast* or *Weather*. Another type of node is the payoff node such as *Utility* which is represented by a diamond. The payoff node holds the utility or the profit of the given decision. Finally in some influence diagrams you'll have equation nodes; these are usually drawn with as a rectangle with rounded edges. The equation node simply states any equations that may be attached to the other nodes.

Not only do the influence diagrams usually have different types of nodes, but they also have arcs that are pointing to different nodes. Campos et al. (2004) describe two types of arcs, conditional or information arcs. Conditional arcs represent influence from the node at the tail of the arc to the node at the head of the arc. For example if there are two chance nodes connected by a conditional arc it means that the chance at the head of the arc is influenced or has probabilistic dependencies from the chance node at the tail of the arc. If an arc goes from the decision to any other node (chance or payoff) that simply means that the decision made will influence the ending value of the chance or the payoff of the decision. Informational arcs signify that all information at the tail end of the arc will be known at the time the decision needs to be mad. These generally travel between a chance node and a decision node. Campos et al. (2004) notes that the absence of an arc is sometimes a more powerful statement than the presence of one. The absence of an arc indicates conditional independence where the presence of an arc signifies only the possibility of dependence.

In Figure 7, Campos et al. (2004) offer an example influence diagram that provides a clear understanding of what the nodes are and how they influence each other. There are two chance nodes one for the weather forecast, *F*, and one for the actual weather, *W*. The forecast can be sunny, cloudy or rainy and the actual weather will be either rain or no-rain. The decision maker only has one decision to make, *U*, either to take an umbrella or not take the umbrella. This influence diagram also only has one payoff node, *Utility*, which measures the decision makers overall satisfaction. “The goal of influence diagram modeling is to choose the decision alternative that will lead to the highest expected gain (utility), i.e. to find the *optimal policy* (Shachter, 1986; Zhang, 1998). In order to compute the solutions, for each sequence of decisions, the utilities of its uncertain consequences are weighted with the probabilities that these consequences will occur” (Campos et al. 2004).

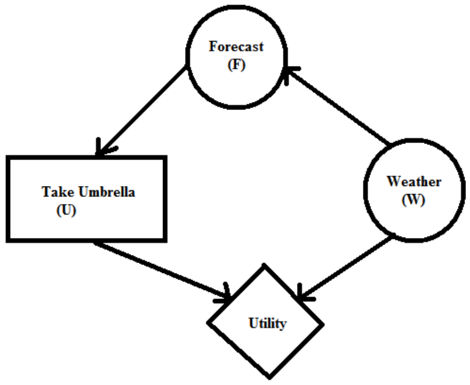


Figure 7: Influence Diagram Example

So the question now is how can decision analysis techniques and methods be applied to counterterrorism? Decision analysis has been applied to many types of disasters, natural or manmade. Terrorism right now is more prevalent than ever before, or at least that's what most of us believe since we are bombarded with terrorism debates and topics every time we turn on our TV or stereo. Decision analysis can provide insight and provide helpful tools and techniques to our government or other agencies that have to make difficult decisions in order to protect our country and national security.

3.4 Decision Analysis applied to Counterterrorism: Decision Trees and Probability Assessment

Man Portable Air Defense System (MANPADS) have been a concern to the department of homeland security since 9/11. The MANPADS are what they call surface-to-air missiles, meaning the missiles can be fired by a person on the ground at a low flying aircraft in the sky.

The Arms Control Associate describes three types of MANPADS which include command line of sight, laser guided, and infra-red seekers. The Command line-of-sight MANPADS are guided by the attacker through a remote control and the Laser-guide devices follow a laser placed on the target. According to the Arms Control Associate, the most common of all MANPADS is the infrared seeker, which is attracted to the heat of the aircrafts engine or the aircrafts exhaust.

In 2004 the U.S. Department of Homeland Security awarded funding of 90 million dollars to research and development of protective measures against a MANPADS attack (Department of Homeland Security). The researchers are modifying protective measures that are currently in use on military aircrafts in hopes of developing a system that could protect aircrafts designed to transport civilians. The first question is even if this technology is possible to develop for use on civilian planes, is it cost effective. Obviously our government is taking the potential for a MANPADS attack seriously but is this research really worth the cost. Winterfeldt and O'Sullivan were asked to perform decision analysis to provide an analysis on whether civilian aircraft deployed directed infrared countermeasures (DIRCMs) are cost effective. The hope of the government is that the DIRCMs will disable the heat seeking device in the infrared seeker of a MANPADS.

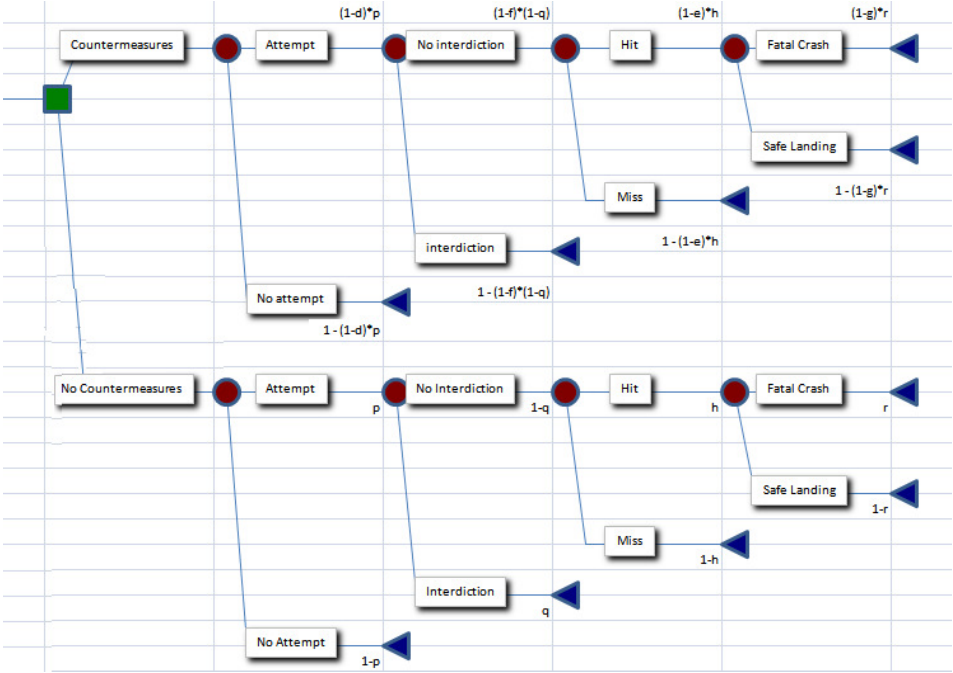


Figure 8: Decision Tree for MANPADS (Winterfeldt & O'Sullivan, 2006)

Figure 8 illustrates the decision tree that was used through the analysis. The decision is whether or not the government should implement countermeasures against the MANPADS. Table 2 shows the inputs that will be used to represent the probabilities and perceived effectiveness of the countermeasures. These values are based on expert elicitation done by the researchers and any other relevant information found in open literature. To demonstrate how to read Figure 8 and combine it with Table 2, take for instance the decision to implement countermeasures. This would mean following the tree up from the first decision node to "countermeasures". We are now at our first chance node, whether the terrorist will attempt an attack. Here the probability that they will attempt is (1-d)*p. The d represents the deterrence factor that is associated with implementing some type of countermeasure, the p is the probability that the terrorist will attack in the next 10 years.

Continuing up the tree, the next chance node represents interdiction by authorities, and there is a chance the attack will be foiled by police, and there is a chance it will not. For the base case the researchers have decided there is a 0% chance of interdiction given an attack attempt. This is because the MANPADS can be launched in a wide radius to the airports and there is little to no surveillance in the potential attack parameter. Next there is a chance as to whether or not there is a hit given the attack attempt. To continue up the tree means that the other branches have happened; so where we are now is that our government has decided to implement countermeasures, the terrorists have made an attempt, and have successfully hit the target. Now the last chance is what the damage from the hit will be. The researchers state that there is much debate on whether a plan can survive a hit from a MANPAD, so on the base case they set the probability of a crash at 0.25.

Table 2: Decision Tree Inputs – Probabilities and Effectiveness ranges (Winterfeldt & O'Sullivan, 2006)

		Min	Base	Max
Probabilities				
p	**Attempted attack in 10 years**	**0**	**0.5**	**1**
q	**Interdiction | attempt**	**0**	**0**	**0.25**
h	**Hit | attack, no countermeasures**	**0.5**	**0.8**	**1**
r	**Crash | Hit**	**0**	**0.25**	**0.5**
Effectiveness of Countermeasures				
d	**Deterrence effectiveness**	**0**	**0.5**	**1**
f	**Interdiction effectiveness**	**0**	**0**	**0.25**
e	**Diversion/destruction effectiveness**	**0.5**	**0.8**	**1**
g	**Crash reduction effectiveness**	**0**	**0**	**1**

Next Winterfeldt and O'Sullivan describe the consequences of an attack at each end node of the tree. They state five consequences they considered:

1. Loss of life (LL)

2. Cost of the plane the MANPADS hit (CP)

3. Overall economic losses due to incident (EL)

4. False Alarm rate (FA)

5. Cost to implement countermeasures (CC)

Table 2 describes the consequence ranges that were used in this decision tree. As you can see the ranges vary dramatically to cover the wide range of possible outcomes from a MANPADS attack. For example the fatality given a crash range from a minimum of 0 and a maximum of 400, but the base case for this model was set at 200. The remaining consequences can also be explained using this format. Parameters *a* and *b* signify the difference in percent loss of passengers given a terrorist successfully hit an aircraft but the pilot lands the aircraft safely, and the percent of passenger loss if the terrorist misses the aircraft completely. Again the values found in Table 3 were researched via open literature available and any expert elicitation possible.

Table 3: Decision Tree Inputs – USD Consequences (Winterfeldt & O'Sullivan, 2006)

Consequences		Min	Base	Max
LL	**Fatalities | Crash**	**0**	**200**	**400**
CP	**Cost of plane (millions)**	**0**	**200**	**500**
EL	**Economic loss | Fatal Crash (billions)**	**0**	**100**	**500**
a	**Precent of loss | hit and safe landing (%)**	**0**	**25**	**50**
b	**Percent of loss | miss (%)**	**0**	**10**	**25**
FA	**Number of false alarms/year**	**0**	**10**	**20**
CC	**Cost of countermeasures (billions)**	**5**	**10**	**50**

Table 3 states that the consequences are evaluated in U.S. dollars denoted in parentheses after the abbreviation description. You should notice that the fatalities given a crash (LL) and number of false alarms per year (FA) do not show dollar amounts. The value of a life (VOL) lost for this research was set at 0 to10 million dollars; the base case is 5 million. The value per incident of a false alarm (VOF) ranges from a minimum of 0 dollars to 100 million dollars. The base case for an incident of a false alarm was set at 10 million dollars; this vast range illustrates the immense uncertainty surrounding a false alarm.

With all the parameters and costs determined the researchers can now calculate the weighted cost at each end node in the decision tree. Winterfeldt and O'Sullivan (2006) determine the equivalent cost (EC_j) = $\Sigma\ c_i x_{ij}$, the indices *i* and *j* denote the specific consequence and end node in the decision tree, respectively. Therefore c_i denotes the equivalent cost of one unit of consequence, and x_{ij} denotes which consequence at the appropriate node in the decision tree. To clarify consider the top branch of the decision tree (Countermeasures, Attempt, No Interdiction, Hit, Fatal crash). The equivalent cost for the base case values is found by VOL*LL + CP + EL + CC + VOF*FA*10 which equals 0.005*200 + 0.200 + 100 + 10 + 0.010*10*10 = 112 billion dollars. Figure 9 displays the values found. All the units were converted to billions therefore the value of a life (VOL) equals 0.005 billion which is equivalent to 5 million which is the base case stated above. Also for the last part of the equation VOF*FA*10, the 10 denotes the 10 year time horizon that is incorporated into all the other parameters and therefore the false alarm rate also had to be converted to a 10 year time horizon for consistency.

Note that the branch for No countermeasures has a double slash indicating that it is not the preferred path. When folding back the tree the optimal decision to minimize cost for the government would be to implement countermeasures because this would only cost 15 billion dollars, and No countermeasures would cost 19 billion dollars when considering the base case for this analysis.

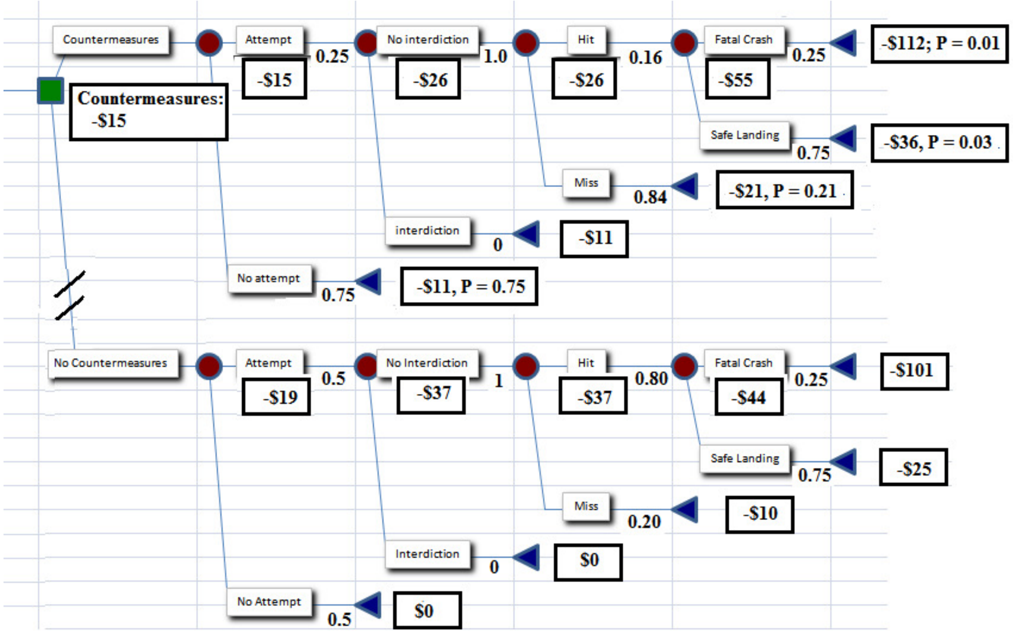


Figure 9: Decision tree solved (Winterfeldt & O'Sullivan, 2006)

Winterfeldt and O'Sullivan (2006) discovered as they presented the base case results they would encounter strong opposition from opposing parties of MANPADS countermeasures. Therefore they determined the best way for everyone to understand the valuable results of the analysis was to present the sensitivity analysis first. The value of this research is not necessarily the base case decision tree, due to the vast uncertainties surrounding the input probabilities and/or consequence costs. They would show two sensitivity analysis results, one in favor of MANPADS countermeasures and the other opposing MANPADS countermeasures.

The differences in the analyses performed for both sensitivity results, the one in favor of MANPADS and the other opposing MANPADS, are the inputs for the chance of a MANPADS attack in the next 10 years, and the overall economic impact. All other inputs for both analyses are identical. The case for MANPADS countermeasures used the likelihood of a MANPADS attack on the United States in the next 10 years as 50%. This is what the base case in the original analysis called for. This probability can be considered high, but Winterfeldt and O'Sullivan note that it is not considered unreasonably high by some subject experts.

When the believed optimal decision is to put *no* countermeasures in place for a MANPADS attack, the value used for the probability of a MANPADS attack on the United States in the next 10 years is considered to be only a 25% chance instead of 50% used in the base case. Also the value of economic consequence used is considered to be only 50 billion instead of 100 billion in the base case. These two parameters are so extremely vital in the analysis that this adjustment completely changed the overall result. This is used to show the audience that these values need to be researched further and to make sure we are using appropriate and accurate values in the analysis.

Varying parameters at the researcher's discretion can be very useful to see the potential changes in the optimal decision that will occur when changing those given parameters, but it can also be useful to perform sensitivity on all the parameters to see how and when they will change over specified ranges. To do this type of sensitivity analysis the researchers created a tornado diagram. A tornado diagram in allows us to simultaneously vary the input variables between their high and low values and see the effect on the output variable (whether to implement countermeasures or not). For example the economic loss given a fatal crash is varied through its entire range from 0 to 500 billion. While this variable is varied all other variables remained fixed at the base case values. This way we can determine the effect that this one particular variable has on the overall outcome. The input variables with the longest bars represent the variables with the most influence over the outcome. Winterfeldt and O'Sullivan found that the economic loss given a fatal crash, the cost of the countermeasures, and the attempted attack in 10 years, variables were the top three variables that have the most influence over the overall outcome.

Another type of sensitivity analysis that can be done on all of the input variables discovered that when the economic loss due to a hit and crash is less than 74.3 billion dollars the optimal decision to be to implement *no* countermeasures, but when the economic loss increases above 74.3 billion, the optimal decision is to implement countermeasures against MANPADS.

So far all the sensitivity analysis that has been done on the variables has independently varied while all other inputs stay consistent with the base model. However, it is also important to analyze how variables interact simultaneously. Therefore Winterfeldt and O'Sullivan (2006) also included a joint sensitivity analysis on certain parameters. We will look at one joint sensitivity analysis as an example of this type of sensitivity analysis. When varying the probability of an attempt in the next 10 years and the economic loss due to a hit and crash, the optimal decision of whether or not to implement countermeasures or no countermeasures changes. When the probability of an attempt is very low and the economic loss is low, the decision is never to implement the countermeasures. However, once economic loss increases and the probability of an attempt increases, the decision changes to implementing the countermeasures. It appears that the turning point for the decision to implement countermeasures is when the probability is approximately 0.2 and the economic impact is above $200 billion. To see the exact results, please refer to Winterfeldt and O'Sullivan (2006).

This analysis is a great basic example of how decision tree analysis along with sensitivity analysis can help policy makers identify the most significant variables and visualize how changes in those variables will affect the overall decision that should be made. In this analysis three variables were determined to have the most significant influence on the decision:

1. The economic consequence due to a MANPADS attack
2. The probability a MANPADS attack will be carried out on the United States in the next 10 years
3. The cost of the countermeasures that are to be implemented

The overall result of this analysis is that more research needs to be done to create more certainty surrounding the most influential variables. If these variable values could be narrowed down to a more reasonable span the policy makers would have a better idea of what the optimal decision should be. With the information available in open literature the ranges are so large that an optimal policy is hard to determine. This is an important benefit of decision analysis, even if the overall result cannot be determined as to whether the implementation of countermeasures is optimal given the base case values, determining the most important variables and being able to justify further research to narrow the scope of values for those variables is an extremely important part of this process. Once those values can be narrowed, this research can be performed again and the policy makers would have a clear optimal policy.

3.5 Counterterrorism: Values and Objectives

Protecting the public from natural disasters is fundamentally different than protecting against terrorist attacks. Although there are some practices that could help lower the expected number of lives lost, like emergency preparedness that will be affective in both natural disasters and manmade disasters such as terrorist attacks. Goals will also be uniform across manmade and natural disasters such as minimizing the number of lives lost, minimizing economic impact of a disaster, and limiting any and all impact on the lives of those touched by the disaster. Although there are many similarities between response and preparation when analyzing any time of disaster, terrorism requires a whole new set of thinking than historical disaster preparation techniques. Terrorist can change their minds and operate rationally. Analysis by Keeney (2007) illustrates the usefulness of developing detailed lists of objectives for a decision and how this can help develop value models for the Department of Homeland security and for terrorists. If we can understand the objectives of terrorists and the possible priorities and/or actions they may take, that information can be used by antiterrorism groups to foil future terrorist acts.

Keeney (2007) lists four facts his research relies on, first decisions should reflect what the decision makers desire to accomplish; second the objectives of the decision should be explicit and should quantify what those decision makers wish to accomplish; third we have the resources to create quality value models and fourth the knowledge of such values is important to be able to make an educated decision. These steps seem fairly intuitive, but a lot of details are hidden behind these four steps. For instance the first step which was for the decision to reflect what the decision makers desire to accomplish means the decision makers have to develop their objective function. Keeney states that the objective function can also be called the value model. He believes that the term value model brings more validity to the modeling process because the value model is constructed using the same process that's needed to construct any type of analytical model. To construct the value model we need to complete five steps:

1. Identify objectives,
2. Organize objectives and select the fundamental objectives,
3. Identify attributes for the fundamental objectives,
4. Specify relative preferences for different levels of the single attributes,
5. Define the value tradeoffs that prioritize the different objectives.

Although the construction of the value model is outlined in these five steps, it should be noted that many iterations among the steps will most likely be necessary before a finished product is achieved. Not all of the possible objectives of this analysis may be represented in a monetary fashion therefore utility functions can be used to create weighted values to determine the preferences among the alternatives, much like we demonstrated using Mhairi's dilemma in Section 3.2. The preference between alternatives in a model can be determined through the expected utility; the alternatives with higher expected utilities are desired over alternatives with lower utility values which is consistant with Mhairi's dilemma.

Assessing value models for the Department of Homeland Security is more difficult than one might think. Keeney (2007) notes that of all the objectives that individuals will list as important, there are about that many other important objectives that the individuals will forget to list (Bond et al., 2007; Keeney, 2007). Inputs from a number of different organizations and therefore individuals inside the DHS are required, which makes the task of developing a comprehensive list of all fundamental objectives even more difficult. To fully develop the fundamental objectives requires a lot of revisions, lists, and organizing from all individuals involved. Unfortunately not all objectives can always be achieved at their fullest potential simultaneously. For example maximizing the benefit of terrorism countermeasures is in complete conflict with minimizing the cost of terrorism countermeasures. Therefore there has to be some sort of give take in this analysis or tradeoffs. This allows the decision maker to apply utilities to the alternatives and use tradeoffs to see the overall performance, ranked by utilities, of all alternative strategies. This allows the DHS to visually see the advantages and disadvantages of each alterative relative to the other alternatives (Kim and Bridges, 2006).

The number of alternatives can grow rapidly, so it's wise to try to keep the alternatives to a minimum. Once the alternative list has been developed the expected outcome of each alternative can be determined. An option in decision analysis is to graphically compare the outcomes of each alternative over all fundamental objectives to determine whether any type of dominance exists (Kim and Bridges, 2006). If there is dominance from one alternative to another on all fundamental objectives, the inferior alterative can then be eliminated from further analysis. This weeding out of inferior alternatives can make the remaining analysis easier for the researchers and the lower number of possible alternatives can make the analysis easier for the decision makers to understand.

Trying to assess value models for terrorists will be the same as assessing value models for the DHS. Obviously we will have more uncertainty about the preferences of terrorists because we cannot ask them directly, but overall the same process will apply. Not all terrorist or terrorist groups have the same preferences or objectives, therefore Keeney notes that it important to consider a specific terrorist individual or terrorist group when trying to assess their value models.

When creating a value model for the terrorist we will rely heavily on information from experts. We will need to elicit the terrorist's objectives, determine attributes and define tradeoffs. When trying to elicit this information about the terrorist's preferences it is important to use reputable sources for the information. Such a source could be a government agency that arrests, interrogates, studies, or has firsthand knowledge of the terrorist or terrorist group in question. Another source may be a member of the terrorist group that may be imprisoned. Whoever the source may be, it's important to make sure they have accurate and unbiased information regarding the probabilities and preferences that will be used in the value model. The model can only give information to make an informed decision if the inputs are accurate.

Most of the objectives of the terrorist would be in complete opposition to those of the DHS; however some would remain consistent between both parties. For instance minimizing cost is probably a concern of both the DHS and the terrorist or terrorist organization. Defining the attributes and assigning the utility function for the terrorists would be done in the same manner it was for the DHS. We would run a sensitivity analysis on the uncertainties surrounding the terrorist's preferences to determine where/if their preferences would change depending on our beliefs of their preferences. Again, it should be noted that defining variables that need to be further researched before an accurate account of the decision can be made, is an important part of decision analysis.

Keeney (2007) illustrates a value model of terrorist preferences through an example. The judgments made about the terrorist objectives, attributes, and utility functions came from subject matter experts at Lawrence Livermore Laboratory (Keeney, 1977). Keeney states the terrorist objectives as 1) maximize the amount of plutonium acquired 2) maximize the purity of the plutonium 3) minimize the radiation danger to the terrorist. The experts determine the following attributes:

X_1 = plutonium extracted, measured in grams (g.Pu.),

X_2 = purity of stolen material, measured in grams of uranium per liter of material (g.U./L),

X_3 = radiation dose, measured in Rads./hour.

The attributes need to be given ranges as to the worst and best cases from the view of the terrorist. Table 4 outlines these ranges given to the attributes.

Table 4: Terrorist Attribute Ranges (Keeney, 2007)

Attribute	Measure	Worst	Best
X_1 = Plutonium	g.Pu.	10	2500
X_2 = Purity	g. U./L	333	0
X_3 = Radiation	Rads./hour	100	0

Keeney (2007) then creates the utility function $u(x_1, x_2, x_3)$, where x_i is a specific level of attribute X_i, $i = 1, 2, 3$, just like in Table 3. To illustrate this consider $u(150, 27, 5)$ which would be the utility of the terrorist obtaining 150 g of plutonium with purity 27 g.U./L, which gives off 5 Rads./hour. Keeney then establishes the appropriateness of the additive or multiplicative utility function by determining if some assumptions are upheld. More details are explained about the assumptions and requirements in Keeney and Raiffa (1976). The additive utility function is actually a special case of the multiplicative where the scaling constants in the multiplicative utility function approach zero. Therefore determining which utility function to use, either additive or multiplicative, really depends on the answers given from the experts.

By holding two attributes at a constant level and varying the third, single attribute utility function curves can be found. For instance Keeney (2007) states that for the grams of plutonium obtained by the terrorist, he asked a scientist knowledgeable in this subject to consider a lottery. The lottery would yield a 50 percent chance of the terrorist acquiring 10 grams of plutonium or a 50 percent chance of acquiring 2,500 grams, these two numbers represent the worst and best case scenarios as displayed in Table 4. The scientist was then asked a series of questions to determine at what point the terrorist would prefer to choose the lottery over a predefined quantity. When the predefined quantities were 1,500 or 1,000 grams taking either of these quantities was preferred to taking the chance with the lottery. However, when asked about 500 grams, the preferred action was the take the chance with the lottery. The quantity of 800 grams was determined to be the indifference point, where the scientist decided he was indifferent to taking his chances with the lottery or taking the 800 grams for certain. The other attributes were evaluated using similar techniques.

To determine the value tradeoffs of the terrorist two attributes have to be evaluated simultaneously while the third is held constant. By again using the idea of indifference points the scaling constants in the additive and multiplicative utility functions can be evaluated. It was determined that the multiplicative utility function was the most appropriate for this analysis. It was determined that for the worst utility for the terrorist is $u(10, 333, 100) = 0$ and the best utility is $u(2500, 0, 0) = 1$. Any possible target that can be characterized by the three attributes stated can now be evaluated using the utility function for this particular terrorist. As noted, this analysis is for a single terrorist the preferences and values are likely to change given the individual or group of terrorists in question.

The overall benefit of this model is that through the use of this value model we can evaluate any possible target and determine which target has the highest utility and therefore would be the most attractive to the terrorist. Of course no matter how experienced or knowledgeable the experts that provide the probability and preference information, we will never know for sure how accurate our value models are. Therefore extensive sensitivity analysis is required to ensure an educated decision is made.

Keeney demonstrates the flow of decisions when involving the government, terrorists, and the public. First the DHS would have a decision to make, then the terrorist would make a decision and implement some type of action, the DHS would view this action and implement their own response, the terrorist would then view that response and have their own response, and the public would react to this sequence of actions. This structure of decision analysis can be implemented in a variety of ways. Parnell et al.(2005) use a similar process flow when they evaluate allocations of counterterrorism resources. Research that has be done that could benefit from evaluating their decision using the format outlined by Keeney could include Bier et al. (2007), which studied whether it was worthwhile for the government to invest millions of dollars to improve security to one particular stationary target. The targets spotlighted were major dams or nuclear power stations.

3.6 Other Decision Analysis Applications in Counterterrorism

Terrorists are very intelligent and try to locate targets that will cause mass casualties, panic, and economic damage. Leung et al. (2004) acknowledge that bridges may be a vulnerable target for terrorist attacks. Leung et al. (2004) use a Risk Filtering, Ranking, and Management (RFRM) method for their counterterrorism analysis which builds on hierarchical holographic modeling (HHM) (Haimes, 1981, 1998) to identify risks. The risks are then ordered to help the decision maker realize what the most important risks are and prioritize the risks. Then risk management can be used to uncover alternatives and potential plans of action. Of course this is again a decision analysis technique which means the last phase of the technique is to review the problem and objectives to see if multiple iterations are necessary. Hamill et al. (2002) also used hierarchy in their analysis to appraise the value of information being sent through information systems. Once the risks are identified the hierarchy technique is again used and the risks can then ordered to help the decision makers focus on the most important risks and vulnerabilities of the information systems and help the decision maker develop alternative strategies. Buckshaw et al. (2005) implements a similar structure when evaluating alternatives designed for the protection of critical information systems.

