The Dissertation Committee for Rebecca Morgan Ward Certifies that this is the approved version of the following dissertation:

A Game Theoretic Approach to Nuclear Safeguards Selection and Optimization

Committee:

Erich Schneider, Supervisor

Steven Biegalski

David Morton

Felicia Durán

Alan Kuperman

A Game Theoretic Approach to Nuclear Safeguards Selection and Optimization

by

Rebecca Morgan Ward, BA; MSE

Dissertation

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

August 2013

Dedication

To my parents— for all the early Saturday morning games, all the long nights with the flashlight looking for Baby Sleeping, all the late mornings with the bumps in my hair, and all the times you made me look it up in the dictionary. Now I know a lot of words, and it's all because of you. Thank you.

Acknowledgements

I would like to gratefully acknowledge Dr. Schneider for his support, guidance, flexibility, and incredible intellectual creativity. Without your direction and gentle coaxing, this project would still be a whisper of an idea stuck in the annals of my mind. Thank you for helping me make my intellectual vision show up on my computer screen.

I would also like to thank Dr. Biegalski for your support through my Masters and your continued mentorship and guidance over the past five years. Thanks for all the life lessons and career advice, both silly and serious.

I am grateful to my funders, the DoD/DHS Nuclear Forensics Graduate Fellowship and the Stanton Foundation for their generous support and the flexibility with which they allowed me to pursue a research topic that truly inspired me.

Thank you also to Dr. Felicia Durán and Sandia National Labs for an excellent lab experience and for your continued mentorship. Felicia- you are an incredible professional female role model, and I'm grateful for all you've taught me through example and conversation.

Alex and Robert- thanks for the MCNP runs, the ORIGEN runs, and the logistical support on the ground. You have no idea how valuable your help was.

Roger- Thanks for all the times you've flagged a yellow cab and flown a silver bird, all just to get to me. Your patience and love exceed my understanding, but not my capacity to appreciate them. Thank you for everything. Yankees talk funny, but they're alright.

A Game Theoretic Approach to Nuclear Safeguards Selection and Optimization

Rebecca Morgan Ward, Ph.D.

The University of Texas at Austin, 2013

Supervisor: Erich Schneider

This work presents a computational tool that calculates optimally efficient safeguarding strategies at and across nuclear fuel cycle facilities for a cost-constrained inspector seeking to detect a state-facilitated diversion or misuse. The tool employs a novel methodology coupling a game theoretic solver with a probabilistic simulation model of a gas centrifuge enrichment plant and an aqueous reprocessing facility. The simulation model features a suite of defender options at both facilities, based on current IAEA practices, and an analogous menu of attacker proliferation pathway options. The simulation model informs the game theoretic solver by calculating the detection probability for a given inspector-proliferator strategy pair and weighting the detection probability by the quantity and quality of material obtained to generate a scenario payoff. Using a modified fictitious play algorithm, the game iteratively calls the simulation model until the equilibrium is reached and outputs the optimal inspection strategy, proliferation strategy, and the equilibrium scenario payoff. Two types of attackers are modeled: a breakout-willing attacker, whose behavior is driven by desire for high value material; and a risk-averse attacker, who desires high-value material but will not pursue a breakout strategy that leads to certain detection. Results are presented demonstrating the sensitivity of defender strategy to budget and attacker characteristics, for an attacker

known to be targeting the enrichment or reprocessing facility alone, as well as an attacker who might target either facility. The model results indicate that the optimal defender resource allocation strategy across multiple facilities hardens both facilities equitably, such that both facilities are equally unattractive targets to the attacker.

Table of Contents

List of Tables

List of Figures

BACKGROUND

Chapter 1: Introduction

The threat posed by the illicit production of nuclear weapons worldwide has gained increased attention in recent years, in part due to a number of incidents where stolen nuclear material was recovered and in part due to the discovery of clandestine weapons programs in sensitive nations. In April 2009, President Obama raised this threat as a security priority, noting that, "The technology to build a bomb has spread… Our efforts to contain these dangers are centered in a global non-proliferation regime, but as more people and nations break the rules, we could reach the point when the center cannot hold. This matters to all people, everywhere." [1] Concern over nuclear proliferation has elevated in concert with increased global interest in civilian nuclear power and a divergence in commercial fuel cycle technologies. This confluence of factors has placed heavy demands on International Atomic Energy Agency (IAEA), the organization tasked with verification of peaceful nuclear activities.

While the IAEA's workload continues to grow, the resources available to it remain relatively stagnant. The IAEA operated on a zero-growth budget from the mid 1980's into the early 2000's, finally receiving a substantive budget increase in 2003 [2]. Even against an increased threat backdrop, the IAEA's verification budget rose from approximately $145 million in 2007 to $160 million in 2010, a rate only marginally higher than inflation [3]. Traditionally IAEA safeguards are applied in a prescriptive manner at declared nuclear facilities, with the application of safeguards varying little from state to state regardless of perceived threat or size of the nuclear program. The safeguarding implementation is largely transparent to the states except for random on-site inspections. The regime thus places high demand on physical inspections, which are costly and inefficient.

Budget constraints have spurred efforts to increase IAEA efficiency through the development of tools to aid in resource allocation decision-making. Many such tools focus on diversion pathway analysis and are based on probabilistic techniques. While probabilistic techniques are valuable for describing fundamentally random events, like natural disasters, their use has received criticism recently for application to adversarial problems. A 2010 National

Research Council report questions the use of probabilistic techniques for adversarial risk analysis, noting that data in this area is too scarce to characterize adequately the threat or consequences of an attack. Further the study suggests that probabilistic techniques may not fully capture the behavior of intentional actors, like a malevolent state or terrorist [4]. Intentional actors represent a special class of threat, as they possess the ability to observe defenses and adjust their actions accordingly. Cox voices similar skepticism in his work, criticizing especially the use of chance nodes in fault tree analysis to model adversary decisions, arguing that these decisions are chosen based on adversary judgment, not governed by chance [5]. Cox's paper and the NRC report alike suggest that a game theoretic approach to intelligent risk analysis may be more appropriate.

To address the aforementioned shortcomings in current nonproliferation analysis tools, this work develops a game theoretic approach to safeguards strategy selection and resource allocation. A state or state-supported insider group is treated as an intelligent adversary seeking to achieve his most desirable outcome through diversion strategy selection. The interaction between the IAEA inspector (defender) and the proliferator (attacker) is modeled as a two-person, zero-sum, simultaneous play game, where the defender is the maximizing player seeking to maximize the payoff, and the attacker is the minimizing player seeking to minimize the payoff. Both players select their strategies to optimize their own outcomes in the worst-case scenario.

One of the common criticisms of game theoretic risk analysis approaches is that current models do not contain enough realistic complexity to be useful for real decision-making [4]. This problem derives largely from lack of experimental or historical data with which to populate a game theoretic model. Cox suggests the use of probabilistic techniques to support game theoretic models in this manner, providing uncertain values as input to payoff matrices [5]. Consistent with Cox's recommendation, this work employs the use of a simulation model to inform the game model with payoff values for different strategy pairs. Representative overall detection probabilities for a diversion scenario will be factored into payoffs, along with material attractiveness and quantity. The game model will serve as an optimization tool and repeatedly call the simulation, searching the strategy space for the strategy that maximizes the defender's payoff, given that the attacker also selects his optimal strategy.

The value of game theory for adversarial analyses lies in this prescient optimization; a real adversary is intelligent and will choose strategies to optimize his payoff or to minimize the defender's payoff, and the defender should choose her strategy accordingly. Many probabilistic analysis techniques fail to capture motivated adversary behavior and do not optimize the defender's strategy in the context of its probable effect on adversary behavior. Such an approach to adversarial analysis is particularly germane to IAEA strategy analysis given that budget constraints are pushing the IAEA away from traditional, prescriptive safeguards toward information-driven safeguards (IDS). The IDS approach dictates that the Agency use any information available to it to advise resource allocation, thus ensuring that safeguarding resources are being applied where the need is greatest [6]. The game theoretic methodology presented here provides a framework for guiding IDS and informed resource allocation decision-making.

To replicate the challenges facing the IAEA, the defender is cost-constrained and must select the best strategy available given her budget. The simulation model features a gas-centrifuge enrichment plant and an aqueous reprocessing facility under IAEA safeguards. The defender has a menu of safeguarding options to choose from for each facility, based on current IAEA practices at that type of facility. Likewise the attacker has a set of diversion and misuse options from which to use, again based on plausible diversion and misuse scenarios at the respective facilities. The model investigates optimal safeguarding and diversion strategies across the two facilities by allowing the defender to distribute resources across both facilities.

Taking a game theoretic approach to safeguards selection is not in itself new, and a rich body of literature exists on the use of game theory for inspection games and resource allocation problems. The novelty of the work presented here lies in the coupling of a game theoretic model to a full-scale simulation model, thus demonstrating a platform for informing the game with meaningful detection probabilities. Most game theoretic inspection models are largely theoretical and are of limited complexity to allow for analytical solutions. The use of a simulator to provide numerical values to the game theoretic model enables increased fidelity and richness of diversion scenarios, enhancing the scope and realism of the output. In addition to producing meaningful values for a real facility, this work investigates optimal safeguarding strategies across two facilities. Current proliferation and safeguarding analyses generally focus on only

one facility and evaluate safeguards systems within that facility. A 2009 National Academy of Science study recommended the use of a "systems approach" to assessing safeguards architecture [7]. This work demonstrates a proof-of-concept systems approach to optimization across the fuel cycle by optimizing diversion and safeguarding strategies across two facilities, an enrichment plant and reprocessing facility. Like the coupling of the simulation and game model, this optimization across fuel cycle facilities represents a new contribution to this area.

This document is structured into three major sections: background, methodology, and results and conclusions. Chapter 2 supplements the information provided in the introductory chapter by providing a detailed survey of the literature. The next major section describes the methodology employed in this work; specifically the development of the computational tool. In this section, Chapter 3 presents a description of the game model and an overview of the coupling of the simulation models and game models, while Chapter 4 and Chapter 5 provide detailed descriptions of the enrichment and reprocessing simulation models, respectively. Both simulation chapters present detailed information about the reference facilities modeled, the attacker and defender options, analytical expressions used to calculate detection probabilities for different defender-attacker strategy pairs, payoff calculation inputs, and budget calculations. The final major section is results and conclusions, which is broken down into three chapters: Chapter 6 provides the results for both single-facility models, Chapter 7 gives the results of the integrated model (system of enrichment and reprocessing facilities), and Chapter 8 offers general conclusions and policy implications, as well as remarks on the intellectual value and novelty of the work.

Chapter 2: Literature Review

2.1 SIMULATION

Simulation tools have been used extensively to explore diversion pathways and safeguarding strategies, particularly to evaluate system effectiveness of a physical protection system (PPS). One of the earliest applications of this type is the Insider Safeguards Effectiveness Model (ISEM), developed at Sandia National Laboratories [8]. This tool is designed to evaluate a facility's PPS against an insider attack, though it also has a module for overt attack. The user inputs information about facility layout, facility safeguards, and security features, as well as information about adversary path through the facility. The model is written in the FORTRAN-based GASP IV simulation language and simulates an attack in a discrete-state continuous-time stochastic process [9]. Because the model stochastically simulates one theft pathway per run, it is run using a Monte Carlo method to estimate overall PPS effectiveness against the specified attack. The model estimates the adversary's success probability. This tool represents an early application of computer simulation to diversion pathway analysis at a nuclear facility.

ISEM is the predecessor to more sophisticated tools developed at Sandia. The Systematic Analysis of Vulnerability Intrusion (SAVI) also assesses the vulnerability of a facility's PPS to attack, though SAVI is designed for forceful, outsider attacks [10]. This tool allows the user to input facility specific information in an adversary sequence diagram, including different areas at the facility, protection elements contained in each area, and performance data for each protection element. SAVI employs the Critical Detection Point (CDP) methodology. The CDP is the last point in time at which an adversary can be detected with sufficient time to interrupt the attack. This methodology assumes that an attacker seeks to minimize his detection up to the CDP, after which he seeks to minimize his delay. SAVI determines the ten most vulnerable pathways through the facility, as well as suggestions for improvements to the PPS. The suggestions offered are generally elements that could be added to increase detection before the CDP or increase delay after it. ATLAS and ASSESS are PPS effectiveness evaluation tools that followed SAVI [11], [12]. Both employ the use of adversary sequence diagrams and the CDP methodology. Like ISEM, ASSESS contains an insider module for insider threat analysis, while ATLAS is

designed for overt threat analysis only. These tools perform optimization through direct enumeration.

In an extension of the probabilistic pathway analysis codes described above, Durán integrates material control and accounting (MC&A) activities into the PPS system for insider theft analysis [13]. The MC&A activities are used to provide additional detection opportunities against the insider, as PPS systems may not be effective against this type of adversary. The work also presents a probabilistic framework for incorporating MC&A detection opportunities into the current PPS pathway analysis methodology. This framework characterizes insider theft as a "race" between the insider and the MC&A activities to detect the theft and employs an Excel-based simulator to calculate daily and cumulative theft DPs. To create a higher fidelity model of MC&A DPs, human reliability analysis is incorporated to model human performance. The research presented in this document draws on Durán's insider theft methodology and implements a similar human performance-based MC&A structure in the simulation model for certain safeguarding activities.

Systems dynamics models have also been used to evaluate the effectiveness of safeguarding systems. Dayem, formerly with Los Alamos National Lab, used the GASP IV simulation language to model a dynamic process and measurement system, the Materials Measurement and Accounting System (MMAS), intended to deliver near real-time accounting at nuclear facilities [14]. The flow of material through a reference facility is simulated, as is the system response. A set of coupled differential equations describes the material and SNM flow through the facility, with the user specifying initial parameters. A Monte Carlo method is used to simulate the measurements at key measurement points, and inventory differences are tracked across the plant. This work specifically focuses on the sensitivity of the MMAS system at a real plant and identifying measurement control problems. Though no diversion scenarios were run, this paper represented an early attempt at making a quantitative assessment of safeguards system effectiveness using simulation techniques.

A more extensive material accounting model has been developed in recent years at Sandia. The Separation and Safeguards Performance Model (SSPM) is a Simulink-based dynamic process model of a hypothetical aqueous reprocessing facility [15]. Like Dayem's model, the SSPM uses a set of coupled differential equations to describe the flow of SNM and

material through the facility and stochastically simulates mass and volume measurements of that material at key points, at which inventory differences are calculated. Process monitoring and material control and accounting (MC&A) alarms are simulated when inventory differences are statistically significant, as calculated using the Page's test. Diversion scenarios are modeled explicitly in the SSPM, with the user specifying the adversary's pathway through the facility. In addition to process monitoring and accounting alarms, physical protection and administrative procedures are also integrated into the SSPM [16]. This integration represents a novel approach to facility safeguards analysis, as information from these systems is traditionally not integrated at real facilities. While the sophistication of the model makes it attractive for obtaining a comprehensive picture of facility operations and safeguarding measures, it also proves somewhat computationally burdensome. Like many of the models discussed above, the SSPM stochastically generates detection probability for a given diversion scenario. Consequently, Monte Carlo methods are necessary to produce a reliable estimate of detection probability against a specific threat. Major drawbacks of the SSPM are that the user must specify the diversion scenario and no safeguarding optimization occurs.

The LLNL Integrated Safeguards System Analysis Tool (LISSAT), developed at Lawrence Livermore National Laboratory, is another continuous-time model for evaluating safeguards system effectiveness at fuel cycle facilities [17], [18]. This model uses a digraph fault tree structure to examine possible points of safeguards system failure for different diversion scenarios. The user inputs information about the process at the facility and the safeguards system. The process is modeled as a continuous, natural flow, and the safeguards system is modeled as lists possible removal nodes. Diversion scenarios are designed for each removal node, and a digraph is constructed for each diversion scenario. A fault tree is then constructed for each digraph, with safeguards system failure serving as the top event. The system outputs the probability that the diversion pathway is successful, as well as the quantity and value of the material removed. Using this information, fault tree analyses for a series of diversion scenarios can be compared, and the most attractive scenarios are sent through an Extend simulation model. The simulation model shows how the range of various safeguard systems parameters varies from the base-case for a diversion scenario, thus establishing a signature for different diversion scenarios.

A Markov-model based proliferation assessment tool was developed at Brookhaven National Laboratory [19]. This work simulates operations at a hypothetical Experimental Sodium Fast Reactor. The model features both intrinsic and extrinsic barriers to proliferation, including a suite of IAEA safeguards options. It also considers false alarm probabilities and human performance. The model outputs several metrics, including minimum time to and cost of proliferation, as well as the detection probability and technical difficulty. While this model represents a more sophisticated optimization scheme than the direct enumeration used in many pathway analyses, diverter strategy is still an input, meaning the proliferator's intelligence is not fully captured.

While the two studies above both examine vulnerable proliferation pathways at a single facility, other work has been done characterizing proliferation resistance across a fuel cycle system. A Proliferation Resistance & Physical Protection (PR & PP) evaluation methodology has been developed by an expert group of the Generation VI International Forum [20]. In an effort to aid policy decision making regarding future nuclear energy systems, this methodology focuses on evaluating the proliferation resistance of a nuclear energy system as a whole relative to other nuclear energy systems. The methodology encompasses three major steps: (1) defining the threat, which includes state and non-state actors with various capabilities and strategies, and identifying proliferation pathways; (2) determining system response; and (3) evaluating the outcomes. The outcome is evaluated using several metrics, including detection probability, proliferation time, and "safeguardability". The second step, in which calculations are performed to determine system response, relies on probabilistic techniques. While the ability of this methodology to be applied across a fuel cycle system distinguishes it from many of the other methodologies presented here, the underlying computational techniques employed are not themselves new or appreciably different from many of the other previous techniques. Further this methodology does not perform any optimization and relies heavily on analyst input. These shortcomings mean that while the PR&PP may be a useful tool for its intended purpose to assessing the relative proliferation resistance of fuel cycle systems, it is not an ideal tool for guiding safeguarding resource allocation decisions.

2.2 GAME THEORY

Game theory is a popular technique for modeling adversarial situations because of its ability to capture and systematically model human cognition and behavior. In fact, a comprehensive body of work devoted to game theoretic treatment of safeguarding strategy and analysis exists [21]. Avenhaus presents a comprehensive game theoretic treatment of data and material accountancy verification at nuclear facilities [22]. An analysis of attribute sampling across multiple strata is considered, and the mathematical formulation for optimal inspector strategy is given. This formulation is consistent with the current IAEA attribute sampling paradigm. Random, interim inspections are also treated, and the frequency with which they must be conducted to ensure timely detection of illegal behavior is derived. The tradeoff between timely detection and sensitivity is explored, and it is shown that an inspector cannot simultaneously optimize his safeguard accountancy system with respect to both criteria. Defensive resource allocation across multiple facilities is examined, and optimal inspector and inspectee strategies are given for a scenario with a small number of facilities.

Bier et al. also investigate defensive strategies across multiple assets. Their work presents a two-person non-zero sum sequential-play game in which a cost-constrained defender must defend two assets, of which the attacker will attack only one [23]. The defender plays first, allocating her resources between the two sites, and the attacker observes this allocation before committing to his strategy. Bier describes the effect of decentralizing defenses and provides results in support of centralized defenses. The work also examines the effect on defense strategy as the number of assets to protect becomes large, and concludes that the optimal strategy collapses.

Kilgour and Avenhaus use game theory and decision theory to examine the cost-effectiveness of IAEA inspections and recommend strategies to improve efficiency [24]. The work proves that an inspection program deters violations only if it sufficiently effective. It also shows that a state's motivation to violate depends on political parameters—the penalty the state perceives for detected illegal behavior and the reward the state perceives for undetected illegal behavior—as well as a technical parameter, inspection effectiveness. A calculation of how effective one inspection must be to deter two states from illegal behavior is made.

All of the work presented above represents a significant contribution to safeguarding and/or adversarial analysis; however, all the work is theoretical in construct, presenting the mathematical formulation for strategies and detection probabilities with little or no attempt made to assign meaningful values to the input parameters. Further the complex nature of the game formulation requires that the model be sufficiently limited in scope to allow for the calculation of Nash equilibrium. While these studies provide valuable insights into concepts underlying defensive resource allocation, the need remains for work that is more applied and quantitative in nature.

Brown et al. present a more applied two-stage Stackelberg game representing an interdictor trying to maximally delay a proliferator who is trying to produce a first batch of fissile material [25]. A max-min game is formulated between an interdictor attempting to maximize delay time and a proliferator attempting to minimize delay time. The model assumes that the proliferator observes the interdictor's defense strategy and adjusts his strategy accordingly. Model output includes optimal interdictor and proliferator strategy. The incorporation of a detailed project management sub-model to generate scenario data which is coupled with the game model for optimization allows for far more realistic complexity than is found in many purely theoretical game models. This idea of relying on a sub-model to generate scenario data is used in an adapted form in the research presented here.

2.3 Risk Assessment and Defensive Investments

Previous work on risk assessment and defensive investment in the field of nuclear security has been conducted by Wyss et al. at Sandia National Laboratories. To assess the risk posed by a given attack scenario, standard risk assessment approaches rely on triplets containing scenario description, probability of scenario, and consequence of scenario. In their updated framework for risk-based cost-benefit analysis, Wyss et al. propose replacing the highly uncertain 'probability of scenario' value with a quantitative metric to describe 'adversary difficulty' [26], [27]. The resulting analysis is a target and scenario specific risk assessment. The framework also draws on the game theoretic principle of utility functions to present the notion of undominated attack scenarios, or scenarios that are higher consequence and lower difficulty than all other scenarios. The work indicates that these scenarios will be most attractive to adversaries,

and suggests that such an analysis can be used to prioritize investment decisions. Though the work presented in this dissertation considers defensive investments for nuclear safeguards, and not nuclear security, similar conclusions are drawn about defensive investment prioritization across multiple facilities.

2.4 HUMAN RELIABILITY ANALYSIS

Many safeguarding activities rely heavily on activities performed by humans, making human error a major factor in the effectiveness of these safeguards. Human reliability analysis (HRA) describes a collection of techniques used to quantify human error probability [28]. In the context of safeguarding a nuclear facility, human error can have a detrimental effect on the detection capability of the safeguards system. One technique used to quantify such error is the modeling of a dependency relationship among activities in which human involvement is critical to success. This dependency relationship describes the following behavioral characteristic: when a human performs a checking task, such as an inspection, and fails to detect an anomaly, she becomes less likely to detect the anomaly for each successive inspection at the same location. The extent to which this degradation of per-inspection DP occurs for subsequent inspections is characterized by the dependency among inspections. Durán employs this HRA methodology in her work, modeling six dependency levels: zero, low, moderate, high, and complete, with increasing dependencies corresponding to greater reduction in per-inspection DP [13]. In this sense dependency is a proxy for manpower, as more unique inspectors performing a task lower dependency, implying that the per-inspection DP remains higher when 'fresh eyes' are brought in to conduct successive inspections. The mathematical relationship between DPs for successive inspections is given in Equation 2.1. Figure 2-1 shows this relationship graphically, plotting daily DP for different dependencies in the case of daily inspection with initial DP of 0.02.

$$P(F_M|F_{M-1}) = \frac{1 + aP_{M-1}}{a + 1} \tag{2.1}$$

where $P(F_M|F_{M-1})$ is the conditional probability that anomaly M is not detected, given that anomaly M-1 was not detected, and P_M is the unconditional probability that anomaly M is not detected. The parameter a is related to dependency with a = 19, 6, 1, and 0 for low, moderate, high, and complete dependency, respectively.