Feng and Keller (2006) used a multiple objective decision analysis approach to assess potential distribution plans in a specified region of potassium iodide to counter the release of radioactive iodine due to a terrorist attack or an accident. Rosoff and Winterfeldt (2007) explored an analysis which combined several risk analysis tools to assess the consequences in terms of economic and public health impacts of a successful terrorist attack involving a radiological dispersal device (RDD) on the ports of Los Angeles and Long Beach.

The decision analysis process forces involved parties to communicate their objectives and preferences more clearly than might be achieved without the decision analysis process. This process makes the decision makers really carefully think about what they consider important and why. A DHS model can be used to spark conversation and evaluate objectives which in turn can uncover other fundamental objectives that otherwise may have been missed. During this process the DHS might discover alternatives that were not previously thought of or mentioned. The creation of a terrorist model may give the government a better idea of what the terrorists may be plotting. Both of these models can be very important tools to the government when trying to implement counterterrorism measures.

3.7 Decision Analysis Conclusions

Decision analysis can be used in a variety of ways to help the decision maker understand the decision in its full context and be able to accurately assess the alternatives and tradeoffs among the fundamental objectives (Kim and Bridges, 2006). Clarifying the decision for the decision maker is such a valuable tool of decision analysis.

Decision analysis helps the decision maker incorporate the uncertainties involved in a problem mathematically. Decision analysis can also handle very large and complex problems by integrating multiple perspectives and providing a structured process in evaluating preferences and values from the individuals involved. The process can still ensure that the decision still focuses on achieving the fundamental objectives. In the decision analysis process value tradeoffs are evaluated to review alternatives and attitudes to risk can be quantified to help the decision maker understand what aspects of the problem are not under their control. The process forces the decision maker to be consistent; it is easy to alter our decisions when the pieces are presented to us differently. Decision analysis will provide consistency by asking plenty of questions and ensuring the decision maker understands what they are saying fully. Most of all decision analysis provides insight that may not have been captured for fully understood if decision analysis was not incorporated into the decision making process. All of these factors make decision analysis essentially to making an informed decision.

Combining Decision Analysis and Game Theory Methods Applied to Counterterrorism

4.1 The use of Game Theory in Decision Analysis

In the past, game theory models have been completely separate from decision analysis models. However, it has been discovered that combining the two techniques we could develop a more comprehensive and accurate tool for modeling terrorism. “Early work in using game theory in reliability analysis focused on linking probabilistic risk analysis models with basic game theoretic models to incorporate the effects of strategic interactions into reliability analysis” (Guikema, 2009). Guikema (2009) notes that work by Hausken (2002) provide the first analysis that linked probabilistic risk analysis and game theory into reliability analysis when treating system reliability as a public good. Major (2002) uses a zero-sum game with minimax defense strategies to model possible strategies for the defense of a potential terrorist target. With the zero-sum game it is assumed that both the attacker and defender have exact opposite utility functions and the defense strategy of the defender is to minimize their maximum potential loss.

Zhuang and Bier (2007) determine when considering the position of defender. This one issue is far from simple, there are many underlying questions inside this including: where should I protect, how much of my resources should I put at that location, how much effort should I put into defending a particular location, and when should I defend that location? These questions are hard to answer, even more so when they are subject to various constraints such as limited funds or personnel, which make this even more complicated.

Zhuang and Bier (2007) observe that the resource allocation issues would be similar in structure to those of the attacker. The obvious difference is instead of minimizing the potential damage like the defender, the attackers are maximizing the likelihood of destruction. The attacker's questions would include when to attack, where to attack, how much damage that should be inflicted during the attack, and what materials to use during the attack (e.g. dirty bomb, nuclear materials, biological weapons). Of course, the attacker is subject to constraints as well such as available resources, windows of opportunity for that attack, money to fund the attack, as well as other constraints. The issues that face the attacker and defender are similar in structure. The overall objective is where the opposition really comes into light.

Zhuang and Bier (2007) focus on how the defender should allocate resources intended to minimize the likelihood of destruction from an attack. They consider an attack to either be a natural disaster such as a hurricane, or a terrorist attack. In the case of a terrorist related attack, they find that the defender should publicize their defensive investments and play a sequential game so the defender can have the first move advantage.

In the single location case, Zhuang and Bier (2007) find when there is only one possible terrorist target that "the probability of damage from terrorism, can be considered an analogue of a *strategic reaction function*" (Zhuang and Bier, 2007). When the cross derivative is positive, they found that the attacker investment and defenders investment are *strategic complements*. This means that if the defender invests more in their defensive resources, the attacker must also invest more to increase the probability of a successful attack. Therefore, if the defender has enough resources, they could increase the defensive investment enough such that the target could become unattractive to the attacking party. When the cross derivative is found to be negative, the effort of the attacker and investment of the defense are found to be *strategic* substitutes. Consequently, this could mean that by investing in defense mechanisms the defender could actually increase the attractiveness to terrorist for an attack.

Rios Insua et al. (2009) use adversarial risk analysis to analyze counterterrorism decisions. Adversarial risk analysis (ARA) incorporates intelligent adversaries and uncertain outcomes into the problem by combining game theory and decision analysis methods. Rios Insua et al. (2009) discuss several variations of ARA problems, including a Bayesian approach. When one opponent does not know the inputs needed for the typical use of game theory or decision analysis methods such as the utility of the adversary or the probabilities of outcomes, that opponent can use the Bayesian approach. The unknown information will force the opponent to analyze the problem from the adversary's point of view. The opponent can then express this uncertainty using a Bayesian strategy that puts a distribution over the inputs which includes the adversary's expected utility. The opponent can then use Monte Carlo simulation to get the information they need to solve the problem. Rios Insua et al. (2009) believe this Bayesian approach has more to offer the study of ARA than the traditional Nash equilibrium.

Paté-Cornell and Guikema (2002) create a model for setting priorities among threats and among countermeasures, which combines aspects of probabilistic risk analysis, decision analysis, and game theory. First they develop an *overarching model*, which will bring together all the information needed for the model. This information includes the different threat scenarios, the different groups of attackers, the attacker's distinct objectives, and the types of potential damage they could achieve given a successful attack scenario. The potential damage is dependent on their individual resources, such as people, money, materials, and skill. The damage due to an attack also depends greatly on the defenders response and preparedness. Second there needs to be a detailed analysis on the potential targets and the corresponding weaknesses of that target. Paté-Cornell and Guikema (2002) note that at this second level there needs to be representation of interdependencies among systems, for example, the loss of power on operations at a military base in the Middle East. They describe this step as being important, because it can help determine the need for redundancies or other improvements.

The third step in Paté-Cornell and Guikema's (2002) analysis is to determine the consequences that would be felt by the defender from each attack scenario. This should not only include the immediate and direct consequences such as loss of life or economic effects but also the ripple effects that might be felt after the initial attack. For example, because the weapons used on September 11, 2001 were commercial passenger planes, the impact on the airline industry was immediate and overwhelming. US airlines had to cut staffing almost immediately. At the close of 2001, the airlines reported 80,000 layoffs and net losses of more than seven billion dollars (Belobaba, 2006). However these effects were not only felt immediately, but they were felt years later. In 2003, Richard J. Newman stated that even two years after the incident, airlines continuously had to make sacrifices to stay in business. Many airlines were still implementing pay cuts to employees, grounding hundreds of aircraft and eliminating services. In a desperate attempt to avoid company bankruptcy, American Airlines persuaded their employees to give up pay and benefits. Newman also reported, "For the third year running, every major carrier except Southwest will lose money in 2003, with combined losses approaching $7 billion" (Newman, 2003). Newman's article along with many others proves that the effects of September 11, 2001 are still being felt by the US airlines today.

The model Paté-Cornell and Guikema (2002) focuses on the first step of developing an *overarching model*. "The model described here is designed to gather diverse kinds of information, and is based on risk analysis (Apostolakis, 1990), decision analysis (Raiffa, 1968; Keeney and Raiffa, 1976), systems analysis and game theory (Gibbons, 1992), including the dynamics and game aspects that are needed to permit updating over time" (Paté-Cornell and Guikema, 2002). The objectives of their analysis is to identify: "1) The elements of the US infrastructure, networks and socio-economic components that need to be strengthened in priority order, 2) The most effective means of reducing the overall threat, for example, by disruption of the terrorists' supply chain (cash, people and skills, materials and communications, etc.), 3) The type of intelligence information that needs to be gathered in priority, focusing on the quality, the timeliness, and the relevance of the signals given resource constraints (costs, people, space assets, etc.)" (Paté-Cornell and Guikema, 2002).

The overarching influence diagram model that is developed by Paté-Cornell and Guikema (2002) is shown in Figure 10. The inputs and probabilities assigned to the attackers preferences and goals of each attack were determined by U.S. experts in related fields and through the use of rational decision analysis. This is the main assumption of this model because these probabilities and preferences were determined by parties that are not the true attackers and therefore determined by beliefs of how the actual attackers behave and prioritize attacks.

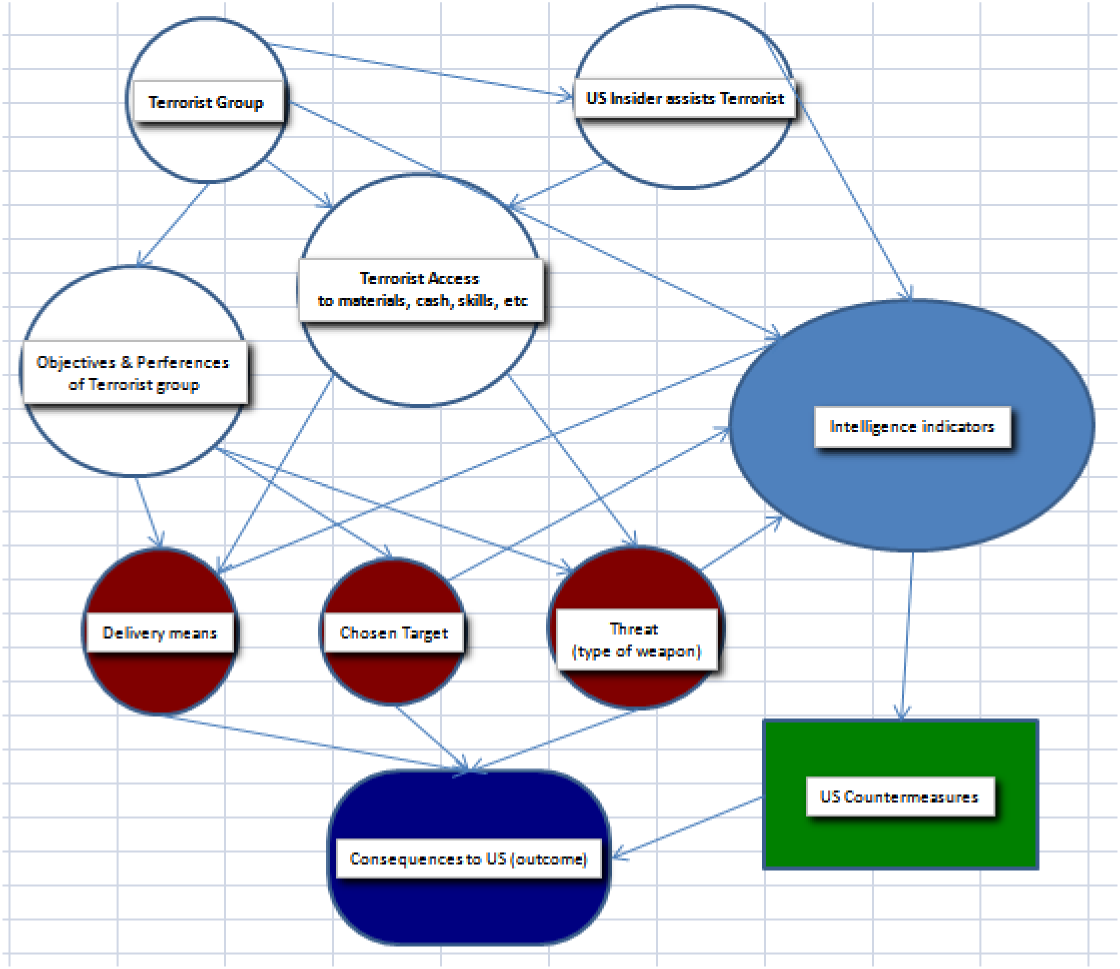


Figure 10: Influence diagram representation of overarching model

Table 5, contains the inputs for the illustrative example provided by Paté-Cornell and Guikema. This example looks at two distinct terrorist groups, Islamic Fundamentalists (IF) and American disgruntled (AD). There are four distinct terrorist attack methods in this example, a nuclear warhead explosion, a nuclear incident (dirty bomb), a small pox attack, and repeated attacks on urban areas with conventional weapons. They determined values from the United States point of view for the terrorist (group j) for each type of attack (i) for each of three attributes (k). The attributes are as follows, (X_1) denotes the symbolism of the attack by the terrorist, (X_2) denotes the economic consequences of the attack, and (X_3) signifies the political consequences due to the attack. The expected utilities for each scenario are displayed in Table 5.

Table 5: Data and terrorist calculations for basic model (Paté-Cornell and Guikema 2002)

Nature of the threat (weapon)	Group	P_{TE}(Success|Intent [I_j] and weapon [W_i])	Attractiveness to perpetrators of successful outcome of W_i				Expected Utility to the terrorist groups
			X_1	X_2	X_3	Total Utility U_{ij}	
Nuclear warhead explosion	IF	0.01	10	10	10	30	.27
	AD	-	-	-	-	-	-
Nuclear incident	IF	0.5	8	3	5	16	5.6
	AD	0.5	4	2	5	11	1.1
Smallpox attack	IF	0.7	2	7	8	17	8.3
	AD	0.6	2	7	8	17	3.1
Continuous conventional attack on urban areas	IF	0.9	4	2	9	15	12.2
	AD	0.9	4	2	9	15	12.2

Legend X_1 symbolism of the attack, X_2 number of casualties and amount of destruction caused by attack, and X_3 degree to which the attack leads to political destabilization and erosion of U.S. power

Table 6 shows the results from the model. The expected disutility is the negative utility that the United States can expect to feel given a successful attack. For this example, it is assumed that the Islamic Fundamentalist launch their attack with a 40% chance and a 10% chance the American disgruntled will launch their attack per time period. This is assumed across all possible weapon choices.

Table 6: Results for basic model (Paté-Cornell and Guikema 2002)

Nature of the threat (weapon)	Group	Probability of Attack of type i from group j: $P_{TE}(W_i \mid I_j)$	Probability of success of attack of type i from group j: $P_{US}(S \mid W_i,I_j)$	Negative value (disutility) of outcome to the U.S. of a successful attack of type i $U_{US}(S,W_i)$	disutility of outcome to the U.S. of a successful attack of type i to U.S. $EU_{US}(S,W_i)$
Nuclear warhead explosion	IF AD	0.01 -	.50 -	-10,000	-20
Nuclear incident	IF AD	0.21 0.7	0.2 0.15	-10	-0.18
Smallpox attack	IF AD	0.31 0.19	0.6 0.6	-100	-8.6
Continuous conventional attack on urban areas	IF AD	0.47 0.74	0.9 0.5	-10	-2.1

Probability of Intention: $P_{us}(I_1)=0.4$; $P_{us}(I_2)=0.2$; 1:Islamic Fundamentalist. 2: American Disgruntled

Given the results of Table 6, Paté-Cornell and Guikema (2002) note there are many ways of now ranking the threats, in terms of weapons, felt by the United States. They could be ranked according to the biggest negative impact given a successful attack, according to the probability of a successful attack, or according to the expected disutility of a successful attack. The benefit of analyzing counterterrorism efforts based on the disutility is the United States then has the ability to consider both the probability and the effect of a successful attack of a given type simultaneously.

Paté-Cornell and Guikema (2002) reveal their single period, two sided global influence diagram. It shows the influence diagram from the perspective of the terrorists and a separate influence diagram for the United States perspective. The utility values of the influence diagram in the perspective of the terrorist are assumed to be influenced only by the symbolism of the attack and the loss of life accrued. The utility values of the influence diagram for the United States is based on the symbolism of the attack, the loss of life, and the direct economic consequences.

The influence diagram considers five different types of terrorists instead of just two types: 1) the Islamic fundamentalist groups, 2) Islamic fundamentalist individual,3) the disgruntled American groups, 4) disgruntled American individual, and 5) foreigners with anti-U.S. mentalities. There are three attributes considered for this model: 1) the direct economic consequences (D), 2) the symbolism of the attack (Sy), 3) the number of lives lost (L). The analysis assumes linearity of preferences, the expected disutility function for the United States is given in Equation 1.

Equation 1

$$E\underline{U} = \sum_{i} p_i(S, W_i)x[10L_i + 3Sy_i + D_i]$$

After combining the assessments of success probabilities for each scenario and the believed capabilities and preferences of each terrorist category, the output of the left side of **Error! Reference source not found.** is shown in Table 7. Combining the probabilities and the consequences to obtain the expected disutility of each scenario are given in Table 8.

Table 7: Illustrative results for the marginal probabilities of classes of attack scenarios without countermeasures (Paté-Cornell and Guikema, 2002)

Class of Scenarios	Approximate Probability of Occurrence per time unit
All scenarios involving attack with a nuclear warhead	7.8×10^{-4}
All scenarios involving attack with a biological weapon	9.8×10^{-4}
All scenarios involving attack with conventional explosives	1.9×10^{-3}
All scenarios involving an attack on a government building	1.2×10^{-3}
All scenarios involoving an attack on an urban population	6.8×10^{-4}
All scenarios involving an attack on a symbolic building	1.4×10^{-3}
All scenarios involving an attack on a transportation networ	4.8×10^{-4}
All attacks made by truck	1.3×10^{-3}
All attacks made by plane	1.0×10^{-3}
All attacks made by individual carriers	1.4×10^{-3}

Table 8: Illustrative results for the expected disutilities of the different classes of scenarios given that each of them is attempted without additional countermeasures (Paté-Cornell and Guikema, 2002)

Class of Scenarios	Approximate Expected Disutility to the U.S.
All scenarios involving attack with a nuclear warhead	1.62×10^{5}
All scenarios involving attack with a biological weapon	2.4×10^{3}
All scenarios involving attack with conventional explosives	1.4×10^{3}
All scenarios involving an attack on a government building	3.7×10^{4}
All scenarios involoving an attack on an urban population	3.4×10^{4}
All scenarios involving an attack on a symbolic building	3.6×10^{4}
All scenarios involving an attack on a transportation networ	3.3×10^{4}
All attacks made by truck	3.0×10^{4}
All attacks made by plane	3.0×10^{4}
All attacks made by individual carriers	3.4×10^{4}

Both Table 7 and Table 8 represent the results when no countermeasures are in place to deter a terrorist attack. To evaluate potential counterterrorism measures it would be useful to see the difference in disutility with and without counterterrorism measures. With the implementation of a countermeasure there is an associated cost (CT). Therefore per time period, for example a week, there is a CT value for protecting certain targets. For example protecting a government building $20 million, urban population centers $300 million, transportation networks and symbolic buildings both $75 million. Paté-Cornell and Guikema (2002) reiterate many times that all the numbers seen are for illustrative purposes only and should not be interpreted for truth. Equation 1 has been modified to reflect the new CT measures and is displayed in Equation 2.

Equation 2

$$E\underline{U}_{US}(L_n, Sy_n D_n CT_n) = \sum_i p_i(S_i, W_i|CT_n)x[10xL_i(CT_n) + 3xSy_i(CT_n) + D_i(CT_n)] + Cost(CT_n)$$

Table 9 displays the resulting expected disutilities for the four potential countermeasures of the United States. It is assumed that only one countermeasure can be implemented at one time and that the countermeasure will only affect the probability of a successful attack at that one location where the countermeasure was implemented.

Table 9: Expected Utilities based on examples of countermeasures (Paté-Cornell and Guikema, 2002)

Countermeasure	Expected Disutility to the U.S. with the considered measure
Protect Government Buildings	-9,031
Protect Urban Populations	-18,918
Protect Symbolic Buildings	-9,045
Protect Transportation Networks	-9,367
No Countermeasures	-31,312

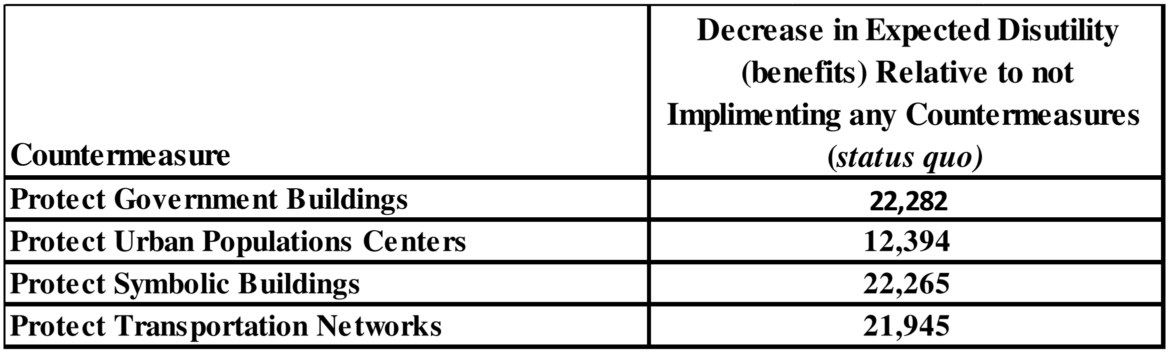
Table 10 compares the probabilities of having no countermeasures ("Nothing") and protecting only one other area with a countermeasure. In all instances the probabilities decrease due to the countermeasure. If the goal is to minimize the probability of an attack with a given countermeasure against a biological weapon the best implementation would be to protect symbolic buildings.

Table 10: Net benefits of U.S. countermeasures in terms of variation of the probability of a successful attack of each type, given that such an attack is attempted per time unit. (Paté-Cornell and Guikema, 2002)

Class of Scenarios	Conditional Probability of Success per time unit if Protecting:				
	Nothing	Government Buildings	Urban Populations	Symbolic Buildings	Transportation Networks
All scenarios involving attack with a nuclear warhead	0.175	0.135	0.164	0.135	0.138
All scenarios involving attack with a biological weapon	0.18	0.129	0.158	0.121	0.132
All scenarios involving attack with conventional explosives	0.757	0.523	0.66	0.527	0.536

Table 10 considers the reduction in probability in a particular attack given a countermeasure. The highest benefit given the probability reduction is to protect symbolic buildings from a biological attack. However, that does not take into consideration the lives lost or economic effects. To get a more comprehensive view of the benefits of the countermeasures, we need to compare the disutilities. According to Table 11, implementing countermeasures for government buildings results in the highest decrease in expected disutility.

Table 11: Net benefits of U.S. countermeasures in terms of variation of disutilities per time unit (Paté-Cornell and Guikema, 2002)



Countermeasure	**Decrease in Expected Disutility (benefits) Relative to not Implimenting any Countermeasures (*status quo*)**
Protect Government Buildings	**22,282**
Protect Urban Populations Centers	**12,394**
Protect Symbolic Buildings	**22,265**
Protect Transportation Networks	**21,945**

Both Table 10 and Table 11 are beneficial for understanding the benefits of countermeasures. Table 11 has a more comprehensive view of the overall benefit of countermeasures and therefore may be more beneficial for policy makers than Table 10. However, Paté-Cornell and Guikema (2002) note that the information in Table 10 may be important for protection against immediate threats.

To make this model dynamic and a true game-theoretic model a new step would need to be added for updating after each time unit passed. The information would update the probabilities for random variables would need to be updated based on the observed signals from the previous time period. This updating process would make all observed information in previous time periods available to both parties. For instance, if the terrorist made an improvement to technology for developing a nuclear warhead in the previous time period, the United States would observe this move and use the information to update any probabilities they have for successful attacks given nuclear warheads. Another example is if the United States made progress in the development of some countermeasure technique the terrorist may observe this and alter their likelihood of using a weapon affected by this countermeasure improvement.

Paté-Cornell and Guikema (2002) describe that in practice the game-theoretic model should include continuous updates on the following aspects: 1) Model design, interdependencies should constantly be reviewed to see if nodes or links should be added, modified, or removed, 2) The understanding of each variable in the model is critical, 3) All probabilities assigned to the variables, 4) The overall objective of the model and therefore the objective function.

The overarching model game-theoretic formulation is shown in Figure 11. The red dividing line symbolizes the division of information sets. This means that the United States is uncertain about the terrorist actions or moves when they make their move in a given time period and the terrorists are uncertain about the United States' actions or moves in that same given time period. Each party is making their moves given the information from previous time periods. The notation p_i for the terrorist and q_i for the United States denote the probability assessments for that party.

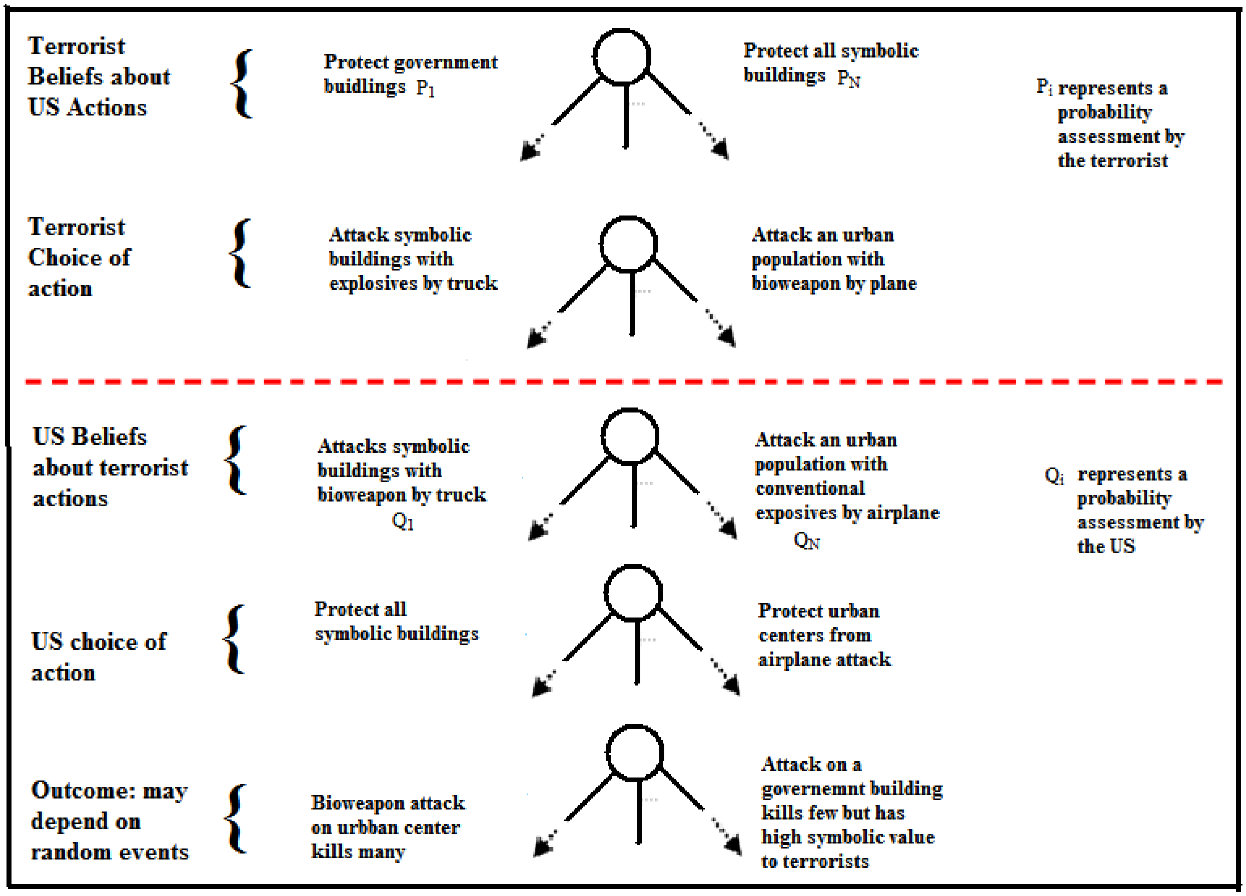

Terrorist Beliefs about US Actions
Protect government buidlings P_1
Protect all symbolic buildings P_N
P_i represents a probability assessment by the terrorist
Terrorist Choice of action
Attack symbolic buildings with explosives by truck
Attack an urban population with bioweapon by plane
US Beliefs about terrorist actions
Attacks symbolic buildings with bioweapon by truck Q_1
Attack an urban population with conventional exposives by airplane Q_N
Q_i represents a probability assessment by the US
US choice of action
Protect all symbolic buildings
Protect urban centers from airplane attack
Outcome: may depend on random events
Bioweapon attack on urbban center kills many
Attack on a governemnt building kills few but has high symbolic value to terrorists

Figure 11: Overarching Model Game-Theoretic Formulation (Paté-Cornell and Guikema, 2002)

The model presented by Paté-Cornell and Guikema (2002) includes probabilistic dependencies in the analysis which makes this approach more applicable to real world problems. Their quantitative approach allows comparisons of the disutilities of different threats and combination of dependent factors. The information needed for this type of analysis will come from cooperation from many different experts and across many different fields therefore utilizing many experts and areas of expertise.