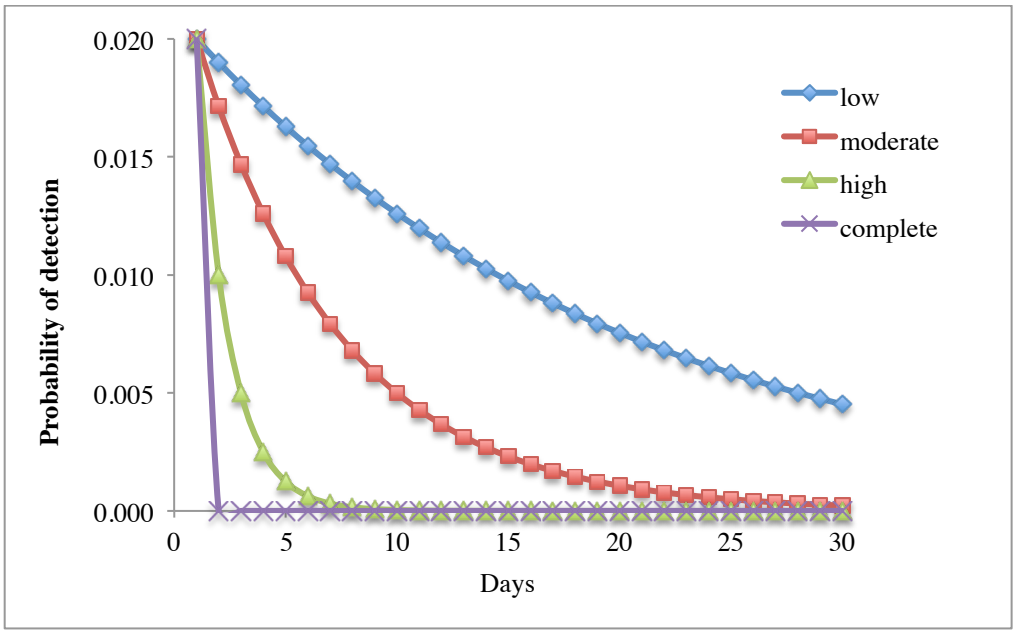

Figure 2-1. Daily DPs for different dependency levels for a daily inspection with initial DP = 0.02

METHODOLOGY

Chapter 3: Game Model and Model Coupling

This chapter presents a novel coupling of a simulation model and game theoretic solver to generate optimal strategies for strategic, cost-constrained decision-making. The game theoretic solver performs the optimization, calling the simulator as necessary to generate payoff values for a given defender-attacker pairs. The payoff values populate the game's payoff matrix. Solving the game using standard methods, the entire payoff matrix would be populated upfront, and the equilibrium value and strategies would be calculated by formulating and solving a linear or mixed-integer programming problem. Instead here the game is solved using fictitious play, a myopic iterative algorithm that can be executed without pre-populating the entire payoff matrix. Section 3.1 describes the general logic for the game, simulation, and the coupling of the two and Section 3.2 outlines the fictitious play algorithm.

3.1. MODEL LOGIC

Before the fictitious play algorithm commences, a comprehensive enumeration of attacker and defender strategies is generated and stored. A defender strategy is a unique permutation of safeguards where any number of safeguards can be active, and the parameters characterizing each safeguard above can take on a number of values from a discrete set of options. For an attacker strategy, only one attacker option is active, and this option is characterized by a set of parameters that can take on a discrete set of values.

The game modeled is a two-person zero-sum simultaneous play game. A two-person zero-sum game is used to model the interaction between two players with diametrically opposing goals—in this case, the attacker seeks to minimize the payoff and the defender seeks to maximize the payoff. In a simultaneous play game, both players have full knowledge of the strategy options available to the other player, but each player must commit to his strategy before observing what strategy the other player commits to. Note that this assumption about perfect knowledge represents a modeling idealization and simplification; in reality, it is unlikely that an

adversary would have perfect knowledge of the options available to the defender and their associated detection probabilities. While an over-simplification, this assumption is more realistic for insider adversaries, like a proliferant state, than for outsider adversaries because of their increased knowledge of security measures and operational procedures. Further, this assumption is, in most cases, a conservative one, as it finds the optimal defender strategies against a more informed and thus more capable adversary.

Figure 3-1 depicts a flowchart of the game model and its interaction with the simulator. Defender and attacker strategies are indexed by i and j, respectively, where $i \in [0, I]$ and $j \in [0, J]$. Pure attacker and defender strategies are denoted by y_j and x_i, respectively. The payoff for defender strategy x_i and attacker strategy y_j is v_{ij}. **x** is an I-element vector that holds the defender's mixed strategy history; the *ith* element of **x** is incremented when the defender plays pure strategy x_i, and the values in the vector are re-normalized such that the I elements in **x** sum to 1. **y** is the analogous attacker mixed strategy history. The strategies are generated and stored, and the fictitious play (FP) algorithm is then initiated by the attacker randomly choosing and playing pure strategy, y_j. The simulator is called and solves for the payoffs v_{ij} for all defender strategies x_i, given the attacker's strategy **y**, and these values are stored in the payoff matrix. Knowing the payoffs for all defender strategies that can be played in response to y_j, the defender then chooses the pure strategy response, x_i, that will maximize her payoff in the next round. After selecting the best response, the cost of the strategy is checked to see if the strategy is under budget. If so, the strategy is played and the defender's mixed strategy is updated. If not, the defender then picks her next best pure strategy response. The defender continues to pick her next best pure strategy response until she chooses one that she can afford. Once the defender has played a pure strategy within her budget, the variable v_{low} is set equal the value of v_{ij}, the payoff for the strategy pair. The game scans the payoff matrix to see if payoffs for the pure defender strategy have already been calculated. If not, the simulator is called and payoffs v_{ij} are calculated for all attacker strategies y_j. The attacker than chooses his best pure strategy response, v_{ij}, given the defender's current strategy history, **x.** The variable v_{low} is set equal to this payoff value. The attacker plays his pure strategy best response and his mixed strategy is updated accordingly. This constitutes one fictitious play loop; here the game checks to see if the number of iterations completed equals a user-defined maximum number of iterations or if convergence between v_{low}

and v_{up} has been achieved, signifying the approach to Nash equilibrium.[1] For this model, convergence is considered achieved when $(v_{up}-v_{low})/v_{up} < 0.001$. Then the mixed strategies **x** and **y** are the equilibrium defender and attacker strategies, respectively, and $v_{up} = v_{low} = v$, the equilibrium value of the game. If convergence is not yet achieved, control is returned to the FP loop.

Figure 3-2 details the logic flow for the simulation model. When calling the simulation, the game passes defender and attacker strategy information to the game. The simulation uses these inputs to create schedules of defender and attacker events for the course of the simulation period. The length of the simulation period is determined by the attacker strategy. It is assumed that the attacker always begins his malevolence on day 1 in simulation time, and he specifies the duration of the attack (unless the attack is a discrete, in which case it proceeds for only one day). The simulation period extends for a user-defined period of time after the end of the attack, providing the defender time to detect missing material and place the facility in an "alert state" [13]. For the results presented here, the extra detection time was set to thirty days to correspond to the IAEA timeliness goals for the detection of a significant quantity of HEU [30].

The first simulation day then begins by selecting the first safeguards and checking to see if that safeguard is active on day t=1, which is dictated by the defender strategy. If the safeguard is not active, control is returned to the safeguards loop and the next safeguard is checked. This continues until a safeguard that is active on day t is found, or until every safeguard has been determined to be inactive. Once an active safeguard is selected, a check is conducted to see if that safeguard is effective against the active attacker strategy. This information is stored in an array that contains information about which safeguards are effective against which attacker options. If the safeguard k is effective against attacker strategy y_j, the detection probability is calculated for the pair. Here k indexes across all safeguards, where $k \in [0, K]$. The algorithm used to calculate DP varies for each safeguard-attacker option pair; these algorithms are presented below in Section 4.4. Once the DP has been calculated, the payoff is calculated by weighting the DP by material quantity and attractiveness, as described in Section 4.7. This value is stored and control is returned to the safeguards loop for the next safeguard- attacker option

[1] Fictitious play converges to Nash equilibrium for all TPZSG [29]

payoff to be calculated. After the payoffs for all active safeguards on a given day have been calculated, this process is repeated for the next day and every subsequent day, until the simulation time has been exhausted. The cumulative DP for each day is the multiplicative sum of the DP from each safeguard. An overall scenario DP is calculated by combining the daily DPs, and scenario payoff is calculated by weighting the scenario DP by material quality and quantity. A detailed description of payoff functions used for calculation is given in Section 4.7.2. The scenario payoff value is returned to the game.

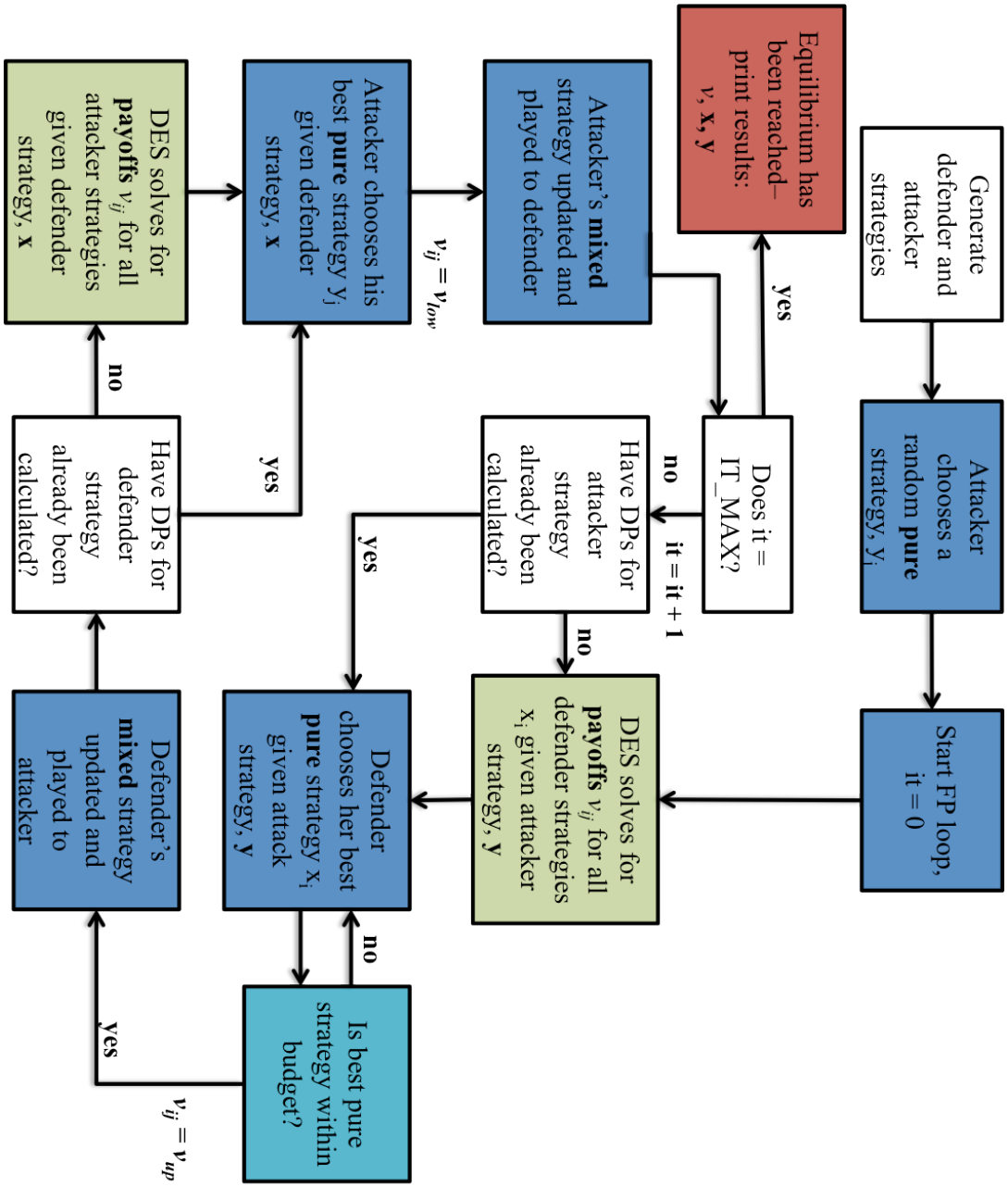

Figure 3-1. Fictitious play logic and interaction with simulator

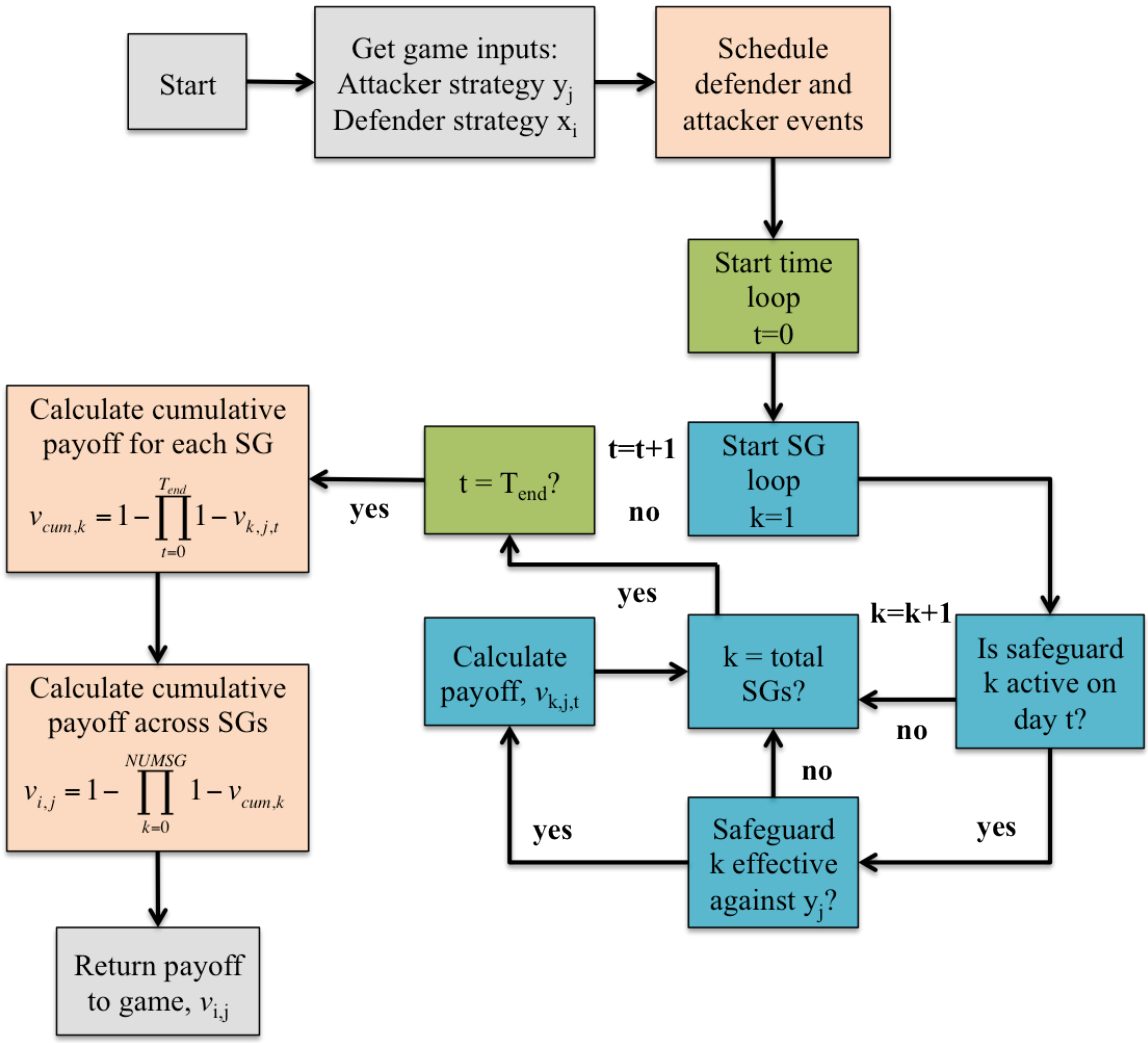

Figure 3-2. Simulation logic

3.2 FICTITIOUS PLAY

As mentioned above, the fictitious play algorithm was used to solve the game because of the computational benefits it offers over the linear programming approach. This section describes the theory behind fictitious play and the convergence to equilibrium.

3.2.1 Description

Fictitious play is a myopic learning algorithm first introduced by Brown for finding the value of a two-person zero-sum game (TPZSG) [31]. Fictitious play is an alternative to the Simplex method first introduced by von Neuman, and can be advantageous for large linear systems [32]. In the fictitious play (FP) process, each player assumes her opponent is playing a stationary strategy, and the two players engage in an iterative finite game. In each round a player chooses her myopic best response to the distribution of strategies played by her opponent up to that point; that is, she selects the response that will maximize her expected payoff in the next round of play. The process is said to converge to equilibrium as the payoff values approach the Nash equilibrium value of the game. Julia Robinson showed that all TPZSGs converge to the equilibrium value as the number of iterations approach infinity [29].

Take an TPZSG, $(x_i,y_j)_{mxn}$, with a maximizing row player and a minimizing column player.[2] In the first round, $k = 1$, the column player randomly selects a column, y_j^1, to play and the row player selects her pure best response, x_i^1.[3] Let V^k be an m-dimensional vector and U^k an n-dimensional vector. Define $V^1(i) = a_{i,j^1}$ to be the payoff to the row player for strategy x_i at $k = 1$. Similarly define $U^1(j) = a_{i^1,j}$ to be the payoff to the column player for strategy y_j at $k = 1$ in response to the row strategy x_i^1. At iteration $k = 2$, the column player will act myopically and play pure strategy y_j^2, such that it minimizes his payoff in this round, based on his opponent's current history.

$$y_j^2 \in argmin_j U^1(j), \tag{3.1}$$

The column player's cumulative payoff vector, U, should thus be updated as follows

[2] Mathematical description adapted from [33].

[3] Brown's original description of the FP process provided that the two players played in turn. Subsequent work often assumes the two players choose strategies simultaneously. In this work Brown's original formulation is assumed.

$$U^2(j) = U^1(j) + a_{i^2,j}. \tag{3.2}$$

The row player will then seek to maximize her payoff against the column player's current history and will play pure strategy x_i^2, such that

$$x_i^2 \in argmax_i \; V^1(i). \tag{3.3}$$

and update her payoff vector

$$V^2(x_i) = V^1(i) + a_{i,j^2}. \tag{3.4}$$

More generally, the row player and column player will continue to play strategies x_i^k and y_j^k, respectively, such that

$$\begin{aligned} x_i^k &\in argmax_i V^{k-1} \\ y_j^k &\in argmin_j U^{k-1}, \end{aligned} \tag{3.5}$$

and the payoff vectors will be updated

$$\begin{aligned} V^k(i) &= V^{k-1}(i) + a_{i,j^k} \\ U^k(j) &= U^{k-1}(j) + a_{i^k,j}. \end{aligned} \tag{3.6}$$

At any iteration k, the upper bound on the value of the game is given by the largest entry in the V payoff vector divided by the number of iterations, which gives a current average payoff to the row player.

$$v_{up} = max_i \frac{V^k(i)}{k} \tag{3.7}$$

Similarly, the lower bound on the game at iteration k is the smallest value in the U payoff matrix divided by the number of iterations.

$$v_{low} = min_j \frac{U^k(j)}{k} \tag{3.8}$$

The empirical mixed strategy for the row player at iteration k, denoted x^k, and by column player at iteration k, denoted y^k, are given by

$$x^k = \frac{1}{k} \sum_{\tau \leq k} e_{i_\tau} \tag{3.9}$$

$$y^k = \frac{1}{k}\sum_{\tau \le k} e_{y_\tau}$$

where τ is some iteration, and i_τ is the row strategy played at iteration τ. Here e_i represents a pure strategy played in round τ and is a vector whose only non-zero element is the *ith* element, which is 1. This mixed strategy represents a weighted average of all the pure strategies played over k iterations.

Julia Robinson proved that for TPZSGs, the upper and lower bounds on the value of the game given above converge to equilibrium as the number of iterations approach infinity, and that equilibrium value is the Nash equilibrium value for the game [29]. She showed that

$$\lim_{k\to\infty} \max \frac{V^k}{k} = \lim_{k\to\infty} \min \frac{U^k}{k} = v \tag{3.10}$$

where v is the value of the game. In the infinite limit, the empirical mixed strategies also approach the Nash equilibrium strategies for the game [33].

3.2.2 Convergence

The FP process for TPZSGs will converge to equilibrium, but the rate of convergence is slow [32]. Shapiro showed that for an *mxn* game the convergence order is at worst $O(k^{-1/(m+n-2)})$, and Szép and Forgó have conjectured that the actual convergence rate is $O(k^{-1/2})$, where k again represents the number of iterations [34], [35]. While these expressions describe the rate of convergence for a given number of iterations, more information is needed about the relationship between the accuracy of the approximation and number of iterations to enable the comparison of the computational speed of the FP algorithm and the simplex algorithm for a given game. For the game described above, define a residual, ϵ, by

$$\left| \max \frac{V^k}{k} - \min \frac{U^k}{k} \right| \le \epsilon \tag{3.11}$$

The residual is effectively the difference between the upper and lower bound values as they converge to the equilibrium value. For $\epsilon > 0$, it can be shown that (x^k, y^k) is an ϵ-approximate Nash equilibrium to the game, if the following condition on k is met [33]:

$$k \geq \left(\frac{R_{max}}{\epsilon}\right)^{\Omega(m+n)} \tag{3.12}$$

Where R_{max} is the largest entry in the payoff matrix, $R_{max} = max_{i,j}(|R_{ij}|)$, and m and n are the rows and columns of the payoff matrix, respectively. The big omega appearing in the exponent indicates that the exponent is bounded from below by the sum of the payoff matrix dimensions. This condition on k relates the accuracy of the approximation to the number of iterations, which is meaningful in the context of comparing the computational speed of the fictitious play algorithm to the Simplex algorithm.