4.2 A New Approach

Game theory and decision analysis both play important roles in counterterrorism efforts. However, they both have their weaknesses. Decision analysis techniques such as probabilistic risk analysis can provide incorrect assessments of risk when modeling intelligent adversaries as uncertain hazards. Game theory analysis also has limitations. For example when analyzing a terrorist or terrorist group using game theory we can only take into consideration one aspect of the problem to optimize at a time. Meaning the analysis is either analyzing the problem from the defenders perspective or from the attacker's perspective. Parnell et al. (2009) was able to develop a model that simultaneously maximizes the effects of the terrorist and minimizes the consequences for the defender.

Parnell et al. (2009) listed six components they considered necessary for their model: the initial actions of the defender to acquire defensive capabilities, the attacker's uncertain acquisition of the agents (e.g., A, B, C), the attacker's target selection and method of attack(s) given agent acquisition, the defender's risk mitigation actions given attack detection, the uncertain consequences, and the cost of the defenders actions. The initial actions of the defender to acquire defensive capabilities in this case include adding another city to the BioWatch program or to buy vaccine reserves which make up the two decisions by the defender in this model. The agent acquisition by the attacker is an unknown and out of the defenders control, the target and method of attack are decisions that will be made by the attacker, the consequences are again an unknown and uncontrolled value, and the costs in this model are considered to be known.

The risk represented in the model is the fatalities and economic consequences felt by the United States following the attack. The fatalities of an attack are measured by the maximum potential fatalities, the warning time given to the defender between the time of a release and the time needed to distribute vaccines, and the effectiveness of the agent A vaccine. Parnell et al. (2009) modeled the economic effects with a linear model with a variable that is dependent on the number of fatalities and therefore increases as the number of fatalities increases, and a fixed economic effect that is independent of the fatalities. The probabilities representing the risk is modeled using a multiobjective additive model which Parnell et al. (2009) note is similar to multiobjective value models by Kirkwood (1997). The interesting factor in this analysis is that Parnell et al. (2009) simultaneously model the defender minimizing the risk and the attacker maximizing the risk.

Parnell et al. (2009) created a decision tree and influence diagram that represents the model accurately. Figure 12 and Figure 13 are a representation of the decision tree and influence diagram created by Parnell et al. (2009). Notice the decisions are represented by yellow boxes have the corresponding decision maker in parenthesis. This distinguishes the decisions made by the United States or the terrorist. The chance nodes are represented by green circles in both the influence diagram and the decision tree.

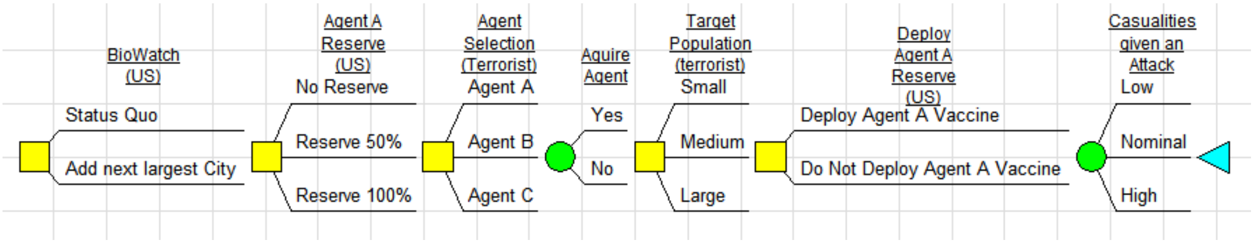


Figure 12: Decision tree (Parnell et al., 2009)

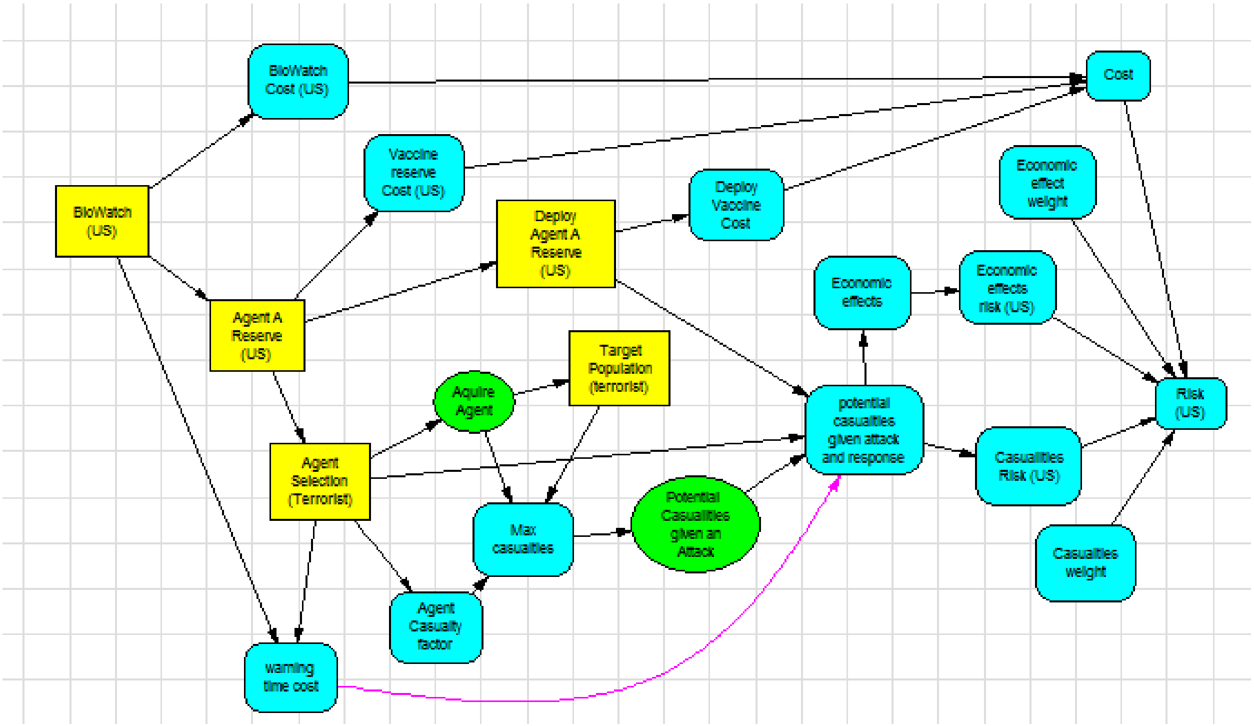
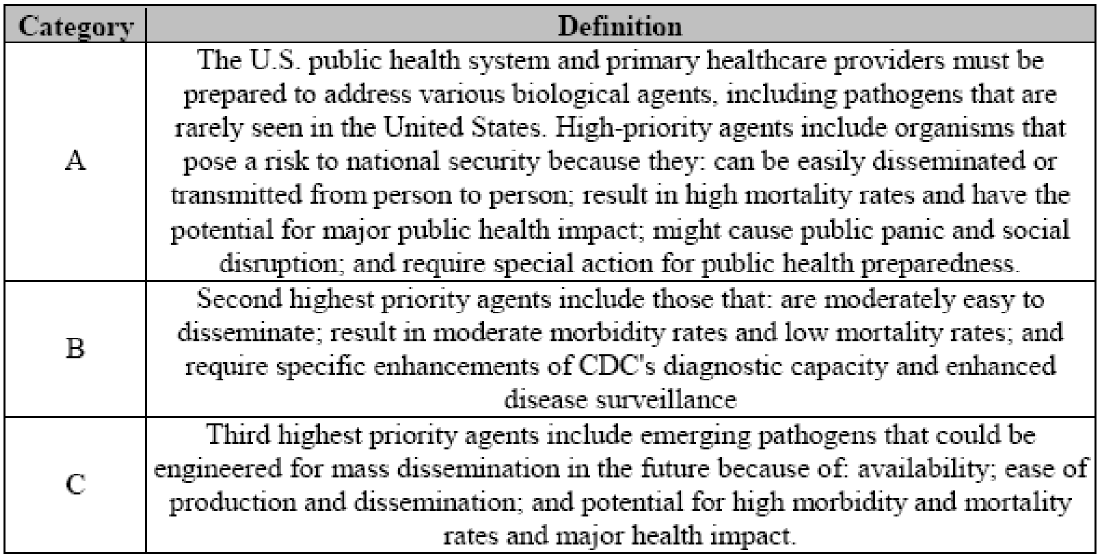


Figure 13: Influence Diagram (Parnell et al., 2009)

Following Figure 12 we see that the first decision represented is for the United States. The goal of this decision is for the United States to decide whether they want to be more prepared for a bioterrorist event. For simplification purposes the model only considers the BioWatch Program for agents A and B and the decision about whether or not to acquire a reserve will only be for vaccine A in this model. The definitions and explanations for the differences between agents A, B, and C are listed in Table 12.

Table 12: CDC BioTerror Agent Categories (CDC; Parnell et al., 2009)



Category	Definition
A	The U.S. public health system and primary healthcare providers must be prepared to address various biological agents, including pathogens that are rarely seen in the United States. High-priority agents include organisms that pose a risk to national security because they: can be easily disseminated or transmitted from person to person; result in high mortality rates and have the potential for major public health impact; might cause public panic and social disruption; and require special action for public health preparedness.
B	Second highest priority agents include those that: are moderately easy to disseminate; result in moderate morbidity rates and low mortality rates; and require specific enhancements of CDC's diagnostic capacity and enhanced disease surveillance
C	Third highest priority agents include emerging pathogens that could be engineered for mass dissemination in the future because of: availability; ease of production and dissemination; and potential for high morbidity and mortality rates and major health impact.

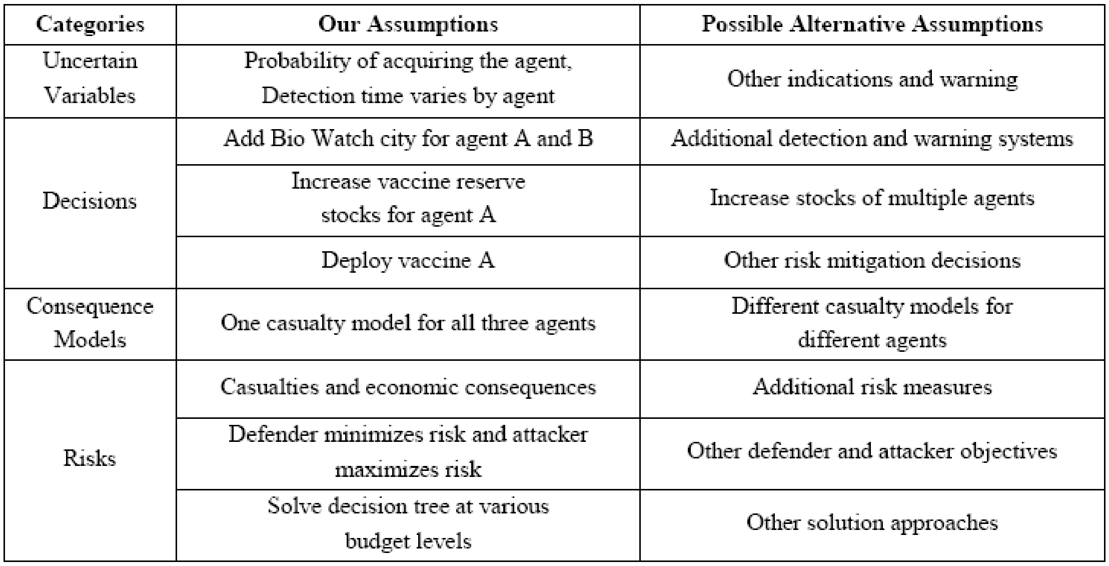
“The function of the BioWatch Program is to detect the release of pathogens into the air, providing warning to the government and public health community of a potential bioterror event” (BioWatch, 2003). The purpose of the BioWatch Program is to minimize the time between detection of a release and the reaction of the government to implement the countermeasures for preventing public exposure. In the model by Parnell et al. (2009) agent C is not detectable by the BioWatch program. This is realistic since not all agents are detectable and therefore will serve no benefit in detection.

The second decision is whether or not to keep a reserve of vaccine for agent A. If the U.S. government decided to keep a reserve amount high enough to vaccinate all people if a full scale biological agent A attack was rendered on the U.S. that would be a 100% reserve for agent A. Of course if this were the case the adverse consequences for a biological attack using agent A would significantly decrease, however the costs associated with the storage and production of the vaccine would drastically increase. The decision is therefore not an easy one. The choices that Parnell et al. (2009) chose to model are a 100% reserve, 50%, or no reserve at all.

Once the U.S. has made their two initial decisions the attacker then has two decisions to make, which type of agent to use and where to attack. The defender has the choice between agent A, B, and C, each having benefits and drawbacks. Each agent has a different probability of the attacker being able to acquire that particular agent. Each agent also has its own set of consequences from being exposed. Also as an added benefit, agent C is not detectable by the BioWatch program which may be seen as a significant benefit by the attacker. Once the attacker has decided on the agent to select and has actually acquired that agent, the attacker now has to decide on what population to attack. Obviously the higher the population, the more potential deaths or adverse economical impacts may occur.

Next the defender gets warning of the attack of agent A and the defender now needs to decide whether or not to deploy the vaccine A reserves. This of course depends on the previous decision the defender made about whether to acquire vaccines for agent A. It also depends on whether the attack was made with agent A, and how much time elapsed from the implementation of the attack until the defender could distribute vaccines to the infected populations, the amount of time that past could affect the effectiveness of the vaccine. And of course there is a cost associated with the distributing the vaccine. Table 13 supplies a synopsis of all the modeling assumptions in the Parnell et al. (2009) model.

Table 13: Modeling Assumptions (Parnell et al., 2009)



Categories	Our Assumptions	Possible Alternative Assumptions
Uncertain Variables	Probability of acquiring the agent, Detection time varies by agent	Other indications and warning
Decisions	Add Bio Watch city for agent A and B	Additional detection and warning systems
	Increase vaccine reserve stocks for agent A	Increase stocks of multiple agents
	Deploy vaccine A	Other risk mitigation decisions
Consequence Models	One casualty model for all three agents	Different casualty models for different agents
Risks	Casualties and economic consequences	Additional risk measures
	Defender minimizes risk and attacker maximizes risk	Other defender and attacker objectives
	Solve decision tree at various budget levels	Other solution approaches

Figure 14 graphically shows the effects of the defenders budget verse the defenders risk. As you can see when the budget is at its lowest the risk is at its peak. The attacker will choose agent A in this situation and this should encourage the defender to increase the budget and protect against an attack involving agent A. As the defender increases the budget and defenses against agent A, at some point the attacker will switch the most desired agent from A to B. As the budget continues to increase the defender can now add a city to BioWatch and the attacker will therefore switch from B to C since agent C cannot be detected through the BioWatch program. Parnell et al. (2009) note that this analysis is done with notional data but if the DHS was to use more accurate data the model can provide a quantitative way to evaluate the potential risk reduction of their defense options and provide a way for them to make cost benefit decisions.

Table 14: Key U.S. budget vs U.S. Risk

Owner	Decisions	1) Green	2) Blue	3) Red	4) Purple
US	Bio Watch	Status Quo	Status Quo	Status Quo	Add Next City
US	Agent A Storage	No Reserve	50%	100%	100%
Adversary	Agent Used	Agent A	Agent A	Agent B	Agent C
Adversary	Target Population	Large	Large	Large	Large
US	Deploy Agent A Storage	No	Yes	No	No
Casualties		375,300	261,000	168,500	156,800
Economic Impact (in Billions)		$378	$270	$170	$160

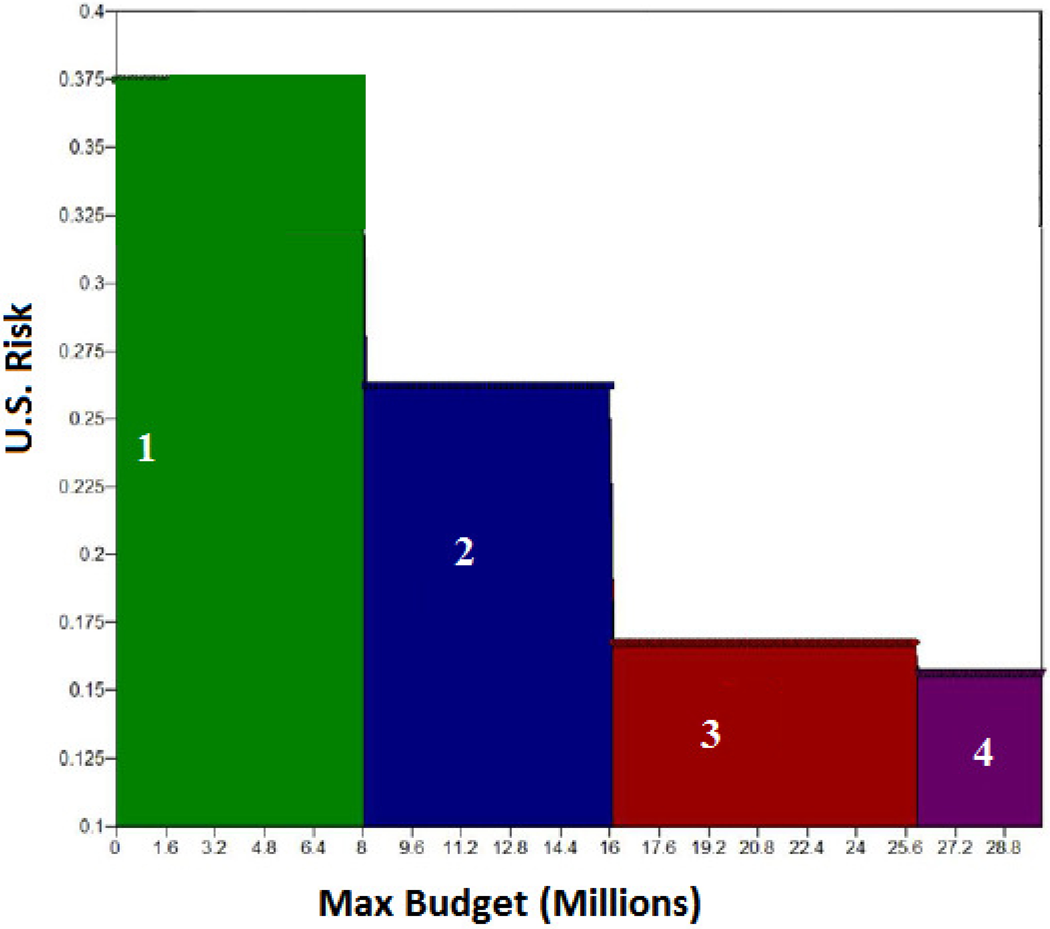
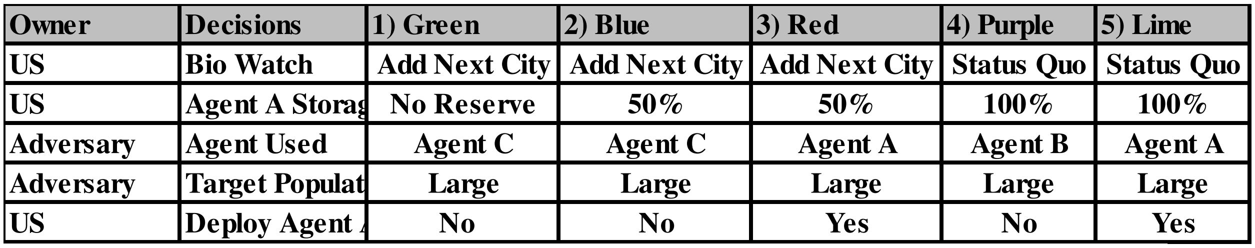


Figure 14: Defense budget vs Risk (Parnell et al., 2009)

The next analysis that risk managers may want to view is the value of control or the value of correlation diagram which will show what nodes the outcomes are most directly affected and which nodes are correlated. Parnell et al. (2009) note that the results are not surprising since they only had two uncertainty nodes in their model. The result shows that the attacker's ability to acquire the agent is positively correlated with the defenders risk. Since there are only two uncertainty nodes this example is very straightforward but when the complexity of a problem grows this analysis is very important because it can determine which nodes have the most influence over the outcomes and it can determine what nodes are highly correlated. This can help the defender determine which nodes to closely monitor or if there is a certain node that needs more research since the entire analysis may be highly influenced by the information in that node.

Sensitivity analysis is a very important aspect of any decision analysis project. Sensitivity analysis allows us to determine how critical our input parameters are and how they can influence the outcomes of the analysis. Here Parnell et al. (2009) using COTS software performed sensitivity analysis on their key assumptions. As seen in the Value of Correlation diagram above the attacker's ability to acquire the agent is a very important variable in their model. Figure 15 demonstrates how the decisions can change as the probability of acquiring agent A increases. The color changes in Figure 15 represent the decision changes for both the attacker and the defender. As you can see if the probability of acquiring agent A is very low the attacker is going to go with an easier alternative, in this case agent C. The attacker would select agent C rather than the alternative agent B, because when the probability for agent A is very low the defender chooses to add the city to BioWatch which means we can detect agent A and B but not C. Parnell et al. (2009) note that Figure 15 was created using a budget level of $20 million. They also note that in the original model the defender would not add a city to BioWatch, they would store 100% of vaccine for agent A, but they would not deploy the vaccine because the attacker chose to use agent B according to the model. As you can see when the probabilities associated with acquiring agent A increase, the optimal strategies change for both the attacker and the defender. Parnell et al. (2009) note that the risk management decisions for the defender change drastically when the probability that the attacker can acquire agent A are varied.

Table 15: Key Probability to acquire agent A vs U.S. Risk graph



Owner	Decisions	1) Green	2) Blue	3) Red	4) Purple	5) Lime
US	Bio Watch	Add Next City	Add Next City	Add Next City	Status Quo	Status Quo
US	Agent A Storag	No Reserve	50%	50%	100%	100%
Adversary	Agent Used	Agent C	Agent C	Agent A	Agent B	Agent A
Adversary	Target Populat	Large	Large	Large	Large	Large
US	Deploy Agent /	No	No	Yes	No	Yes

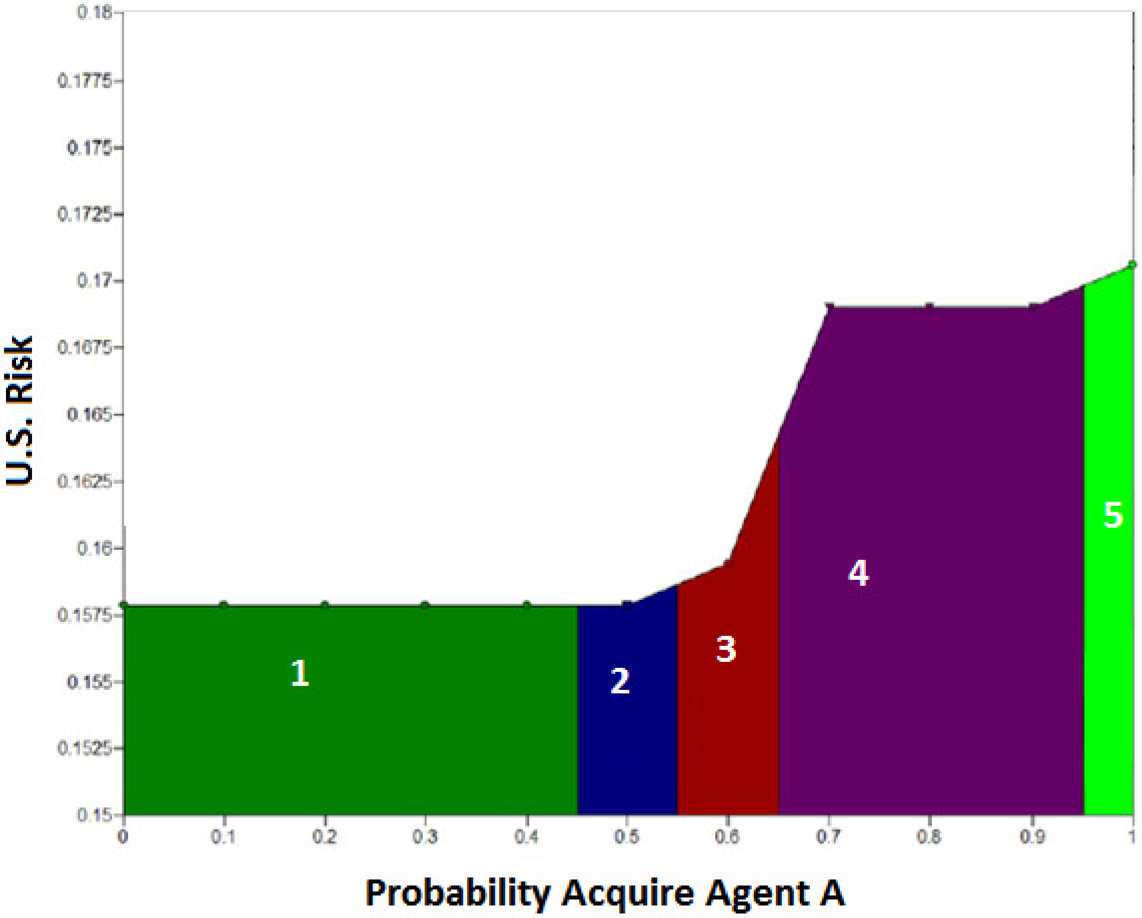


Figure 15: Probability to acquire agent A vs US risk

The defender-attacker-defender decision analysis model provided by Parnell et al. (2009) provides a clear and more accurate assessment of risk which in turn provides information for risk-informed decision making. The sensitivity analysis done provides the decision maker with important information on correlations and nodes that have high influence over the outcomes of the model which can provide valuable insight. Through the use of this model the defender can have a better understanding of the risk and use the information to make better risk-informed decisions.

Cargo Container Model Introduction

5.1 Motivation and Subject Background

The terrorist attacks against the United States have highlighted the vulnerabilities of our national security system. As a direct result of the terrorist attacks of September 11, 2001, aviation security underwent some drastic changes. By the end of 2002, the Transportation Security Administration (TSA), “had hired and deployed about 65,000 passenger and baggage screeners, federal air marshals, and others, and it was using explosives detection equipment to screen about 90 percent of all checked baggage” (Dillingham, 2003). The TSA has been developing techniques for advanced passenger screening that utilize national security and commercial databases to help employees accurately identify passengers that could pose a security risk. These improvements to aviation security are important, but there are other vulnerable entryways to the United States have thus far been neglected. For example, our nation’s ports are a vital entry way to the United States, and security measures and improvements have not been prioritized or organized.

A pressing concern of the United States is the illegal passing of plutonium or highly enriched uranium (HEU) through one of our nation’s ports. This is due to the fact that either of these materials can be used to construct a nuclear bomb or a dirty bomb. “According to best estimates, the global nuclear inventory includes more than 30,000 nuclear weapons, and enough HEU and plutonium for 240,000 more" (Allison 2004). Unfortunately, there are places in the world, where these materials have gone years without being secured. In recent years, the security standards have begun to improve due to the Second Line of Defense program. However, before the security improvements, some nuclear material could have been stolen, up for sale, or potentially already sold to terrorist. As reported by the Illicit Trafficking Database (ITDB) there were 332 confirmed incidents which involved the theft or loss of nuclear or other radioactive materials, as of December 2006 (IAEA, 2006). This only confirms that the threat of a terrorist obtaining the needed materials to construct a nuclear device is a real threat. There are significant vulnerabilities in the security measures that have been implemented by the United States; clearly we still need to improve our security measures.