Note that in this work, the convergence criterion used, denoted by ϵ, is related to but not the same as the residual introduce in Equation 3.11. The convergence criterion is calculated using Equation 3.13. Because of this non-trivial difference in definition, the ϵ value used for computation throughout this work cannot be substituted directly into Equation 3.12 to relate the accuracy of the approximation and the number of iterations required to achieve said accuracy.

$$\frac{\left|\max\frac{V^k}{k} - \min\frac{U^k}{k}\right|}{\max\frac{V^k}{k}} \leq \epsilon \tag{3.13}$$

For the purposes of this work, the fictitious play algorithm offered a significant computational advantage over the Simplex method because of how the algorithm was implemented. The explanation of the FP algorithm provided above assumes the existence of a populated payoff matrix A comprised of payoff entries $a_{i,j}$, with $i \in m$ and $j \in n$. Instead, in this work the payoff matrix was populated as needed by the algorithm. For example, if a the row player played strategy x_i, the payoffs $a_{i,j}$ for all j would then be calculated. Populating the matrix as rows and columns were played in the FP algorithm, rather than pre-populating the entire matrix, resulted in far fewer rows and columns being populated overall, as the players generally only played a very small fraction of the strategies available to them, which saved significant computation time because the calculation of each payoff value required a simulation call.[4] More

[4] The players in the reprocessing model played the largest percentage of the strategies available to them, with the attacker generally playing around 2-5% of his strategy options, and the defender playing less than 1% of her options. For both the enrichment and integrated models, the defender played at most 0.003% of her available options.

details on the practical implications and empirical results of this modified fictitious play algorithm are presented in Section 6.1.5.

Chapter 4: Enrichment Simulation

The game model serves as the optimizer in this model, but it relies on input from the simulator to populate the payoff matrix. This section details specific information about the enrichment simulation model, including defender and attacker options, how the detection probabilities and payoffs are calculated, and how budget resources are allocated.

4.1 Model GCEP Facility

A gas-centrifuge enrichment plant (GCEP) with an annual capacity of 465,000 kg-SWU is modeled. The plant uses natural uranium feed with ^{235}U enrichment of 0.711%, and enriches product to 4.5% ^{235}U, producing tails with 0.22% enrichment. Annual material throughput under normal operating conditions is shown in Table 4-I. The required number of IAEA samples based on current IAEA sampling algorithm is given in Table 4-II for reference purposes only; the number of NDA and DA samples performed by the defender in this model is determined by the strategy the defender selects. The third column of Table 4-I gives the number of each type of cylinder assumed to be in storage at any given time. It is assumed that approximately 84 days worth of feed is kept on site at all times, and that the operator is required to hold all product cylinders for a period of 28 days (at least one inspection cycle).[5]

Table 4-I. Annual throughput for 465,000 kg-SWU GCEP[6]

Material	Mass UF_6 (kgU)	Cylinders	Cylinders in Storage in Model
Feed	552 500	65	13
Product	63 390	41	3
Tails	489 200	57	---

[5] It is standard to keep 75 days worth of feed on-site; 84 is used here to simplify calculations (exactly 3 inspection cycles) [36]

[6] Calculated directly; calculations validated against enrichment calculator at uxc.com

Table 4-II. IAEA Sampling Plan[7]

Measurement		# of Samples
NDA & Weight	Feed	19
	Product	12
	Tails	18
	Total	48
DA & Weight	Feed	6
	Product	2
	Tails	15
	Total	22

4.2 ATTACKER OPTIONS

This section provides a qualitative description of each attacker option. These options fall into three major categories: (1) diversion of LEU; (2) enriching above declared levels; (3) undeclared LEU production.

Diversion of LEU:

1. Diversion of cylinder from storage:

The adversary diverts feed or product cylinders from storage in an abrupt, one-time diversion. The attacker selects the number of cylinders [1, 2, 3 cylinders], and whether to steal from the feed or product area. The type of material the attacker obtains depends on the area from which he steals—natural uranium from feed storage and LEU product storage.

2. Diversion of some feed/product from cylinder in storage:

The adversary removes a portion of the material from a feed or product cylinder, with no attempt to conceal the missing mass. The cylinder may be either sealed or unsealed, based on defender decision to apply a seal. This is a continuous diversion that can occur up to once a day. The attacker selects the frequency of attack [1 $days^{-1}$, 7 $days^{-1}$, 30 $days^{-1}$] and the duration of the attack [7 days, 30 days, 360 days], with the constraint that the attack duration must be equal to or greater than the frequency (e.g. the attacker cannot attack with a frequency of 30 days over a 7-day period). The attacker chooses the total material to divert over the course of the attack [40 kg, 110 kg, 775 kg], and the number of cylinders from which to take the material [1, 2, 3 cylinders].

[7] Number of samples calculated based on ratios presented in [37]

The goal material quantities were chosen such that the largest possible quantity aligns with IAEA significant quantity (SQ) goals: 775 kg of low-enriched UF_6 is a sufficient quantity such that if the attacker diverted it to a clandestine enrichment facility, it could be used to produce 25 kg of HEU. The 40 kg and 110 kg material goals were chosen to represent an attacker who wishes to employ a conservative, protracted strategy that may extend beyond the one-year time frame used in this model.

3. Diversion of some feed/product from cascade:

The adversary removes some gas that is in process into a 5A cylinder. The mass that is missing because of this diversion is distributed evenly among all the product cylinders in storage, such that each of the three cylinders is missing one-third of the total missing mass. This is a continuous diversion scenario that can occur up to once a day. The attacker selects the frequency [1 $days^{-1}$, 7 $days^{-1}$, 30 $days^{-1}$] and duration of the attack [7 days, 30 days, 360 days], as well as the number of cascades to attack [1, 6, 30 cascades], and the mass to remove from each cascade [0.010 kg, 0.100 kg]. As with the material theft from a cylinder, the cascades may or may not be sealed, based on the defender strategy.

Enriching above declared levels:

4. Cascade re-piping:

The adversary reconnects the cascade pipes to alter process flow and produce uranium enriched above declared levels. The re-piping is an abrupt, one-time event, but the misuse is continuous and is assumed to occur daily. The attacker selects the fraction of the cascades that are dedicated to the misuse [0.0167, 0.10, 0.50, corresponding to 1, 6, and 30 cascades, respectively] and the duration of the misuse [7 days, 30 days, 360 days]. The attacker also chooses the desired product enrichment [0.197, 0.50, 0.90]. It is assumed that declared feed material with enrichment 0.711% ^{235}U is used. The attacker stores over-enriched product in declared product storage and attempts to conceal it in plain site by adding lead shot to the cylinder, such that the cylinder's weight matches the weight of a full declared product cylinder. It is assumed that the lead shot does not line the entire interior surface of the cylinder, so the inspector is still able to obtain gamma spectroscopy information from the cylinder.

5. Recycling through cascade:

The adversary takes declared LEU product and recycles it though the cascade to produce enrichments higher than declared. This is a continuous misuse. As with cascade re-piping, the attacker selects the size of the misuse [1, 6, 30 cascades] and the duration of the misuse [7 days, 30 days, 360 days]. For this scenario the attacker also specifies the frequency of attack [1 $days^{-1}$, 7 $days^{-1}$, 30 $days^{-1}$], and the desired product enrichment [0.197, 0.50, 0.90]. It is assumed that the feed material is the declared product with an enrichment of 4.5% ^{235}U. As with re-piping the cascades, the attacker conceals the over-enriched product in plain site by using lead shot to falsify the weight of the product cylinder. The attack uses this same method to conceal the missing product mass that has been used as feed material for cascade recycle. Thus in this scenario, there are three cylinders in product storage, as explained in Section 4.1 and all three cylinders have masses consistent with a nominal full product cylinder: one is a full, declared product cylinder; one contains over-enriched product and lead shot; and one is a cylinder of declared product material and lead shot.

Undeclared LEU Production:

6. Introduction of undeclared feed for production of undeclared product:

The attacker introduces undeclared feed into the cascade to produce undeclared product material with declared product enrichment. This is a continuous diversion that can happen up to once per day. The attacker selects the frequency [1 $days^{-1}$, 7 $days^{-1}$, 30 $days^{-1}$] and duration [7 days, 30 days, 360 days] of the attack, the number of the cascades dedicated to the misuse [1, 6, 30 cascades]. It is assumed that the undeclared product material is stored in a secret location, possibly off-site, that is not inspected during basic or special inspections.

4.3 DEFENDER OPTIONS

This section provides information about the implementation of defender options in the enrichment model. For a more detailed description of how the safeguards are implemented by the IAEA, see Appendix A: IAEA Gas-Centrifuge Enrichment Plant Safeguards. The detection probability calculation algorithms presented in this section and in Section 4.4 are notional, albeit representative. An effort was made to accurately capture the relative effect of different defender

and attacker parameters on DP (i.e. stealing larger quantities of material is more likely to be detected than stealing smaller quantities of material); however, the values are not necessarily accurate in an absolute sense.

Detector-Type Safeguards

Several of the safeguards for the enrichment and reprocessing facilities employ detectors to check for anomalies. These safeguards are modeled as "detector-type" safeguards, meaning the readings are assumed to follow a Gaussian distribution with standard deviation s_n about some mean *n*. The detection probability for these safeguards is modeled using a standard receiver-operator curve (ROC), which characterizes the relationship between the probability of registering a true positive result (detection probability) and the probability of registering a false positive result (false alarm probability). For each detector-type safeguard, there is some threshold reading *t* above or below which the detector will alarm. The detector alarms above this value in situations like NDA at an enrichment facility, where counts above the threshold might indicate higher-than-declared enrichment, and it alarms below the threshold for safeguards like mass balance, where a lower reading indicates missing material. The threshold value is calculated using Equation 4.1.

$$t = n + \sqrt{2} \cdot s_n \text{erf}^{-1}(1 - 2FAP) \tag{4.1}$$

Where *t* is the threshold weight, *n* is the nominal reading, s_n is the standard deviation of the nominal reading, and FAP is the false alarm probability, which is selected by the defender in some cases and held constant in other cases. The detection probability for a mass reading is found by integrating the cumulative distribution function for the Gaussian distribution from the threshold to positive infinity, resulting in Equation 4.2. A thorough derivation of Equations 4.1 and 4.2 is given in [38].

$$DP = 1 - {}^{1}/_{2}\left(1 + \text{erf}\left(\frac{t - s}{\sqrt{2} \cdot s_s}\right)\right) \tag{4.2}$$

Where *s* is the observed signal and s_s is the standard deviation of that reading. Note that these equations are for situations where the detector alarms for readings above threshold; for situations

where readings below threshold trigger an alarm the equations take the same form with a sign difference. For many of the detector-type safeguards, the error in the reading is due to sources of systematic and random uncertainty, which are generally expressed as relative uncertainties (relative to the mean reading). The total uncertainty is thus calculated using Equation 4.3.

$$s_{s_{rel}} = \sqrt{{s_{s_{sys}}}^2 + {s_{s_{ran}}}^2} \tag{4.3}$$

Where $s_{s_{sys}}$ is the systematic uncertainty and $s_{s_{ran}}$ is the random uncertainty. The standard deviation is then calculating by multiplying the total relative uncertainty by the reading, as shown in Equation 4.4.

$$s_s = s_{s_{rel}} \cdot s \tag{4.4}$$

Certain safeguards that detect radiation are treated as a special sub-class of the detector-type safeguard. Because radioactive decay is a Poisson process, a Poisson distribution is assumed for counts in these detector-type safeguards, meaning the variance of the signal equals the mean, as shown in Equation 4.5. This assumption is used for radiation-based detectors for which uncertainties information is not available, such as CEMO.

$${s_n}^2 = n \tag{4.5}$$

Cumulative Sum Calculation

For some of the defender options, like seals, the defender inspects multiple items and there is a non-zero probability of detecting a violation for each item. In other instances, like taking physical inventory, the inspector has some probability of detecting a violation at each inspection. In both cases, these discrete detection probabilities can be combined into an overall detection probability using a cumulative sum calculation. Equation 4.6 gives the formula for the cumulative sum, where DP_i is an individual event DP or item DP, and *N* is the total number of individual DPs.

$$DP_{cum} = 1 - \prod_{i=0}^{N} DP_i \tag{4.6}$$

A. Inspection

A general inspection is comprised of three components: physical inventory- item counting, mass balance verification, and examination of logged video surveillance images. Additional safeguarding measures can be added on to the general inspection—namely passive seal verification, non-destructive assay samples, and destructive assay samples. These additional verification activities can be done as frequently as or less frequently than random inspections, but cannot be done more frequently. Details of the three staple inspection activities are presented below.

Physical Inventory- Item Counting

Because physical inventory is a checking operation conducted by humans, it is susceptible to human error. In their human reliability analysis work, Swain and Guttman seek to mathematically model this behavior [39]. A key concept from their analysis is dependency, a term coined to describe the following phenomenon: if a person conducts a checking operation on day t with probability P of detecting an anomaly, and the person fails to detect the anomaly, the probability that said anomaly will be detected on day $t+1$ is less than P, and the amount by which the probability decreases depends on the *dependency*, that is the extent to which subsequent checking operations are dependent on previous results. For a detailed description of dependency and related human reliability concepts, see Section 2.4.

The detection probability developed in this work for a person or team of persons conducting physical inventory draws on the human reliability concept described above and a model from the financial auditing sector. In their work on allocating audit resources to detect fraud in the business sector, Newman et al. present a model for the detection probability in the case of fraud or theft.[8] The model takes the form of Equation 4.7, given below, with the DP varying exponentially with the size of the theft and the audit resources dedicated to detecting the theft [40]. In the case of diverting product cylinders from storage, the size of the theft is the

[8] The paper addresses the case of fraud, but notes that the difference between a theft detection and fraud detection model is that the former is described by simultaneous play, while the latter is described by sequential play. Thus the detection probability relationship presented for fraud detection is used here for theft detection.

number of cylinders diverted (n), and the resources dedicated to detecting theft is the size of the team conducting the inventory (characterized by the team factor- F_{team}). The constant in the exponent in Equation 4.7was calculated empirically such that for the theft of one cylinder and a medium-sized detection team, the detection probability equals 0.99. This value is taken from Swain and Guttman's work on baseline human error probabilities (BHEP), in which they establish the BHEP for inventory auditing as 0.01, making the detection probability 0.99 [39]. Thus the constant in Equation 4.7 was chosen such that in the base scenario, the DP is 0.99, and the DP increases with inspection effort (larger inspection team) and the number of cylinders stolen.

$$DP = 1 - exp(-0.65 * (F_{team} + 1) * n) \tag{4.7}$$

where F_{team} is the team factor and n is the number of cylinders. F_{team} takes a value of 1 for a small team and a value of 19 for a large team. Note the team factor is a mathematical construction and is related to the size of the team, but does not *equal* the size of the team (i.e. F_{team} of 19 does not imply a 19-person team, but a large team).

Equation 4.8 gives the degradation of the detection probability for inspection event i, given that the anomaly was not detected at inspection event $i-1$.

$$DP_i|ND_{i-1} = 1 - \frac{1 + F_{team} \cdot ND_{i-1}}{F_{team} + 1} \tag{4.8}$$

Mass Balance Verification

During routine visits inspectors do a mass balance verification to verify material flow. Cylinder masses are obtained using the load cell based weighing system (LCBS). The masses and dimensions of the two relevant cylinder types—30B (product) and 48Y (feed/tails) are given in Table 4-III. Figures from different sources are compiled in the table, and the values vary slightly. The empty cylinder weights from Areva and max UF_6 weights from Eccleston were used for calculations. Readings from the LCBS have less than 1% error [41].

Table 4-III. Enrichment cylinder specifications

Cylinder	Purpose	Empty Weight (lbs)[a]	Max UF_6 Weight (lbs)[c]	Max UF_6 Weight (kg)[b]	Max Weight (kgU)[b]	Diameter (cm)	Wall thickness (cm)
30B	Product	6 420	5 020	2 270	1 540	76	1.27
48Y	Feed/ Tails	32 761	27 560	12 500	8 450	122	

[a] [42]
[b] [43]
[c] all data not explicitly cited from [44]

The LCBS is modeled as a detector-type safeguard, as described above, with a systematic uncertainty of 0.05% and a random uncertainty of 0.05% [45]. Combining these uncertainties using Equation 4.3 gives a total relative uncertainty of 0.07%. If that attacker removes some mass, Δm, from a full cylinder, the detection probability is given by:

$$DP = 1 - {}^{1}/_{2}\left(1 - \mathrm{erf}\left(\frac{t - (n - \Delta m)}{\sqrt{2} \cdot 0.0007 \cdot (n - \Delta m)}\right)\right) \tag{4.9}$$

Video Surveillance- logged images

Distributed video surveillance systems are used for security applications in a number of sectors, including transportation. Sacchi and Regazzoni describe the use of a distributed video surveillance system to identify abandoned objects in a waiting room at an unattended railways station [46]. This situation is analogous to a storage yard at a GCEP, where very little change in background is expected. Sacchi and Regazzoni present experimental data for the probability that the video surveillance system will correctly locate and classify an abandoned object or person. The paper reports this probability as 0.86 for a person [46]. The value for a person was used in this work, as a person moving into or out of a storage yard without proper authorization would trigger alarm at a GCEP.

Detecting an incident by video surveillance actually includes two actions: sensing and assessment [47]. Sensing is the technical ability of the video equipment to react to a stimulus and register an alarm, while assessment is the determination by a human as to whether the alarm

is due to an attack or a nuisance alarm [47]. Probability of sensing and probability of assessment are related to DP as shown in Equation 4.10.

$$DP = P_S \cdot P_A \tag{4.10}$$

Based on the information described above, a sensing probability of 0.85 was assigned for material diversion from a storage yard under surveillance. An assessment probability of 0.50 was assumed for logged image that must be manually checked by an inspector during an inspection. This value was invented to reflect the large space for human error in such an operation, and is meant to have value relative to the higher assessment probability assigned to transmitted video. Inserting values provided above into Equation 4.10, a detection probability of 0.43 is used for logged video.

B. Passive Seals

Two types of seals used by the IAEA are considered in this model: CAPS and VACOSS. CAPS are passive metallic seals that are used to seal material containers. They are removed by inspectors during inspections and sent to headquarters for post-mortem analysis to verify their integrity. Inspectors then apply new seals. These seals are one-time use items, are relatively inexpensive, and can be attached and detached quickly by inspectors during inspections [41].

The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory has conducted numerous tests on both active and passive seals, attempting to defeat the seals [48]-[50]. Defeat is defined as breaking the seal to gain access to the asset it protects, and then replacing or duplicating the seal such that evidence of tampering cannot be detected. The VAT was consistently able to defeat 100% of the seals it tested, categorizing defeat into four categories: 1) tampering will not be detected with usual inspection process, but will be detected if unusual efforts are made (i.e. seal is disassembled and examined); 2a) tampering will not be detected if the inspector follows usual protocol and visually inspects the exterior of the seal in detail; 2b) tampering will not be detected if the inspector follows usual protocol and if the inspector disassembles the seal and examines it in meticulous detail and 3) tampering will not be detected by even advanced post-mortem analysis. The tests indicate that the sophistication and cost of the seal do not correlate well with difficulty of defeat or time required to defeat the seal;

in fact, Roger Johnston, the lead author, notes that in many cases sophisticated, active seals are actually easier to defeat because they must transmit information from the seal itself to some information center [49]. In a 2002 study, the VAT tested 198 seals—192 passive seals and 6 active seals—and defeated the seals with 289 attacks, defeating each seal at least once. The results of this test indicated that of the attacks perpetrated against the seals, 15% are type 3 defeats and approximately 45% were type 2b defeats [49].

Because material cylinders are sealed with CAPS, which are verified using post-mortem analysis, only type 3 defeats are considered successful in the context of material theft from a cylinder. Thus the detection probability for passive seals is 0.85.

C. Non-Destructive Assay

Non-destructive assay is done on feed and product cylinders to verify the assay of the contents. In this work, only NDA measurements on product cylinders are considered. Typical NDA measurements are taken at the surface of the cylinder using a handheld gamma ray spectrometer to count the 186-keV peak. Standard count times range from 300-1000 seconds [51]. The error associated with these measurements is given in Table 4-IV [45]. The last column of Table 4-IV gives the total relative error, as calculated using Equation 4.3.

Table 4-IV. Errors associated with NDA measurements

Material Type	Random Error	Systematic Error	Relative Error
NU (Feed)	0.10	0.08	0.13
LEU (Product)	0.04	0.02	0.04

The approximate count rate at the surface of a uranium cylinder can be calculated using Equation 4.11 [52]. Table 4-V defines each variable and provides the value used in the calculation, as well as references and notes for the values, when necessary. The values shown are for a product cylinder; the enrichment and count rate differ for a feed cylinder.

$$R = E_w \frac{\epsilon S A}{\mu_u} \exp\left(-\mu_c \rho_c t_c\right) \tag{4.11}$$

Table 4-V. Variable definitions and values for NDA count rate calculation

Variable	Definition	Nominal Value	Note
R [counts/s]	count rate	25	
x_p [weight fct ^{235}U]	enrichment	0.045	
$\boldsymbol{\epsilon}$ [counts/gamma]	detector efficiency at 186 keV	0.10	1
S [gamma/s-g]	specific intensity	4.3×10^4	2
A [cm^2]	collimator area	0.56	3
$\boldsymbol{\mu_u}$ [cm^2/g]	uranium mass attenuation coefficient	1.06	4
$\boldsymbol{\mu_c}$ [cm^2/g]	steel container mass attenuation coefficient	0.144	2
$\boldsymbol{\rho_c}$	steel container density	7.8	2
t_c [cm]	container thickness	1.27	2

1- [53]
2- [52]
3- The collimator slit is 56 mm; a slit thickness of 1 mm was assumed, resulting in a slit area of 56 mm^2 [54]
4- The mean free path for solid UF_6 is 0.20 cm, and the density of solid UF_6 is 4.7 g/cm^3. The mean free path is equal to $1/\mu\rho$. From this information, μ_u was calculated for solid UF_6 [52]. The value for solid UF_6 is valid for NDA on feed cylinders, as they contain solid material, but may or may not be a good approximation for product cylinders, based on the state of the material.

Based on this calculation, the average count rate due to ^{235}U at the surface of a cylinder is 25 cps for a product cylinder. In addition to counts from ^{235}U gamma emission, there are also counts in the 186-keV energy region from Compton scattering of higher energy photons. The higher energy photons are emitted by ^{238}U and by ^{238}U daughter products, whose abundances vary based on the age of the cylinder, as some material adheres to the cylinder walls and then decays over time. The peak-to-background ratio in this region is about 0.2 to 0.5 cps [55]. Thus the average total count rate in the 186-keV region is 88 cps for a product cylinder.

The detection probability for NDA on product cylinders is similar conceptually to the DP for mass balance. The standard deviation for the nominal product signal is related to the relative uncertainties displayed in Table IV and is given in Equation 4.12. Equation 4.13 gives the DP.

$$s_{n_{LEU}} = 0.04 \cdot n_{LEU} \tag{4.12}$$

$$DP = 1 - 1/2\left(1 - \operatorname{erf}\left(\frac{t - \left(\frac{x_p}{4.5} \cdot n_{LEU}\right)}{\sqrt{2} \cdot 0.04 \cdot \left(\frac{x_p}{4.5} \cdot n_{LEU}\right)}\right)\right) \tag{4.13}$$

D. Destructive Assay

Destructive analysis is performed on select samples using highly sensitive mass spectrometry techniques to obtain a detailed and accurate analysis of the material composition. Because this analysis is performed over an extended period of time at an off-site location with highly sensitive tools, it is assumed that it will positively identify the true isotopics of a material with a probability of one. Destructive analysis is thus a form of attribute sampling. Avenhaus and Canty liken attribute sampling to "distinguishing between lads and lasses"; that is, if the inspector takes a DA sample from a cylinder that the attacker has filled with material enriched above declared levels, she will know for certain [22].