The United States has made major efforts when it comes to research and development of new security measures. The DHS was formed in response to September 11, 2001 to better manage who and what enters our country. Maritime experts have also developed programs to improve security measures at ports, while minimizing the interruptions to the flow of container traffic. The programs were mainly driven by the Maritime Transportation Security Act of 2002, which required a universal security program to identify and deter threats from entering our ports. Other security improvements include the expansion of the 24-hour Notice of Arrival (NOA) rule to a 96-hour NOA which gives the Bureau of Customs and Border Protection (CBP) adequate time to evaluate the threat level of an approaching vessel. The Container Security Initiative (CSI) program is another program that was designed to improve security by pre-screening containers at foreign ports. The goal of the CSI is to identify a container carrying illicit material and to contain the situation on foreign soil, eliminating the threat of that container ever entering the United

States. The Customs Trade Partnership Against Terrorism (C-TPAT) agreement allows accelerated processing to these containers, if the containers fulfill CBP regulations. These initiatives are definitely a step in the right direction, but they are a long way away from improving port security to its optimal level. More research efforts need to be implemented to ensure security vulnerabilities are eliminated. One vulnerable area that has been highlighted recently is the 261 American ports. These ports are extremely important to the U.S. economy. Currently the United States is responsible for eleven-percent of the world trade traffic involving cargo containers, which means that 1/9 of all cargo containers go to or from the United States (US DOT, 2007). According to the Bureu of Transportation Statistics, on average 50,000 twenty-foot equivalent units (TEUs) enter the United States daily and is expected to increase. Trying to maintain an efficient flow of legitimate traffic, while also maintaining a satisfactorily level of security to prevent a potential terrorist attack with this magnitude of cargo traffic, is proving to be a major problem for port security officials (US DOT, 2007).

Unfortunately, it's not uncommon for cargo containers to be delivered to their destination before their very first inspection. This is unacceptable. Obviously with the 332 confirmed cases of illegal distribution of nuclear or other radioactive materials, we cannot afford to wait until delivery to inspect a cargo container. Cargo container could not only be used by the terrorist to transport the materials needed to construct a nuclear bomb, they may actually use the containers to enter our country illegally. Instances have been reported where cargo containers were found, modified and equipped for a terrorist to travel inside. A suspected al-Qaeda terrorist was found in one such cargo container traveling to Canada. The terrorist has already discovered the world's ports as a means to enter the United States, and could potentially be transporting illicit materials in them as well. We need to be proactive in eliminating our vulnerabilities and implementing security changes to prevent illicit nuclear material from entering the United States. Through the use of operations research, we have the opportunity to development cost effective security implications, security improvements, and innovative ideas that could drastically improve our nation's port security operations.

5.2 Introduction

There are enormous economic consequences when our nation's port security system is compromised. Interdicting nuclear material being smuggled into the United States on cargo containers is an issue of vital national interest, since it is a critical aspect of protecting the United States from nuclear attacks. However, the efforts made to prevent nuclear material from entering the United States via cargo containers have been disjoint, piecemeal, and reactive, not the result of coordinated, systematic planning and analysis. Our economic well-being is intrinsically linked with the success and security of the international trade system. International trade accounts for more than thirty percent of the United States economy (Rooney, 2005). Ninety-five percent of international goods that enter the United States come through one of 361 ports, adding up to more than 11.4 million containers every year (Fritelli, 2005; Rooney, 2005; US DOT, 2007). Port security has emerged as a critically important yet vulnerable component in the homeland security system.

Despite the importance of port security to our nation's economy, a small proportion of cargo entering United States ports are inspected for nuclear and radiological material. The Bureau of

Customs and Border Protection (CBP) physically inspects approximately five-percent of all cargo containers entering United States ports (Robinson et al., 2005; Ramirez-Marquez, 2008). Screening resources are targeted at high-risk containers, and the Automated Targeting System (ATS) is used to prescreen each cargo container and classify it as high-risk as low-risk (Strohm, 2006). Cargo containers entering the United States at other entry points, such as land border crossings, are extremely unlikely to be physically inspected (Parrish, 2008). Strategies that use radiation detectors to interdict nuclear material on these otherwise uninspected cargo containers have the potential to prevent a nuclear attack.

It is difficult to screen many cargo containers as they enter the United States, particularly those that enter the United States at land border crossings (as opposed to ports) and those that are transported by trains or barges. Cargo containers can be screened at security stations that are not limited to the points of entry to the United States or at foreign ports, where most screening is currently performed. This chapter considers such a scenario, and it focuses on the screening operations within a single station. The methodology used in this thesis can be used as part of a diverse security system to intercept nuclear material with security stations at truck weigh stations along interstates, loading docks, train stations, or at ports.

The approach taken in this thesis utilizes the model developed by Parnell et al. (2009) which was discussed in Section 4.2. We modify the model introduced by Parnell et al. (2009) to analyze screening techniques and procedures when considering both the decisions made by the United States and by the terrorists. This model will help determine whether actually screening cargo containers that enter the United States is a worthwhile investment in the efforts of protecting our country from a terrorist attack.

5.3 Basic Model and Results for Cargo Container Screening

The basic decision tree structure for our model assumes that the defender first decides whether or not to add a new type of radiation detector. This decision has two choices, one to remain at the current level of screening technology or to add a new level of screening technology. To remain at the status quo, the associated cost would be zero dollars, since no new technology is being implemented. It has been estimated that purchasing or upgrading container-scanning devices can vary between $1-5 million per device (Allen, 2006). Using this information we made an educated guess that including the personnel, time, equipment, research and development to create the technology, plus the rigorous testing to eventually implement the new container screening device, would bring the expected costs up to around $100 million.

The second decision is by the terrorist which is what agent they should select to build their weapon. Two agents were modeled one that gives off alpha rays and the other gamma rays; uranium and cobalt-60 respectively. Depending on the agent selected by the terrorists a different probability of technical success is determined. It is believed that a lot of consideration goes into agent selection by the terrorists. These considerations can include such things as material availability, potential damage that can be inflicted given a successful attack, the detection rate, costs, etc. We believe that the decision of the United States of whether to add a detector will also affect the decision of the terrorist for which agent he will select.

Some of the considerations taken into account by the terrorist when deciding which agent to select are also relevant when determining the probabilities of the terrorist's technical success in developing the actual weapon. Since not all the information is readily available for us to take all of these considerations into account, we made approximations for these probabilities. The model is flexible and if we had more information on the true values of these probabilities we could make the adjustments with just one entry change and the whole model would be updated.

The technical success of a terrorist or terrorist group in the development of a bomb is subject to certain conditions. For example, the source the attacker wishes to use must be first obtained; therefore the availability of the source must be taken into consideration in this uncertainty. Say the material is obtained; now the attacker must be educated enough to build the bomb. In the case of uranium many researchers believe many terrorist groups would be able to build a nuclear bomb with highly enriched uranium (HEU), however, they believe that it would be very hard for the terrorists to acquire enough of this material to build the bomb. A National Research Council study reported, "The basic technical information needed to construct a workable nuclear device is readily available in the open literature. The primary impediment that prevents countries or technically competent terrorist groups from developing nuclear weapons is the availability of SNM, especially HEU" (National Research Council, 2002). SNM stands for special nuclear material which includes materials like fissile plutonium and of course HEU. The probabilities chosen to represent technical success of a uranium weapon were 0.6 for success and 0.4 for failure. "Cesium-137, cobalt-60, and americium-241 are considered to be the most likely materials for use in a dirty bomb due to their availability and their relative ease of handling"

(ABC News, 2005). For ease of modeling we chose agent cobalt-60 to be the selected agent by the terrorist to build a dirty bomb. Since the availability and handling of cobalt-60 is simpler that uranium we assume that the probability of success 0.8 and probability of failure 0.2 for this material.

The United States has its own uncertainty in technical success when developing the new radiation detectors. The United States is constantly developing and improving their techniques for detecting contraband materials that are trying to enter our country. The technical success of the United States depends firstly on the decision made, whether or not to add a new type of radiation detector. If the United States decides to remain at the status quo the technical success is 1 for success and 0 for failure. This is because the United States is remaining at the same level of screening that we currently have, and therefore have no risk of failing at creating a new type of technology. On the other hand if the United States decides to invest in a new technology there is a chance we could try to develop a certain type of radiation detector and fail. Therefore, we have assigned a probability of 0.8 of technical success for the United States in developing a new screening radiation detector and a probability of 0.2 for trying to develop the technology and failing.

There is also a cost associated with the technical success of the United States when developing this new technology. If the United States develops the technology and implements it, as stated at the beginning of this section, we assume the cost to be $100 million. If the United States tries to develop a new radiation detector with new technology and fails, there will still be an associated cost; we have estimated that cost as $40 million. It is believed if the United States attempts to develop a new technology and is unsuccessful, the cost will be significantly less since there will be no implementation, training, or decisions on where or how to actually install the new container scanner. To estimate the cost per container, take the cost of technical success and spread it over the expected 11.4 million containers that will enter our ports, which equals $8.77 per container. Similarly, we take the cost of technical failure and divide it over the expected 11.4 million containers and determine the expected cost for technical failure per container is approximately $0.35 per container.

The next uncertainty in the model is an alarm. This uncertainty is conditioned on two other uncertainties. First is which type of detector is being used, either the new technology or the old technology. Second is what type of threat we are trying to detect either cobalt-60 or uranium, or no threat at all. These two uncertainties influence the rate of an alarm. If we stay with the old technology and there is no threat the false alarm rate is set at 0.025 and our true alarm rate is 0.80 according to Bakir (2008). The false alarm rate of 0.025 and the true alarm rate of 0.80 were both used in this model for both uranium and cobalt-60. Of course if we implement some type of new technology we would like to improve the alarm rate given there is a threat in the container, but we'd also like to lower the false alarm rate. Therefore with the implementation of a new radiation detector we have improved the true alarm rate to 0.90 and lowered the false alarm rate to 0.01. The false alarm rate is mainly based on alarms from NORM sources such as ceramic tiles, irradiated iron, cat litter, or legitimate medical equipment (Merrick and McLay, 2009). Using the logic described in Merrick and McLay (2009) we use 0.03125 as our input for the probability of a NORM source of radiation in the container.

The decision made by the port authorities and CBP of the United States about whether or not to physically inspect the cargo container is absorbed into the alarm node. There is no associated cost with an alarm itself, but there is an associated cost with a physical inspection. The physical inspection has to include the costs of the personnel performing the inspection and the cost of delaying the cargo inside the container. Merrick and McLay (2009) use an estimate by Bakir (2008) of approximately $600 per container that is physically inspected. If there is an alarm we assume that the United States will always inspect the container; if there is no alarm, we assume that the United States will never inspect the cargo container. Therefore, each time we have an alarm, we incur the $600 physical inspection cost.

Now we have a chance node which will represent whether or not the United States will find the illicit material. This node is dependent on two others, first the decision of whether or not there was an alarm, and whether or not there is illicit material inside that cargo container. To find the probability that there will be a threat in any given container we use an estimate of Bakir (2008) stating that the probability of a terrorist smuggling nuclear material inside a cargo container is 0.1 in the next 10 years (Merrick and McLay, 2009). When Bakir (2008) divides this over the amount of cargo containers expected to enter the United States in the next 10 years they get the probability of $5 \text{x} 10^{-10}$ that a threat is in any given container. Of course if there is no illicit material there will be no material to find and therefore the probability of finding the material is zero. If there is uranium or cobalt-60 inside the cargo container and we physically inspect we will find the material with a probability of 0.9. If we do not physically inspect and there is illicit material inside the cargo container we will never find the material which is represented by a 1.0 probability of not finding the material. If the United States does inspect and does find the material there is an associated cost with the removal. Merrick and McLay (2009) explain that when the material is found the removal involves experts with the correct equipment and containment; this is estimated to be $100,000 per found material.

The probability of an attack is represented by the last chance node. Whether the terrorists can attack is dependent on two other chance nodes. First whether or not the United States was able to find the material and whether there is a threat inside the container. If there was an illicit material inside the container and the United States finds the material, the terrorist have a zero chance of attacking using that material since it is now in the hands of the United States. Merrick and McLay (2009) estimate that if a container passes through that does contain illicit material there is a 0.5 chance of an attack. This probability will remain constant for both cobalt-60 and uranium. The expected cost of a successful attack has been estimated at $40 billion dollars (Merrick and McLay, 2009). Therefore we have assigned the cost of an attack with the agent uranium and with agent cobalt-60 to cost $40 billion dollars, and $35 billion dollars respectively. An attack with uranium is believed to inflict greater economic impact than cobalt-60, which is why there is an increase in attack cost when the terrorist selects uranium.

Figure 16 shows a simplified decision tree describing the decision concept. The decision tree shown is an overview of the model. Figure 17 shows the dependencies that exist in an influence diagram. One node that we have not discussed is the Total Cost (US). This sums all the costs of the defender (United States) throughout the model. Both models shown in Figure 16 and Figure 17 were developed using DPL.

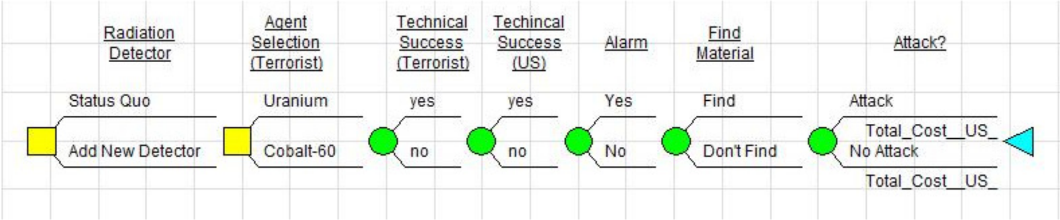


Figure 16: Decision Tree for Basic Model

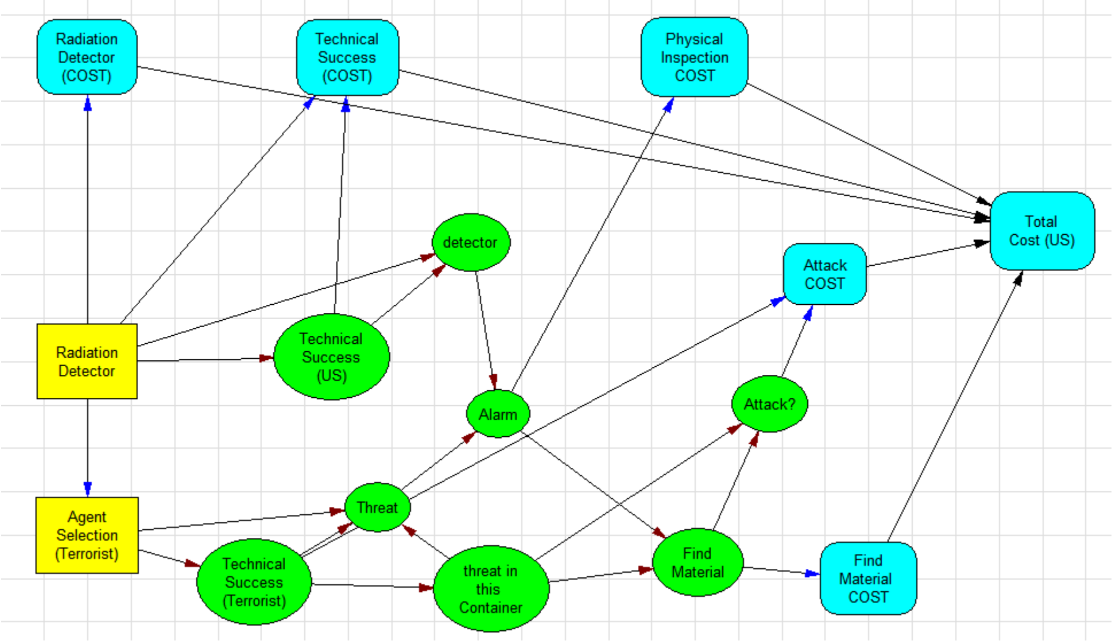


Figure 17: Influence Diagram for Basic Model

The optimal decision according to this model is for the United States to invest in a new detector, and for the terrorists to choose agent cobalt-60, as indicated by the bold lines in Figure 18. This is mainly due to the prominence of false alarms and the high costs associated with screening all of these false alarms, since as mentioned before, every time there is an alarm we assume the container is physically inspected. With the new detector technology the prominence of false alarms decreases and the true alarm rate increases, the cost savings associated with this change in the new technology outweighs the cost of technical success or failure. Since the United States is attempting to minimize their expected cost per container, the optimal choice is to invest in the new detector, however, it should be noted that the expect cost is very close. Therefore sensitivity analysis in this case will be very important and if more information was known about the true probability values or associated costs, the outcome of this model could easily change. As mentioned previously, the United States is attempting to minimize the cost, whereas the terrorist is trying to maximize the cost for the United States, therefore they chose cobalt-60 as their weapon of choice since it has the greater expected cost.

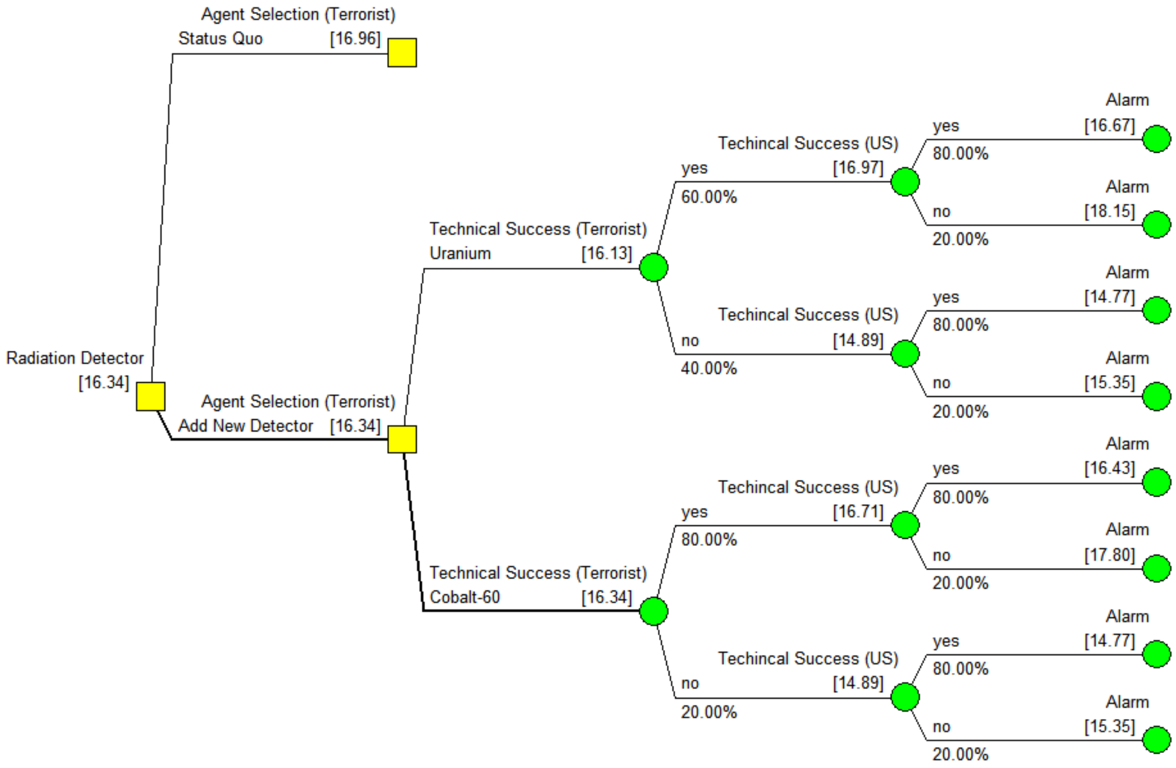


Figure 18: Model Policy Tree

Some interesting results were obtained while performing sensitivity analysis on the basic model. We varied the cost of the physical inspection variable (given an alarm has sounded, so a physical inspection is performed) from $0 to $1000 and the optimal choice would always be for the United States to remain at the status quo when the cost is below $547.50, once the cost exceeds this amount the optimal choice is for the United States to invest in the new detector. This is believed to be due to the decrease in false alarms and increase in true alarm rates, so the need to physically inspect containers would decrease with the new alarm technology.

Another confirmation that the cost screening false alarms is just too high to justify remaining at the status quo is displayed in Figure 19. As long as the false alarm probability is well below the current rate of 0.025 with the status quo, the choice is to always implement the new detector. Once the true alarm probability increases, the false alarm probability is allowed to increase slightly as indicated by Section 1 of Figure 19. In Section 2 the decision is to always remain at the status quo. Once the false alarm probability increases there is no longer enough benefit to justify adding a new detector.

Table 16: Key to New Detector True Alarm vs False Alarm graph

Owner	Decisions	1) Green	2) Blue
Adversary	Agent Selection	Cobalt-60	Cobalt-60
U.S.	Radiation Detector	Add New	Status Quo

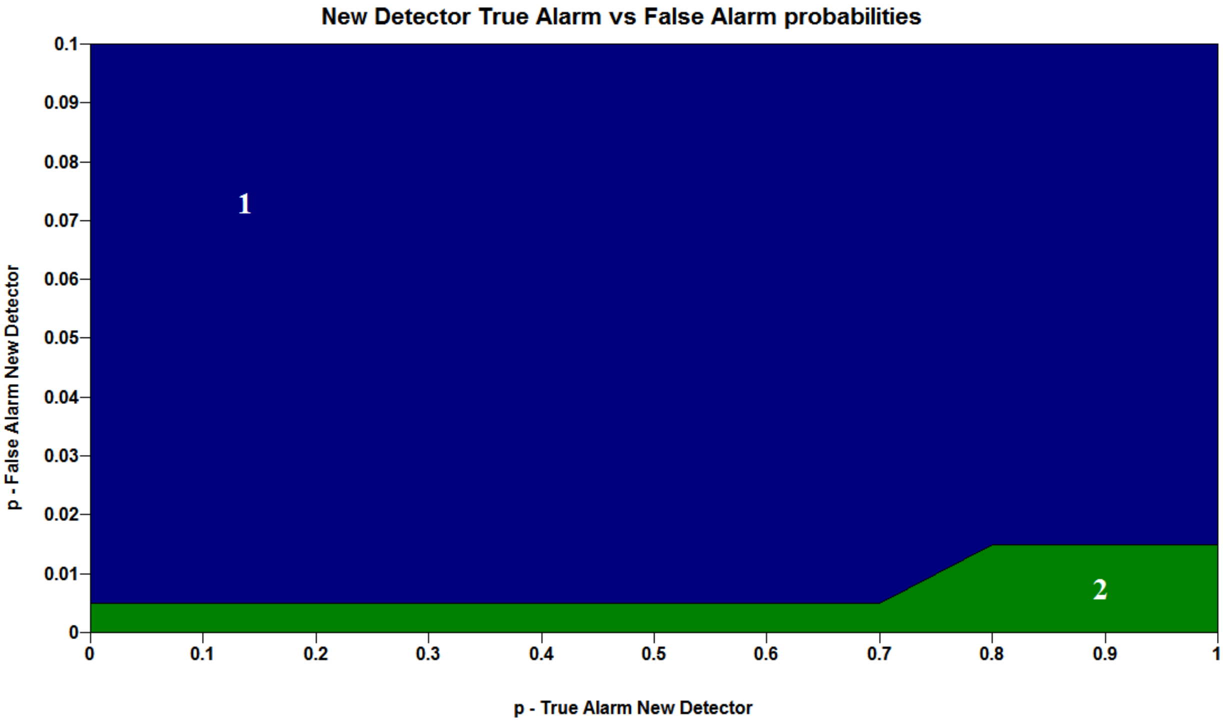


Figure 19: New Detector True Alarm vs False Alarm probabilities

We also ran sensitivity analysis on the cost associated with the technical success of the United States for adding a new detector. We varied the technical success from $0 to $12 and technical failure from $0 to $45 dollars. When both costs are at their lowest, the successful implementation of a new detector ranging from $0 to $9.52, and technical failure ranging from approximately $0 to $38, the United States would want to invest in the new detector 100% of the time. Once either cost rose from that range, it was no longer cost effective for the United States to invest in a new detector.

When performing sensitivity analysis on the probability of finding the material given a physical inspection from 0.7 to 1, the optimal choice is remains consistent to add a new detector. We also varied the probability of an attack taking place given a threat passed through the system. We decided to vary this probability from 0.4 to 1; the marginal probability set in the original model was 0.5. It is believed that even if the terrorist successfully smuggle the material through the port security system, there may be other opportunities for authorities to intercept the material. It is also thought that not all the components of a weapon will be shipped in one container so there is still a possibility that the terrorists will not have all the required materials to build and successfully detonate the weapon. The optimal choice given by our model is to again add a new detector for all values of an attack (given a threat passed through the system) ranging from 0.4 to 1. The optimal choice for the terrorist is to choose cobalt-60. This is due to the assumed higher technical success rate with cobalt-60 rather than uranium.

Figure 20 displays a two way rainbow diagram to view the differences in decision when varying the probability a threat is in this container and the cost of a successful attack using uranium. The results change depending on what values both the probability a threat is in this container and the attack consequences range between. The United States' decision remains to add a new detector throughout Section 1 and 2 of Figure 20. The agent selected by the terrorist changes from uranium or cobalt-60, depending on the cost of an attack and the probability of a threat in the container. If the probability of a threat being in the container is very low, the terrorist would choose uranium as their weapon of choice. Once the probability of a threat being in the container rises, the terrorists preferred weapon becomes cobalt-60. Unfortunately, the DPL program used is unable to determine the exact probability of a threat being in the container where the decision of the terrorist changes from uranium to cobalt-60. But it is an important finding that when the probability of a threat actually being inside a container is very low, the terrorist would risk the decrease in technical success probability to smuggle in a uranium weapon, with the hopes of causing more economic damage to the United States.

Table 17: Key to Probability of a Threat in this Container vs. Attack Cost using Uranium Graph

Owner	Decisions	1) Green	2) Blue
Adversary	Agent Selection	Uranium	Cobalt-60
U.S.	Radiation Detector	Add New	Add New

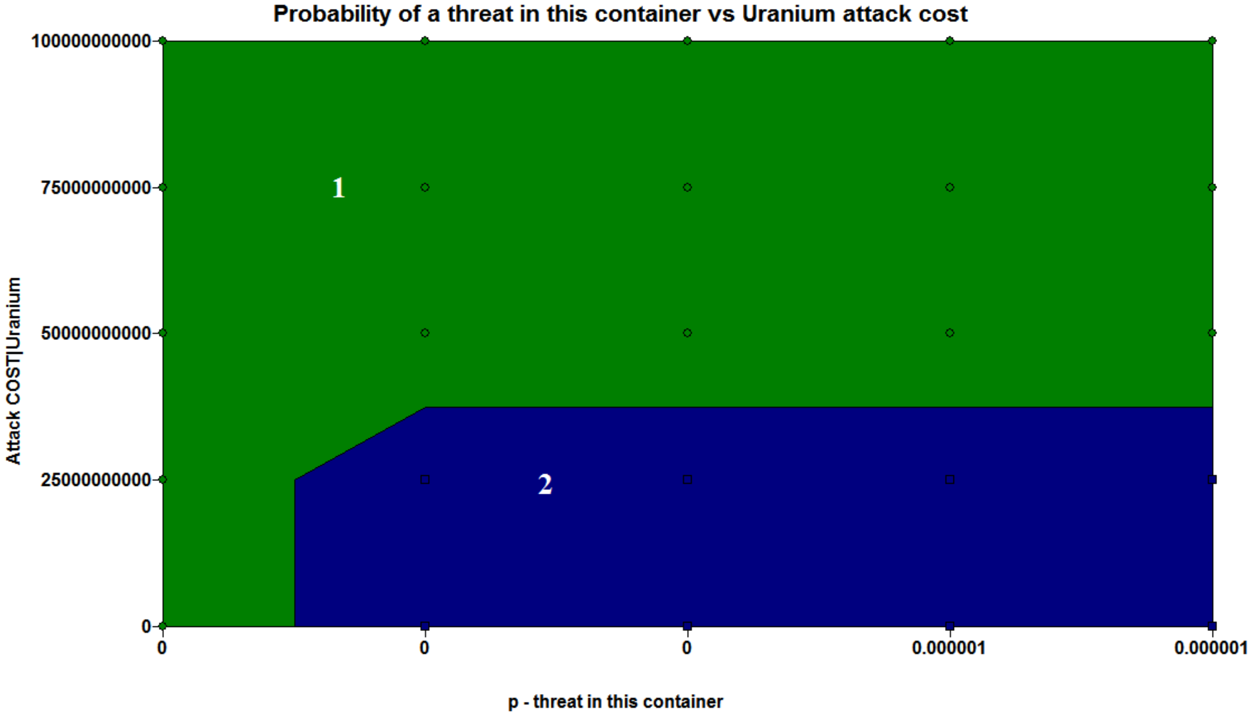


Figure 20: Probability of a Threat in this Container vs. Attack Cost using Uranium

This model is extremely sensitive to the expected cost of implementing the technology needed to develop a new type of detector. The nominal value estimated in this model is $8.77. The decision of adding a new detector would remain the same if the expected cost rose to $9.52. Once the expected cost rises from $9.52 to $9.53 the optimal decision is for the United States to remain at status quo and not to invest in the new technology. Obviously, with this extreme fluctuation in optimal decision, there should be special focus on estimating the expected cost accurately.