The probability that the inspector will select a "falsified" cylinder for DA sampling depends on the number of cylinders in storage, the number of cylinders sampled, and the number of falsified cylinders. Because it is assumed that once the inspector takes a sample from a cylinder, she will not sample from that same cylinder a second time during that inspection, this situation can be modeled by the hypergeometric distribution, which describes sampling without replacement.

Here this safeguard is only applicable to attacker strategies where the attacker is enriching to above declared levels. The DP approach assumes that the illicit product is stored in one cylinder among N total cylinders in the storage area. Equation 4.14 gives the detection probability for DA sampling. The number of cylinders in storage, N, is 3 under normal operating conditions, as stated in Section 4.1.

$$DP = 1 - \frac{\binom{N-n}{k}}{\binom{N}{k}} \tag{4.14}$$

where
N = number of cylinders in storage
n = 1, number of cylinders falsified
k = number of cylinders sampled

E. Video Surveillance- remote transmission

As in the case with logged surveillance images, the probability of sensing using video surveillance is 0.85; however, unlike in the previous scenario, the probability of assessment is

higher, due to the automatic transmission of the image when an anomaly is observed. Assuming large amounts of data are transmitted daily to the assessors at headquarters, such that analyzing all data in great detail is a cumbersome task for a human, an assessment probability of 0.75 was assigned. Thus by Equation 4.10, the baseline DP for a cylinder diversion from a storage yard is 0.64.

F. Active Seals

VACOSS seals are active fiber optic and electronic seals used to secure valves and piping at enrichment facilities. These seals are looped around the item they secure, and a light pulse is sent through the loop every 250 ms. Information about any opening or closing of the loop is stored in the seal. VACOSS seals can be verified in situ by inspectors or can be used for remote monitoring to transmit information about a tampering incident to the IAEA [41]. In contrast to the passive seals described above, these active seals are relatively expensive, but can be used multiple times. The batteries must be replaced every two years.

VACOSS seals are used to seal pipes and valves, and can be used to detect cascade re-piping or altering a valve setting to remove material directly from the cascade. It is assumed that the seals transmit information about tampering to an off-site assessment team in real time. The seals can be defeated by a type 2b or type 3 attack (described in Section 4.3). Thus the total defeat probability is 0.60, resulting in a baseline DP of 0.40 for detecting material theft from the cascade or cascade re-piping with an active seal. It is further assumed that active seals have only one opportunity to detect tampering with the pipes. If a seal is broken and detection does not occur, the defender does not replace the seal because she does not know it has been tampered with, so no further detection opportunities exist.

G. Continuous Enrichment Monitor (CEMO)

Currently CEMO monitors are designed to be attached to the low-pressure portion of the feeder pipe, with pressures under 10 torr. The count rate in the detector is directly proportional to the enrichment and pressure of the material flowing through the pipes. Table 4-VI gives experimental data collected using the CHEM system, which should have count rates very similar to the CEMO system, except that the detector was attached to the high-pressure portion of the

pipe [56]. Using this data and accounting for the over five-fold difference in pressure, the nominal count rate for 186-keV gammas entering the NaI detector of a CEMO unit can be estimated at around 8 cps (at 10 torr). Because the pressure is actually lower than 10 torr on the low-pressure side of the pipe, a count rate of 5 cps was used in calculations. The standard counting time for CEMO is 2.5 hours [56].

Table 4-VI. CHEM Experimental Data

Enrichment	Pressure	Counts
3.3%	50 torr	28 cps
4.5%	50 torr	38 cps

If the gas in the pipes is enriched to levels above the declared level, there will be a greater concentration of ^{235}U, meaning there will be stronger emission of the 186-keV gamma (relative to standard operating conditions). CEMO is modeled as a detector-type safeguard that will alarm if the reading is above the threshold (too much ^{235}U). However, an important characteristic of the CEMO operating system is that it is a go/no-go measure, meaning it is designed only to confirm the absence of material enriched above 20%. Thus the DP for material enriched to levels above the declared level but below 20% is zero. The DP for material enriched above 20% can be calculated using Equations 4.17 and (4.18, with the values for *n* and *s*, given in Equations 4.15 and 4.16 respectively. CEMO is modeled as a radiation-based detector-type safeguard, as described in Section 4.3, with the variance equaling the mean.

$$n = r_n \cdot t_c \tag{4.15}$$

$$s = \frac{x_p}{4.5} \cdot n \tag{4.16}$$

$$t = r_n \cdot t_c + \sqrt{2} \cdot s_n \mathrm{erf}^{-1}(2FAP - 1) \tag{4.17}$$

$$DP = 1 - {}^{1}/_{2}\left(1 - \mathrm{erf}\left(\frac{t - \left(\frac{x_p}{4.5} \cdot n\right)}{\sqrt{2 \cdot \left(\frac{x_p}{4.5} \cdot n\right)}}\right)\right) \tag{4.18}$$

Where r_n is the 186-keV count rate in the detection under normal conditions (5 cps), t_C [s] is the count time, and x_p [$\%^{235}$U] is the product enrichment under anomalous conditions.

H. Visual Inspection

During special inspections, inspectors do a visual inspection of the facility to detect anomalies, including examining inside cascade halls and performing design information verification to ensure that the settings on valves and pipes match design specifications. Inspectors are given access to the cascade hall only during special inspections, not during regular inspections, making this type of inspection intrusive and disruptive from the operator's perspective. Accordingly special inspections are performed less frequently than regular inspections. For this activity, the detection probability depends on the ability of a person to search a visual field and pick out a specific, anomalous feature. An analogous activity is inspecting ships for fractures before they go to sea, a topic that has been studied in the literature. In his work on visual inspection of ships, Demsetz conducts in situ experiments to determine an experienced inspector's ability to detect both critical and non-critical fractures. He concludes that the average detection probability for a critical fracture is about 0.60, while the average detection probability for a non-critical fracture is 0.29 [57]. Based on this work, a value of 0.60 is used here as the DP for major anomalies, like those that may exist during a misuse scenario in the cascade hall. A DP of 0.29 is used for minor indicators, like those that might exist from repeated material diversion from a cylinder in storage. Visual inspections are capable of detecting a diversion or misuse only if the diversion or misuse is ongoing at the time of the inspection. It is assumed that once a diversion has concluded, the attacker carefully conceals any signs that such a diversion occurred. For this reason visual inspection is not effective against cylinder theft, because cylinder theft is a one-time event that occurs on the first day of the simulation.

I. Environmental Sampling (ES)

The analysis procedure for environmental sampling is identical to that of destructive analysis; the key difference between these two techniques is the sampling procedure. Environmental samples are taken on small cotton swipes, so the amount of detectable material is

often lower than for a DA sample. Additionally ES is only undertaken during special inspections, and the swipes are taken inside the cascade hall, offering a wealth of information about plant processes. Here it is assumed that if the inspector swipes around one of the cascades that is being used for illicit material production after the misuse has begun, the detection probability is 1.[9] As with DA, the hypergeometric distribution is used to calculate the DP. The hypergeometric distribution is given in Equation 4.14, where here N is the total number of cascades [60], n is the number of cascades dedicated to misuse [1, 6, 30 cascades], and k is the number of swipes taken [6, 12 swipes].

4.4 Detection Probability Calculations

The specific formulations used to calculate DPs for each defender/attacker option are presented below, along with payoff information. Table 4-VII provides an overview of which safeguards are effective against which attacker strategies. The numbers correspond to the attacker strategy numbers presented in Section 4.2 Attacker Options and the letters correspond to defender options in Section 4.3 Defender Options. The yellow shading for safeguards H (visual inspection) and I (ES) serves as a reminder that these safeguards occur only during special inspections, not continuously or during routine inspections like all other safeguards. A description of each attacker pair is provided along with a derivation of the algorithm used to calculate the DP for the pair. The information for each pair is compiled in summary tables beneath the descriptions to serve as a clear, comprehensive reference for each strategy pair. The Figure of Merit (FOM) used to quantify the attractiveness of material obtained in the scenario is provided under the heading "Payoff" in the summary tables.

[9] In reality ES can theoretically detect misuse anywhere in the facility, but this ability depends on the effort the proliferators dedicate to concealing UF_6 gas emissions. The stated assumption above serves as a proxy for modest proliferator efforts to contain gas emissions.

Table 4-VII. Defender-attacker strategy pair summary table for enrichment facility

Defender Options	Attacker Options					
Activity	1	2	3	4	5	6
A	A1	A2	A3			A6
B		B2				
C				C4	C5	
D				D4	D5	
E	E1	E2				
F			F3	F4		
G				G4	G5	
H			H3	H4	H5	H6
I				I5	I6	

Defender Options:

A. Inspection
B. Passive seals
C. Non-destructive analysis (NDA)
D. Destructive analysis (DA)
E. Video surveillance- remote transmission
F. Active seals
G. Continuous Enrichment Monitoring (CEMO)
H. Visual inspection
I. Environmental Sampling (ES)

Attacker Options:

1. Diversion of cylinder from storage
2. Diversion of some material from cylinder in storage
3. Diversion of some material from cascade
4. Cascade re-piping
5. Cascade recycling
6. Undeclared production from undeclared feed

4.4.1 Inspection DP Calculations

A1. Cylinder diversion from storage detected by inspection

Inventory

The inspector can detect cylinders during any inspection over the course of the residence period. Once the residency period has expired, it is assumed that new cylinders are brought into the storage area and the inspector no longer has the opportunity to detect missing cylinders. The initial DP is determined by the number of cylinders diverted, as described in Equation 4.7 in Section 4.3, and the per-inspection DP is calculated using human reliability techniques described in Equation 4.8. The extent to which the DP decreases per inspection is determined by the size of the inspection team.

Mass Balance Verification

Mass balance verification is not an effective means to detect the diversion of a cylinder from storage; thus the $DP_{mb} = 0$.

Video Surveillance- logged images

The inspector can detect an attack using logged video only in the first inspection after the attack has occurred, because it is assumed that at each inspection she watches only video from the previous period. Because cylinder diversion is a discrete, one-time act, the defender thus has only one opportunity to detect the attack. The DP_{vl} is 0.43.

Total Inspection Probability

The total inspection probability on each day is the cumulative sum of DP_{inv}, DP_{mb}, and DP_{vl}. This probability can be calculated using Equation 4.19.

$$DP_{insp} = 1 - (1 - DP_{inv}) * (1 - DP_{mb}) * (1 - DP_{vl}) \quad (4.19)$$

DP_{insp}	$DP_{inv,i=1} = 1 - exp(-0.65 * (F_{team} + 1) * n)$ $DP_{inv,i} \mid ND_{i-1} = 1 - \frac{1 + F_{team} \cdot ND_{i-1}}{F_{team} + 1}$ $DP_{vl} = 0.43$ $DP_{insp} = 1 - (1 - DP_{inv}) * (1 - DP_{mb}) * (1 - DP_{vl})$	per inspection event
Defender Parameters		
F_{team}	size of inspection team, F_{team} = {1,19}	
f	inspection frequency, f= {7 days^{-1}, 28 days^{-1}}	
Attacker Parameters		
n	number of cylinders stolen, n = {1,2}	
Payoff		
NU	0.033	
LEU	0.1	

A2. Diversion of some material from cylinder detected by inspection

Inventory

Inventory is not effective against this type of diversion, as no items are missing, so $DP_{inv} = 0$.

Mass Balance Verification

Based on the model enrichment plant specifications (see Section 4.1 Model GCEP Facility for more details), under normal operating conditions the facility should use 65 feed cylinders annually and produce 41 product cylinders annually. For this work, it is assumed that there are always 13 feed cylinders and three product cylinders present in storage. The 13 feed cylinders contain enough material to operate the facility for 84 days, and a product residency time of 28 days was assumed to calculate the number of product cylinders in storage. It is assumed that the three cylinders live in product storage for the entire residence period specified, and then are replaced by new, full cylinders after that period. If the attacker attacks multiple times during the 28-day periods, he removes materials from the same cylinders, and the missing mass is cumulative. It is further assumed that the mass balance periods coincide with the residence periods, so after 28 days, the books reset and any previous mass discrepancy is forgotten. The inspector weighs every product and feed cylinder at every inspection. The amount of material taken per cylinder per attack event, j, is given by Equation 4.20.

$$\Delta m_{cyl,j} = \frac{\Delta \mathrm{m}}{totevents \cdot n} \tag{4.20}$$

Where $\Delta m_{cyl,j}$ is the mass missing per cylinder per inspection, Δm is the total mass taken during course of entire attack scenario, $totevents$ is the total number of attacker events during course of entire scenario, and *n* is the number of cylinders from which material is taken. The total number of events over the course of the entire simulation is calculated using Equation 4.21, where *T* is attack duration and f_{attack} is attack frequency.

$$totevents = \left\lceil \frac{T}{f_{attack}} \right\rceil \tag{4.21}$$

The mass missing from a cylinder at the *ith* inspection during a residence period is given in Equation 4.22. The *i*-index and *events* reset after each 84 or 28-day residence period concludes.

$$\Delta m_{cyl,i} = \Delta m_{cyl,j} \cdot events \tag{4.22}$$

Where $\Delta m_{total,i}$ is the mass missing from each cylinder at the *ith* inspection in a residence period and $events$ is the attacker events to date during current residence period.

The detection probability for *each cylinder* attacked is given below in the summary table as DP_{cyl}. The DPs for each cylinder from which mass has been removed are assumed to be independent. The total probability for *each inspection event* is given by DP_{insp}. This probability is calculated as the cumulative sum of the individual cylinder DPs, using a formula analogous to Equation 4.19. When the attacker opts to attack only one cylinder, the cylinder DP and inspection DP are equal. When he attacks two or three cylinders, the inspection DP is greater than the cylinder DP.

Values for the weight of full 48Y feed cylinders and 30B product cylinders are given in Table 4-VIII. These values are used to calculate the threshold weights in the DP calculation. Note that these weights include the mass of material and the mass for the cylinders themselves. The threshold weights given below are for a FAP = 0.01.

Table 4-VIII. Nominal weights and alarm thresholds for uranium cylinders

Cylinder Type	Cylinder	Nominal weight, *nom* (kg)	Threshold weight, *t* (kg)
Feed	48Y	27 360	27 315
Product	30B	5 180	5 172

Video Surveillance- logged images

To steal some material from a cylinder in storage, the adversary must enter the storage yard, which is under video surveillance. The DP for detecting a diversion from logged video surveillance decreases over the course of the simulation due to human reliability factors, as described previously. The DP for detecting *one attack event* at inspection *i*, DP_i, is given by Equation 4.8, where the initial DP is 0.43. However, this scenario is a continuous diversion, meaning the attacker will repeatedly enter the storage yard with some frequency of his choosing. Depending on the attack and inspection frequency, multiple attacks may occur between inspections, meaning the inspector has multiple detection opportunities at a single inspection when viewing the surveillance log. The total DP at inspection *i*, $DP_{insp,i}$, is the cumulative sum of DP_i over all of the attack events that have occurred since inspection *i-1*. This calculation is shown in Equation 4.23.

$$DP_{insp-vl,i} = 1 - (1 - DP_i)^{btevents} \tag{4.23}$$

where $btevents$ is the number of events since the last inspection. Note that the degradation in DP that occurs due to human reliability analysis is performed on the per-event DP, DP_i, not the total DP.

Total Inspection Probability

The total inspection detection probability is given by Equation 4.19.

A3. Diversion of some material from cascade detected by inspection

DP	$t = n + \sqrt{2} \cdot s_n \mathrm{erf}^{-1}(2FAP - 1)$ $DP_{cyl} = 1 - {}^1/_2\left(1 - \mathrm{erf}\left(\frac{t - (nom - \Delta m_{cyl,i})}{\sqrt{2} \cdot 0.0007 \cdot (nom - \Delta m_{cyl,i})}\right)\right)$ $DP_{insp-mb} = 1 - (1 - DP_{cyl})^n$ $DP_{vl-i=0} = 0.43$ $DP_{insp-vl,i} = 1 - \left(\frac{1 + F_{team} \cdot ND_{i-1}}{F_{team} + 1}\right)^{btevents}$ $DP_{insp} = 1 - (1 - DP_{inv}) * (1 - DP_{mb}) * (1 - DP_{vl})$	per inspection event per cylinder per inspection event
Defender Parameters		
FAP	false alarm probability, FAP = {0.01,0.001}	
F_{team}	team factor, F_{team} = {1,19}	
f	frequency, *f* = {7 days^{-1}, 30 days^{-1}}	
Attacker Parameters		
T	attack duration, T = {7 days, 30 days, 360 days}	
f	frequency, *f* = {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
Δm	total mass removed over entire attack scenario, Δm = {40, 110, 775 kg}	
n	number of cylinders from which some material is removed, n = {1,2,3}	
area	storage area from which cylinder is taken, *area* = {feed, product}	
Payoff		
NU	0.033	
LEU	0.1	

Inventory

Inventory is not effective against this type of diversion, as no items are missing, so $DP_{inv} = 0$.

Mass Balance Verification

As with the diversion of some material from a cylinder, it is assumed that the mass balance period over which mass balance verification is conducted is the residence period for the cylinders, such that any missing material accumulates over the course of the mass balance period, but not beyond. For this scenario it is assumed that product is withdrawn directly from the cascade, so the inspector has the opportunity to detect that this material is missing from a product cylinder. It is assumed that the attacker is clever and distributes missing mass among all

three product cylinders; that is, all three cylinders are missing one-third of the total missing material. The total mass missing at the *ith* inspection of a residence period is the product of the mass taken per attack event per cascade, the number of cascades attacked, and the total number of attack events to date, as shown in Equation 4.24. The mass missing from each cylinder is given in Equation 4.25.

$$\Delta m_{tot,i} = \Delta m \cdot n \cdot totevents \tag{4.24}$$

$$\Delta m_{cyl,i} = {}^{\Delta m_{tot,i}}/_{3} \tag{4.25}$$

Using the mass diverted from each cylinder, the per cylinder DP, DP_{cyl}, can be calculated using Equation 4.9, where n is the nominal product cylinder mass under normal operating conditions, s_n is the standard deviation of this reading, t is the threshold mass below which the balance "alarms", and $\Delta m_{cyl,i}$ is the missing mass from each cylinder, as described above. The total DP for each inspection, DP_{insp}, is the cumulative sum of the DPs for all three cylinders that are missing some material.

Video Surveillance- logged images

Surveillance is not conducted inside the cascade hall, so this safeguard is not effective against this type of attack. $DP_{vl} = 0$.

Total Inspection Probability

The total inspection probability equals the mass balance DP, because that is the only inspection activity that is effective against this kind of attack.

DP	$DP_{insp} = DP_{mb}$ $t = n + \sqrt{2} \cdot s_n \mathrm{erf}^{-1}(2FAP - 1)$ $DP_{cyl} = 1 - {}^{1}/_{2}\left(1 - \mathrm{erf}\left(\frac{t - (n - \Delta m)}{\sqrt{2} \cdot 0.0007 \cdot (n - \Delta m)}\right)\right)$ $DP_{insp-mb} = 1 - (1 - DP_{cyl})^3$	per inspection event per cylinder per inspection
Defender Parameters		
FAP	false alarm probability, FAP = {0.01,0.001}	
Attacker Parameters		
T	attack duration, T = {7 days, 30 days, 360 days}	
f	frequency, f = {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
Δm	mass removed from cascade, Δm = {0.010 kg, 0.100 kg}	
n	number of cascades attacked, n = {1, 6, 30}	
Payoff		
NU	0.033	
LEU	0.1	

A6. Undeclared feed detected by inspection

Inventory

Inventory is not effective against this type of diversion, as no items are missing, so $DP_{inv} = 0$.

Mass Balance Verification

Mass balance verification is not effective against this type of diversion, as no declared material missing, so $DP_{mb} = 0$.

Video Surveillance- Logged Images

Video surveillance does not occur inside the cascade halls, but it is assumed here that the surveillance surrounding the cascade halls would detect some anomalous activity, like the unexplained movement of undeclared feed and product cylinders, or movement of cylinders during non-operational hours. Unlike the situations described above, where image recording is triggered by movement in a low-activity area (like storage), and the inspectors have a limited number of images to review, the detection of this activity by video surveillance would require the inspector to watch hours of footage in search of anomaly. One can imagine this type of comprehensive video surveillance review might occur if other anomalies were uncovered by inspectors, and they wished to investigate further. Because detection in this case depends on a

detailed, time-consuming review of video surveillance by inspectors, the assessment probability for this safeguard against this attack strategy is assumed to be 0.25, half of the value assumed against other attacks. Using the 0.85 sensing probability described above, a DP of 0.22 is assumed for detecting undeclared feed using logged video images. For scenarios with multiple inspections, human reliability analysis techniques are applied in the regular manner.

DP	$DP_{i=0} = 0.22$ $DP_{insp,i} = 1 - \frac{1 + F_{team} \cdot ND_{i-1}^{\ btevents}}{F_{team} + 1}$	per inspection
Defender Parameters		
F_{team}	team factor, F_{team} = {1,19}	
f	frequency, f = {7 days^{-1}, 28 days^{-1}}	
Attacker Parameters		
T	attack duration, T = {7 days, 30 days, 360 days}	
f	frequency, f = {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
Payoff		
LEU	0.1	

4.4.2 Passive Seals DP Calculation

B2. Diversion of some material from cylinder detected by passive seals

Passive seal verification can occur as frequently as or less frequently than general inspections. Using this safeguard, it is assumed that an attack can be detected at only the first inspection (where passive seal verification is performed) after an attack. In other words, if the attacker has attacked since the last inspection, a detection opportunity exists. A post-mortem analysis time of ten days is assumed to complete analysis on seals that have been sent to the laboratory for verification. As such, the detection opportunity for passive seals actually occurs ten days after the inspection at which the verification was performed.

The defender has the option to verify all passive seals or to verify half of the passive seals. Recall from above that the baseline DP for a passive seal, DP_{pseals}, is 0.85. If the defender verifies all of the seals, the per-inspection DP, DP_i, is simply the cumulative sum of the DP for each seal broken, as shown in Equation 4.6. If only half of the seals are verified, the DP depends

not only on the probability of detecting an event given that a seal is verified, but also the probability that an attacked seal is chosen for verification. As described above for DA, the hypergeometric distribution is used to calculate the probability that at least one attacked seal is selected for verification, P_{sel}. The overall DP for the inspection is then the product of P_{sel} and the conditional probability that detection occurs, given that one or more attacked seals are selected. This scenario is described by Equation 4.26.

$$DP_{insp,i} = \left(1 - \frac{\binom{N-n}{k}}{\binom{N}{k}}\right) \cdot DP_{pseals} \tag{4.26}$$

Where,
N = number of cylinders in storage
n = number of cylinders falsified
k = number of cylinders sampled

DP	DP_{pseals} = 0.85 if *frac* = 1.00 $DP_{insp,i} = 1 - (1 - DP_{pseals})^n$ if *frac* = 0.50 $DP_{insp,i} = \left(1 - \frac{\binom{N-n}{k}}{\binom{N}{k}}\right) \cdot DP_{seals}$	per inspection per inspection
Defender Parameters		
frac	fraction seals verified, *frac* = {0.50,1.00}	
f	inspection frequency, *f* = {7 days^{-1}, 30 days^{-1}}	
Attacker Parameters		
n	number of seals attacked, *n* = {1,2}	
T	durations, *T* = {7 days, 30 days, 360 days}	
f	attack frequency, *f* = {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
Payoff		
NU	0.033	
LEU	0.1	

4.4.3 Non-Destructive Assay DP Calculations

C4/C5. Cascade re-piping or recycle detected by non-destructive assay

Non-destructive assays samples can be taken as frequently as or less frequently than general inspections occur. In this model, only the assay of the product cylinders is considered. It

is assumed that the inspector assays all of the product cylinders. The DP is related to the FAP probability chosen by the defender and the product enrichment chosen by the attacker.

DP	$t = n + \sqrt{2} \cdot s_n \text{erf}^{-1}(2FAP - 1)$ $DP = 1 - {}^{1}/_{2}\left(1 - \text{erf}\left(\frac{t - \left(\frac{x_p}{4.5} \cdot n_{LEU}\right)}{\sqrt{2} \cdot 0.04 \cdot \left(\frac{x_p}{4.5} \cdot n_{LEU}\right)}\right)\right)$	per inspection
Defender Parameters		
FAP	false alarm probability, FAP = {0.01, 0.001}	
f	inspection frequency, f = {7 days^{-1}, 30 days^{-1}}	
Attacker Parameters		
x_p	product enrichment, x_p = {19.7%, 50%, 90%}	
Payoff		
LEU	0.991	
HEU	1.69, 2.15	

4.4.4 Destructive Analysis DP Calculations

D4/D5. Cascade re-piping or recycle detected by destructive analysis

As is the case for passive seal verification, destructive analysis requires an extended analysis time after the inspection event. The post-mortem analysis time used in this model is 14 days, which is an optimistic estimate. It is assumed that a new DA sample is not analyzed until results from the previous one have been processed. Thus the frequency of DA sampling is the regular inspection frequency, but the inspection opportunity does not occur until 14 days after the inspection. The per-inspection DP for this scenario is given in Equation 4.14.

DP	$DP = 1 - \frac{\binom{N-n}{k}}{\binom{N}{k}}$	per inspection
Defender Parameters		
k	number of cylinders sampled, k = {1,4}	
f	inspection frequency, f = {7 days^{-1}, 30 days^{-1}}	
Attacker Parameters		
n	number of cylinders falsified, n = {1}	
Payoff		
LEU	0.991	
HEU	1.69, 2.15	

4.4.5 Transmitted Video DP Calculations

E1. Cylinder diverted from storage detected by transmitted video images

Inspectors have the ability to detect a diversion using transmitted video images only on the day that the diversion occurs. In this case, because cylinder theft is a one-time event, the inspector has one chance to observe the diversion. As described above, because of the relatively high assessment probability, the DP for this event is 0.64.

DP	0.64	per scenario
Defender Parameters		
	none	
Attacker Parameters		
	none	
Payoff		
NU	0.033	
LEU	0.1	

E2. Diversion of some material from cylinder detected by transmitted video images

When the attacker enters the storage yard to divert material from a cylinder, a video image should automatically be transmitted to the information center for analysis, meaning every attack event is followed immediately by a detection opportunity. As mentioned above, the DP each attack event, DP_{vt} = 0.64. The overall DP depends on the number of attack events. Because analysis and assessment are being conducted by humans who are charged with processing high volumes of data, HRA techniques are applied to this safeguard.

DP	$DP_{vt} = 0.64$ $DP_i = 1 - \frac{1 + F_{team} \cdot ND_{i-1}}{F_{team} + 1}$	per inspection event
Defender Parameters		
F_{team}	team factor, F_{team} = {1,19}	
Attacker Parameters		
T	duration, T = {7 days, 30 days, 360 days}	
f	frequency, f = {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
Payoff		
NU	0.033	
LEU	0.1	

4.4.6 Active Seals DP Calculations

F3. Diversion of some material from cascade by active seals

If a cascade is sealed with an active seal, and the attacker wishes to attack that cascade, he must break the seal. The first time the attacker attacks the cascade and breaks the seal, information that the seal has been broken is transmitted to the data center. A detection opportunity occurs only the first the attacker breaks the seal. As described above, the DP for an active seal, DP_{aseals}, is 0.40.

The defender can choose to seal all or half of the cascades. If the defender seals half the cascades (*frac* = 0.50), the DP = 0, because this is a transparent defense. The attacker can see the active seals and thus simply chooses to attack the cascades that are not sealed. If the defender seals all of the cascades (*frac* = 1.00), the DP is the cumulative sum of the per-seal DP over the number of seals broken.

DP	DP_{aseals} = 0.40 if *frac* = 0.50, DP_{insp} = 0 if *frac* = 1.00, $DP_{insp} = 1 - (1 - DP_{aseals})^n$	per inspection
Defender Parameters		
frac	fraction seals verified, *frac* = {0.50,1.00}	
Attacker Parameters		
n	number of cascades attacked, n = {1, 6, 30}	
Payoff		
NU	0.033	
LEU	0.1	

F4. Cascade re-piping detected by active seals

The detection probability for this scenario is identical to the DP for detection diversion of some material from a cascade using active seals (**F3**).

DP	DP_{aseals} = 0.40 if *frac* = 0.50, DP_{insp} = *0* if *frac* = 1.00, $DP_{insp} = 1 - (1 - DP_{aseals})^n$	per inspection
Defender Parameters		
frac	fraction of cascades sealed, *frac* = {0.50,1.00}	
Attacker Parameters		
n	number of cascades attacked, n = {1, 6, 30}	
Payoff		
LEU	0.991	
HEU	1.69, 2.15	

4.4.7 CEMO DP Calculations

G4. Cascade re-piping detected by CEMO

CEMO is an active safeguard, so if the defender selects it, it is active every day for the duration of the simulation. Recall also that if that attacker chooses to re-pipe, it is assumed that he perpetrates an attack daily for the duration he selects. The DP on any given day due to CEMO

is determined by the product enrichment the attacker chooses. This daily DP is given in Equation 4.18. As mentioned above, CEMO is a go-no go measure, so the DP is 0 for any product enrichment less than 20%.

DP	$t = r_n \cdot t_c + \sqrt{2} \cdot s_n \text{erf}^{-1}(2FAP - 1)$ if $x_p < 0.20$, $DP_{CEMO} = 0$ if $x_p \geq 0.20$, $DP_{CEMO} = 1 - {}^{1}/_{2}\left(1 - \text{erf}\left(\frac{t - \left(\frac{x_p}{4.5} n\right)}{\sqrt{2 \cdot \left(\frac{x_p}{4.5} n\right)}}\right)\right)$	per day
Defender Parameters		
FAP	false alarm probability, *FAP* = {0.01, 0.001}	
t_C	count time, t_C = {300 s, 3600 sec}	
Attacker Parameters		
T	attack duration, *T* = {7 days, 30 days, 360 days}	
x_p	product enrichment, x_p = {0.197, 0.50, 0.90}	
Payoff		
LEU	0.991	
HEU	1.69, 2.15	

G5. Cascade recycle detected by CEMO

The DP for CEMO against cascade recycle differs from the DP against re-piping because the attacker does not have to recycle material every day. Accordingly, despite the fact that CEMO is active every day, a detection opportunity only occurs on days that the attacker perpetrates an attack.

DP	$t = r_n \cdot t_c + \sqrt{2} \cdot s_n \text{erf}^{-1}(2FAP - 1)$ if $x_p < 0.20$, $DP_{CEMO} = 0$ if $x_p \geq 0.20$, $DP_{CEMO} = 1 - {}^{1}/_{2}\left(1 - \text{erf}\left(\frac{t - \left(\frac{x_p}{4.5} n\right)}{\sqrt{2 \cdot \left(\frac{x_p}{4.5} n\right)}}\right)\right)$	per attack event
Defender Parameters		
FAP	false alarm probability, *FAP* = {0.01, 0.001}	
t_C	count time, t_C = {300 s, 3600 sec}	
Attacker Parameters		
T	attack duration, *T* = {7 days, 30 days, 360 days}	
f	attack frequency, *f* = {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
x_p	product enrichment, x_p = {0.197, 0.50, 0.90}	
Payoff		
LEU	0.991	
HEU	1.69, 2.15	

4.4.8 Visual Inspection DP Calculations

H2/H3/H5. Some material diverted from a cylinder/cascade or cascade recycle detected by visual inspection

Because these are continuous diversions, visual indicators of malevolent behavior may be present, like misplaced equipment used to remove material from the cylinders or cascades. Based on the presence of these minor anomalies, the DP is 0.29 for this attacker scenario while the attack scenario is ongoing. Once the attack has concluded, it is assumed that the attacker will carefully remove any indicators that a diversion occurred, and the DP = 0.

DP	for $t \leq t_{end}$, $DP = 0.29$ for $t > t_{end}$, $DP = 0$	per inspection event
Defender Parameters		
f	inspection frequency, *f* = {30 days^{-1}, 90 days^{-1}}	
Attacker Parameters		
t_{end}	last day of diversion, t_{end} = {0,30,360}	
Payoff		
NU	0.033	
LEU	0.1	

H4. Cascade re-piping detected by visual inspection

When visual inspection is conducted on special inspections, design information verification is performed inside the cascade hall. This means that an inspection team compares the valve and pipe settings of the cascades to the design specifications. Additionally there will be other visual indicators of anomalous operating conditions, like portable feed/withdrawal equipment or extra cylinders in the cascade hall area [58]. For this reason, the DP for detecting re-piping using visual inspection is higher than the DP for other attack scenarios. The DP for this scenario depends on the size of the misuse. If the attacker dedicates 1 cascade or 6 cascades to the misuse (*frac* = 0.0167, 0.10), this constitutes a minor anomaly and a DP of 0.29 is assumed. If the attacker dedicates 30 cascades to the misuse (*frac* = 0.50), this constitutes a major anomaly, and a DP of 0.60 is assumed. As with previous attacker strategies, visual inspection is only affective if the attacker strategy is ongoing.

DP	for $t \leq t_{end}$, $if\, n \in \{1,6\},\ DP = 0.29$ $if\, n = 30,\ DP = 0.60$ for $t > t_{end}$, $DP = 0$	per inspection
Defender Parameters		
f	inspection frequency, f = {30 days^{-1}, 90 days^{-1}}	
Attacker Parameters		
n	number of cascades dedicated to misuse, n = {1, 6, 30}	
Payoff		
LEU	0.991	
HEU	1.69, 2.15	

H6. Undeclared feed detected by visual inspection

Some of the indicators of HEU production may also be indicators of undeclared feed, like portable feed/withdrawal stations and extraneous uranium cylinders in the cascade hall. These visual indicators can easily be obscured or removed by the attacker, so the DP for minor anomalies is used for this scenario.

DP	for $t \leq t_{end},\ DP = 0.29$ for $t > t_{end},\ DP = 0$	per inspection
Defender Parameters		
f	inspection frequency, f = {30 days^{-1}, 90 days^{-1}}	
Attacker Parameters		
t_{end}	last day of diversion, t_{end} = {0, 30, 360}	
Payoff		
LEU	0.1	

4.4.9 Environmental Sampling DP Calculations

I4/I5. Cascade re-piping or recycle detected by environmental sampling

As is the case destructive analysis, environmental sampling requires an extended analysis time after the inspection event. The post-mortem analysis time used in this model is 10 days, which represents an expedited turnaround versus DA. This shorter analysis period is used because environmental sampling is conducted only on special inspections, and it is thus assumed that analysis of these samples is high priority, reducing the time required to process them. The per-inspection DP for this scenario is given in Equation 4.14.

DP	$DP = 1 - \frac{\binom{N-n}{k}}{\binom{N}{k}}$	per inspection
Defender Parameters		
k	number of swipes taken, k = {6,12}	
f	special inspection frequency, f = {30 days^{-1}, 90 days^{-1}}	
Attacker Parameters		
n	number of cascades dedicated to misuse, n = {1, 6, 30}	
Payoff		
LEU	0.991	
HEU	1.69, 2.15	

4.4.10 Detection Probability Calculations Sources Summary

As described in detail above, the detection probability calculation algorithms have been developed by drawing on a variety of sources, including safeguards literature, analogous

literature in other fields, and first principle calculations. Table 4-IX summarizes the principle or reference on which each DP calculation algorithm is based.

Table 4-IX. Source for enrichment DP calculations

Defender Option	Source
Inventory	Financial auditing literature [40]
Mass balance	Physical principles- CDF of Gaussian
Video surveillance	Railway station surveillance [46]
Seal verification	Seal vulnerability analysis literature [48]-[50]
Non-destructive assay	Physical principles- CDF of Gaussian
Destructive assay	Attribute sampling as described in [22]
Continuous Enrichment Monitoring	Physical principles- CDF of Gaussian
Visual inspection	Visual inspection of ship fractures [57]
Environmental sampling	Attribute sampling as described in [22]

4.5 Exogenous Detection Probabilities

In addition to the safeguards described above, exogenous sources of detection capability are incorporated into the model using a background DP. Background DP serves as a proxy for all other safeguards and sources of detection probability not explicitly considered, including the increased detection capability that intelligence information offers, generally *at no cost to the inspector*. The background DP is a daily probability and is attacker strategy-specific, in that the value is non-uniform across different attacker strategies. This implementation is intended to represent the reality that intelligence is better suited to detect certain diversion/misuse scenarios.

4.6 Enrichment Safeguards Costs

A budget assignment scheme was formulated to allocate relative costs to each safeguard. These costs are estimates based on available information about the necessary technology or manpower needs in analogous fields. The cost values used in the model, referred to as "simulation dollars" (s$), are the based upon the estimated real values of selected safeguards divided by 100. For example, a piece of equipment that costs $1000 costs 10 simulation dollars. This paradigm is used for convenience and to emphasize that the costs here retain meaning in a relative sense, but are not claimed to be faithful to the actual absolute costs. The cost associated with each safeguard has two components: capital and operations and maintenance (O&M).

Capital costs are amortized over the serviceable lifetime of the equipment. These are one-time costs incurred for large pieces of equipment, such as a mass spectrometer. O&M costs fall into two categories: fixed and variable. Fixed O&M costs are associated with the upkeep of the equipment, and are incurred whether the equipment is used regularly or not. Variable O&M costs are costs that the defender pays when he uses the service, such as analyzing a sample, assessing surveillance feed, or inspecting a facility. The per-item cost of certain safeguards is also considered a variable O&M cost, such as the cost of a seal. The total cost for a safeguard is the sum the annual equipment, fixed, and variable O&M costs, as shown in Equation 4.27.

$$C_{tot} = C_{equip} + C_{m_f} + C_{m_v} \tag{4.27}$$

Where,
C_{tot} =total cost [s$/yr]
C_{equip} = equipment costs, including per item costs [s$/yr]
C_{m_f} = fixed maintenance costs [s$/yr]
C_{m_v} = variable maintenance costs, including manpower [s$/yr]

4.6.1 General Cost Information

Capital Costs

Estimated capital costs are divided by the estimated lifetime of the equipment, giving an undiscounted annual equipment investment cost. Table 4-X gives the capital costs for each safeguard. The basis for each of these values is presented below in the safeguard-specific section.

Table 4-X. Annual capital costs

Safeguard	Annual Capital Cost (sim dollars/yr)
Mass balance	12
Video-logged	16.5
NDA	3.6
DA	8.93
Video-transmitted	32.5
CEMO	18
ES	8.93

Operations and Maintenance Costs- Fixed

The annual fixed O&M cost for each safeguard was considered to be low, medium, or high. Fixed O&M cost assessments were made based on maintenance estimates, factoring in man-days of maintenance and equipment requirements annually. A safeguard also incurs high O&M when it requires a medium number of maintenance days, but maintenance is arduous due to the location of the equipment (e.g. CEMO). Fixed O&M costs are calculated as a percentage of the capital cost: low maintenance costs 2% of the annual capital cost, medium maintenance costs 6%, and high maintenance cost 10%.[10] Fixed O&M costs are given in Table 4-XI.

Table 4-XI. Fixed O&M costs

Safeguard	Annual Fixed O&M	Annual Fixed O&M Cost (sim dollars/yr)
Mass balance	low	0.24
Video-logged	high	1.65
NDA	low	0.07
DA	low	0.18
Video-transmitted	high	3.25
CEMO	high	1.80
ES	low	0.18

Operation and Maintenance Costs- Variable

Variable O&M costs are the manpower costs associated with implementing each safeguard, and the per-item cost of select safeguards. Four major types of manpower costs are considered: inspection, special inspection,[11] analysis, and assessment. Inspection costs occur when inspectors physically visit a facility and perform a set of tasks. The cost of inspection time considers not only the inspectors' time, but also the cost of traveling to the facility. The cost for additional inspection activities is assumed to be a fraction of the cost of inspection time, as the inspector is already at the facility conducting an inspection. Special inspections occur less frequently and on short notice, and give the inspector access to the cascade hall, making them more expensive financially and politically. Analysis costs are used when a safeguard requires

[10] Percentages were formulated using the standard 6% O&M costs for a reactor as a median value. Assignments for each safeguard were made based on expert judgment.

[11] Recall that LFUA activities are grouped as "special inspection" activities in the model

post-mortem analysis of an element, and the analysis is not conducted in the field, as is the case with passive seal verification and destructive analysis samples. The final type of manpower cost is assessment cost, which is incurred when a person must remotely monitor a signal coming from the enrichment facility, as is the case for remotely transmitted video images and active seals.

One IAEA inspection day costs $3000-5000 [59]. Assuming this price includes three inspectors, inspection costs are estimated at $1000/person/day, giving a cost of 10 simulation dollars. Each additional inspection activity performed is assumed to cost the defender an additional 20% of the inspection cost, or 2 s$. The defender must purchase a given inspector strategy for the entire year, despite the length of the simulation.

Because of the short-notice and intrusive nature of special inspections, they have a higher monetary cost and a much higher political cost than normal inspections. Here both of those expenses are rolled together and represented by the simulation dollar cost. Thus special inspections are assumed to be three times more costly than regular inspections at 30 s$ per day. As with regular inspections, additional activities at special inspections cost an extra 20%, or 6 s$.

The IAEA does some analysis on safeguards samples in-house at the Safeguards Analytical Laboratories, and also send samples to laboratories in the Network of Analytical Laboratories (NWAL) for further evaluation and independent verification [60]. A standard rate charged for mass spectroscopy and similar analytical services is $250/hr, so 2.5 s$ is used as the base cost per batch of samples. This cost assumes that each time a material's isotopic composition needs to be verified, multiple samples are actually taken and analyzed—one at the Safeguards Analytical Labs, and another at an NWAL laboratory for independent verification.

Assessment costs differs from inspection and analysis costs in that it does not strictly depend on how often the safeguard is used. Assessment time is required for the remote, active safeguards, such as active seals, transmitted video images and CEMO, and so this cost is incurred every day for which the safeguard is active, whether any sort of diversion activity occurs or not. It was assumed that an employee performing assessment costs $30/hr,[12] and that roughly a quarter of his time is dedicated to assessment for the relevant safeguard. Thus the

[12] According to the U.S. Bureau of Labor Statistics, the mean salary for an employee in a protective service occupation is $20.54/hr and an employee making $21.08 per hour costs the employer $30.23/hr [61].

employee's time costs $60/day, making the assessment cost 0.60 s$ per day. The total assessment cost for a defender strategy is the base assessment cost times the number of assessment days that occur over the course of a simulation year.

Table 4-XII gives the base cost for each type of manpower. For each defender-attacker strategy pair, the cost of the defender strategy is calculated based on the number of inspection days, analysis events, or assessment days that would occur annually.

Table 4-XII. Manpower costs

Type of Manpower Cost	Cost in Simulation Dollars
Inspection	10 per small team per insp
Additional inspection activities	2 per additional activity per insp
Special inspection	30 per inspection
Analysis	2.5 per sample
Assessment	0.60 per day

In addition to variable O&M costs associated with manpower (i.e. inspector time or analysis time), variable costs arise from safeguards that incur a per-item equipment cost, namely passive and active seals. The variable equipment cost for these safeguards is the per-item cost times the number of items that would be required annually to maintain the selected defender strategy. These costs are given in Table 4-XIII.

Table 4-XIII. Per item equipment costs

Safeguard	Per Item Cost
Passive seal	0.01
Active seal	0.50

4.6.2 Safeguard-Specific Cost Information

A. Inspection

Inspection costs are governed by the inspection manpower costs shown above. In addition, the cost of an inspection depends on the size of the team used, as described by the F_{team} variable (see Section 4.3 for more detail). The 10 dollar base price assumes a small team, F_{team} = 1. If a large team is used, F_{team} = 19, it is assumed that additional personnel cause each inspection

to cost three times as much, making the price 30 dollars per inspection. The total inspection for a defender strategy is the per-inspection cost times the number of inspections required to maintain that strategy for a year.

Note that when the defender plays an inspection strategy, she must purchase inventory, mass balance verification, and reviewing logged video images together, even if any of these three safeguards is not effective against the attacker strategy. These three activities constitute a basic inspection. Additional inspection activities can be added to this basic inspection (i.e. passive seal verification, NDA, or DA), but the defender only pays the base inspection cost once, and then pays 2 s$ per activity for each additional inspection activity.

Inventory

The costs associated with inventory are only the manpower costs given in Table 4-XII.

Mass Balance Verification

Mass balance verification has an associated false alarm probability. In this case, false alarms are inexpensive, because they occur when the inspector is physically present at the facility, meaning resolving the false alarm can be done relatively quickly and without additional travel. The low false alarm probability, 0.001, comes at no cost to the inspector. The higher false alarm probability, 0.01, is assumed to make the inspectors' time cost 1.1 times the base price. This reflects a 10% increase in the number of man-hours spent on the inspection as the inspectors are called upon to resolve additional false alarms.

To calculate the equipment costs associated with mass balance verification, the cost of a load-cell based scale (LCBS) had to be used. The cost of the LCBS was estimated at $24,000, and it was assumed that a scale is operational for 20 years [62]. The scale is calibrated annually by the IAEA, making its fixed maintenance low. The annual equipment cost for mass balance is thus $1200/year for the scale and $24/year for maintenance, giving a total cost of 12.24 s$. This value is added to the total inspection cost.

Logged Video Images

It is assumed that a 30-camera, wired video surveillance system is used at the enrichment facility for this safeguard. The size of the system was invented based on the layout of a model

GCEP facility [63]. The equipment costs are estimated at $16,500, which is based on the scaling up of a commercially available six-camera system [64]. The system is assumed operable for ten years, and requires high maintenance ($165/year), making the total estimated annual cost $1815/year, or 18.15 s$.

Total inspection costs are the sum of the yearly manpower costs, mass balance verification equipment costs, and logged video equipment costs.