The optimal decision determined by our model is for the United States to invest in a new detector, and for the terrorists to choose agent cobalt-60, shown in Figure 18. As discussed previously this is mainly due to the prominence of false alarms and the high costs associated with screening all of these false alarms. With the new detector technology the false alarms decrease and the true alarm rate increases, which in turn provides a cost savings greater than the associated risk with the new detectors technical success. However, as shown by the sensitivity analysis, by varying some of the probabilities and costs in this model, we can manipulate the results from adding a new radiation detector to remaining at the status quo. We can also vary the results for the terrorist to choose uranium rather than cobalt-60. We believe that the marginal probabilities and costs that are in the basic model are in line with other papers and open literature. Of course, if the values could be reevaluated by the government and more accurate values were inserted into the model, the results would be more precise for real world use.

5.4 Extensions of Basic Model

5.4.1 Random Physical Inspections

The conclusions based on the model described in Section 5.3 indicate that at the nominal values set in our model, it is cost effective to add a new detector to scan cargo containers for radiation that are entering the United States. How would that change, if we could extend the model to reflect more realistic assumptions and then reevaluate whether it is cost effective to add a new detector? Perhaps, instead of assuming the United States physically inspects each and every container that sets off an alarm, it may be more cost efficient for the United States to randomly physically inspect a portion of those containers. Likewise, instead of never physically inspecting a container that does not set off an alarm, we would assign a probability for those to be physically inspected as well. By implementing random physical inspections of cargo containers rather than making a decision for all cargo containers, it may be possible to keep some of the deterrence factor and possibly reduce the cost for inspecting each cargo container that sounded an alarm.

Say for instance instead of assuming that every time an alarm sounds, a physical inspection occurs, we insert a chance node. Now we can enter a probability for physically inspecting given an alarm sounds and a probability for physically inspecting when no alarm sounds. Say we choose to inspect 80% of all cargo containers that sound an alarm and 0.01 when no alarm sounds as our base case. The cost of a physical inspection remains at its nominal value of $600, and $0 if we do not physically inspect. Figure 21 displays the resulting decision tree given the new parameters we've set in our model.

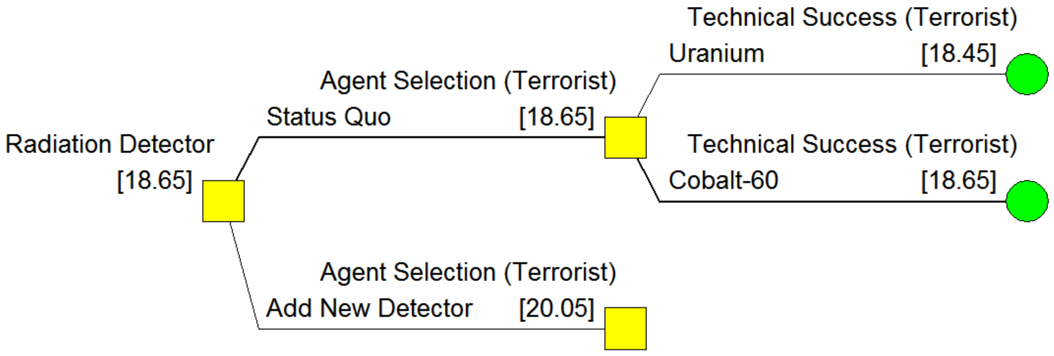
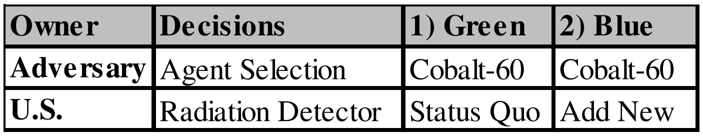

Radiation Detector
[18.65]
Agent Selection (Terrorist)
Status Quo
[18.65]
Agent Selection (Terrorist)
Add New Detector
[20.05]
Technical Success (Terrorist)
Uranium
[18.45]
Technical Success (Terrorist)
Cobalt-60
[18.65]

Figure 21: Decision Tree for Random Physical Inspections

The expected cost increased from $16.34 in the previous model to $18.65. This is because instead of the assumption we always physically inspect when an alarm sounds, we have a set probability of what we will physically inspect instead. By adjusting the probabilities of whether to physically inspect given an alarm, or no alarm, we can change the expected value of our model. Figure 22 illustrates how the expected cost of inspecting would vary depending on the probability we set for physical inspections given an alarm. As the probability of a physical inspection given an alarm goes up, the expected cost goes up accordingly. When we set the probably lower than approximately 0.625, the expected cost becomes lower than the basic model we described in Section 5.3. However, even if we decided to set a probability lower than 0.625, the optimal decision for this model is to remain at status quo for the United States, which differs from the basic model's optimal decision. Once the probability for physically inspecting the cargo container increases to approximately 0.9, the decision switches and the optimal decision for the United States is to add a new detector.

Table 18: Key to Varying Physical Inspection Cost if Alarm Sounds graph



Owner	Decisions	1) Green	2) Blue
Adversary	Agent Selection	Cobalt-60	Cobalt-60
U.S.	Radiation Detector	Status Quo	Add New

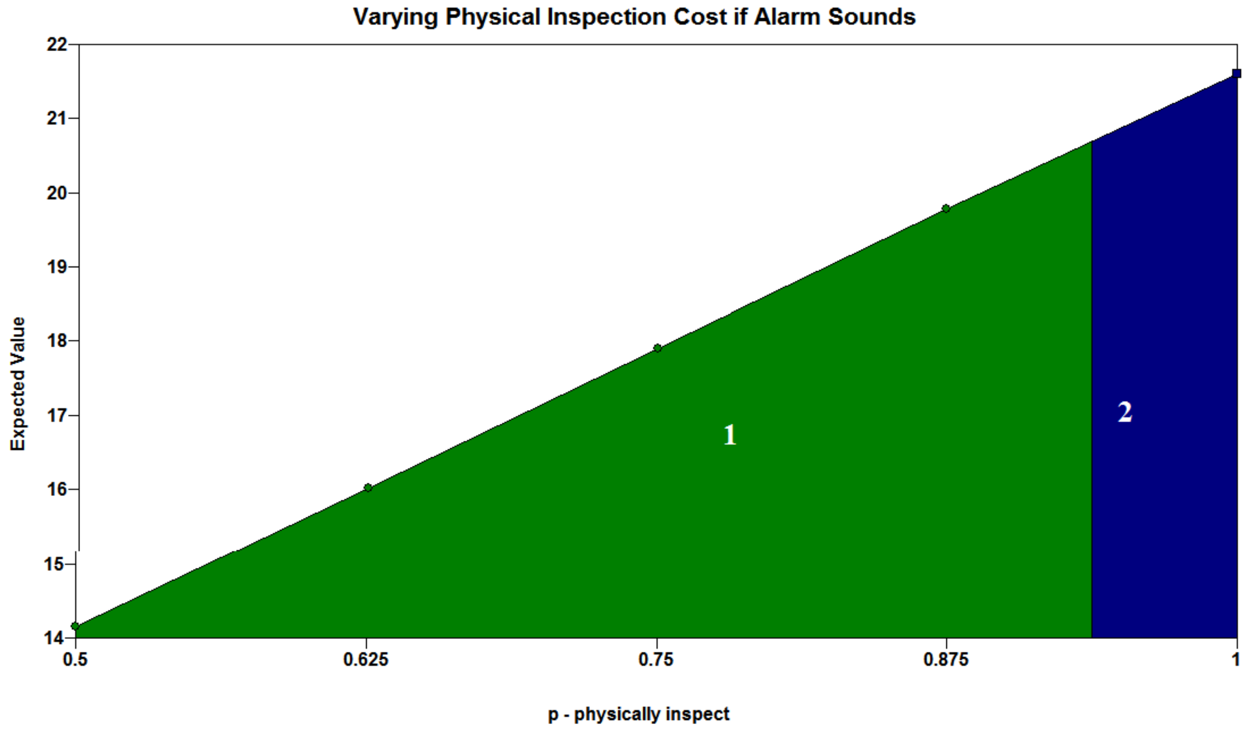


Figure 22: Varying Physical Inspection Cost if Alarm Sounds

The decision of the terrorist should again remain to choose cobalt-60 as their selected agent, which is consistent with the basic model described in Section 5.3. This again is due to the believed higher technical success with cobalt-60 than uranium. However, what if we varied the technical success for the terrorist on both cobalt-60 and uranium, how would that change the preferred agent? According to Figure 23, if the technical success for the terrorist was equal with both agents, the terrorist would always choose uranium. It's when the technical success starts to be higher for cobalt-60 than uranium, the decision switches to the terrorist always choosing cobalt-60.

Table 19: Terrorist Technical Success Uranium vs Cobalt-60 graph

Owner	Decisions	1) Green	2) Blue
Adversary	Agent Selection	Uranium	Cobalt-60
U.S.	Radiation Detector	Status Quo	Status Quo

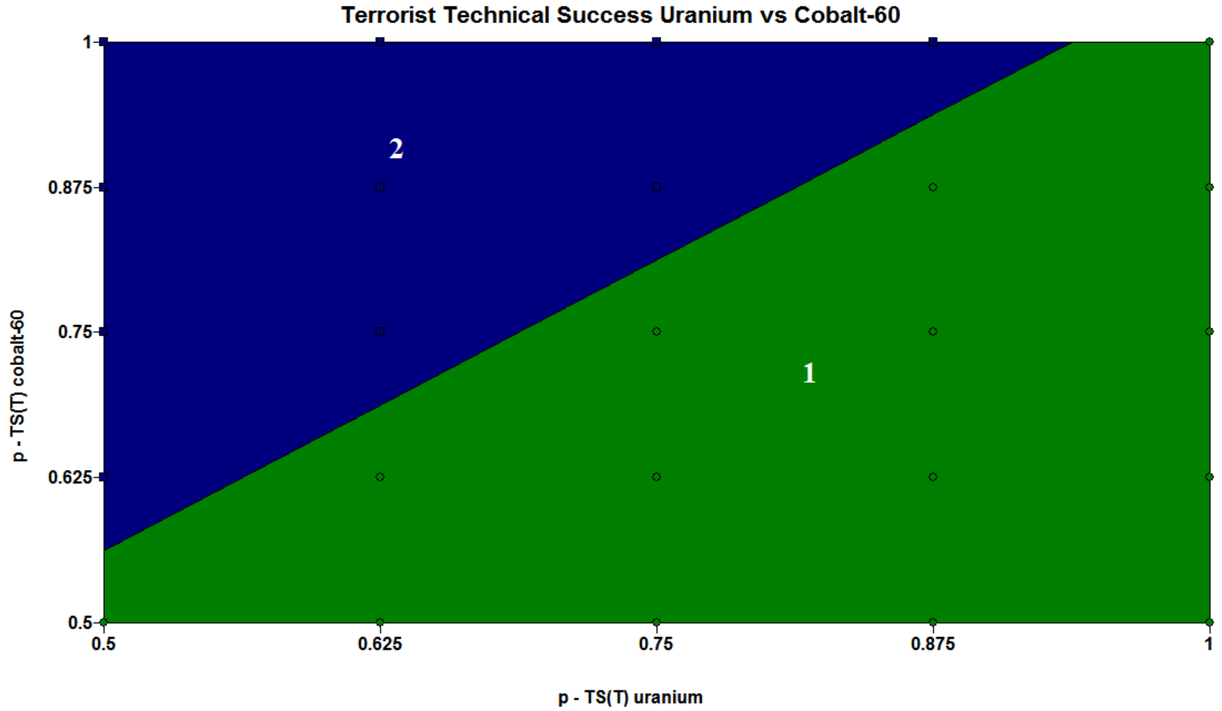


Figure 23: Terrorist Technical Success Uranium vs Cobalt-60

5.4.2 Nuclear Bomb vs. Dirty Bomb

The basic model described in Section 5.3 considers two types of dirty bomb attacks, the first involving uranium, and the other involving cobalt-60. Both of these types of dirty bombs could inflict massive amounts of economic consequences. However, the consequences of a dirty bomb would be miniscule compared to a true nuclear bomb detonation inside the United States. "By one estimate, a 10- to 20-kiloton weapon detonated in a major seaport would kill 50,000 to 1 million people and would result in direct property damage of $50 to $500 billion, losses due to trade disruption of $100 billion to $200 billion, and indirect costs of $300 billion to $1.2 trillion" (Medalia, 2005).

To represent this change in the model we now consider the choice of uranium by the terrorist to be weapon grade highly enriched uranium (HEU). We have varied the cost of an attack to reflect the estimates of a nuclear attack, which we will use a nominal value of $1.2 trillion and the nominal amount previously discussed in Section 5.3 of 40 billion for the dirty bomb attack. All other values remained consistent with the basic model from Section 5.3. The results are displayed in Figure 24; the United States should add a new detector, and the terrorist should choose uranium, which represents the nuclear bomb. Due to the drastic increase in consequence from a detonation of a weapon comprised of the materials that pass through the port, the optimal choice for the agent selection by the terrorist changed from cobalt-60 in the basic model to uranium. In this new model uranium means the terrorist plans to build a true nuclear bomb. Even though the probability of the terrorist successfully building a true nuclear bomb is less than the probability of the dirty bomb, the increase in economic consequence that will be felt by the United States, outweighs the risk for the terrorist.

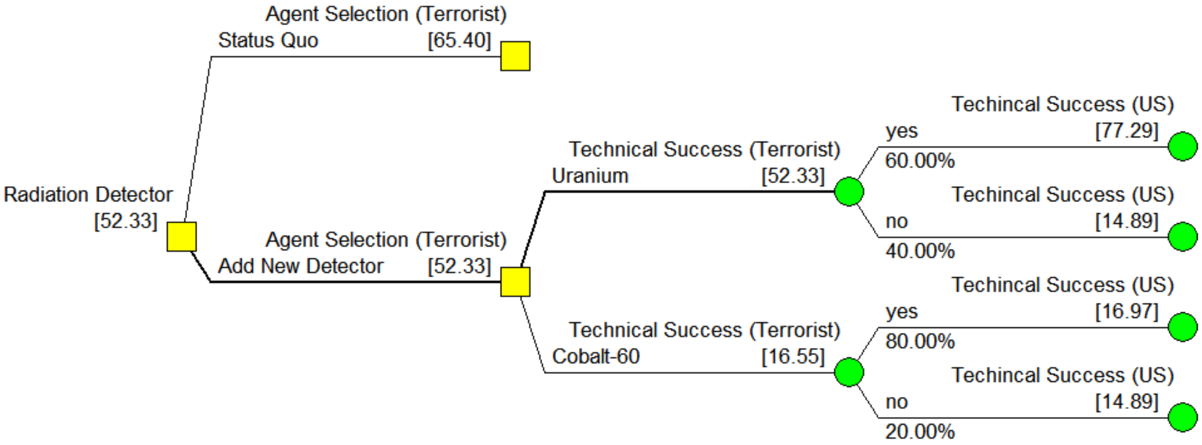


Figure 24: Decision Tree for Nuclear vs. Dirty Bomb

During the sensitivity analysis, it was found that when the economic consequences of both the nuclear and the dirty bomb are equal to the basic models nominal value the terrorist's choose to build the dirty bomb. This is because the technical success of a dirty bomb is higher than a true nuclear bomb and if the consequences are set back to the basic model values, there is no benefit to building a nuclear bomb compared to the dirty bomb. Figure 25 displays the results graphically. Section 1 represents when the terrorist should choose to build a dirty bomb rather than a nuclear bomb. Section 2, in the right bottom corner represents when the terrorist's decision to build a nuclear bomb. As you can see, when the cost of detonating a dirty bomb is equal to the nuclear bomb, the terrorist should always choose to build the dirty, because of the higher success rate.

Table 20: Key Cost of an Attack graph

Owner	Decisions	1) Green	2) Blue
Adversary	Agent Selection	Cobalt-60	Cobalt-60
U.S.	Radiation Detector	Add New	Add New

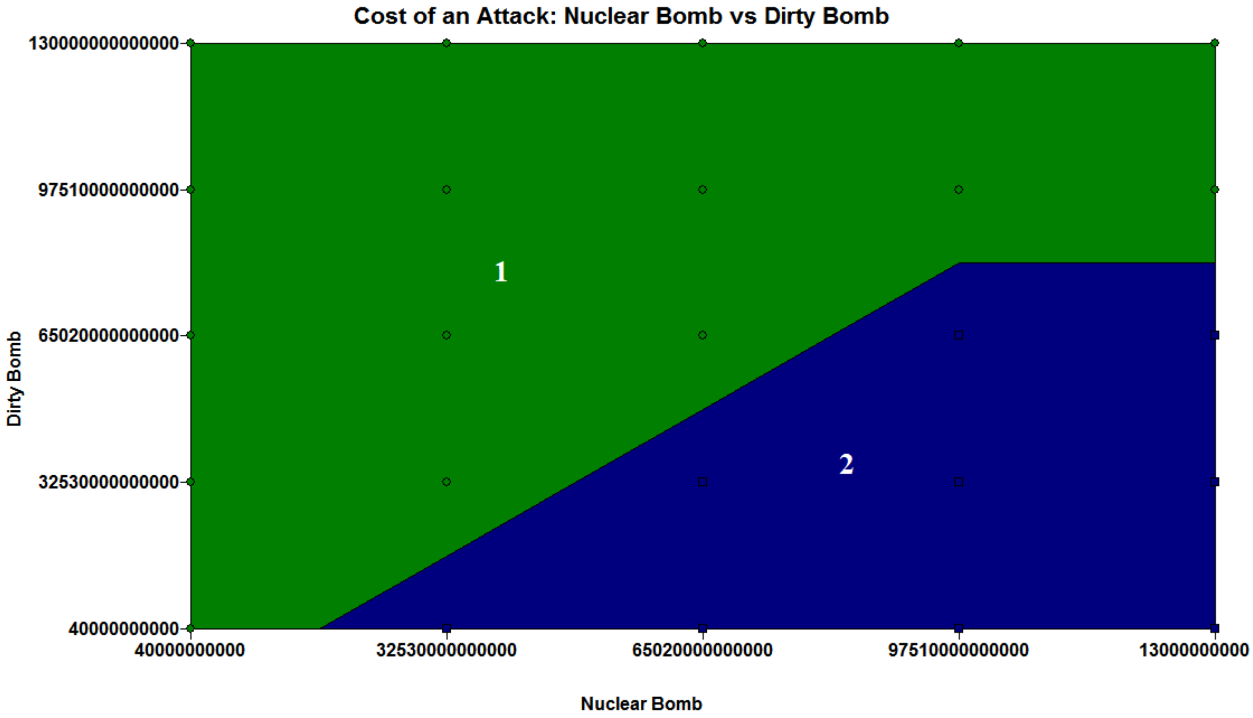


Figure 25: Cost of a dirty bomb attack vs. a nuclear attack

Figure 26 shows that there is a point when the terrorist will still choose the nuclear bomb even when the probability of technical success with a dirty bomb is 100%. In Figure 26 you can see that Section 1 represents when the terrorist should choose to build a dirty bomb. This is again when the economic consequences are equal to a dirty bomb attack set at 40 billion dollars to somewhere around $67 billion is when the nuclear bombs consequences are so much higher than the dirty bomb that the terrorist should always choose the nuclear bomb even when the success of the nuclear bomb is lower than the dirty bomb. This is because the model is working with expected values and the expected value of the nuclear attack costing 1.2 trillion dollars vs. the dirty bomb at 400 billion, even when the probability is substantially lower; the expected value is still higher to select the nuclear bomb.

Table 21: Key Nuclear Bomb Attack vs Terrorist Technical Success with Dirty Bomb

Owner	Decisions	1) Green	2) Blue
Adversary	Agent Selection	Uranium	Cobalt-60
U.S.	Radiation Detector	Add New	Add New

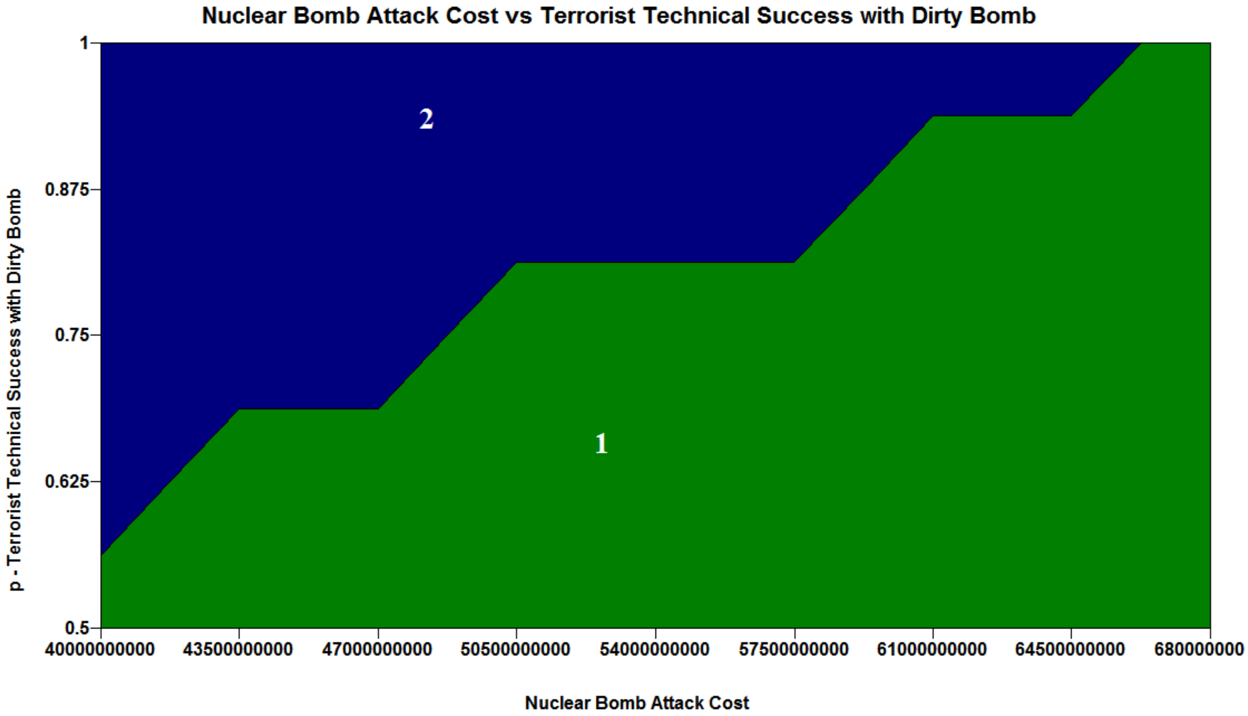


Figure 26: Terrorist technical success with a dirty bomb vs. cost of an attack with a nuclear bomb

5.5 Model Comments

The modeling shown in Section 5.3 introduces a technique that provides a more realistic risk assessment of the true situation being modeled. Using this model the decision maker can construct more accurate judgments based on the true situation. This increase in accuracy could save lives with the decisions being made. The model can also help the decision maker understand the interdependencies of the model and visually see how his resource allocations affect the optimal decisions of the defender and the attacker.

The two extensions shown in Section 5.4 are just a few of the potential variations that could be made to this model. By adding information, changing nodes, and/or changing the inputs we can see how the optimal decisions change. This model is extremely versatile and adaptable. Because of its easy manipulations, this model could be a valuable tool to the counterterrorism departments of the United States. The inputs and parameters could be edited in seconds and could provide an even more accurate assessment of the real world situation that it is designed to model. Again, the ability for it to be changed so easily makes it such a great decision making tool.

As with any modeling program there are limitations. For example the number of decisions can quickly grow out of control; therefore it is important to incorporate only the most important decisions and inputs into the model.

A Linear Programming Framework for Screening Cargo Containers

6.1 Introduction

This chapter summarizes the methodology introduced by McLay et al. (2010) for screening cargo containers for nuclear material at security stations throughout the United States using knapsack problem, reliability, and Bayesian probability models. We introduce the Container Reliability Knapsack Problem (CRKP), a linear programming model for using existing screening technologies (e.g., radiation portal monitors) to screen cargo containers on truck trailers at a security station using knapsack problem, reliability, and Bayesian probability models. The approach investigates how to define a *system alarm* given a set of screening devices, and hence, designs and analyzes next-generation security system architectures. Containers that yield a systems alarm undergo secondary screening, where more effective and intrusive screening devices are used to further examine containers for nuclear and radiological material. It is assumed that there is a budget for performing secondary screening on containers that yield a systems alarm. This chapter explores the relationships and tradeoffs between prescreening intelligence, secondary screening costs, and the efficacy of radiation detectors. The key contribution of this analysis is that it provides a risk-based framework for determining how to define a system alarm when screening cargo containers given limited screening resources and Bayesian probability models. The analysis suggests that prescreening intelligence is the most important factor for effective screening, particularly when radiation detectors are highly dependent, and that radiation detectors with high true alarm rates can mitigate some of the risk associated with low prescreening intelligence.

6.2 Background

There has been a dearth of research that applies operations research methodologies to problems in detecting nuclear material in cargo containers. Wein et al. (2007) analyze cargo containers on truck trailers passing by a series of screening devices at the port of Hong Kong. They apply queuing theory and optimization to determine the optimal placement and scanning time for radiation portal monitors such that a desired detection probability is achieved. Their analysis is based on a fixed cost for the total screening budget and variable passing times for each truck. Although CRKP also analyzes the scenario when cargo containers pass by a series of radiation detectors, there are several key differences between CRKP and the model by Wein et al. (2007). First, a solution to CRKP defines a system alarm, whereas Wein et al. (2007) do not address this issue in their optimization model. Rather, Wein et al. (2007) focus on the spatial positioning of RPMs in a security station at a port to improve detection. In addition Wein et al. (2007) do not consider the effects of prescreening intelligence.

Wein et al. (2006) analyze an 11-layer screening system for containers entering the United States by considering a fixed budget and port congestion. They determine an alternative screening design that allows the weapon placement in the truck to vary and the detection capabilities of the system to be improved relative to the current design. Morton et al. (2005, 2007) and Pan (2005) use stochastic network models to detect smugglers and nuclear material based on paths traversed as part of the Second Line of Defense program. Ramirez-Marquez (2008) proposes inspection strategies of cargo containers that minimize costs of inspection at ports using decision trees. The strategies involve selecting different sensors that have varying reliability and associated costs. Using the decision tree, a minimum cost inspection strategy is presented that maintains the required detection rate. Additionally, an algorithm for efficiently determining an optimal solution is included. Ramirez-Marquez (2008) assume that various sensors screen containers in a selected order, whereas order is not a factor in CRKP. Moffitt et al. (2005) develops a model using information gap decision making to determine how to inspect a number of targets to shed light on robust decisions.

McLay et al. (2008) examine risk-based issues in detecting explosives in aviation security baggage screening models. They examine the tradeoff between intelligence and screening technology for aviation baggage security screening systems using a cost-benefit analysis when there are two types of screening technologies, one for low-risk baggage and another for high-risk baggage. The more accurate and expensive baggage screening technology is targeted at passenger baggage classified as high-risk. It is concluded that more expensive screening technologies are warranted only if effective prescreening is available. There are several key differences between the model employed by McLay et al. (2008) and CRKP. First, McLay et al. (2008) evaluate the scenario when a single device is used to screen baggage for explosives whereas CRKP evaluates the scenario when multiple screening devices are used to screen for nuclear material. Moreover, CRKP assumes that the same screening device is used to screen both high-risk and low-risk containers, whereas McLay et al. (2008) assume that there are two different types of screening technologies available. A third difference is that CRKP assumes that screening costs are limited whereas the model by McLay et al. (2008) assesses the screening costs but does not limit them.

Kobza and Jacobson (1997) consider the design of security system architectures using reliability models in the context of aviation security baggage screening systems. Different objects (aviation bags) can take different paths through the system, and hence, are screened by varying subsets of screening devices. Their model is analyzed based on Type I (a false alarm is given) and Type II (a threat is not detected) errors, and it is formulated for a series of dependent devices. Kobza and Jacobson (1997) define a system alarm in one of two possible ways: at least one device alarm signals a system alarm, or all device alarms signals a system alarm. Their results indicate that multi-device systems can be more effective than single-device systems, taking into account the probability of errors by each sub-system. CRKP generalizes this framework by considering systems alarms to be defined more generally as a k-of-n reliability model. In CRKP, a system alarm is defined by the number of devices that yield an alarm response and by classification status (i.e., high-risk or low-risk).