B. Passive Seals

Passive seals require inspectors to install and collect the seals, as well as analysis of the seals at an off-site laboratory. Thus the manpower costs associated with passive seals include a base cost per inspection plus 2.5 s$ per batch of passive seals collected. The defender has the option to verify only half of the seals deployed in the field; if the defender chooses this option, she incurs an analysis cost of 1.25 s$, or half the per-batch cost of analysis. Additionally, there is a per-seal cost for the seals themselves, but this cost is very low at 0.01 s$ per seal. The defender must purchase enough seals to use for an entire year of her selected strategy.

C. Non-Destructive Assay

General inspection costs are associated with non-destructive assay, as well as capital costs. As mentioned under the mass balance section, a higher false alarm probability increases the cost of the inspector's time. In terms of equipment, one large, ruggedized NaI gamma detector costs about $9,000 [65].[13] It is assumed that two detectors are used for NDA, so that both can be used simultaneously to expedite the survey or so that if one is out of commission for maintenance, the other can be used. It is also assumed that these detectors service only this facility, and are locked in a tamper-indicating storage cabinet between inspections. This results in a total cost of 18 s$. If the detectors are operable for five years, the-per year cost is 3.6 s$. This cost is in addition to the annual 0.07 s$ fixed O&M cost.

[13] Based on price for GAMMA-RAD5

D. Destructive Assay

Destructive assay occurs during inspections, incurring general inspection costs. Additionally, there is a high equipment cost associated with this safeguard. A thermal ionization mass spectrometer (TIMS), one of the primary pieces of equipment used for isotopic analysis, costs about $750,000 [66]. Assuming a serviceable life of ten years, the amortized capital cost is $75,000 per year. It is estimated that this piece of equipment is used at the Safeguards Analytical Labs by at least 84 front-end fuel cycle facilities worldwide and analyzes an average of 600 samples per year total [60], [67]. Capital costs are estimated by dividing the $75,000 capital cost by the 84 facilities using the TIMS, assuming each facility shares an equal burden, giving a per-facility capital cost of just under $893, or 8.93 s$. The fixed O&M cost is $18 per year, or 0.18 s$.

Each sample must also be analyzed, requiring analysis manpower. As mentioned previously, a $250/batch analysis rate is assumed for DA samples. The defender has the option to sample either half or one-eighth of the cylinders in product storage. If she samples half of the cylinders, she is charged the full $250 (2.5 s$); if she samples one-eighth of the cylinders, she charged only half that rate (1.25 s$).

E. Transmitted Video

Viewing transmitted video images to detect anomalous activity is an assessment activity, if the defender plays this safeguard, she must buy assessment time every day for the duration of the simulation. Additionally, the defender can choose a small or large assessment team, and as with general inspections, using a large time costs three times more than using a small team. As was the case for logged video images, the capital cost assumes a 30-camera system, only in this case a wireless system is assumed. The cost of the wireless video surveillance system is estimated at $32,500, again scaled up from a six-camera wireless system [64]. Again this system is assumed serviceable for ten years, giving an annual cost of $3,250 per year, in addition to a high annual maintenance cost of $325 per year. Thus the total annual equipment costs are $3,575 per year, or 35.75 s$.

F. Active Seals

Active seals require paying for assessment time on each day of the simulation, and paying a per-seal cost for each active seal installed. Based on the prices of commercially available active RFID seals used for high-value assets, the cost of one active seal was estimated at $100, or 1 s$ [68]. Active seals remain in use in the field for multiple years; here it is assumed they can be used for two years, giving an annual, per-item cost of 0.50 s$. It is also assumed that the defender must purchase two seals annually for every one seal that she deploys, such that a duplicate is available for replacing a seal that has failed or been tampered with.

G. CEMO

As with the previous two active safeguards, CEMO requires assessment costs every day. In this case, if the defender chooses the high false alarm probability, the manpower costs are assumed to be doubled, as resolving this type of false alarm requires inspectors to travel to the facility. An equipment cost of $18,000 was assumed for a CEMO unit. Little information was available about the cost of CEMO units, so this value was calculated simply by doubling the cost of the handheld gamma detectors used for non-destructive assay. It is assumed that a CEMO detector can be used for ten years, yielding an annual equipment cost of $1,800, plus a high annual fixed O&M cost of $180. Thus the total cost for CEMO is 19.8 s$, plus assessment time.

H. Visual Inspection

Visual inspection occurs inside and around the cascade halls during special inspections. Because this activity requires no equipment, there are no costs aside from manpower associated with it. Thus the total cost of visual inspection is 30 s$ per inspection.

I. Environmental Sampling

Environmental sampling is an additional activity that can occur during a special inspection. As such it costs 6 s$ per inspection. The analysis performed for environmental sampling closely resembles that of destructive analysis, so the annual equipment cost is the same for both safeguards at 8.93 s$, with low fixed O&M of 0.18 s$ per year. There are two assumptions made about analysis for ES: 1) Because this is a special inspection, analysis is

expedited and results are produced on a shorter timeline than a normal DA sample, and 2) Either six or 12 samples are processed for each inspection. Due to these two assumptions, analyzing a batch of ES swipes is assumed to cost twice as much as analyzing a batch of DA samples, making the cost 5 s$ per batch of swipes. Here a batch is 6 samples; if the defender chooses to take 12 swipes, the analysis cost is 10 s$.

Table 4-XIVsummarizes the capital, O&M, manpower, and total cost for each enrichment safeguard, and Table 4-XV demonstrates a sample cost assessment for a sample defender strategy where the defender has purchased each safeguard, but has chosen to play each one in the least expensive way possible. Parameters for this strategy are specified in Table 4-XVI. The table provides a breakdown of each type of cost for each safeguard and gives a total strategy cost in the bottom row.

Table 4-XIV. Enrichment safeguards cost summary

Safeguard	**Capital Cost (s$/year)**	**Fixed O&M (s$/year)**	**Variable O&M (s$/year)**		**Total Fixed Cost (s$/year)**
Insp- Inventory Insp- Mass balance Insp- Video logged			**Manpower**	**Other**	
	0	0	10/insp	0	0
	12	0.24	0	0	12.24
	16.50	1.65	0	0	18.15
Passive seals	0	0	2/insp 2.50/batch	0.01/seal	0
NDA	3.6	0.07	2/insp	0	3.67
DA	8.93	0.18	2/insp 2.50/batch	0	9.11
Video transmitted	32.50	3.25	0.60/day	0	35.75
Active seals	0	0	0.60/day	0.50/seal	0
CEMO	18	1.80	0.60/day	0	19.80
Visual inspection	0	0	30/insp	0	0
ES	8.93	0.18	6/insp 5/batch	0	9.11

Table 4-XV. Sample strategy cost demonstration

Safeguard	Capital Cost (s$/year)	Fixed O&M (s$/year)	Variable O&M (s$/year)		Total Cost (s$/year)
			Manpower	Other	
Insp- Inventory	0	0	120	0	120
Insp- Mass balance	12	0.24	0	0	12.24
Insp- Video logged	16.50	1.65	0	0	18.15
Passive seals	0	0	22 13.75	2.52	38.27
NDA	3.60	0.07	22	0	25.67
DA	8.93	0.18	22 13.75	0	44.86
Video transmitted	32.50	3.25	216	0	251.75
Active seals	0	0	216	15	231
CEMO	18	1.80	216	0	235.80
Visual inspection	0	0	120	0	120
ES	8.93	0.18	24 20	0	53.11
Total	91.53	7.19	861.50	17.52	742.94

Table 4-XVI. Parameters for sample strategy used in cost demonstration

Parameter	Value
Inspection frequency	30 $days^{-1}$
F_{team}	1
FAP	0.001
Fraction seals verified	0.50
Fraction cascades sealed	0.50
DA samples per inspection	1
Special inspection frequency	90 $days^{-1}$
ES swipes per inspection	6

4.7 PAYOFFS

The payoff to the defender and attacker for a given strategy pair is the detection probability weighted by the quantity and attractiveness of the material obtained. The material attractiveness is valued using Bathke's Figure of Merit (FOM) method [69], described in greater

detail below. Because the payoff function is subjective and potential adversaries' motives may not be identical, two different functions were used for analysis and the results from each are presented. These functions are described in detail below.

4.7.1 Figure of Merit Calculation

The FOM method assigns a value up to three to fissile material, based on the bare critical mass, the heat rate and the dose rate. Material valued between 0-1 is impractical for weapons use, material from 1-2 is attractive, and material with a FOM greater than 2 is preferred. For an advanced proliferant state or a sub-national group unconcerned with yield, the FOM is calculated using Equation 4.28. A second FOM formula can be used for less advanced proliferant nations who are concerned with pre-initiation, for whom spontaneous fission may be a substantial obstacle to weapons development.

$$FOM_1 = 1 - \log_{10}\left[\frac{M}{800} + \frac{Mh}{4500} + \frac{M}{50}\left(\frac{D}{500}\right)^{\frac{1}{\log_{10} 2}}\right] \qquad (4.28)$$

where:

M = bare critical mass (kg)
h = heat content in unpurified metal form (W/kg)
D = dose rate of 0.2 □M at 1 m (rad/h)

Bare critical mass and heat rate

The FOM was calculated for all material available to the attacker in the enrichment simulation: natural uranium, and 4.5%, 19.7%, 50% and 90% ^{235}U enriched uranium. For each material type, bare critical mass, heat content and dose rate need to be calculated as inputs to Equation 4.28. Bare critical mass and heat rate were calculated using an Excel-based tool. The tool does a one-group diffusion calculation to determine the bare critical mass, and uses specific decay power values from the Origen2.2 data libraries to calculate heat content. Note that the tool has low fidelity for enrichments below 10% ^{235}U, so values are not reported for natural or 4.5% enriched uranium. The value for each of the enriched materials is given below in Table 4-XVII.

Table 4-XVII. Calculated metrics used in FOM calculation

Material	M (kg)	h (10^{-5} W/kg)
19.7% enr. U	817	1.96
50% enr. U	163	3.40
90% enr. U	57	5.30

Dose rate for 0.2·M at 1 m

MCNPX was used to calculate the dose rate of 20% of the critical mass at 1 m. A spherical volume source was modeled, and the radius of the sphere was calculated from the density of uranium and the mass. Two separate runs were done—one with the spontaneous fission (SF) card and one with the spontaneous photon (SP) card. The DF card was used to modify the tally and produce dose in rem/hr as an output. Because the input to the FOM equation must be in rad/hr, the neutron tally results were binned into six groups: thermal, up to 0.01 MeV, up to 0.1 MeV, up to 2 MeV, up to 20 MeV, and greater than 20 MeV. The dose in rem/hr in each of these bins was then divided by the appropriate radiation weighting factor to obtain the dose in rad/hr. The dose rates in each bin were summed, along with the gamma dose rate, to give the total dose rate. The runs done with the SF and SP cards gave very similar results, so only the results from the spontaneous fission run are considered. The dose rates for each material type are given in Table 4-XVIII.

Table 4-XVIII. Dose rate or 0.2*M at 1 m

Enrichment	Dose rate (10^{-6} rad/hr)
19.7%	0.105
50%	0.0185
90%	0.00184

Using the inputs presented above, the FOM for 19.7%, 50%, and 90% enriched uranium were calculated. FOM for natural and 4.5% enriched uranium could not be calculated; however, values were assigned to characterize the attractiveness of these materials relative to the other enriched uranium products. These values are given in Table 4-XIX.

Table 4-XIX. FOM values for enrichment facility

Enrichment	FOM
0.711%	0.033[14]
4.5%	0.1
19.7%	0.991
50%	1.69
90%	2.15

4.7.2 Payoff Functions

The FOM value is combined with the material quantity and DP using a payoff function. Two different functions, given in Equations 4.29 and 4.30, respectively, were used to model the breakout-willing attacker and the risk-averse attacker. Here α is a weighting factor that describes the degree to which the attacker is motivated by high-value material. Recall that the attacker is the minimizing player, meaning he desires the lowest payoff possible. The payoff function given in Equation 4.29 describes an attacker who minimizes his payoff by seeking to avoid detection if possible, but ultimately by obtaining large quantities of high value material at any cost, even at the expense of being detected for certain. Thus this function is used to model a breakout-willing attacker who is willing to accept that he will be detected and nonetheless pursues a breakout strategy—an aggressive strategy to produce or divert large quantities of high-value material. Payoff 1 continues to decrease as the denominator increases, so that this attacker will find large amounts of high-FOM material an attractive target even if the DP associated with obtaining it approaches unity. Conversely Payoff 2 asymptotes to a large value as the DP approaches unity, which is highly undesirable for the attacker. Thus Payoff 2 gives the payoff function for a risk-averse attacker who is still incentivized by high-value material, but unlike the breakout-willing attacker, will reject any strategy that results in certain detection, if alternatives are available.

$$payoff1 = \frac{DP}{(FOM \cdot quantity)^{\alpha}} \tag{4.29}$$

[14] A FOM-like value of 0.1 was assigned to 4.5% enriched material, and the value of 0.033 for natural uranium was assigned one-third of that value based on the fact that enriching 1 kg of NU to 90% requires approximately three times the enrichment capacity as enriching 4.5% enriched material to 90%.

$$payoff2 = \frac{DP}{(FOM \cdot quantity)^{\alpha}} \cdot \frac{1}{(1 + e - DP)} \tag{4.30}$$

Where m is the mass of material obtained [kg], α is the material weighting parameter, and e is 0.001, a small non-zero value used to ensure that as the DP approaches unity, the payoff approaches infinity. The value for α is a value varied from 0 to 0.7 to simulate an attacker with different levels of material motivation. Note that the alpha = 0 case is not a realistic scenario, because all adversaries would prefer better material to worse material and more material to less material; however, alpha = 0 serves as the limiting case of an extremely conservative attacker. Alpha values were varied only up to 0.7 because at this value the attacker has already committed to a single attack strategy that is dominated by his desire for high-value material. Note that for the breakout-willing attacker, the strategy to which he commits is the breakout strategy, and for the risk-averse attacker, the strategy is the one that obtains the maximum possible amount of material while still keeping evading certain detection (DP < 1). The breakout strategy is the strategy in which the attacker seeks the maximum quantity of high-value material, even though he knows he faces certain detection. Figure 4-1 shows both payoffs as a function of DP for alpha = 0 and alpha = 0.2.

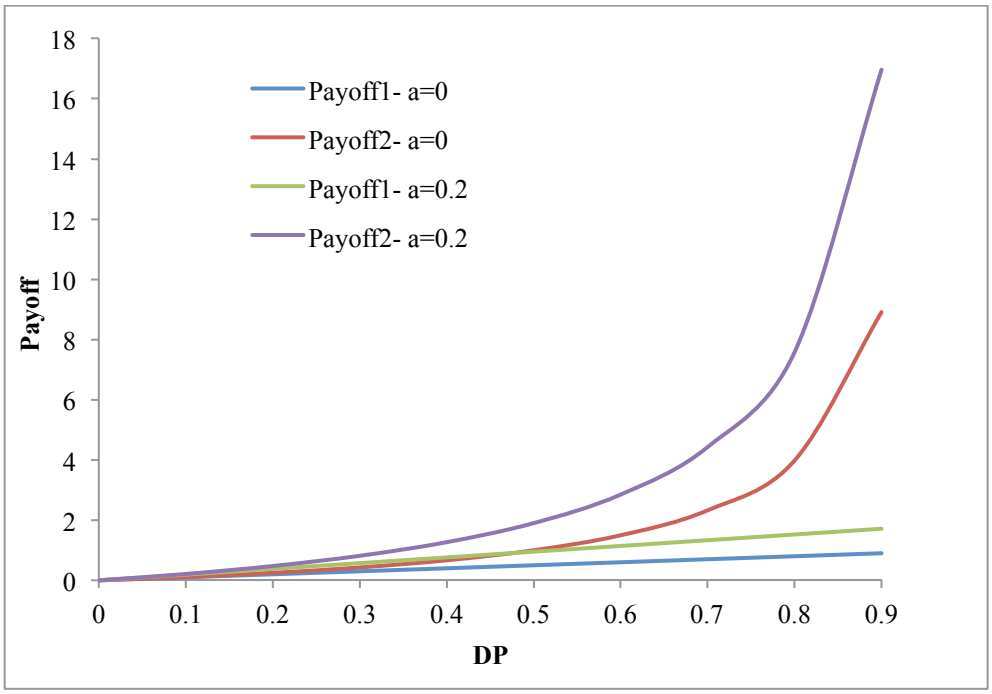

Figure 4-1. Payoff functions as a function of DP

Figure 4-2 shows payoff 2 as a function of DP for two different material utilities at alpha = 0.1, where material utility is defined as $FOM \cdot Q$, or the FOM times the quantity of TRU obtained. $(FOM \cdot Q)_1$ takes a value of 0.016, corresponding to the material utility in attacker strategy A33, the strategy generally chosen by the attacker at the reprocessing facility at alpha equals zero when he seeks to avoid detection. $(FOM \cdot Q)_2$ takes a value of 576, corresponding to attacker strategy A47, the breakout strategy in the reprocessing model. It is clear that for any alpha value greater than zero, the attacker prefers $(FOM \cdot Q)_2$ to $(FOM \cdot Q)_1$.

Inherent in the attacker's strategy selection is a trade-off between maximizing material utility and evading detection. The horizontal black line on Figure 4-2 intersects both curves at a payoff value of 2. The attacker is indifferent between these two strategies at this alpha value because both strategies yield a payoff of 2. As the alpha value is decreased, and the attacker's behavior is less influenced by material utility, the attacker will select the strategy that yields $(FOM \cdot Q)_1$, because this strategy results in a lower DP. Here the payoffs for both strategies asymptote towards positive infinity as the DP approaches one, so the attacker is incentivized to

pursue lower value material to keep his DP lower. Conversely, for the breakout-willing attacker, shown in Figure 4-3, the attacker is not indifferent between the two strategies, as demonstrated by the black line. In this case, the attacker minimizes his payoff by selecting the breakout strategy ($(FOM \cdot Q)_2$), even though the DP for this strategy is 1. This point occurs when the payoff is around 0.5. Beyond this payoff value, no additional defender investment makes a difference in the attacker's behavior, because he has already been pushed to the breakout strategy.

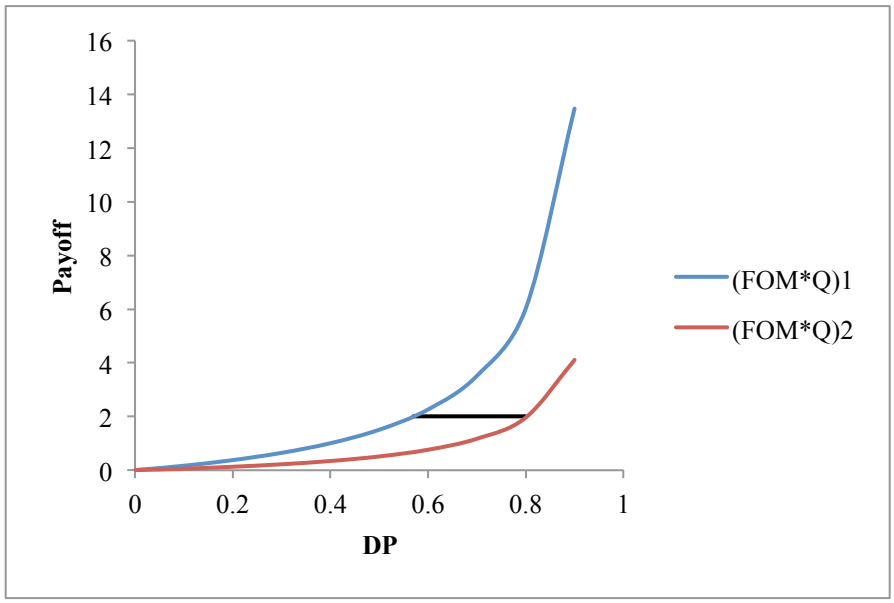

Figure 4-2. Payoff 2 as a function of DP for two material utilities (alpha = 0.1)

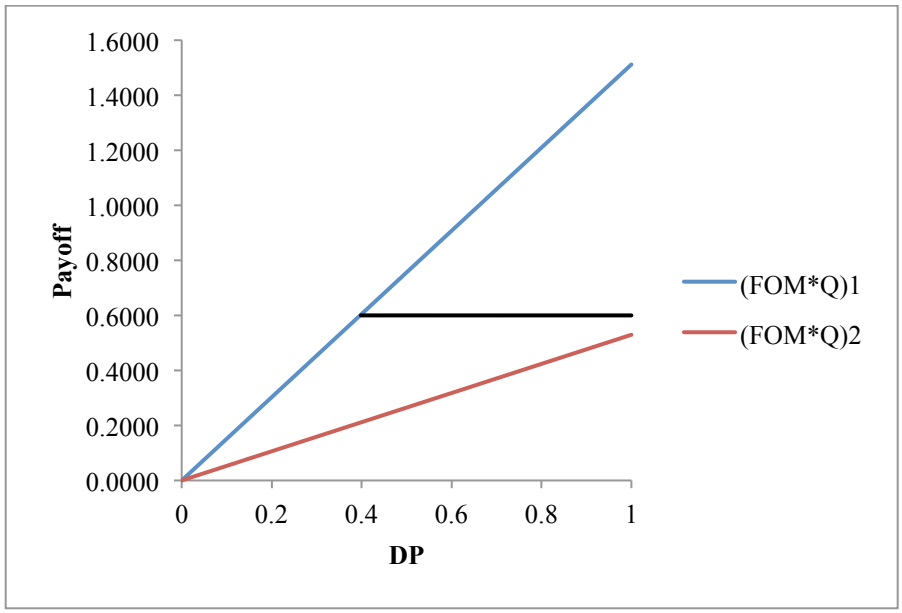

Figure 4-3. Payoff 1 as a function of DP for two material utilities (alpha = 0.1)

Additionally, a 'normalized payoff' is calculated for both payoff 1 and 2. This normalizes the payoff value by the maximum possible material value available to the attacker. This payoff ranges from zero to one, and takes the value 1.0 when the two conditions defining the breakout scenario are met: (1) the attacker obtains the best possible material, and (2) the scenario DP is one. This payoff eliminates the artificial drop in payoff value with increasing alpha that is seen for both payoff 1 and 2. The normalized payoff was calculated using Equation 4.31 for normalized payoff 1, and Equation 4.32 for normalized payoff 2. The notation $(FOM_{y'} \cdot quantity_{y'})$ indicates the maximum possible material utility for the attacker.

$$payoff1' = \frac{DP}{(FOM \cdot quantity)^{\alpha}} \cdot (FOM_{y'} \cdot quantity_{y'})^{\alpha} \tag{4.31}$$

$$payoff2' = \frac{DP}{(FOM \cdot quantity)^{\alpha}} \cdot \frac{1}{(1 + e - DP)} \cdot e \cdot (FOM_{y'} \cdot quantity_{y'})^{\alpha} \tag{4.32}$$

Chapter 5: Reprocessing Simulation

This section presents the reprocessing simulation model. The first sub-section describes the reference reprocessing facility that the model is based on. The second section provides qualitative information about defender and attacker options, and the third section expands on this information with quantitative DP calculation algorithms. The fourth and fifth sections are analogous to Sections 4.6 and 4.7, providing cost and payoff information for the reprocessing model.

5.1. Reference Reprocessing Facility

A UREX+ aqueous reprocessing facility with an annual capacity of 200 MTHM is modeled.[15] The facility can process spent LWR fuel from approximately ten reactors annually, separating about 2000-kg of TRU oxide product.[16] It is assumed that the facility operates continuously 24 hours per day, 240 days per year [72]. Based on this assumption, the facility produces an average of slightly greater than one significant quantity (8 kg) of plutonium per day. A 10-year cooling time between reactor discharge and reprocessing is assumed. Figure 1 gives an overview of the major steps in the UREX+1a aqueous reprocessing process. Fuel is received in spent fuel bundles from a reactor. Fuel attributes are measured using non-destructive assay techniques (NDA) and operator declarations are compared to inspector burnup calculations and NDA measurements. The fuel is then stored until it is ready to be processed. The storage is under constant containment and surveillance (C/S), including cameras and directional radiation detectors [72].

5.1.1 Process flow

The spent fuel enters front-end operations and is first mechanically chopped and sheared. The spent fuel pellets are then dissolved in nitric acid. Undissolved material, including cladding and undissolved fuel, are removed from the process stream ("hulls"). The raffinate then enters a

[15] This facility size was chosen by scaling the model facility in the SSPM model down by an order of magnitude [70].
[16] Based on fact that U.S. produces approximately 2100 MTHM/yr spent fuel total at 104 reactor facilities [71].

series of centrifugal contactors or mixer settlers that comprise the UREX extraction step. In this step, uranium and technetium are co-extracted from the solution using TBP as a solvent. The uranium and technetium are then partitioned to be stored separately.

After the uranium is extracted from solution, the remaining solution contains TRU products (Pu, Np, Am, Cm), fission products, and lanthanides. CCD-PEG solvent is used to extract Cs and Sr from solution, which pose a large repository burden due to their short half-lives and high heat generation rates. The solution is then sent to the TRUEX process, where non-rare earth fission products are extracted to be stabilized and stored. Finally in the TALSPEAK process phase, the rare earth fission products are separated out [73]. The plutonium and minor actinides (MA) solution is solidified, and the Pu + MA product is stored on-site until shipment.

5.1.2 Material flow and characteristics

It is assumed that output batches from the TRU product tank are withdrawn once every 24 hours. Based on the 240 days in an operational year, the plant produces 240 TRU product batches per year, meaning each batch contains approximately 8 kg of TRU product. The initial composition of plutonium in used LWR fuel is approximately 0.9%, while minor actinides comprise approximately 0.1% [71]. Assuming this ratio is maintained to the first approximation during reprocessing, there is about 7.2 kg of plutonium in the 8 kg of TRU product. Based on this estimation, each TRU product batch is produced from approximately 800 kg of spent fuel (excluding cladding). It is assumed that each chemical process takes 24 hours to complete except for the TALSPEAK process,[17] meaning it takes the material 24 hours to move from the chopper to the front-end accountability tank, 24 hours to move from the accountability tank to the UREX contactors, 24 hours to move from the UREX contactors to the TRUEX contactors, 24 hours to move from the TRUEX contactors to the TALSPEAK contactors, and 24 hours to move from the TALSPEAK contactors to the TRU product tank.

The nominal volume in front-end accountability tank is 2,880 liters with a plutonium concentration of 2.5 g/L, and the nominal volume in the TRU product tank is 31 L with a

[17] Based on Cipiti, who notes that it takes 27 hours for material to move from the dissolution to the UREX contactors [16]

plutonium concentration of 0.25 kg/L.[18] The nominal density of the tanks is estimated based on the mass of solute and the volume. In the front-end accountability tank, it is assumed that all 800 kg of spent fuel are dissolved in solution. Note that in reality this is not strictly true as some mass would be lost either by design, as is the case with volatile fission products that are driven off, or due to process loss, such as hold-up in the pipes or material remaining undissolved and moving with the hulls to a waste stream. This assumption is made here to simplify calculations while retaining accuracy to a first approximation. Using these assumptions, the density in the front-end accountability tank is approximately 300 g/L.[19] The density of the TRU product tank is the mass of TRU product, 8 kg, divided by the volume of the tank, also resulting in a density of 300 g/L.

One of the material characteristics that makes spent fuel relatively easy to detect and difficult to handle is that it is highly radioactive. In this work, only the material's neutron emission rate is considered, because it assumed that non-destructive assay is done using neutron counting, though in reality spent fuel also has a high gamma emission rate. Two major mechanisms contribute to the high neutron emission rate of spent fuel: spontaneous fission and (α, n) reactions. At the time of discharge, (α, n) reactions account for about 7% of all neutrons emitted from spent fuel, but this percentages decreases over time [75]. As stated previously, it is assumed that material is cooled for ten years before reprocessing. Ten year after discharge, the neutron rate is totally dominated by spontaneous fission of Cm-244, so much so in fact that the total neutron emission rate is effectively the spontaneous fission rate for this isotope [75]. For a standard boiling water reactor (BWR) fuel assembly with fresh fuel enrichment of 4.4% and a burnup of 40 MWd/kgU, the Cm-244 neutron emission rate at discharge is 4.39 x 10^7 n/s/assembly. The count rate after the ten year decay period can be calculated using Equation 5.1, where T_C is the cooling time [seconds], S_p^0 is the primary Cm-244 source at time T = 0 (discharge) [n/s/assembly], and λ is the decay constant for Cm-244 (1.2135 x 10^{-9} s^{-1}).

$$S_p(T_C) = S_p^0 e^{-\lambda T_C} \tag{5.1}$$

Inserting the proper values into Equation 5.1, the neutron emission rate for Cm-244 ten years after discharge is 2.99 x 10^7 n/s/assembly. An average BWR assembly contains about 210

[18] Pu concentration was taken from [74], 15-volume tank example. The volume is calculated from product mass and Pu concentration.

[19] Note that only one significant figure is used due to the approximate nature of the solute mass value

kg of material, making the neutron rate approximately 1.4 x 10^5 n/s/kgSF (neutron per second per kg of spent fuel) [76]. This Cm-244 source term is assumed equal to the total neutron emission rate for both the spent fuel and the TRU product. No further decay-correction is made for the TRU product to account for time in process due to the insignificance in the neutron emission reduction over this short time. The total neutron source term for a batch of spent fuel (800 kg) is 1 x 10^8 n/s, and this is also the neutron source term for the TRU product tank, because the UREX+ process co-extracts MA and Pu, so all Cm-244 remains in the product.

Table 5-I summarizes the nominal operating and material parameters described in this section. These values are referenced below in the DP calculations for different defender-attacker pairs.

Table 5-I. Reprocessing process characteristics under normal operating conditions

	Front-end Accountancy Tank	**TRU Product Tank**
Material mass (kg)	800	8
Pu mass (% total mass)	0.9	90
MA mass (% total mass)	0.1	10
Volume (L)	2,880	31
Pu concentration (g/L)	2.5	250
Density (g/L)	300	300
Neutron source term (n/s)	1 x 10^8	1 x 10^8

5.1.3 Diversion points

Figure 5-1 provides an overview of the UREX process. The red boxes indicate some potential points of diversion. The possible points of diversion depicted are: diverting spent fuel from storage, diverting TRU into the hulls, diverting material from any of the solvent extraction steps, or diverting TRU product from storage. Diversion of solution into hulls or from the extraction steps can be done with or without replacement with nitric acid to maintain mass and volume levels. The diagram also indicates key safeguards measurements points, where either NDA or DA samples are taken by an automatic sampling system and analyzed in an on-site laboratory.

The diversion points pictured are a subset of the possible diversions at an aqueous reprocessing facility and should not be considered an exhaustive list. The number of attacker

options considered in this model was limited to keep the scope of work manageable. To that end, the attacker options modeled in this work are indicated by the red dots and the "AO" labels. These options are: (1) diverting chopped fuel pieces from a hot cell before dissolution, and (2) diverting TRU solution from the TRU product tank. Figure 5-2 and Figure 5-3, adapted from [16], show the front and back-end process steps in greater detail. Here the specific process steps from which the attacker can divert material are shaded in red.

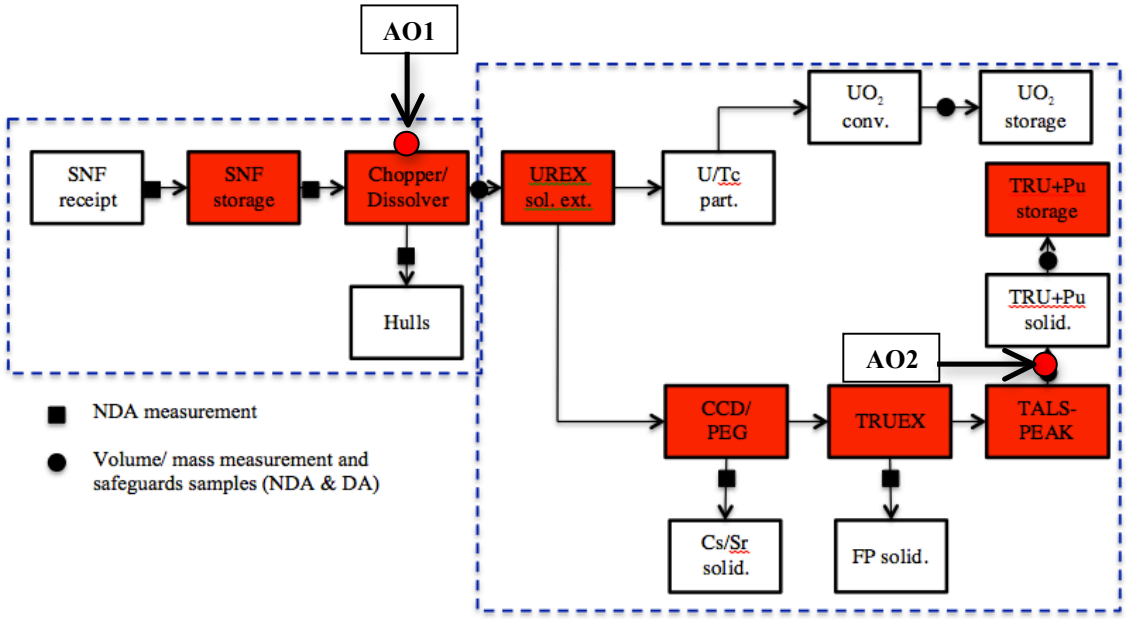

Figure 5-1. UREX+ process overview and points of diversion

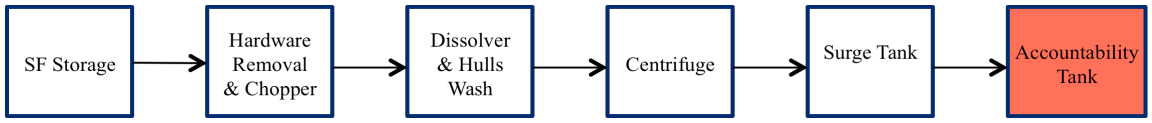

Figure 5-2. Front-end of UREX+ process with diversion location shaded in red

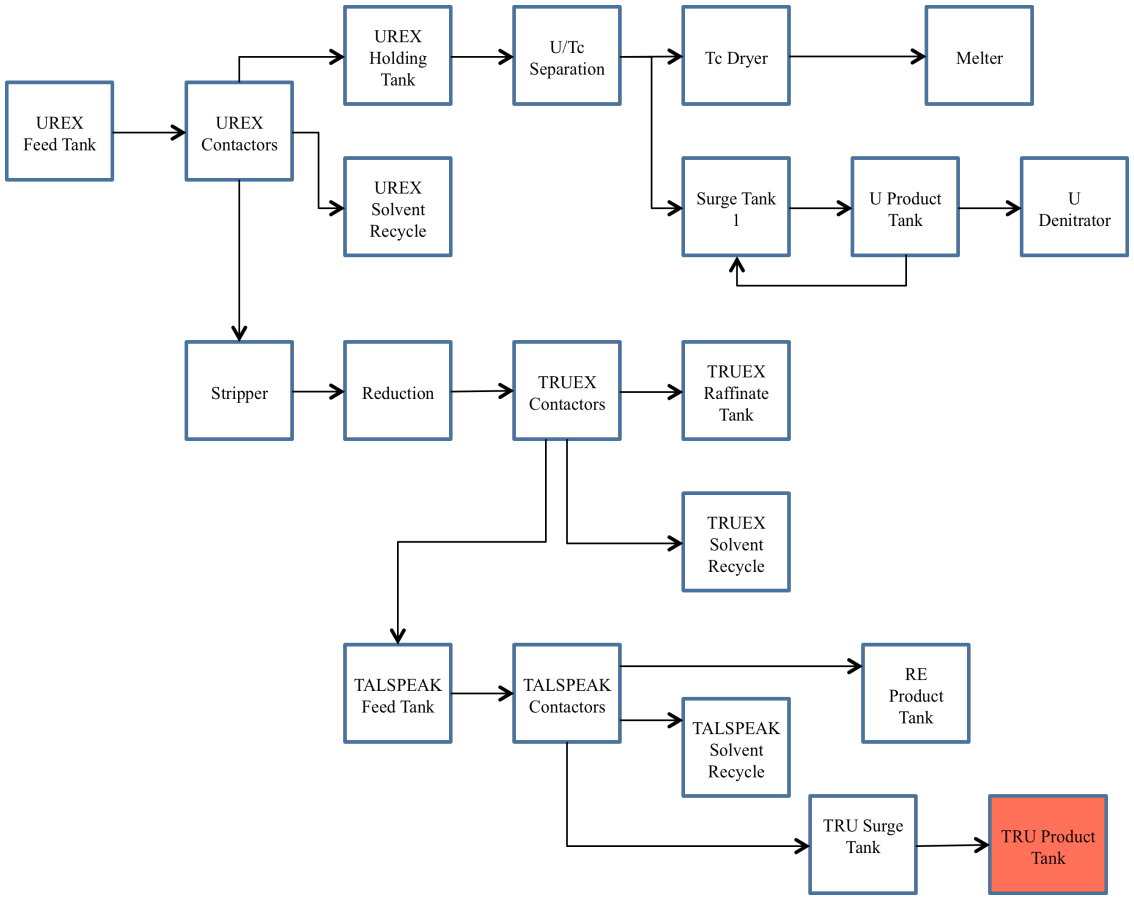

Figure 5-3. Back-end of UREX+ process with diversion location shaded in red

5.2 ATTACKER OPTIONS

1. Diversion of chopped spent fuel pieces before dissolution

In this diversion scenario, the attacker diverts chopped spent fuel pieces from a hot cell to an undisclosed location for additional processing. The attacker can select the frequency of the attack, the duration of the attack, and the mass stolen per attack. It is assumed that the attacker has authorized access to the material without creating any additional penetrations or forcing his way into the hot cell. Note that this diversion can be detected by four safeguards: C/S, the SMMS, DA sampling, and DIV. Of these safeguards, two of them (C/S and DIV) are applied at the Hardware Removal and Chopper process step, and two are applied downstream at the front-end accountability tank (SMMS and DA), which results in a slight delay in detection. As mentioned above, it is assumed that it takes material 24 hours to move from the Hardware Removal and Chopper process step to the front-end accountability tank.[20]

2. Diversion of TRU solution from TRU product tank

In this diversion scenario, that attacker diverts TRU solution from the TRU product tank to an undisclosed location for additional processing. The attacker selects the frequency and duration of attack, as well as the quantity of material diverted. It is assumed that the tank is at static volume when the attacker diverts material; that is, a batch of material has filled the tank to a specified volume and the tank is now in "wait" mode, waiting to send the material on to the next process step. It is further assumed that the attacker diverts the material through an undeclared pipe to an undeclared tank [74]. As described above, it is assumed that each chemical separation step takes 24 hours to complete, so it takes the material 120 hours, or five simulation days, to get from the front-end accountability tank to the TRU product tank.

5.3 DEFENDER OPTIONS

A. Dual Containment and Surveillance and NDA(cameras and directional radiation detectors)

Containment and surveillance is installed around the facility to ensure the proper, undisturbed flow of materials. C/S is also of particular utility in storage areas, where little

[20] This time is estimated based on the 27 simulated hours that is required for dissolver solution to reach contactor bank in solvent extraction unit in SSPM

movement or change in scenery is expected. Dual C/S is comprised of both cameras and directional radiation detectors. Here C/S and NDA are considered together, with the directional radiation detectors serving as a non-destructive technique for verifying the presence of the appropriate quantity of TRU material. Modeling of the video portion of this safeguard is identical to that of logged video images from the enrichment facility. It is assumed that anomalous motion at the facility (i.e. human activity in a hot cell where human presence is rarely or never expected) can trigger the video system to record images, and that the inspector reviews these images during every inspection.

The directional radiation detectors (DRD) are modeled as a small network of gross neutron counters that measure static volume vessels to estimate the TRU inventory. The detectors register an anomalous reading if a suppressed neutron count is detected, indicating the possible diversion of TRU material. This safeguard is modeled after the Plutonium Inventory Measurement System at the Rokkasho facility, which uses a network of 142 ^{3}He detectors to continuously measure plutonium hold-up in glove boxes and pipes. Cipiti asserts that tanks that contain large plutonium inventories, such as the TRU product tank, require high-certainty sampling for accountancy measures, but for tanks with small plutonium inventories, less sensitive non-destructive counting techniques with errors as high as 20% are sufficient [16]. In this model, it is assumed that DA sampling is performed on tanks with large Pu inventories, specifically the front-end accountancy tank and the TRU product tank, to detect bias defects, like alterations to process conditions, but this type of sampling is unable to detect the diversion of homogenized TRU product solution. Thus it is assumed that directional radiation detectors are employed as a complementary measure to detect gross defects, such as the diversion of a large quantity of solution or chopped spent fuel pieces. A total measurement uncertainty of 10% is assumed [77].

The operational characteristics ascribed to DRD are similar to those of the video surveillance; an anomalous reading is recorded and must be reviewed by an inspector during an inspector in order for detection to occur. The defender chooses the frequency with which she inspects (and reviews the C/S records) and the size of the inspection team.

B. Design information verification

During design information verification, inspectors ensure that physical features of the facility are consistent with declared design specifications. A 3-Dimensional Laser Range Finder Detector (3DLRFD) is used to help inspectors find anomalous plant features, such as undeclared pipes, or features that have changed since the last inspection, such as valve settings. Figure 5-4 shows actual scans from the 3DLRFD— (a) is the initial scan of an area, (b) is a second scan, and (c) shows detected differences in red. The instrument itself detects and highlights the differences. Design information verification is performed during on-site inspections, and the defender chooses the frequency with which it is performed.

Use of the 3DLRFD is a time-intensive process. Building a 3D image of one cell requires six scans, which takes two hours [77]. The defender also chooses whether design information for the front-end or back-end of the facility is verified on each visit.

Figure 5-4. Scans taken using 3DLRFD: (a) initial scan, (b) second scan, (c) detected differences shown in red [77]

C. Solution Measurement and Monitoring System

The SMMS is a process monitoring system in use at Rokkasho to provide continuous monitoring of the chemical portion of operations. At Rokkasho, both the Input Accountability Vessel (analogous to the front-end accountability tank in this model) and the Pu Product Output Accountability Vessel (analogous to the TRU product tank in this model) are equipped with instruments to measure absolute pressure directly. Additionally the Input Accountability Vessel is equipped with six probes that together can determine the solution density in the vessel [78].

While twelve "strategic" vessels are monitored by IAEA equipment, other vessels at Rokkasho are monitored by the operator's equipment, and signals from this equipment are split off and shared with the IAEA for increased continuity of knowledge. In this model, it is assumed that the SMMS provides volume, pressure, density, and temperature information at the front-end accountancy tank and the TRU product tank, and from this information can be used to calculate the mass of solute.

At a real reprocessing facility, such as Rokkasho, the sampling frequency is on the order of seconds or minutes for many of the online safeguards, like the SMMS. A large number of samples can be collected over an extended period, such as a day, and these samples can be analyzed using alarm algorithms to check for trends in data. For example, if there is a single low reading that is within the measurement uncertainty for the instrument, an alarm may not be triggered, but a series of low readings within measurement errors may trigger an alarm. In an effort to differentiate trends in data from random uncertainty, statistical tests, like the Page's test, are used to determine whether the readings constitute a trend. Such alarm algorithms are not modeled in this work for simplicity; instead, a single measurement is used as a proxy for a series of measurements. It is assumed for the purposes of this work that over a similar period of time, a single long measurement replicates the information generated by applying Page's test to a series of many much shorter measurements.

It is assumed that SMMS measurements are performed automatically and continuously, without inspector intervention, and alerts are sent to the defender remotely. The defender chooses the false alarm probability for this safeguard, where a larger false alarm probability increases DP but represents a nuisance to facility operators and inspectors and incurs extra costs.

D. Destructive Analysis sampling

Samples are taken from front-end accountability tank and TRU product tank for destructive analysis to determine the isotopic actinide concentrations. As with the NDA measurements, it is assumed that DA samples are taken automatically at specified interval and sent to an on-site laboratory for processing, but that detection cannot occur until the next inspection when the inspector reviews the records. This automatic sampling procedure is modeled after operations at the Rokkasho reprocessing facility [79]. A systematic and random

error of 0.2% are assumed for this process, for a total uncertainty of 0.3% [16]. As with NDA, the defender chooses the sample + analysis frequency.

5.4 Detection Probability Calculations

Table 5-II shows the defender and attacker options for the model reprocessing facility and defines the defender options that are applicable to each attacker option. Of these options, only two attacker options and five defender options are modeled in detail. The options that are not explicitly modeled are shown in grey in the table. As mentioned previously, this work focuses on a small subset of defender-attacker pairs to keep the scope manageable while still demonstrating investment decision making across multiple facilities; a more comprehensive treatment of defender-attacker options is a subject for future work. The defender options modeled in this work are based on two sources: (1) safeguards in place at the Rokkasho Reprocessing Plant in Japan; and (2) safeguards modeled in the Separations and Safeguards Performance Model [16]. Defender options A and B, shaded in green, are activities that occur during an inspection. These are containment/surveillance (C/S) and design information verification (DIV). Reviewing records from C/S activities is considered a routine inspection activity, and it occurs at every inspection the defender purchases. Design inventory verification is also considered a routine inspection activity, and it is conducted as frequently as C/S at no additional manpower cost to the defender. Destructive assay (DA) is an online monitoring system that can be operated essentially continuously (daily) or less frequently (every few days), depending on defender strategy. Though this system operates autonomously, inspector presence is required to review alerts raised by the DA sampling system, as these alerts are not transmitted remotely to an off-site assessor. Conversely, the Solution Measurement & Monitoring System (SMMS) is an online monitoring safeguard that operates continuously and sends alerts to inspectors remotely if an anomaly is detected. As noted for the enrichment facility, the detection probability calculation algorithms presented in this section are notional values with relative meaning, and as such they are not intended to be interpreted in an absolute sense.