6.3 Screening Framework

In this section, terminology and parameters are introduced for the Container Reliability Knapsack Problem (CRKP). In CRKP, all cargo containers first undergo *prescreening* to classify each cargo container as high-risk or low-risk. Cargo containers enter a security station to undergo *primary screening*. It is assumed that each container is on a truck trailer, although CRKP can be interpreted more generally to screen any types of objects using dependent screening devices. When a cargo container enters a security station, it is driven by several *sensors* that surround the truck. These sensors are radiation detectors such as Radiation Portal Monitors (RPMs), which screen each cargo container for radiation that is emitted by nuclear material such as plutonium and highly enriched uranium (HEU). Detecting nuclear material is a concern because it is a necessary ingredient in the assembly of nuclear bombs. Each sensor yields an alarm or clear response, based on how the sensor operates and the characteristics of the cargo container. Each truck trailer drives a cargo container through the security station sequentially, and after each cargo container is screened, the total number of sensor alarms is known (between zero and *n*), and based on this total number of sensor alarms, a system response is given. The system response has one of two outcomes, either a system alarm is given or the container is cleared. If the cargo container is cleared, it exits the security station and continues along its path to its destination. The cargo containers that yield a system alarm undergo *secondary screening*. All cargo containers undergo primary screening and CRKP is used to determine the subset of these cargo containers that undergo secondary screening. Note that it has been observed that the costs associated with secondary screening dominate the costs associated with primary screening (Wein et al., 2007).

Each container is either a threat or a nonthreat. Ideally, the system yields a clear response for all of the nonthreat containers and yields an alarm response for all of the threat containers. The objective of CRKP is to determine which containers yield a system alarm, based on the total number of alarms given by the *n* sensors. The system response (either alarm or clear) is a function of the device outcomes and can be defined in one of several ways (Kobza and Jacobson 1996, 1997). Note that this framework is defined generally for any type of radiological and nuclear sensor, and it makes no assumptions about how the sensors work together. Therefore, this framework can be used for a broad range of security screening operations.

The parameters for CRKP are classified into two groups: (1) probability parameters and (2) cost and screening parameters.

(1) Probability parameters

- P_{HR} = the probability that a cargo container is classified as high-risk,
- P_{LR} = the probability that a cargo container is classified as low-risk,
- P_T (P_{NT}) = a cargo container is a threat and contains nuclear material (not a threat),
- P_{kA} = the probability that a cargo container yields *k* alarms (of the *n* sensors), $k = 0, 1,\ldots, n$,
- $P_{TA} =1 - P_{FC}$ = the probability that a threat container yields a true alarm (false clear) at a single sensor,
- $P_{FA} =1 - P_{TC}$ = the probability that a non-threat container yields a false alarm (true clear) at a single sensor,

The screening process yields one of four possible outcomes: a true alarm, false clear, false alarm, or true clear. The probability of these outcomes occurring depends on how the sensors are operated, as well as the size, type, location, and shielding of the source for threat containers. If each sensor operates differently, then the single sensor true alarm and false alarm probabilities for sensor *i* are P_{TA}^{i} andP_{FA}^{i}, $i = 1, 2, \ldots, n$. Each cargo container is classified as high-risk or low-risk, based on a prescreening system such as ATS. The characteristics that determine whether a container is classified as high-risk is classified. The probability that a container is classified as high-risk is based on the proportion of containers passing through a security station that are classified as high-risk, once a large number of cargo containers has been evaluated. The probability that a cargo container is a threat is a random variable that is assessed by personnel within the Department of Homeland Security (DHS) based on the perceived threat level. This value is considered highly sensitive and may change based on changes in national or international situations, intelligence information, or the risk level of the Homeland Security Advisory System. The probability that a cargo container yields *k* (of *n*) alarms depends on how the sensors operate, and it is assumed to only depend on whether a container is a threat or non-threat.

(2) Cost and screening parameters

- N = number of cargo containers to be screened in the security station,
- B = total secondary screening budget,
- SS = a threat is selected for secondary screening,
- C_{SS} = cost to perform secondary screening on a container,
- β = ratio of high-risk containers that are threats to low-risk containers that are

threats, where $\beta = P_{T\backslash HR}/P_{T\backslash LR}$.

The total number of containers is a deterministic value that represents the number of cargo containers that pass through a given station in a year, or another period of time. The event that a threat is selected for secondary screening is based on the response of the *n* sensors and may be deterministic or random. The budget for secondary screening is a deterministic value based on available resources. The cost to perform secondary screening is a deterministic value based on information collected and analyzed by DHS and CBP. It is in part based on salaries paid to the employees hired to perform secondary screening. It is assumed that the cost to resolve an alarm with secondary screening is the same for threat (true alarms) and nonthreats (false alarms). Note that this budget reflects only the cost of secondary screening, and hence, the additional costs that are incurred by a true alarm are not assessed against the budget.

6.4 Risk and Reliability Model

This section describes the risk and reliability models used by CRKP. A prescreening system such as ATS classifies each container as either high-risk or low-risk, which varies according to the container characteristics. The *risk model* captures the ability of the prescreening system to correctly identify threat containers as high-risk. Ideally, all threat containers are classified as high-risk. The probability that a threat container is classified as low-risk is given by $P_{\mathrm{HR|T}}$. Given that $\beta = P_{\mathrm{T|HR}} = P_{\mathrm{T|LR}}$ and $P_{\mathrm{HR|T}} + P_{\mathrm{LR|T}} = 1$ and using Bayes Rule,

Equation 3

$$P_{HR|T} = \frac{\beta P_{HR}}{1 - P_{HR} + \beta P_{HR}},$$

with $P_{\mathrm{LR|T}} = 1 - P_{\mathrm{HR|T}}$. Likewise,

Equation 4

$$P_{HR|NT} = \frac{P_{HR} - P_{HR|T}P_T}{1 - P_T},$$

with $P_{\mathrm{LR|NT}} = 1 - P_{\mathrm{HR|NT}}$ and $P_{\mathrm{LR|T}} = 1 - P_{\mathrm{HR|T}}$.

Note that computing the conditional probability that there are *k* alarms given that a container is a threat or non-threat is not trivial if there is dependence between the sensors, which is likely to hold in practice. Finding these conditional probabilities can be accomplished by computing the reliability of a *k*-out-of-*n* system, in which the system yields an alarm response (i.e., the container is selected for secondary screening) if at least *k* sensors yield an alarm.

For the *reliability model*, define the following parameters. The state of the system is defined by the vector Y = ($Y_1, Y_2, \ldots, Y_n$), where $Y_i = 1$ if sensor *i* yields an alarm and 0 otherwise.

- $R_{(k,n)}$ = reliability of the *k*-out-of-*n* system (i.e., a container yields *k* or more alarms),
- $U(s) = P\{\prod_{i \epsilon s} Yi = 0\}$ = joint unreliability of the components of a subset *s* of the *n* sensors ($s \subseteq \{1, 2, \ldots, n\}$),
- $S(r)$ = family of *r*-subsets of $\{1, 2, \ldots, n\}$,
- C_k^n = binomial coefficient.

The reliability of the system is given by

Equation 5

$$R_{(k,n)} = 1 - \sum_{i=0}^{k-1} (-1)^i C_i^{n-k+i} \, U_{(n-k+i+1)},$$

where $U(r) = \sum_{s \in S(r)} U(s)$ (Koucky 2003). Then, the probability that there are exactly k alarms P_{kA} is given by

Equation 6

$$P_{kA} = R_{(k,n)} - R_{(k+1,n)}, k = 0, 1, \ldots, n-1,$$

with $P_{nA} = 1 - \sum_{k=1}^{n} P(kA)$.

Note that the number of alarms can be computed separately for threat and nonthreat containers, yielding $P_{kA|T}$ and $P_{kA|NT}$ *0*. Computing these probabilities may be simple if sensors are independent. Note that the number of alarms for threat containers depends on the source (i.e., the type of nuclear material), the amount of nuclear material, the level of shielding, and its placement within the container. However, it is assumed that the probability that a threat container yields a k alarms is the same for all threat scenarios, k = 0, 1, …, n. Although this is not likely to hold in practice, this assumption is reasonable, since the system can be defined to detect a particular threat scenario. For example, if a nuclear source is stolen, a particular threat scenario may be based on this stolen nuclear source. Therefore, the conditional probability of k alarms for threat containers $P_{kA|T}$ is assumed to be the same for each threat container, k = 0, 1, …, n.

6.5 The Container Reliability Knapsack Problem

This section introduces CRKP. The objective of CRKP is to determine which high-risk and low-risk containers yield a system alarm (and undergo secondary screening) in order to maximize the expected number of detected threats, given the number of alarms from the n sensors.

Variables:

- x_{HR}^{k} = fraction of high-risk containers with k-of-n alarms to undergo secondary screening,
- $x_{LR}^{k}\,LR$ = fraction of low-risk containers with k-of-n alarms to undergo secondary screening,

In CRKP, it is assumed that each container is screened independently of the other containers. It is also assumed that the sensors work the same regardless of whether a container is classified as high-risk and low-risk. Rather, sensor operation depends only on whether a container is a threat. After each container goes past the sensors, the number of alarms is known, and a decision is made about whether secondary screening is used to screen each the container. The objective is to maximize the total number of threats selected for secondary screening subject to a screening budget. Note that $x_{HR}^{k} = P\{SS|T\bigcap kA\bigcap HR\}$ and $x_{LR}^{k} = P\{SS|T \bigcap kA\bigcap LR\}$. Although selecting a threat container for secondary screening does not guarantee that it is detected, procedures for secondary screening, such as physically opening and unloading a cargo container and using radiation isotope identification devices, have a high probability of detecting nuclear material. Cargo containers that are not selected for secondary screening are cleared, and hence, there is no chance of interdicting the nuclear material. The objective of CRKP is to move the expected number threat containers selected for secondary screening.

max E[Number of threats selected for secondary screening]

$$= NP\{\text{A threat container is selected for secondary screening}\} = \mathrm{NP}_{\mathrm{SS\cap T}}$$

$$= N\sum_{k=0}^{n} \mathrm{P}_{\mathrm{SS\cap T\cap kA}}$$

$$= N\sum_{k=0}^{n} \mathrm{P}_{\mathrm{SS\cap T\cap kA\cap HR}} + \mathrm{P}_{\mathrm{SS\cap T\cap kA\cap LR}}$$

$$= N\sum_{k=0}^{n} (\mathrm{P}_{\mathrm{kA|T\cap HR}}\ \mathrm{P}_{\mathrm{HR|T}}\mathrm{P}_{\mathrm{T}}\mathrm{P}_{\mathrm{SS|T\cap kA\cap HR}} + \mathrm{P}_{\mathrm{kA|T\cap HR}}\ \mathrm{P}_{\mathrm{LR|T}}\mathrm{P}_{\mathrm{T}}\mathrm{P}_{\mathrm{SS|T\cap kA\cap LR}})$$

$$= N\mathrm{P}_{\mathrm{T}}\sum_{k=0}^{n} \mathrm{P}_{\mathrm{kA|T}}(\mathrm{P}_{\mathrm{HR|T}}x_{\mathrm{HR}}^{k} +\ \mathrm{P}_{\mathrm{LR|T}}x_{\mathrm{HR}}^{k}$$

There is a single budget constraint in CRKP that ensures that the number of containers that undergo secondary screening is less than *B/C_{SS}*.

E[Number of threats selected for secondary screening] $\leq$ B/C_{SS}

$$N\sum_{k=0}^{n} (\mathrm{P}_{\mathrm{SS|kA\cap T\cap HR}}\ \mathrm{P}_{kA|T\cap HR}P_{HR|T}\mathrm{P}_{T} +\ \mathrm{P}_{\mathrm{SS|kA\cap NT\cap HR}}\mathrm{P}_{kA|NT\cap HR}\mathrm{P}_{HR|NT}\mathrm{P}_{NT}$$

$$+\ \mathrm{P}_{\mathrm{SS|kA\cap T\cap LR}}\mathrm{P}_{kA|T\cap LR}P_{LR|T}\mathrm{P}_{T} +\ \mathrm{P}_{\mathrm{SS|kA\cap NT\cap LR}}\mathrm{P}_{kA|NT\cap LR}\mathrm{P}_{LR|NT}\mathrm{P}_{NT})\ \leq\ B/C_{SS}$$

$$N\sum_{k=0}^{n} ((\mathrm{P}_{\mathrm{kA|T}}\ \mathrm{P}_{\mathrm{T}}\mathrm{P}_{\mathrm{HR|T}} +\ \mathrm{P}_{\mathrm{kA|NT}}\mathrm{P}_{\mathrm{NT}}\mathrm{P}_{\mathrm{HR|NT}})\ x_{\mathrm{HR}}^{k} +\ (\mathrm{P}_{\mathrm{kA|T}}\mathrm{P}_{\mathrm{T}}\mathrm{P}_{\mathrm{LR|T}} +\ \mathrm{P}_{\mathrm{kA|NT}}\mathrm{P}_{\mathrm{NT}}\mathrm{P}_{\mathrm{LR|NT}})\ x_{\mathrm{LR}}^{k})$$

$$\leq\ B/C_{SS}$$

CRKP is formulated as a linear programming model, using the objective function value and budget constraint. Note that the objective function value is the expected number of threat containers that are selected for secondary screening.

$$\max\ \ NP_{T}\sum_{k=0}^{n} \mathrm{P}_{\mathrm{kA|T}}\left(\mathrm{P}_{\mathrm{HR|NT}}x_{\mathrm{HR}}^{k} + \mathrm{P}_{\mathrm{LR|NT}}x_{\mathrm{HR}}^{k}\right)$$

$$\text{subject to } \; N\sum_{k=0}^{n}((\mathrm{P_{kA|T}\,P_T P_{HR|T}} + \mathrm{P_{kA|NT}P_{NT}P_{HR|NT}})\,x_{\mathrm{HR}}^{k} + (\mathrm{P_{kA|T}P_T P_{LR|T}}$$

$$+ \mathrm{P_{kA|NT}P_{NT}P_{LR|NT}})\,x_{\mathrm{LR}}^{k}) \;\le\; B/C_{SS}$$

$$0 \;\le x_{\mathrm{HR}}^{k} \le 1, k = 0, 1, \dots, n$$

$$0 \;\le x_{\mathrm{LR}}^{k} \le 1, k = 0, 1, \dots, n.$$

Note that $P_{kA|T}$ and $P_{kA|NT}$ can be computed using the reliability Equation 6. To compute $P_{kA|T}$, note that the joint unreliability of a subset of sensors ($U(s)$) reflects the scenario when all sensors yield a false negative response. To compute $P_{kA|NT}$, note that the joint unreliability of a subset of sensors ($U(s)$) reflects the scenario when all sensors yield a true negative response. In the case when each sensor operates independently and identically with the probability of a single sensor true alarm P_{TA} and the probability of a single sensor false alarm P_{FA}, then$P_{kA|T} \;=\; C_k^n\, P_{TA}^k(1 - P_{TA})^{n-k}$ and $P_{kA|NT} \;=\; C_k^n\, P_{FA}^k(1 - P_{FA})^{n-k}$using the Binomial distribution with parameters n and P_{TA} for threat containers and parameters n and P_{FA} for non-threat containers.

6.6 Structural Properties

This section summarizes the structural properties of CRKP. CRKP is identical to the linear programming relaxation to the 0-1 Knapsack Problem (KP). In KP, there are m items with a reward r_i and weight w_i, i = 1, 2, …, m, and a knapsack capacity c. The linear programming relaxation to KP can be solved in O(m) time. The items are sorted in decreasing order of the ratio of the item reward to weight (i.e., r_1=w_1 ¸ r_2=w_2 ¸ … ¸ r_m=w_m), which is defined as the *optimal* *knapsack sequence*. Starting with the first item, items are greedily inserted into the knapsack in order until there is no remaining capacity in the knapsack. Therefore, the variables are all one or zero for all items except the critical item *s* (where *s* = arg min$_j\left\{\sum_{i=1}^{j} w_i > c\right\}$). KP corresponds to the reliability knapsack model with *m* = 2(*n* + 1), capacity $c = B/C_{SS}$, and rewards equal to the expected number of detected threats of high-risk and low-risk containers that yield *k* alarms that undergo secondary screening, and weight equal to the expected number of high-risk and low-risk containers that yield *k* alarms, *k* = 1, 2, …, *n*.

In CRKP, define the rewards for high-risk and low-risk containers as

$$r_{HR}^{k} = NP_T P_{kA|T} P_{HR|T}, k = 0, 1, \dots, n,$$

$$r_{LR}^{k} = NP_T P_{kA|T} P_{LR|T}, k = 0, 1, \dots, n,$$

respectively. Likewise, define the weights for high-risk and low-risk containers as

$$w_{HR}^{k} = N(P_{kA|T} P_T P_{HR|T} + P_{kA|NT} P_{NT} P_{HR|NT}, k = 0, 1, \dots, n,$$

$$w_{LR}^{k} = N(P_{kA|T} P_T P_{LR|T} + P_{kA|NT} P_{NT} P_{LR|NT}, k = 0, 1, \dots, n,$$

respectively. Therefore, CRKP can be rewritten as

$$\max \sum_{k=0}^{n} \left(r_{HR}^{k} x_{\mathrm{HR}}^{k} + r_{LR}^{k} x_{\mathrm{LR}}^{k} \right)$$

$$\text{subject to} \quad \sum_{k=0}^{n} \left(w_{HR}^{k} x_{\mathrm{HR}}^{k} + w_{LR}^{k} x_{\mathrm{LR}}^{k} \right) \le B/C_{SS}$$

$$0 \le x_{\mathrm{HR}}^{k} \le 1, k = 0, 1, \dots, n$$

$$0 \le x_{\mathrm{LR}}^{k} \le 1, k = 0, 1, \dots, n.$$

The screening scenario captured by CRKP can be viewed as a Bayesian probability model, with the prescreening risk classification defining the prior probabilities, and the number of alarms defining the posterior probabilities. The prior probabilities that high-risk and low-risk cargo containers are a threat are computed using the risk Equation 3and Equation 4 and are given by

$$P_{T|HR} = \frac{\beta P_T}{1 - P_{HR} + \beta P_{HR}},$$

$$P_{T|LR} = P_{T|HR}/\beta = \frac{P_T}{1 - P_{HR} + \beta P_{HR}},$$

respectively, and can be computed using the risk Equation 3.

The posterior probabilities are the conditional probabilities that a cargo container is a threat given that it is high-risk (low-risk) and yields *k* alarms, $P_{T|kA\cap HR}$ ($P_{T|kA\cap LR}$).

Theorem 1 defines the posterior probabilities.

Theorem 1 *The posterior probabilities PTjkA\HR and PTjkA\LR are defined as the ratio of the CRKP reward to the CRKP weights,* r_{HR}^{k}/w_{HR}^{k} and r_{LR}^{k}/w_{LR}^{k}, k = 0, 1, …, *n*.

Proof. First consider high-risk cargo containers. The posterior probability that a high-risk cargo container yielding *k* alarms is a threat is

$$P_{T|kA\cap HR} = \frac{P_{T\cap kA\cap HR}}{P_{kA\cap HR}} = \frac{P_{T\cap kA\cap HR}}{P_{T\cap kA\cap HR} + P_{NT\cap kA\cap HR}} = \frac{r_{HR}^{k}/N}{w_{HR}^{k}/N}$$

The posterior probabilities for low-risk cargo containers are computed in a similar manner. Lemma 1 and Corollaries 1 and 2 quantify the relationships between the CRKP rewards.

Lemma 1 *The objective coefficients* $r_{HR}^{k} > r_{HR}^{k-1}$*only if* $P_{kA|T} > P_{(k-1)A|T}$, *and* $r_{LR}^{k} > r_{LR}^{k-1}$*only if* $P_{kA|T} > P_{(k-1)A|T}$.

Proof. Follows from the objective function.

Corollary 1 *When sensors alarms are independently and identically distributed with the probability of a true alarm* P_{TA}, *then* $P_{kA|T} > P_{(k-1)A|T}$ *only if* $P_{TA} > \frac{k}{n+1}$, $k = 1, 2, \ldots, n$.

Proof. The number of alarms can be modeled as a Binomial random variable with *n* trials and probability of success P_{TA}. Then

$$P_{kA|T} = \frac{n!}{k!\,(n-k)!}P_{TA}^{k}(1- P_{TA})^{n-k} > \frac{n!}{(k-1)!\,(n-k+1)!}P_{TA}^{k-1}(1- P_{TA})^{n-k+1}$$

$$= P_{(k-1)A|T}$$

and rearranging yields

$$P_{TA} > \frac{k}{n+1}$$

Corollary 2 *When sensors alarms are independently and identically distributed with the probability of a true alarm* P_{TA}*, then* $P_{kA|T} > P_{(k-1)A|T}$ *for all k* = 1, 2, …, *n only if* $P_{TA} > \frac{n}{n+1}$.

Proof. Follows from Corollary 1.

For practical reasons, it is desirable for CRKP to identify containers for secondary screening that yield more alarms. The following theorem indicates the conditions under which a high-risk (low-risk) container yielding more alarms makes it more likely to be selected for secondary screening. Note that among only high-risk (low-risk) containers, the order that items are put into the knapsack (i.e., the order in which containers are selected for secondary screening) depends only on how the sensors work together and not on prescreening intelligence, the underlying probability of a threat, or the proportion of containers classified as high-risk.

Theorem 2 *High-risk (low-risk) containers that yield k alarms occur before high-risk (low-risk) containers that yield k* - 1 *alarms in the knapsack sequence,*

$$\frac{r_{HR}^{k}}{w_{HR}^{k}} > \frac{r_{HR}^{k-1}}{w_{HR}^{k-1}}\left(\frac{r_{LR}^{k}}{w_{LR}^{k}} > \frac{r_{LR}^{k-1}}{w_{LR}^{k-1}}\right)$$

only if

$$\frac{P_{kA|T}}{P_{(k-1)A|T}} > \frac{P_{kA|NT}}{P_{(k-1)A|NT}}.$$

Proof. First, consider the high-risk containers. By definition,

$$\frac{P_{kA|T}P_TP_{HR|T}}{P_{kA|T}P_TP_{HR|T} + P_{kA|NT}P_{NT}P_{HR|NT}} > \frac{P_{(k-1)A|T}P_TP_{HR|T}}{P_{(k-1)A|T}P_TP_{HR|T} + P_{(k-1)A|NT}P_{NT}P_{HR|NT}}.$$

Rearranging yields the desired result. The same approach can be taken for the low-risk containers.

Corollary 3 illustrates the particular case when each sensor operates independently and identically.

Corollary 3 *When sensors alarms are independently and identically distributed with the probability of a true alarm P_{TA}, then*

$$\frac{r_{HR}^k}{w_{HR}^k} > \frac{r_{HR}^{k-1}}{w_{HR}^{k-1}} \text{ and } \frac{r_{LR}^k}{w_{LR}^k} > \frac{r_{LR}^{k-1}}{w_{LR}^{k-1}}$$

only if $P_{TA} > P_{FA}$.

Proof. First, consider the high-risk containers. Using Theorem 2, then

$$\frac{P_{kA|T}}{P_{(k-1)A|T}} = \frac{C_k^n P_{TA}^k (1 - P_{TA}^{n-k})}{C_{k-1}^n P_{TA}^{k-1} (1 - P_{TA}^{n-k+1})} > \frac{C_k^n P_{FA}^k (1 - P_{FA}^{n-k})}{C_{k-1}^n P_{FA}^{k-1} (1 - P_{FA}^{n-k+1})} > \frac{P_{kA|NT}}{P_{(k-1)A|NT}}.$$

Rearranging yields

$$\frac{P_{TA}}{1 - P_{TA}} > \frac{P_{FA}}{1 - P_{FA}},$$

and simplifying yields $P_{TA} > P_{FA}$. The same approach can be taken for the low-risk containers.

The Lemma 2 indicates that the ratio of the rewards for high-risk to low-risk containers is a constant factor for each k, $k = 0, 1, \ldots, n$, that depends only on prescreening intelligence and the proportion of containers that are classified as high-risk.

Lemma 2 *The ratio of rewards for high-risk to low-risk containers is*

$$\frac{r_{HR}^{k}}{r_{LR}^{k}} = \frac{P_{HR|T}}{P_{LR|T}} = \frac{\beta P_{HR}}{1 - P_{HR}}$$

for $k = 0, 1, \ldots, n$.

Proof. Follows from the definition of the rewards, since

$$\frac{r_{HR}^{k}}{r_{LR}^{k}} = \frac{P_{HR|T}}{P_{LR|T}}.$$

6.7 Computational Example and Results

This section reports results for CRKP to assess the theoretical properties of CRKP and to understand the tradeoffs between prescreening intelligence (i.e. β), secondary screening costs, and the false alarm and false clear rates associated with each sensor. The results to CRKP not only indicate the likelihood of detecting nuclear material, they also indicate how to define a system alarm, based on a container's risk classification (i.e., high-risk or low-risk) and how many sensors yield an alarm.

The analysis considers two scenarios. The first scenario considers cargo containers on truck trailers that drive by a series of *n* sensors that are independent and operate identically. Therefore, the number of alarms for threat containers is modeled using a Binomial distribution with parameters *n* and P_{TA}, and the number of alarms for threat containers are modeled using a Binomial distribution with parameters *n* and P_{FA}. The second scenario considers a series of *n* sensors that have a degree of dependence between the sensors.

CRKP is analyzed for a single security station over a time horizon of one year. Table 22 contains the base case input parameters for CRKP, which remain constant unless otherwise specified. It is assumed that $N = 100{,}000$ containers enter the security station during the time horizon. The probability that a container is a threat is $1/N$, which was selected such that one threat is expected to pass through the security station. Five percent of all containers are assumed to be high-risk, which is consistent with what is reported in the public domain (Robinson et al., 2005; Strohm, 2006; Ramirez-Marquez, 2008; The Royal Society, 2008). The cost of secondary screening was set to CSS = $50 per container (Wein et al., 2007).

In the analysis, the objective function represents the expected number of threat containers that are selected for secondary screening (the number of true alarms). The expected number of threats in the system is $P_T N = 1$, and hence, 1.0 is an upper bound on the objective function value for the base case. Define the *detection probability* as the probability that a threat is selected for secondary screening. The detection probability is computed as objective function value divided by $P_T N$. CRKP is solved to determine the minimum budget needed to ensure a detection probability of 0.95 (Wein et al., 2007; Levi 2007).

The minimum cost to achieve a detection probability of 0.95 depends on the costs associated with secondary screening as well as the total number of cargo containers passing through the security station. The cost of secondary screening depends on many parameters, such as labor costs and offsite testing costs, and hence, reporting the proportion of containers selected for secondary screening was used as a proxy to report cost. Therefore, the cost to achieve a detection probability of 0.95 is rescaled by $C_{SS}N$ to reflect the proportion of containers that are selected for secondary screening. Let Q_{SS}[DP] denote the proportion of cargo containers selected for secondary screening in order to achieve a specified detection probability (DP), where DP= 0.95 for the scenarios considered.

Note that CRKP is an instance of the linear programming relaxation to KP, and hence, there is at most one fractional variable in an optimal solution. A fractional variable is interpreted to represent the fraction of containers yielding the particular number of alarms that is randomly selected for secondary screening. For example, $x_{LR}^4 = 0.2$ is interpreted to mean that a low-risk container yielding four alarms has a probability of 0.2 of being selected for secondary screening. All other variables are zero (meaning that no containers are selected for secondary screening) and one (meaning that all containers are selected for secondary screening).

The value of the prescreening multiplier β determines the probability that a threat container is classified as high-risk for a given proportion of containers classified as high-risk *PHR*. McLay et al. (2008) report that $\beta = 10$ is realistic, and that $\beta = 100$ is an upper bound for an improved prescreening system. Since β is a function of P_{HR}, it is difficult to compare scenarios with a given β across different values of P_{HR}. As P_{HR} increases for a fixed value of $\beta > 1$, the ratio of the number of threat containers classified as high-risk to the number of threat containers classified as low-risk is constant. However, $P_{HR|T}$ increases as a result of more containers being classified as high-risk, not as a result of an improvement in prescreening intelligence. To avoid this problem, scenarios with a fixed value of $P_{HR} = 0.05$ are compared across different values of β. In this case, $P_{HR|T}$ increases as β increases as a result of improvements in prescreening intelligence. The three values of the prescreening multiplier considered are $\beta = 1, 10, 100$. Note that $\beta = 1$ corresponds to the random screening case. When $\beta = 1$, $P_{T|HR} = P_{T|LR}$, so screening is random and independent of the risk classification.

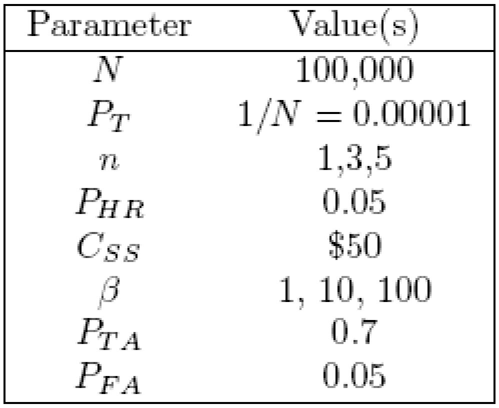
The parameters P_{TA} and P_{FA} represent the probability of a single sensor true alarm and false alarm, respectively. The base case true alarm and false alarm values used in the analysis are set to 0.7 and 0.05, respectively. The false alarm probability is set to 0.05 to be consistent with high false alarm rates experienced at our nation's ports (Slaughter et al., 2003). Publicity reported estimates for the true alarm probability have widely varied (Cochran and McKinzie, 2008, Levi 2007), and hence, the true alarm probability is set to 0.7. Note that Corollary 3 indicates that the true alarm probability should be greater than the false alarm probability when sensors operate identically and independently, and this is consistent with the parameters used in this analysis.

6.8 Case Studies

6.8.1 Case 1: Identical and Independent Sensors

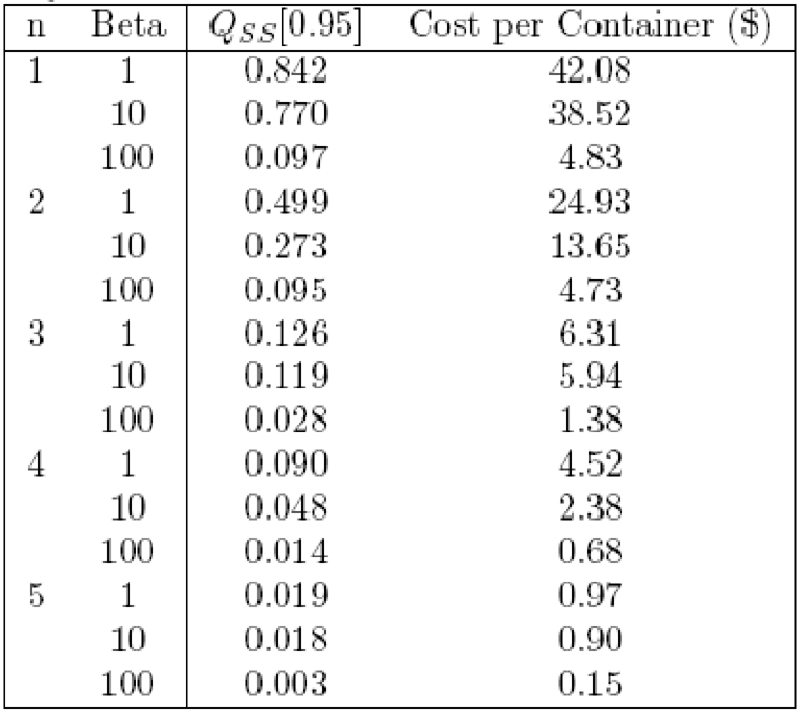
In order to assess CRKP, the values of P_{TA}, P_{FA}, and β are varied for the case when the sensors operate independently and identically. Although there is dependency between sensors currently used to screen containers for nuclear material, Case 1 assumes independence to shed light on how to optimally screen cargo containers using multiple sensors under ideal conditions using next-generation screening technologies with fewer dependencies.

Table 22: Base case parameter values



Parameter	Value(s)
N	100,000
P_T	$1/N = 0.00001$
n	1,3,5
P_{HR}	0.05
C_{SS}	\$50
β	1, 10, 100
P_{TA}	0.7
P_{FA}	0.05

Table 23: Base case costs and minimum proportion of cargo containers selected for secondary screening for a detection probability of 0.95



n	Beta	$Q_{SS}[0.95]$	Cost per Container ($)
1	1	0.842	42.08
	10	0.770	38.52
	100	0.097	4.83
2	1	0.499	24.93
	10	0.273	13.65
	100	0.095	4.73
3	1	0.126	6.31
	10	0.119	5.94
	100	0.028	1.38
4	1	0.090	4.52
	10	0.048	2.38
	100	0.014	0.68
5	1	0.019	0.97
	10	0.018	0.90
	100	0.003	0.15

Each cargo container is assumed to be on a truck trailer that is driven by a series of $n = 1, 3, 5$ sensors. Each sensor operates independently and identically, with the probabilities of true and false alarms being 0.7 and 0.05, respectively. Note that under these conditions, the conditions under Theorem and Corollary 3 are satisfied, and hence, containers that yield more alarms are selected for secondary screening before containers that yield fewer alarms. Table 23 shows the proportion of cargo containers selected for secondary screening in order to achieve a detection probability of 0.95, $Q_{SS}[0{:}95]$, as well as the corresponding cost.

Figure 1 shows $Q_{SS}[0{:}95]$ as β varies from 1 to 100 for P_{TA} values of 0.7 (the base case) and 0.1 in order to illustrate the effect of having inaccurate sensors, since it has been reported that RPMs do not consistently identify nuclear material (Levi 2007, Cochran and McKinzie, 2008). Figure

27 suggests that having accurate sensors is more important for keeping secondary screening costs to a minimum than prescreening intelligence or having many sensors. A single sensor with P_{TA} = 0.7 using random screening (i.e., β = 1) has lower secondary screening costs compared to three sets of scenarios with P_{TA} = 0.1 (n = 1 and $\beta \leq 41$, n = 3 and $\beta \leq 35$, n = 5 and $\beta \leq 29$), which suggests that sensor inaccuracies can be offset by better prescreening intelligence.

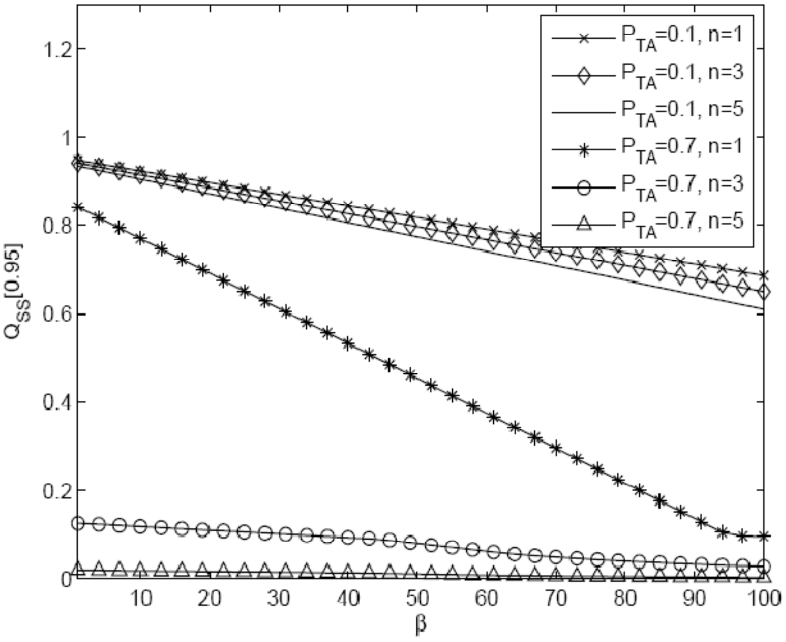
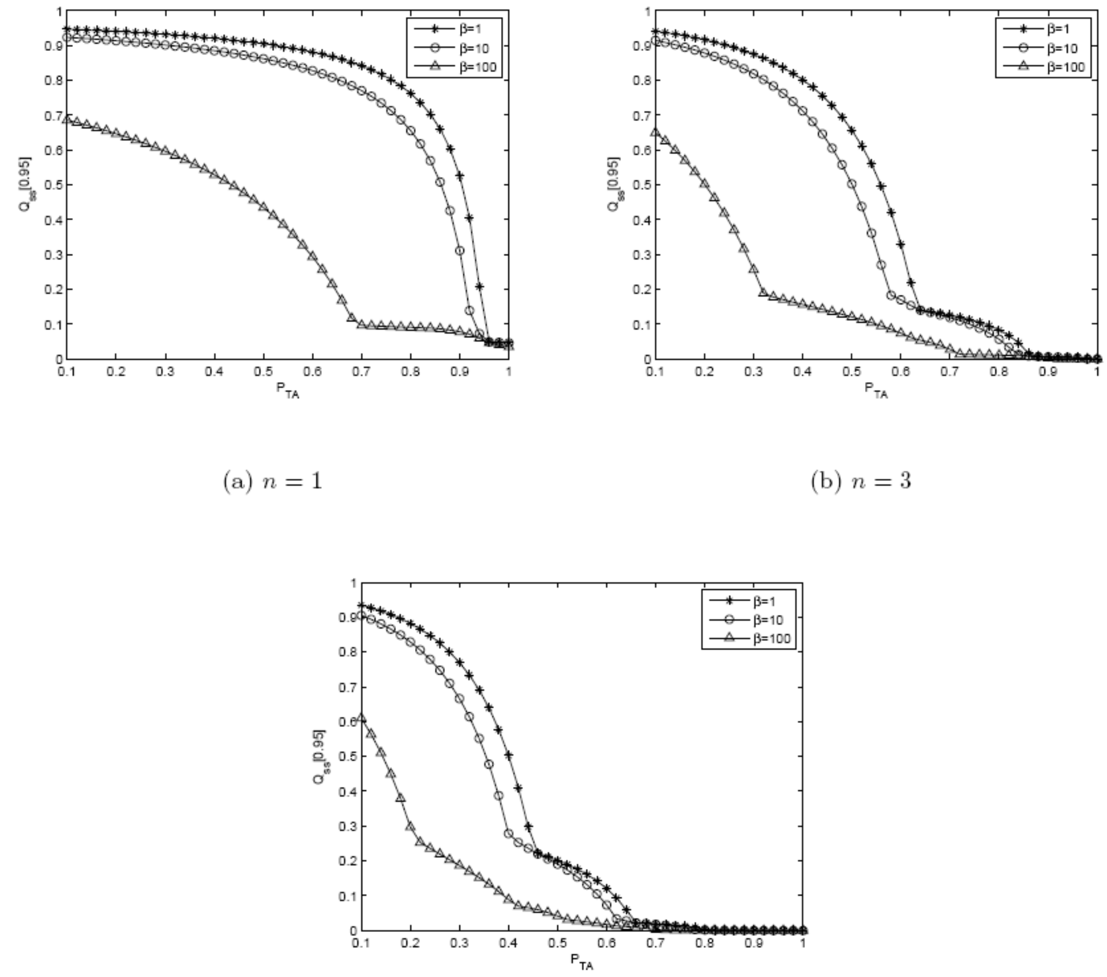


Figure 27: Minimum proportion of cargo containers selected for secondary screening for a detection probability of 0.95 as a function of Beta

To better understand secondary screening costs, sensitivity analysis was performed for P_{TA}, P_{FA}, and β. Figure 28 shows $Q_{SS}[0.95]$ as a function of the probability of a single sensor true alarm. Figure 28 (a) illustrates the case with n = 1, Figure 28 (b) illustrates the case with n = 3, and Figure 28 (c) illustrates the case with n = 5. As the probability of a single sensor true alarm approaches 1.0, the proportion of containers that require secondary screening to maintain a detection probability of 0.95 decreases drastically, which suggests that highly effective sensors can counteract less effective prescreening. However, for more moderate values of P_{TA}, prescreening intelligence is necessary to reduce secondary screening costs.

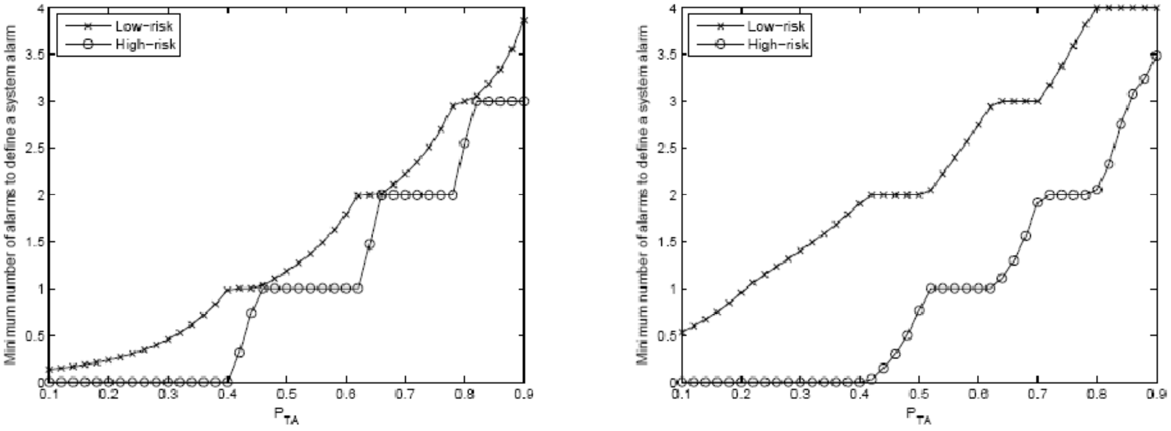


(a) $n = 1$

(b) $n = 3$

Figure 28: Proportion of cargo containers selected for secondary screening for a detection probability of 0.95 as a function of the probability of a single sensor true alarm

Figure 29 shows the system alarm threshold as a function of P_{TA} for the case with n = 5 sensors, with Figure 29 (a) showing the sensor alarms for the β = 10 case and Figure 29 (b) showing the sensor alarms for the β = 100 case. In Figure 29, if the number of observed alarms is greater than the system alarm threshold, then the cargo container is selected for secondary screening. If the number of observed alarms is less or equal to than the system alarm threshold, then the cargo container is cleared. Note that in all instances, high-risk containers require fewer sensor alarms to be selected for secondary screening, and as prescreening intelligence improves, the difference between low-risk and high-risk containers is accentuated. As the probability of a single sensor true alarm increases, the screening process more accurately identifies threat containers, and hence, containers with fewer sensor alarms are less likely to be selected for secondary screening.



(a) $\beta = 10$

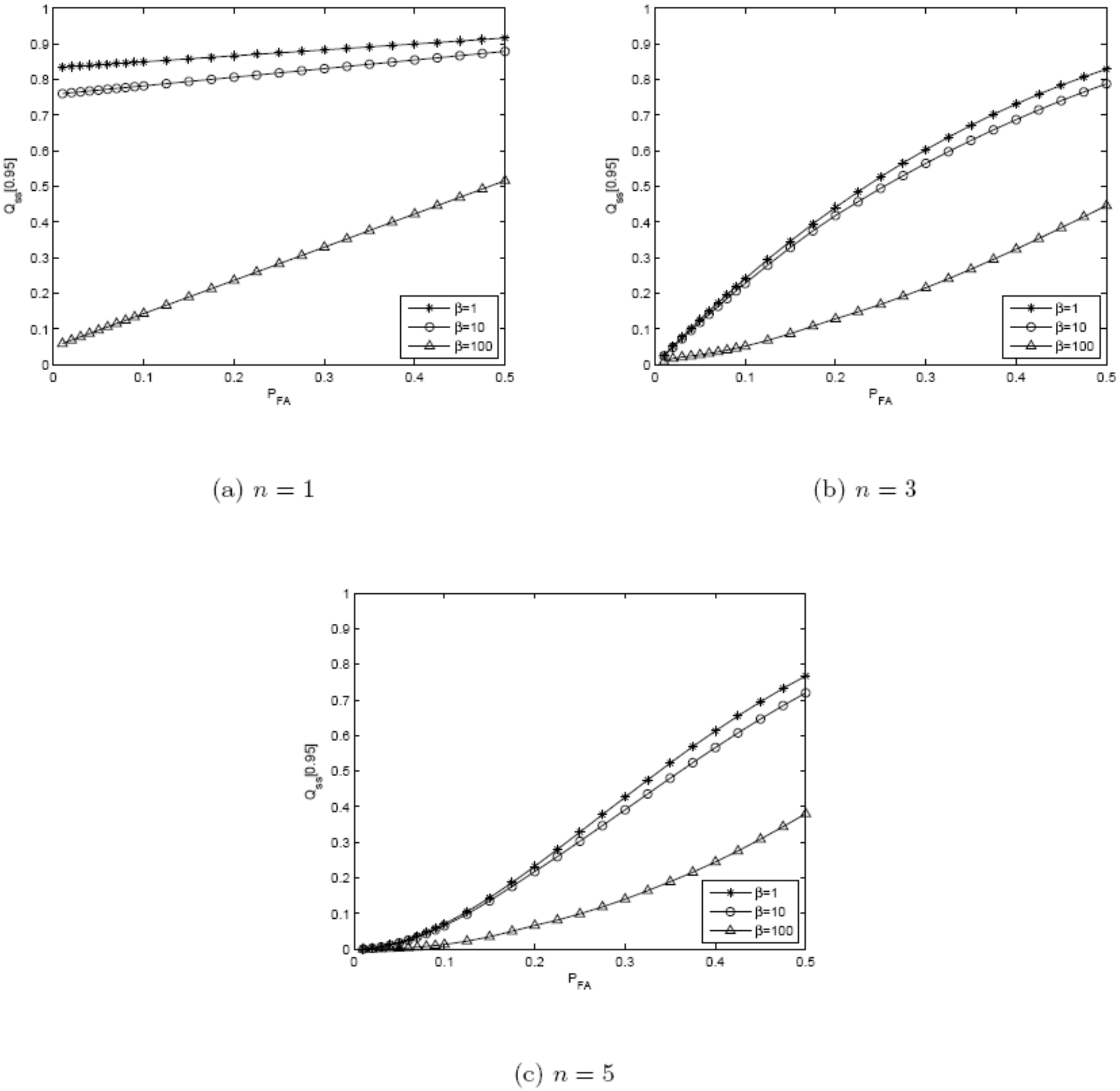
(b) $\beta = 100$

Figure 29: System alarms as a function of the probability of a single sensor true alarm for n = 5 scenarios

Note that in several cases (such as n = 3 and P_{TA} = 0.63 in Figure 28 (b), n = 5, P_{TA} = 0.45 in Figure 28 (c)), there is no difference between the β = 1 and β = 10 case, which indicates that efforts made to moderately improve prescreening intelligence over random screening may not have any impact on security. This observation is counter-intuitive. In the aviation security domain, the opposite conclusion has been drawn, namely that moderate increases in prescreening intelligence have large effects on security (McLay et al. 2008). In CRKP, this occurs when CRKP defines an identical system alarm for both high-risk and low-risk cargo containers (see

Figure 29 (a)), which suggests that how individual sensors operate (i.e., their true alarm and false alarm rates) should also be considered when designing screening systems.

Figure 30 shows $Q_{SS}[0.95]$ as a function of $P_{F}A$. As the probability of a single sensor false alarm increases, so does the proportion of containers that are selected for secondary screening. When $P_{FA} = 0.05$, $\beta = 1$, and $n = 5$, $Q_{SS}[0.95]$ is lower than the corresponding scenarios with $\beta = 100$ and $n = 1, 3$. This suggests that multiple sensors can counteract low prescreening intelligence. Improving β from 10 to 100 significantly reduces the proportion of containers that are selected for secondary screening, which suggests that effective prescreening counteracts sensors with high false alarm rates. Note that the proportion of containers requiring secondary screening when $P_{FA} = 0.5$ and $n = 5$ is smaller than the proportion of containers requiring secondary screening when $P_{FA} = 0.01$ and $n = 1$ for corresponding values of $\beta = 1, 10$. This suggests that using multiple sensors with high false alarm rates may be more effective than using a single sensor with a low false alarm rate.



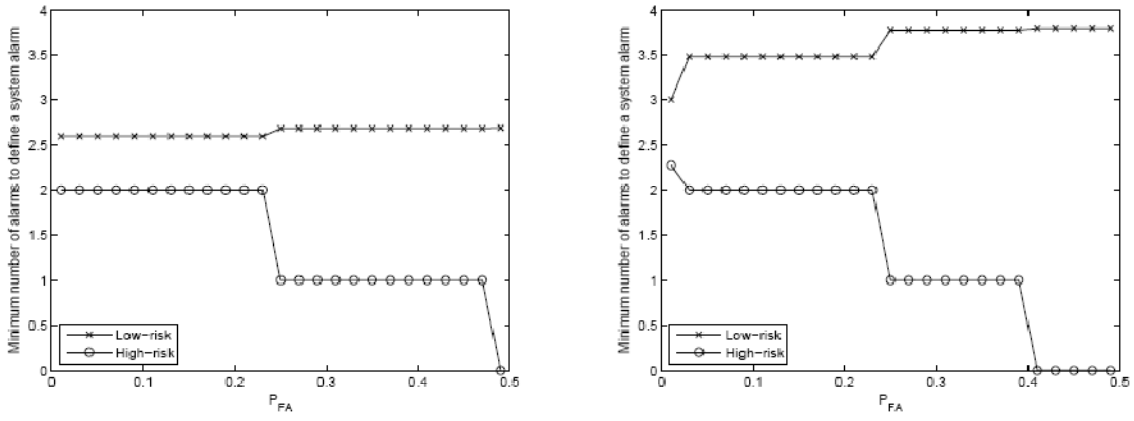
(a) $n = 1$

(b) $n = 3$

(c) $n = 5$

Figure 30: Proportion of cargo containers selected for secondary screening for a detection probability of 0.95 as a function of the probability of a single sensor false alarm

Figure 31 shows the system alarm threshold defined for the case with *n* = 5 sensors, with Figure 31 (a) showing the system alarm threshold for the *β* = 10 case and Figure 31 (b) showing the sensor alarm threshold for the *β* = 100 case. Note that in all instances, high-risk containers require fewer sensor alarms to be selected for secondary screening, and as prescreening intelligence improves, the difference between low-risk and high-risk containers is accentuated. As the probability of a single sensor false alarm increases, the screening process less accurately identifies non-threat containers. As a result, high-risk containers with fewer sensor alarms more likely to be selected for secondary screening whereas low-risk containers with fewer sensor alarms are less likely to be selected for secondary screening, heightening the disparity between low-risk and high-risk containers.



(a) $\beta = 10$

(b) $\beta = 100$

Figure 31: System alarms as a function of the probability of a single sensor false alarm for n = 5 scenarios

6.8.2 Case 2: Dependent Sensors

In practice, there is likely to be a high level of dependence between sensors for detecting nuclear material (Fetter et al., 1990; Levi, 2007). With highly dependent sensors, a sensor is highly likely to yield an alarm (clear) response if other sensors yield alarm (clear) responses.

In order to determine system performance when there are multiple, dependent sensors, the following criteria are used to specify the number of alarms. All sensors are assumed to work identically but not independently. The probability of observing an alarm at the second and subsequent sensors is assumed to be conditional on the response of the first sensor for threat and non-threat containers. Given the response of the first sensor, the remaining *n* - 1 sensors are assumed to operate independently and identically, given the level of dependence. Let *D* define the level of dependence between the first sensor and the remaining *n* - 1 sensors, $0 \leq D \leq 1$. Define A_j ($N\,A_j$) as the event that the *j*th sensor yields an alarm (clear) response. The true alarm and false alarm probabilities for the first sensor (j = 1) are P_{TA} and P_{FA}, respectively. If the first sensor yields an alarm response, then the true alarm and false alarm probabilities for the remaining *n* - 1 sensors are defined as

$$P_{A_j|A1\cap T} = P_{TA} + D(1 - P_{TA}), \qquad j = 2, 3, \dots, n,$$

$$P_{A_j|A1\cap NT} = P_{FA} + D(1 - P_{FA}), \qquad j = 2, 3, \dots, n,$$

respectively. In other words, given an alarm by the first sensor for a threat (non-threat) container, the probability that subsequent sensors yield an alarm response is linearly scaled between P_{TA} (P_{FA}) and one by *D*. If the first sensor yields a clear response, then the true alarm and false alarm probabilities for the remaining *n* - 1 sensors are defined as

$$P_{A_j|N\,A1\cap T} = (1 - D)P_{TA}, \qquad j = 2, 3, \dots, n,$$

$$P_{A_j|N\,A1\cap NT} = (1-D)P_{FA}, \qquad j = 2, 3, \dots, n,$$

respectively. In other words, given a clear response by the first sensor for a threat (non-threat) container, the probability that subsequent sensors yield an alarm response is linearly scaled between zero and P_{TA} (P_{FA}) by D. Note that the sensors operate independently and identically when $D = 0$ and the sensors yield identical responses when $D = 1$.

Figure 32 shows the proportion of cargo containers selected for secondary screening to achieve a detection probability of 0.95 with $n = 5$ sensors. Note that when $D = 0$, the proportion of cargo containers selected for secondary screening is identical to the case when sensors operate identically and independently. When $D = 1$, the $n = 5$ sensors yield identical outcomes, and hence, the proportion of cargo containers selected for secondary screening is identical to the case with one sensor. Therefore, when there is a high level of dependence between sensors, using additional sensors for screening cargo containers have few benefits as compared to using a single sensor. Moreover, the case when sensors operate independently and identically (Case 1) reflects the best-case scenario when each sensor adds the most information to the screening process and any level of dependence reduces the potential effectiveness of the sensors. Figure 32 also suggests that the problems with highly dependent sensors can be mitigated in part when β is large.

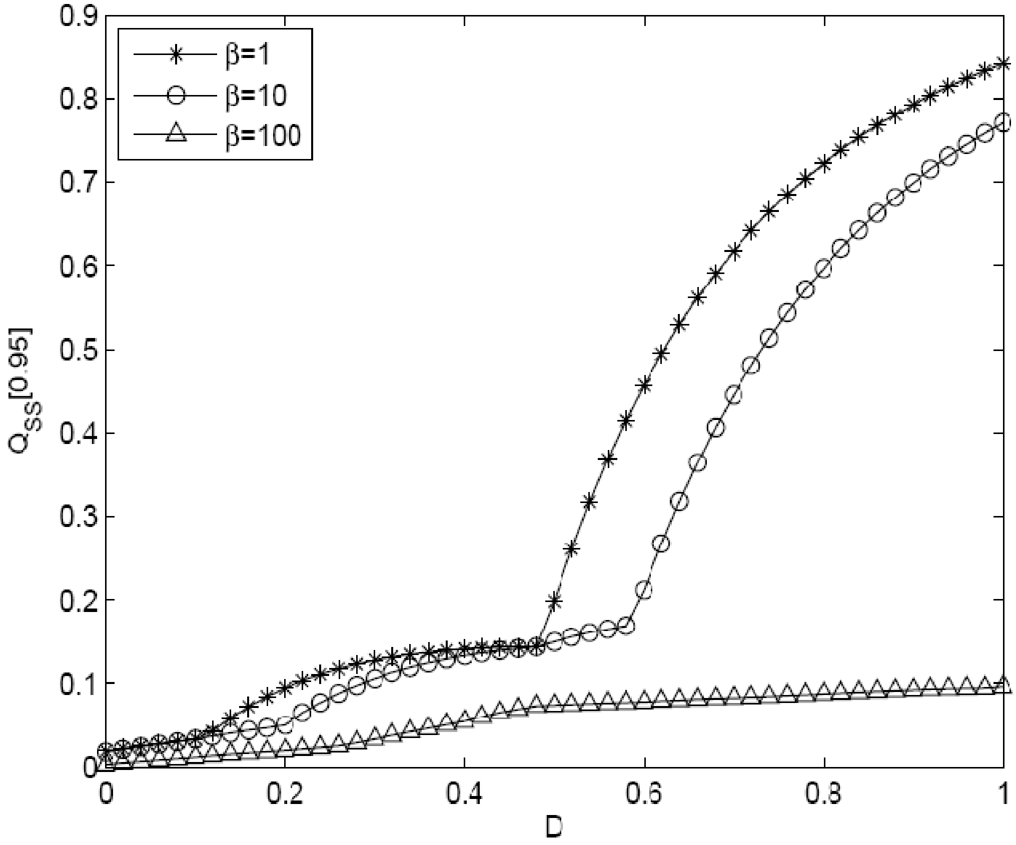


Figure 32: Minimum proportion of cargo containers selected for secondary screening for a detection probability of 0.95 as a function of the level of dependence D for n = 5

6.9 Conclusions

This chapter introduced CRKP, a linear programming model for screening cargo containers for nuclear material at security stations throughout the United States using knapsack problem, reliability, and Bayesian probability models. The approach determines how to define a system alarm and hence, designs and analyzes security system architectures. The analysis provides a risk-based framework for determining how to define a system alarm when screening cargo containers given limited screening resources. Analysis of the models suggests that prescreening intelligence is the most important factor for effective screening, particularly when sensors are highly dependent, and that sensors with high true alarm rates can mitigate some of the risk associated with low prescreening intelligence.

CRKP investigates the issue of how to define a system alarm given a set of screening devices, rather than depend on pre-specified notions of how a system alarm should be defined. CRKP can be used as a general framework to determine how to design next-generation security screening system as well as define a system alarm for any type of problem that relies on a series of screening devices or methods, risk assessments, and a limited secondary screening budget. Therefore, the scope of CRKP extends beyond homeland security and can be used to determine how to identify defective produce in a manufacturing assembly line, for example (Christer 1994).

There are several possible extensions to CRKP. One extension is to consider CRKP as one component is a larger access security system, with secondary screening as additional components in the system (Kobza and Jacobson 1997, Christer 1994).

A second extension to CRKP is to consider a second level of classification for each of the containers. CRKP assumes that each container is classified as high-risk or low-risk, which quantifies the likelihood of the container containing nuclear material. However, the vast majority of system alarms encountered by our nation's ports are due to NORM alarms (due to natural levels of radiation in the contents of the cargo containers), not nuclear materials (Huizenga, 2005). Prescreening can be used to identify which containers have high levels of naturally occurring radiation, and hence, each cargo container can be classified as NORM or non-NORM as well as high-risk or low-risk. Analyzing how the two levels of classification as well as their interaction may shed light on the tradeoffs between prescreening intelligence and the physical contents and characteristics of the containers.

A third extension to CRKP is to differentiate the type of threat, affecting the probability of a true alarm at a given sensor. The probability that a threat container yields an alarm response at a sensor depends on the type of the source, the size of the source, the amount of shielding, and the location of the nuclear material within the container (Fetter et al., 1990; Levi, 2007). This can be addressed by identifying a spectrum of threat scenarios as well as the likelihood of each scenario occurring. Work is in progress to address all of these extensions.

Thesis Conclusions

7.1 Value of work and Ending Remarks

Our country is still under attack by terrorists. The past terrorist attacks against the United States highlighted how fragile our nation's security system really is. As a direct result of the attacks on September 11, 2001, billions of dollars have been spent on improving aviation security in attempt to minimize the likelihood of another terrorist event. Although, the United States spent large capital on advancements in airport security measures, security breaches still happen. On Christmas day, 2009, a Nigerian man allegedly smuggled a sufficient amount of explosives to blow a hole in the side of the aircraft which was carrying 300 passengers. The attempt failed and all passengers and crew landed safety and the suspect was arrested. Al Qaeda has claimed responsibility for this botched terrorist attack (CNN, 2009).

The recent attempt on our country has again spotlighted the weaknesses of our security measures. Aviation security has improved dramatically since September 11, 2001, but there are still flaws that need to be fixed. However, little has been done when it comes to other gateways to our country. Our nation's ports are a vital component of our nation's security, yet the security efforts thus far have been disjoint and unorganized.

If terrorists can gather the materials needed to construct a nuclear bomb or dirty bomb while inside the United States, the consequences would be devastating. Preventing plutonium and highly enriched uranium (HEU) from illegally entering the United States is an area of vital concern, since either of these materials can be used to construct a mock nuclear weapon. Unfortunately, there are places in the world, such as the former Soviet Union, where these materials are not secure. Howard Baker, the former U.S. ambassador to Japan and the former Republican leader of the Senate, testified on Capitol Hill, "It really boggles my mind that there could be 40,000 nuclear weapons, or maybe 80,000 in the former Soviet Union, poorly controlled and poorly stored, and that the world is not in a near-state of hysteria about the danger" (Allison 2004).

Cargo containers are not only vulnerable for the transportation of nuclear materials, but also of the terrorist themselves. One such occasion was reported that a suspected Al Qaeda terrorist was found inside a container traveling to Canada, and he was carrying plans of airports, an aviation mechanic's certificate, and security passes (The Economist, 2002). The terrorists have obviously realized the security weaknesses of the world's ports. Improving port security operations is a critical component in preventing and interdicting illicit nuclear material entering the United States.

Confiscating nuclear material being smuggled into the United States on cargo containers is an issue of vital national interest, since it is a critical aspect of protecting the United States from nuclear attacks. Our economic well-being is intrinsically linked with the success and security of the international trade system. International trade accounts for more than thirty percent of the United States economy (Rooney, 2005). Ninety-five percent of international goods that enter the United States come through one of 361 ports, adding up to more than 11.4M containers every year (Fritelli, 2005; Rooney, 2005; US DOT, 2007). Port security has emerged as a critically important yet vulnerable component in the homeland security system.

This thesis introduces an intelligent adversary risk analysis model for determining whether to use new radiological screening technologies. The modeling—shown in Section 5.3—introduces a technique that provides a more realistic risk assessment of the true situation being modeled. Using this model the decision maker can construct more accurate judgments based on the true situation. This increase in accuracy could save lives with the decisions being made. The model can also help the decision maker understand the interdependencies of the model and visually see how his resource allocations affect the optimal decisions of the defender and the attacker.

This intelligent adversary risk analysis model is extremely sensitive to the expected cost of implementing the technology needed to develop a new type of detector. The nominal value estimated in this model is $8.77. The decision of adding a new detector would remain the same if the expected cost rose to $9.52. Once the expected cost rises from $9.52 to $9.53 the optimal decision is for the United States to remain at status quo and not to invest in the new technology. Obviously, with this extreme fluctuation in optimal decision, there should be special focus on estimating the expected cost accurately.

The model reports that the optimal decision is for the United States to invest in a new detector, and for the terrorists to choose agent cobalt-60, shown in Figure 18. As discussed previously this is mainly due to the prominence of false alarms and the high costs associated with screening all of these false alarms. With the new detector technology the false alarms decrease and the true alarm rate increases, which in turn provides a cost savings greater than the associated risk with the new detectors technical success. However, as shown by the sensitivity analysis, by varying some of the probabilities and costs in this model, we can manipulate the results from adding a new radiation detector to remaining at the status quo. We can also vary the results for the terrorist to choose uranium rather than cobalt-60. We believe that the marginal probabilities and costs that are in the basic model are in line with other papers and open literature. Of course, if the values could be reevaluated by the government and more accurate values were inserted into the model, the results would be more precise for real world use.

The two extensions shown in Section 5.4 are just a few of the potential variations that could be made to this model. By adding information, changing nodes, and/or changing the inputs we can see how the optimal decisions change. This model is extremely versatile and adaptable. Because of its easy manipulations, this model could be a valuable tool to the counterterrorism departments of the United States. The inputs and parameters could be edited in seconds and could provide an even more accurate assessment of the real world situation that it is designed to model. Again, the ability for it to be changed so easily makes it such a great decision making tool.

It should be clear that by taking aspects of both game theory and decision analysis and incorporating it into a comprehensive model we could have better insight and knowledge for making national security decisions. By simultaneously modeling the attacker and defenders objectives in one model, we would have a more complete perspective on the situation. This new understanding of the situation could perhaps lead us to the best allocation of our resources for defending our country, resulting in improved national security.

Even though almost nine years have passed in the catastrophic even of 9/11, we cannot forget that our country is still vulnerable to another terrorist attack. The attempted attack on Christmas day again highlighted the weaknesses and insufficient security measures we have for our nation and the safety of our people. With limited resources and availabilities it is crucial that we spend our security budget wisely and make well informed decisions. Through the use of decision analysis techniques, game theoretic approaches, combinatory measures, and other counterterrorism models, like our model we introduced in Chapter 5, we can aid our government in making better decisions that will ultimately protect our country and save lives.

References

ABC News. *Making a "Dirty Bomb" Sources of Radioactive Material*. (2005). Accessed on 11/28/2009, available at abcnews.go.com/Technology/LooseNukes/story?id=1077341&page=1

ABT Associates. *The Economic Impact of Nuclear Terrorist Attacks on Freight Transport System in an Age of Seaport Vulnerability*. Executive summary, (2003), p. 7, http://www.abtassociates.com/reports/ES-Economic_impact_of_nuclear_terrorist_attacks.pdf

Allison, G. (2004). *How to Stop Nuclear Terror*. The January/February 2004 issue of Foreign Affairs. Accessed on 2/08/2010, available at http://www.nytimes.com/cfr/international/20040101faessay_v83n1_allison.html

Allen, N. H. (2006). *The Container Security Initiative Costs, Implications and Relevance to Developing Countries.* Plublic Administration and Development, Pubic Admin. pp. 439-447.

Apostolakis, G. (1990). *The Concept of Probability in Safety Assessments of Technological Systems*. Science, Vol. 250.

Arms Control Association Fact Sheet: MANPADS at a Glance. Conventional Arms Issues Fact Sheet, (2007). Available at http://www.armscontrol.org/factsheets/manpads accessed on 10/12/2009

Atkinson, S. E., Sandler, T., & Tschirhart, J. T. (1987). *Terrorism in a bargaining framework*. Journal of Law and Economics, 30, (1), (pp. 1–21).

Bakir, N.O. (2008). *A decision tree model for evaluating countermeasures to secure cargo at United States southwestern ports of entry*. Decision Analysis 5(4) 2304-248.

Banks, D. L, Anderson, S. (2006). *Combining Game Theory and Risk Analysis in Counterterrorism: A Smallpox Example.* pp 9-22 in Wilson, A. G., Wilson, G. D., Olwell, D. H. *Statistical Methods in Counterterrorism: Game theory, modeling, syndromic survallance, and biometic authentication* (2006).

Barron, E. N. (1949). *Game Theory: an Introduction*. Wiley-Interscience. A John Wiley & Sons, Inc., Publication.

Bellany, I. (2007). Terrorism and Weapons of Mass Destruction: Responding to the Challenge. Edited by Ian Bellany. Available at books.google.com/books?hl=en&lr=&id=X8Xa__TmqIAC&oi=fnd&pg=PA225&dq=%22game+theory%22+applied+to+counterterrorism&ots=mXgR0Bh82l&sig=gVRmQmn-lnRMz-oJp4h0bd2gcQY accessed on 7/02/2009.

Belobaba, P. P. (2002). *The Airline Industry Since 9/11: Overview of Recovery and Challenges Ahead*. Available at http://web.mit.edu/airlines/conferences/DC-2002_documents/05-DC2002-Belobaba.pdf accessed on 2/16/2010.

Bier, V., Oliveros, S., & Samuelson, L. (2005). *Choosing what to protect: Strategic defense allocation against unknown attacker* Center for Risk and Economic Analysis of Terrorism Events Report. Under Office of Naval Research Grant No. EMW-2004-GR-0112

Bier, V. M. (1997). *Game-theoretic and reliability methods in counterterrorism and security.* Modern statistical and mathematical methods in reliability, edited by A. Wilson, N. Liminios, S. Keller-McNulty, and Y. Armijo, Volume 10 of Series on Quality, Reliability, and Engineering Statistics, (pp. 17-38). Singapore: World Scientific Publishers.

Bier, V. M., Y. Y. Haimes, J. H. Lambert, N. C. Matalas, and R. Zimmerman. (1999). *Assessing and managing the risk of extremes*. Risk Analysis 19 (pp. 83-94).

Buckshaw, D. L., Parnell, G. S., Unkenholz, W. L., Parks, D. L., allner, J. M., & Saydjari, O. S. (2005). *Mission oriented risk and design analysis of critical information systems*. Military Operations Research, 10(2), (pp. 19–38).

Chen, Y.M., Wu, D. Wu, C.K. (2009). *A Game Theory Approach for the Reallocation of Security Forces against Terrorist Diversionary Attacks*. Intelligence and Security Informatics, (pp 89-94), IEEE international Conference.

Chinneck, J. W. (2009). *Practical Optimization: A Gentle Introduction..* Available at www.sce.carleton.ca/faculty/chinneck/po.html accessed on 02/25/2010.

Chong, E. K. P. and Zak, S. H. (2008) *An Introduction to Optimization*. 3rd ed.

Cleaves, D. J., Kuester, A. E., and Schultz, D. A. (2003). *A methodology for managing the risk of terrorist acts against the U. S. Postal Service*. Society for Risk Analysis Annual Meeting, Baltimore, MD.

Clemen, R. T. and Reilly, T. (2001) *Marking Hard Decisions with DecisionTools.* Duxbury Thomas Learning.

Cochran, T. B. and McKinzie, M. G. (2008). *Detecting nuclear smuggling: Radiation monitors at U.S. ports cannot reliably detect highly enriched uranium, which onshore terrorists could assemble into a nuclear bomb*. Scientific American.

de Campos, L. M., Fernández-Luna, J. M., and Huete, J. F. (2004). *Using context information in structured document retrieval: an approach based on influence diagrams.* Information Processing & Management Volume 40, Issue 5, (pp. 829-847) Bayesian Networks and Information Retrieval. Available at www.sciencedirect.com.proxy.library.vcu.edu/science

Department of Homeland Security Bioterrorism Risk Assessment: A Call for a Change. 2008. (2008) Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis. Board on Mathematical Sciences and Their Applications. Division on Engineering and Physical Sciences. Board on Life Sciences. Division on Earth and

Life Studies. National Research Council of the National Academies. The National Academies Press. Washington, D.C., Available at books.nap.edu/openbook.php?record_id=12206&page=6 accessed on 6/15/2009.

Department of Homeland Security Fact Sheet: U.S. Department of Homeland Security Programs Countering Missile Threats to Commercial Aircraft. (2004). Available at http://www.dhs.gov/xnews/releases/press_release_0497.shtm accessed on 10/12/2009

DHS (Department of Homeland Security). (2006). Bioterrorism Risk Assessment. Biological Threat Characterization Center of the National Biodefense Analysis and Countermeasures Center. Fort Detrick, Md.

Dillingham, G. L. (2003). *Aviation Security. Process Since September 11, 2001, and the Challenges Ahead*. Testimony of Gerald L Dillingham before the committee of commerce, science and transportation, U.S. senate.

Enders, W., and Sandler, T. (2004). *What do we know about the substitution effect in transnational terrorism?* In Researching terrorism: Trends, achievements, failures, edited by A. Silke and G. Ilardi. London: Frank Cass.

Federal Aviation Administration Webpage (FAA) *FAA Historical Chronology, 1926-1996.* Available at http://www.faa.gov/about/media/b-chron.pdf, accessed on 2/17/2010.

Federal Bureau of Investigation Webpage. (FBI) (n.d) *Weapons of Mass Destruction*. Available at http://www.fbi.gov/hq/nsb/wmd/wmd_home.htm accessed on July 2, 2009

Feng, T. and Keller, L. R. (2006). *A Multiple-Objective Decision Analysis for Terrorism Protection: Potassium Iodide Distribution in Nuclear Incidents*. Decision Analysis Vol. 3, No. 2, (pp. 76–93)

Fetter, S., Frolov, V. A., Miller, M., Mozley, R., Prilutsky, O. F., Rodionov, S. N. and Sagdeev, R. Z. (1990). *Detecting nuclear warheads*. Science & Global Security , Vol 1, Issue 3 and 4, (pp. 225-253).

Fritelli, J. F. (2005). *Port and maritime security: Background issues for congress*. CRS Report for Congress, Congressional Research Service, The Library of Congress, RL31733.

From U.S. Code Title 22, Ch.38, Para. 2656f(d) definition (2) available at terrorism.about.com/od/whatisterroris1/ss/DefineTerrorism_5.htm, accessed on July 2, 2009.

Gibbons, R. (1992). *Game Theory for Applied Economists*. Princeton University Press, Princeton, New Jersey.

Guikema, S. D. (2009) *Game Theoretic Risk Analysis of Security Threats*. Chapter 2 Game Theory Models of Intelligent Actors in Reliability Analysis, An Overview of the State of the Art. Vol. 128 (pp. 13-32)

Haimes, Y. Y. (1981). *Hierarchical holographic modeling*. IEEE Transactions on Systems, Man, and Cybernetics, 11(9), (pp. 606–617).

Haimes,Y.Y. (1998). *Risk Modeling, Assessment, and Management*. New York: JohnWiley and Sons.

Hamill, J. T., Deckro, R. F., & Kloeber, J. M. (2005). *Evaluating information assurance strategies*. Decision Support Systems, Vol 39, Issue 3, (pp. 463–484).

Hamill, J. T., Deckro, R. F., Kloeber, J. M., & Kelso, T. S. (2002). *Risk management and the value of information in a defense computer system*. Military Operations Research, Vol. 7 No. 2, (pp. 61–81).

Hausken, K. (2002). *Probabilistic risk analysis and game theory*. Risk Analysis Vol. 22 No. 1 (pp.17–27).

Heal, G. and Kunreuther, H. (2005) *IDS Models of Airline Security.* The Journal of Conflict Resolution, Vol. 49, No. 2, The Political Economy of Transnational Terrorism (pp. 201-217) Published by: Sage Publications, Inc. Available at: http://www.jstor.org/stable/30045108 Accessed: 06/08/2009

Huizenga, D. (2005). *Detecting nuclear weapons and radiological material: How effective is available technology?* Statement before the Subcommittee on Prevention of Nuclear and Biological Attacks and Subcommittee on Emergency Preparedness, Science and Technology, The House Committee on Homeland Security.

Kobza, J. E. and S. H. Jacobson (1996). *Addressing the dependency problem in access security system architecture design*. Risk Analysis. Vol. 16 issue 6, (pp. 801-812).

Kobza, J. E. and S. H. Jacobson (1997). *Probability models for access security system architectures*. Journal of the Operational Research Society Vol. 48 issue 3, (pp. 255-263).

Insurance Information Institute, New York, NY: October 21, 2002.

International Atomic Energy Agency (IAEA) (2006). Fact Sheet: *IAEA Illicit Trafficking Database (ITDB).* Available at www.iaea.org/NewsCenter/Features/RadSources/PDF/fact_figures2006.pdf, accessed on 2/17/2010.

Kim, J. and Bridges, T. S. (2006) *Risk, Uncertainty, and Decision Analysis Applied to the Management of Aquatic Nuisance Species*. Aquatic Nuisance Species Research Program. Accessed on 10/19/2009, available at http://el.erdc.usace.army.mil/elpubs/pdf/ansrp06-1.pdf

Keeney, R. L. (2007). *Modeling Values for Anti-Terrorism Analysis*. Risk Analysis, Vol. 27, No. 3.

Keeney, R.L. and H. Raiffa. (1976). *Decision Analysis with Multiple Objectives: Preferences and Value Trade-Offs*. John Wiley and Sons, New York.

Kirkwood, C. (1997). *Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets*. Belmont, CA: Duxbury Press.

Kunreuther, H., & Heal, G. (2003). *Interdependent security*. Journal of Risk and Uncertainty, 26, (pp. 231–249).

Lapan, H. E., & Sandler, T. (1988). *To bargain or not to bargain: That is the question*. American Economic Review, 78, (2), (pp. 16–20).

Leung, M., Lambert, J. H., and Mosenthal, A. (2004). *A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks*. Risk Analysis, Vol. 24, No. 4.

Levi, M. (2007). *On Nuclear Terrorism*. Cambridge, Mass.: Harvard University Press.

McLay, L.A., Lloyd, J. D. and Niman, E. (2010). *Interdicting Nuclear Material on Cargo Containers using Knapsack Problem Models*. Annals of Operations Research (to appear).

McLay, L. A., Jacobson, S. H. and Kobza, J. E. (2008). The tradeoff between technology and prescreening intelligence in checked baggage screening for aviation security. Journal of Transportation Security (to appear). CHECK THIS

Major, J. A. (2002). *Advanced techniques for modeling terrorism risk*. Journal of Risk Finance Vol. 4 No. 1, (pp. 15–24).

Makien, G. (2002). *The Economic Effects of 9/11: A Retrospective Assessment*. Report for Congress, Available at http://www.au.af.mil/au/awc/awcgate/crs/rl31617.pdf accessed on 2/15/2010.

Medalia, J. (2005), *Terrorist Nuclear Attacks on Seaports: Threat and Reponse.* CRS Report for Congress. Specialist in National Defense. Foreign Affairs, Defense and Trade Division. Received through the CRS Web. Accessed 1/13/2010.

Merrick, J. R. W. and McLay, L. A. (2009). *Is Screening Cargo Containers for Smuggled Nuclear Threats Worthwhile?* Virginia Commonwealth University.

Moffitt, L. J., J. K. Stranlund, and B. C. Field (2005). *Inspections to avert terrorism: Robustness under severe uncertainty*. Journal of Homeland Security and Emergency Management Vol. 2 Issue 3. Available at www.bepress.com/jhsem/vol2/iss3/3, accessed 11/22/2006.

Mullin, B., Mullin, M., and Mullin, R. (2008). *Mhairi's Dilemma: A study of decision analysis at work.* With comments by Jack Dowie and Rex V. Brown. Judgment and Decision Making, Vol.

3, No. 8. (pp. 679–689). Available at http://journal.sjdm.org/81128/jdm81128.pdf, accessed 06/14/2009.

National Counterterrorism Center Website (n.d.). Available at www.nctc.gov/about_us/about_nctc.html accessed on July 2, 2009.

National Research Council.(2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* Committee on Science and Technology for Countering Terrorism, Washington, National Academy Press, (p. 40) Available at www.nap.edu/catalog/10415.html

Newman, R. J. (2003). *The New Flight Plan: The nation's airlines miraculously survived their post-9/11 tailspin. Too bad that wasn't their only problem*. U.S. News and World Report.

Office of Homeland Security. (2002). *National Strategy for Homeland Security*. Available at www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf. Accessed on 07/01/2009.

Parnell. G. S., Smith, C. M., Moxley, F. I.(2009). *Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model.* Accepted to Risk Analysis, Journal of the Society for Risk Analysis.

Parrish, W. H. (2008). Personal Interview.

Paté-Cornell, E., and Guikema, S. (2002). *Probabilistic modeling of terrorist threats: A systemsanalysis approach to setting priorities among countermeasures.* Military Operations Research Vol. 7 Issue 4 (pp.5–20).

Public Law 107–296 (2002) 107th Congress available at http://www.nist.gov/director/ocla/Public_Laws/PL107-296.pdf accessed on June 22, 2009.

Raiffa, H. (1968) *Decision Analysis*, Addison-Wesley, Reading, Massachusetts.

Ramirez-Marquez, J. E. (2008). *Port-of-entry safety via the reliability optimization of container inspection strategy through an evolutionary approach*. Reliability Engineering and System Safety Vol. 93 Issue 11, (pp. 1698-1709).

Reifel, C. S. (2006). *Quantitative Risk Analysis for Homeland Security Resource Allocation.* Naval Postgraduate School Monetary, California. Accessed on 11/04/09 available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA462640&Location=U2&doc=GetTRDoc.pdf

Rice, J. S. (n.d.) Boulder, CO http://www.sip.ucar.edu/wasis/pdf/boulder_1/04rice.pdf

Rios Insua, Rios, J. and Banks, D. (2009) *Adversarial Risk Analysis*. Journal of the American Statistical Association.

Robinson, W. H., Lake, J. E. and Seghetti, L. M. (2005). Border and transportation security: Possible new directions and policy options. CRS Report for Congress, Congressional Research Service, The Library of Congress, RL32841.

Rooney, B. (2005). *Detecting nuclear weapons and radiological material: How effective is available technology?* Statement before the Subcommittee on Prevention of Nuclear and Biological Attacks and Subcommittee on Emergency Preparedness, Science and Technology, The House Committee on Homeland Security.

Rosoff, H. and vonWinterfeldt, D. (2007). *A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach.* Risk Analysis, Vol. 27, No. 3.

The Royal Society. (2008). Detecting nuclear and radiological materials. RS policy document 07/08, The Royal Society, London, UK.

Samson, A. (n.d.). *Modeling Terrorism: A Game Theoretical Approach.* Available at www.adamsamson.com/writing/asamson-terrorism-game-theory.pdf Accessed on June 25, 2009.

Sandler, T. and D. G. Arce M. (2003). *Terrorism and Game Theory.* Simulation & Gaming Vol. 34 Issue3. Available at http://www.utdallas.edu/~tms063000/website/Terror_Games.pdf, accessed June 26, 2009.

Shachter, R. (1986). Evaluating influence diagrams. Operations Research 34, (pp. 871–882).

Shea D., Lister S. (2003). *The BioWatch Program: Detection of Bioterrorism.* Washington, D.C.: Congressional Research Service Report, RL 32152. Available at: http://www.fas.org/sgp/crs/terror/RL32152.html#_1_2 , Accessed on 12/14/ 2009.

Siqueira, K. (2003). *Conflict and Third-Party Intervention.* Defence and Peace Economics, Vol. 14, (pp. 389- 400).

Siqueira, K. and Sandler, T. (2004). *The Provision of Collective Goods, Common Agency, and Third Party Intervention*. Bulletin of Economic Research, Vol. 56, (pp. 1-20).

Slaughter, D., Accatino, M., Bernstein, A., Candy, J., Dougan, A., Hall, J., Loshak, A., Manatt, D., Meyer, A., Pohl, B., Prussin, S., Walling, R., and Weirup, D. (2003). *Detection of special nuclear material in cargo containers using neutron interrogation*. Report UCRL-ID-155315, Lawrence Livermore National Laboratory, Livermore, CA.

Stohl, M. (1983). *Demystifying Terrorism: The Myths and Realities of Contemporary Political Terrorism.* In M. Stohl (ed.) The Politics of Terrorism, 2nd edition. Marcel Dekker, (p. 10).

Strohm, C. (2006). *Investigators call cargo security program unreliable*. Gov-Exec.com. available at www.govexec.com/dailyfed/0406/040506cdam3.htm, accessed on 11/22/2006.

Thompson, W. C. Jr. (2002) Comptroller City of New York. *One Year Later, The Fiscal Impact of 9/11 on New York City*. September 4, 2002. Available at www.comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf, accessed on 2/17/2010.

United States Department of Transportation (2007). *America's container ports: Delivering the goods*. Technical report, Research and Innovative Technology Administration, Bureau of Transportation Statistics, Washington, D.C.

U.S. Center for Disease Control (CDC). Bioterrorist Agents/Diseases Definitions by category. Available at: http://www.bt.cdc.gov/agent/agentlist-category.asp, Accessed on February 10, 2009.

U.S. Department of State (1995). Fact Sheet: International Terrorism-American Hostages Bureau of Public Affairs. Available at dosfan.lib.uic.edu/ERC/arms/cterror_briefing/951017cterror.html accessed on 06/12/ 2009.

U.S. Government Accountability Office. (2005). Homeland security: *DHS' efforts to enhance first responders' all-hazards capabilities continue to evolve*. Technical Report GAO-05-652. U.S. Government Accountability Office, Washington, D.C.

Von Neumann, J. (1928). *Zur Theorie der Gesellschaftsspiele.* Mathematishe Annalen 100: 295-320. Translated as "*On the theory of games of strategy*" in Contributions to the Theory of Games, IV (Annals of Mathematics Studies), ed. A. Tucker and R.D. Luce. Princeton: Princeton University Press, 1959.

Weapons of Mass Destruction. (2005). WMD Commission, (p. 504).

Webster, T. J. (1984). *An introduction to game theory in business and economics.* Published by M.E. Sharpe, Inc.

Wein, L. M., Liu, Y., Cao, Z., and Flynn, S. E. (2007). *The optimal spatiotemporal deployment of radiation portal monitors can improve nuclear detection at overseas ports*. Science and Global Security 15, (pp. 211-233).

Wein, L. M., Wilkins, A. H., Baveja, M., and Flynn, S. E. (2006). *Preventing the importation of illicit nuclear materials in shipping containers*. Risk Analysis 26 (5), (pp. 1377-1393).

Wein, L. M. and Atkinson, M. P. (2007). *The Last Line of Defense: Designing Radiation Detection-Interdiction Systems to Protect Cities From a Nuclear Terrorist Attack.* IEEE Transactions on Nuclear Science, Vol. 54, No. 3.

Wenzlaff, K. (2004). *Terrorism: game theory and other explanations*. Student of Philosophy & Economics (Bachelor) at University of Bayreuth.

Wilson, A. Ph.D. (2007). *How DHS Currently Manages Risk*. RISK: Policy, Perception, and Practice Workshop, Statistical and Mathematical Sciences Institute, Research Triangle Park, NC.

Wilson, A. G., Wilson, G. D., Olwell, D. H. (2006). *Statistical Methods in Counterterrorism: Game theory, modeling, syndromic survallance, and biometic authentication*. Springer Science & Business Media, LLC.

Winterfeldt, D. von and O'Sullivan, T. M. (2006). *Should We Protect Commercial Airplanes Against Surface-to-Air Missile Attacks by Terrorists?* Decision Analysis Vol. 3, No. 2, (pp. 63–75).

Zhang, N. (1998). *Probabilistic inference in influence diagrams*. Computational Intelligence 14**,** (pp. 475–497).

Zhuang, J., Bier, V. M.. (2007). *Balancing Terrorism and Natural Disasters—Defensive Strategy with Endogenous Attacker Effort*. Operations Research. Vol. 55, No. 5, (pp. 976–991).

Vita

Jamie Lynn Dauberman was born on April 2, 1985, in Richmond, Virginia, and is an American citizen. She graduated from Louisa County High School, Louisa, Virginia in 2003. She received her Bachelor of Statistical Sciences & Operations Research from Virginia Commonwealth University, Richmond, Virginia in 2008 and subsequently entered the Master's degree program for Operations Research. She quickly accepted a job offer at Dominion Virginia Power, where she is currently working as a Materials Specialist in Supply Chain Management. She was married May 31, 2008 and has some work published under the married name of Jamie Dauberman Lloyd. She received a Master Statistical Sciences & Operations Research from Virginia Commonwealth University in 2010.