It should be noted that at Rokkasho, inspectors use a “continuous inspection approach”, which means that inspectors are present on-site at all times and additional inspectors are brought on-site for monthly and annual inventories. The IAEA conducts routine safeguards inspections at

two reprocessing facilities, the Tokai Reprocessing Plant and the Rokkasho Reprocessing Plant, and these inspections account for 20% of the IAEA's total inspection budget [80]. The range of defender options modeled here is intended to present the defender with the option of selecting a manpower-intensive safeguarding strategy, like the one employed at Rokkasho, but also leave space for the defender to select less manpower-intensive strategies, if the latter is in fact optimal.

Table 5-II. Defender-attacker strategy pair summary for reprocessing facility

Defender Options	Attacker Options								
Activity	1	2	3	4a	4b	4c	4d	5	6
A	A1	A2	A3	A4a	A4b	A4c	A4d	A5	
B	E1	E2		E4a	E4b	E4c	E4d	E5	
C	B1	B2	B3	B4a	B4b	B4c	B4d	B5	B6
D	D1		D3						D6
E	C1	C2	C3	C4a	C4b	C4c	C4d	C5	C6
F	F1							F5	
G									G6
H	H1	H2		H4a	H4b	H4c	H4d	H5	

Defender Options:

A. Dual containment and surveillance (C/S)
B. Design Information Verification (DIV)
C. Solution Measurement & Monitoring System (SMMS)
D. Destructive Assay sampling
E. Non-Destructive Assay (PIMS)
F. Hybrid K-Edge Densitometer [81]
G. Lead Slowing-Down Spectroscopy [82]
H. UV-Vis spectroscopy and flow rate measurements

Attacker Options:

1. Diversion of chopped spent fuel pieces before dissolution
2. Diversion of TRU solution from TRU product tank
3. Diversion of spent fuel rod
4. Diversion of solution from process tanks
    a. UREX process tank
    b. CCD/PEG process tank
    c. Purex process tank
    d. TALSPEAK process tank

5. Diversion of TRU-bearing solution into hulls
6. Falsification of spent fuel specifications

5.4.1 Dual C/S DP Calculations

A1. Diversion of chopped spent fuel pieces detected by C/S

Containment and surveillance around the front-end hot cell containing the chopped spent fuel pieces is comprised of video surveillance and directional radiation detectors. As such, the detection probability for this safeguard is a function of both of these sensors.

Video surveillance

The DP for video surveillance is modeled identically to logged video images as a reprocessing facility. Thus the DP for the first inspection where video images are reviewed, $DP_{i=1}$, is 0.43. Because reviewing surveillance video is a human operation and prone to human error, human reliability analysis techniques are applied to degrade the DP for subsequent inspections. The defender selects the size of the team as part of her strategy, and the size of the team determines the extent to which the detection probability is degraded. A large team sees only small decrease in the DP for multiples subsequent inspections because there are multiple sets of eyes viewing the video, while a small team sees a more marked decrease in DP. The detection probability for this safeguard is calculated using Equation 4.8.

Directional radiation detectors

The directional radiation detectors are designed to verify the presence of a source and determine if the count rate from the source is lower than the nominal value, thus indicating that some material might be missing. If material is removed without proper authorization, the network of detectors records an alert in the C/S system, which is reviewed by inspectors at the next inspection. Unlike the review of video surveillance logs, this activity is not subject to human reliability analysis techniques because detection does not require study of images by humans. It is assumed that there are four neutron detectors arranged in a square at the corners of the base of the hot cell. It is further assumed that the four detectors work independently, and an alarm will be raised if *any* of the detectors registers a reading above the threshold value. An alternative paradigm for a network of detectors would be to apply data fusion methods to define

an alarm condition if any of the detectors raises an alarm or if the average reading for the detectors is above some other threshold. Data fusion is particularly useful for detecting the presence of a weak source against a relatively high background, particularly when the source is located along the edges of the detector arrangement [83]. In this work the network of detectors is used to confirm the presence of a high source term with the expected count rate, which is why data fusion can be neglected with little penalty.

Each neutron detector is modeled as a radiation-based detector-type system, as described in Section 4.3. The detection probability for the four-detector network with no data fusion is given in Equation 5.2.

$$DP = 1 - G_n(t)^4 \tag{5.2}$$

Where $G_n(t)$ is the cumulative Poisson distribution with mean n and threshold t. It is assumed that the four detectors are independent and $G_n(t)$ returns the non-detection probability for a single detector. The neutron source term is 1 x 10^8 n/s, as shown in Table 5-I, and an efficiency of 4% is assumed for each detector.[21,22] Assuming a count time of 60 seconds, the nominal counts in the detector n is 2 x 10^8 n. A constant false alarm probability of 0.01 is also assumed for the directional radiation detectors. An alarm is triggered if the observed neutron count rate is below the threshold level.

If the attacker diverts some mass Δm [kgSF] from the total mass m in solution (800 kg), then the neutron emission rate post-diversion S_P' can be calculated using Equation 5.3.

$$S_P' = (m - \Delta m) \cdot S_{P_{SF}} \tag{5.3}$$

Where $S_{P_{SF}}$ is the spontaneous fission emission rate per kg SF (1.4 x 10^5 n/s-kgSF). The signal observed in each detector is s is:

$$s = \epsilon \cdot t_c \cdot S_P' \tag{5.4}$$

Where ϵ is efficiency (0.04) and t_c is count time (60 sec).

[21] PIMS neutron detector efficiency is 0.9%/detector, with 4-6 detectors around each glove box [84]

[22] It is assumed that this efficiency value accounts for intrinsic efficiency and geometric configuration; thus geometric attenuation is not taken into account when calculating the counts in the detector from the source term.

The total detection probability for C/S against diversion of spent fuel pieces at inspection *i*, DP_{itot}, is the cumulative DP for both video surveillance and radiation detectors. For both the video images and radiation detectors, the equipment has the opportunity to *sense* and record an attacker event at each attacker event; however, *detection* does not occur until the defender reviews and assesses the records. Thus at each inspection when the inspector reviews records, she may view multiply recorded attacks. Her detection probability in this case is the cumulative sum of each individual recorded attack event. For example, if video images of two attack events have been recorded by the first inspection, the defender has an independent probability of 0.43 of detecting each event, or a total DP of 0.68. When HRA is applied to the review of video surveillance records, it is applied to the *per-event DP* (0.43 in the previous example), not to the total DP (0.68 in the previous example).

DP	$DP_{vl,i=1} = 0.43$ $DP_i \mid ND_{i-1} = 1 - \frac{1 + F_{team} \cdot ND_{i-1}}{F_{team} + 1}$ $DP_{drd} = 1 - G_n(t)^4$ $G_n(t) = 1 - {}^1/_2\left(1 - \text{erf}\left(\frac{t-s}{\sqrt{2} \cdot s_s}\right)\right)$ $DP_{i_{tot}} = 1 - (1 - DP_{vl}) \cdot (1 - DP_{drd})$	per inspection
Defender Parameters		
f	inspection frequency, f = {1 day^{-1}, 3 days^{-1}}	
Attacker Parameters		
T	attack duration, T = {7 days, 30 days, 360 days}	
f	frequency, f = {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
Payoff		
SF	0.50	

A2. Diversion of TRU solution detected by C/S

C/S is less effective against TRU solution diversion because the attacker does not physically enter the hot cell to remove material; thus, the cameras are unable to detect such a diversion. The DP for directional radiation detectors is modeled in the same manner as for the diversion of chopped spent fuel pieces, except that in this diversion scenario the attacker is diverting some mass Δm_{TRU} of TRU solution, not a mass of spent fuel. In order to calculate the signal in the detector for this scenario, it is first necessary to calculate the mass of spent fuel

from which Δm_{TRU} was extracted, referred to here as the *equivalent mass of spent fuel*. This value is calculated by dividing Δm_{TRU} by the mass fraction of TRU in spent fuel, as shown in Equation 5.5.

$$\Delta m_{\sim SF} = {}^{\Delta m_{TRU}}/_{x_{TRU}} \tag{5.5}$$

Where x_{TRU} is the mass fraction of TRU in spent fuel (0.01) and $\Delta m_{\sim SF}$ is the equivalent mass of spent fuel. Note that the tilde is used in the subscript as a reminder that the adversary is not actually diverting this mass of material, but is diverting a smaller mass of TRU material that is extracted from this mass of spent fuel. Once the equivalent mass of spent fuel has been determined, the DP can be calculated using Equations 5.3 and 5.4, as described for defender-attacker pair A1.

DP	$DP_{drd} = 1 - G_n(t)^4$ $G_n(t) = 1 - {}^1/_2\left(1 - \text{erf}\left(\frac{t-s}{\sqrt{2}\cdot s_s}\right)\right)$	per inspection
Defender Parameters		
f	inspection frequency, f= {1 day^{-1}, 3 days^{-1}}	
Attacker Parameters		
T	attack duration, T = {7 days, 30 days, 360 days}	
f	frequency, f= {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
Payoff		
TRU	1.85	

5.4.2 DIV DP Calculations

B1. Diversion of chopped spent fuel pieces detected by DIV

Design information verification is one of the core activities performed during a visual inspection at an enrichment facility, as described in Section 4.3. As such, the basis for design information verification detection probabilities for reprocessing is analogous to the DP for visual inspection at enrichment facility, though the DP is increased if the defender elects to use the 3DLRFD at the reprocessing facilities, because this equipment increases the probability of detecting a small visual anomaly.

In this diversion scenario, the attacker is diverting solid pieces of chopped spent fuel from a hot cell, and he is entering and exiting the hot cell through authorized access points. As

such, there will be fewer visual indicators of unauthorized activity than for the back-end scenario, which requires that the adversary install equipment to perpetrate the diversion. It is assumed for the front-end diversion that there may be some small visual indicators that an attack is ongoing, such as a piece of equipment in the hot cell having been moved or extraneous equipment, like equipment needed to handle the hot spent fuel pieces, being left in the hot cell. Recall from the enrichment facility that detection probability for minor indicators such as these is 0.29. This DP is assigned to this diversion scenario if the defender does not purchase the 3DLRFD. If the defender does purchase this additional equipment, it is assumed that the non-detection probability is decreased by 50% to give a DP of 0.65. Note that DIV will only detect the diversion of chopped spent fuel pieces *if the diversion is ongoing*, as it is assumed that once the diversion has concluded the attacker takes care to conceal any signs that a diversion has occurred. The defender also decides in which area to perform DIV if he purchases the safeguard (front-end or back-end), and the DP for this scenario is 0 if the defender chooses to verify the back-end.

DP	*if area* = 0 for $t > t_{end}$, $DP = 0$ for $t \leq t_{end}$ *if 3DLRFD* = 0 $DP = 0.29$ *if 3DLRFD* = 1 $DP = 0.65$	per inspection
Defender Parameters		
f	inspection frequency, *f* = {1 days^{-1}, 2 days^{-1}}	
area	area defender chooses to verify, *area* = {0, 1} where 0 is front-end	
3DLRFD	defender chooses whether or not to purchase equipment, *3DLRFD* = {0, 1}	
Attacker Parameters		
t_{end}	last day of diversion, t_{end} = {0, 30, 360}	
Payoff		
SF	0.50	

B2. Diversion of TRU solution detected by DIV

Unlike the diversion of spent fuel pieces from the hot cell, the diversion of TRU solution requires the installation of an unauthorized pipe to remove material. Thus design information

verification around the TRU product tank should uncover major visual indicators of a diversion. As described in the enrichment section, the DP for a major anomaly such as this is 0.60. If the defender elects to purchase the 3DLRFD, the DP is increased to 0.80. As described for the previous diversion scenario, this safeguard only has a chance of detecting a diversion if it performed in the correct area (in this case, the back-end) while the diversion is ongoing.

DP	*if area* = 1 for $t > t_{end}$, $DP = 0$ for $t \leq t_{end}$ *if 3DLRFD* = 0 $DP = 0.60$ *if 3DLRFD* = 1 $DP = 0.80$	per inspection
Defender Parameters		
f	inspection frequency, *f* = {1 days^{-1}, 2 days^{-1}}	
area	area defender chooses to verify, *area* = {0, 1} where 0 is front-end	
3DLRFD	defender chooses whether or not to purchase equipment, *3DLRFD* = {0, 1}	
Attacker Parameters		
t_{end}	last day of diversion, t_{end} = {0, 30, 360}	
Payoff		
TRU	1.85	

5.4.3 SMMS DP Calculations

C1. Diversion of chopped spent fuel pieces detected by the SMMS

If chopped spent fuel is diverted before dissolution, the solution in the front-end accountability tank will be missing mass, relative to the mass expected based on operator spent fuel declarations. Thus the density will be lower than the nominal front-end density, and the Solution Measurement & Monitoring System might detect this suppressed density. The SMMS is modeled as a detector-type safeguard with nominal density reading of 300 g/L and random and systematic errors of 0.2% [74]. Using Equation 4.3, the total uncertainty is 0.3%. The FAP is selected by the defender and can take values of 0.01 or 0.05.

$$n = 300 \tag{5.6}$$

$$s_n = 0.003 \cdot n \tag{5.7}$$

The total nominal mass in the accountability take is given by the product of volume and density. If the attacker diverts some mass, Δm [g], the actual mass in the tank is the nominal amount less

Δm. Dividing the actual mass by the total tank volume (which is assumed to be unaffected by diverted mass) gives the new density of the solution after the diversion. Equation 5.8 gives the post-diversion density reading, d' [g/L].

$$d' = \frac{V \cdot d - \Delta m}{V} \tag{5.8}$$

Where V and d are the nominal volume [L] and density [g/L], respectively. The new density reading is the detector signal, s, and is assumed to have a standard deviation of 0.3% relative, as described above. The probability of detecting this below-nominal density reading can be calculated using Equation 4.2.

DP	$t = n + \sqrt{2} \cdot s_n \text{erf}^{-1}(2FAP - 1)$ $s = \frac{V \cdot d - \Delta m}{V}$ $DP = 1 - {}^1/_2\left(1 - \text{erf}\left(\frac{t - s}{\sqrt{2} \cdot s_s}\right)\right)$	per day
Defender Parameters		
FAP	false alarm probability, FAP = {0.01,0.05}	
Attacker Parameters		
T	attack duration, T = {7 days, 30 days, 360 days}	
f	frequency, f = {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
Δm	mass of material removed per attack, Δm = {800, 8000, 80000 g}	
Payoff		
SF	0.50	

C2. Diversion of TRU solution detected by the SMMS

Diversion of TRU solution from the TRU product tank does not change the density of the material, because it is assumed that the material is homogenized at the time of theft. It does, however, change the volume level in the tank if the tank was initially at full static volume. As mentioned above, the nominal volume of the TRU product tank is 31 L. The density in this tank is 300 g/L, and it is assumed that all solute at this point is TRU. If that attacker diverts some mass of TRU solution that contains TRU mass Δm [g], then the new volume V' [L] is given by Equation 5.9:

$$V' = \frac{V \cdot d - \Delta m}{d} \tag{5.9}$$

As described for defender-attacker pair B1, the SMMS is a detector-type safeguard, in this case with a nominal reading n of 31 L, a standard deviation of 0.3% relative, and a signal given by Equation 5.7. The threshold below which an alarm will occur is given by Equation 4.1. The DP for the SMMS detecting diversion of TRU solution is given by Equation 4.2, using the specifications for n and s detailed here.

DP	$t = n + \sqrt{2} \cdot s_n \text{erf}^{-1}(2FAP - 1)$ $s = \frac{V \cdot d - \Delta m}{d}$ $DP = 1 - {}^{1}/_{2}\left(1 - \text{erf}\left(\frac{t - s}{\sqrt{2} \cdot s_s}\right)\right)$	per day
Defender Parameters		
FAP	false alarm probability, FAP = {0.01,0.05}	
Attacker Parameters		
T	attack duration, T = {7 days, 30 days, 360 days}	
f	frequency, f = {1 days^{-1}, 7 days^{-1}, 30 days^{-1}}	
Δm	mass of TRU removed per attack, Δm = {8, 80, 800 g}	
Payoff		
TRU	1.85	

5.4.4 DA DP Calculations

D1. Diversion of chopped spent fuel pieces detected by DA

As detailed in the section describing enrichment safeguards, destructive analysis is a sensitive and accurate technique. As such, it is assumed in this model to have a detection probability of 1 if a sample is taken from a batch that has been tampered with. If the attacker chooses to divert chopped spent fuel pieces, the solution in the front-end accountancy tank with have a lower TRU and uranium content than it should. This will be detected by sampling if the defender samples and analyzed the batch from which the attacker has diverted. Recall that it is assumed to take 24 hours for material from the fuel chopper to reach the front-end accountancy tank. Thus if the defender samples the day after an attack has occurred, the detection probability is 1. If the defender samples the day the attack occurs or more than one day after the attack has occurred, the DP is 0.

DP	$if\ t = t_{div} + 1$ $DP = 1$ $if\ t \neq t_{div} + 1$ $DP = 0$	per inspection event
Defender Parameters		
f	inspection frequency, f = {1 days^{-1}, 3 days^{-1}}	
Attacker Parameters		
t_{div}	day on which diversion occurs	
Payoff		
SF	0.50	

5.4.5 Detection Probability Calculations Sources Summary

Table 5-III summarizes the principles or literature sources on which DP calculations were based for the reprocessing defender options.

Table 5-III. Sources for reprocessing DP calculations

Defender Option	Source
Dual containment/ surveillance	Video: Railway station surveillance [46] DRD: Physical principles- CDF of Gaussian and [83]
Design Information Verification	Visual inspection of ship fractures [57]
Solution Measurement and Monitoring System	Physical principles- CDF of Gaussian
Destructive assay	Attribute sampling as described in [22]

5.5 Reprocessing Safeguards Costs

Reprocessing safeguards costs are assigned based on the scheme presented in Section 4.6 for CGEP costs. As with GCEP costs, the total cost for a safeguard is the sum of the amortized annual capital cost, the annual fixed O&M cost, and the annual variable O&M cost. The general cost information section presents costs in sim dollars for each safeguard, and the safeguard-specific cost information section provides details about the basis for these cost assignments.

5.5.1 General Cost Information

Capital costs

The capital costs for each safeguard are given in Table 5-IV. Details about each cost can be found in the safeguard-specific cost information section. Capital costs for DIV are only incurred if the 3DLRFD is employed.

Table 5-IV. Capital costs for reprocessing facility

Safeguard	Annual Capital Cost (s$)
C/S	125.9
SMMS	437.5
DA	750
DIV	(150)

Operations and Maintenance Costs- Fixed

Fixed O&M costs are incurred annually whether equipment is used or not. These costs are a percentage of the capital cost, as described in Section 4.6.1. Safeguards are characterized as requiring low (2% capital), medium (6% capital), or high (10%) capital fixed O&M costs, based on expert judgment. Table 5-V gives the fixed O&M costs.

Table 5-V. Fixed O&M costs for reprocessing facility

Safeguard	Annual Fixed O&M	Annual Fixed O&M Cost (sim dollars/yr)
C/S	video- high drd- low	2.09 2.10
SMMS	high	43.75
DA	low	15
DIV	low	3

Operations and Maintenance Costs- Variable

As for the enrichment facility, variable O&M costs are manpower costs associated with inspection, assessment, and analysis. Inspection costs are incurred when inspectors are present at the facility performing a task, such as reviewing C/S and DA records, or performing DIV with the 3DLRFD. Assessment costs are incurred when a person is tasked with processing and

evaluating incoming data from a system, as is the case with the SMMS. Analysis costs are incurred when a person performs material or chemical analysis, as is the case for DA.

It was noted in the enrichment section that inspector costs are estimated at $1,000 per inspector per day, or 10 s$. It is assumed that as the frequency of inspections increases, the per-inspection cost decreases, due to a decrease in certain costs associated with travel between the facility and headquarters and a decrease in certain per-trip costs, like obtaining a visa. A linearly decreasing relationship is assumed between inspection frequency and per-inspection cost. Table 5-VI lists the cost per inspection for each frequency option available to the defender. Additional inspection activities that are performed to supplement routine inspection activities (such as NDA, DA, and DIV) are assumed to cost 20% of the base inspection cost, because the inspector is already at the facility, so the addition of activities incurs a minor increase in cost. Note that the defender must pay for an entire year of inspections at her desired frequency, irrespective of the length of the simulation.

As for the GCEP, assessment time is estimated based on an employee who costs the defender $30/hr, and it is assumed that roughly 25% of the employee's time is dedicated to a given assessment task. Based on these assumptions, assessment time is assigned a cost of $60/day, or 0.6 s$. As with inspections, the defender must purchase an entire year of the assessment time at the frequency designated by her strategy.

Analysis time is assumed to cost 20% less at the reprocessing facility than at the enrichment facility. This reduction is made to account for the fact that samples do not have to be shipped, because they are analyzed in an on-site laboratory. The cost analysis is $200/batch of samples, or 2 s$. Table 5-VI summarizes the variable O&M costs.

Table 5-VI. Variable O&M costs for reprocessing facility

Type of Manpower Cost		**Cost in Simulation Dollars**
Inspection	Daily	5 per small team per insp.
	$7\ days^{-1}$	6.03 per small team per insp.
Add. Insp. activities	Daily	1 per add. act. per insp.
	$7\ days^{-1}$	1.21 per add. act. per insp.
Analysis		2 per batch
Assessment		0.6 per day

5.5.2 Safeguard-Specific Cost Information

A. Containment/Surveillance

Review of C/S records is part of a base inspection at the reprocessing facility. This activity requires the review of records from two different systems: video surveillance and directional radiation detectors. The total cost for this safeguard is the sum of the fixed costs from these two systems and manpower costs. Note that the review of records from both video surveillance and dual C/S are assumed to be one inspection activity.

Logged Video Images

It was assumed that the facility uses a 38-camera video surveillance system. This assumption is made based on the video surveillance system at Rokkasho, which uses a 38-camera system for surveillance in the process areas [84]. The cost of this system is estimated at $20,900, based on scaling up a commercially available six-camera system [64]. The system is assumed to be operable for ten years, with high fixed O&M costs ($290/year), incurring an annual cost of $2,299, or 22.99 s$ per year.

Directional Radiation Detectors

Based on the number of radiation detectors dedicated to C/S at Rokkasho, it is estimated that there are 14 directional radiation detectors at the model reprocessing facility [84]. Each detector is assumed to be a single-tube ^{3}He neutron detector. The cost for a four-tube neutron detector for radiation portal monitoring applications is approximately $30,000, so the cost for a smaller, one-tube detector was estimated at $7,500 [85]. The detectors in the C/S system are assumed to have a serviceable life of ten years, requiring low maintenance ($210/year), thus incurring a total annual cost of $10,710, or 107.1 s$.

The total cost for C/S is 130.09 s$ per year, plus 5 s$ per inspection day (for the total number of inspections per year).

B. Design Information Verification

Design information verification occurs as part of a basic inspection, and thus necessarily occurs at the same frequency as dual C/S review. Because it is part of basic inspection, there is no additional manpower cost to the defender once a basic inspection has been purchased. The

defender does have the option of purchasing the 3DLRFD, which is assumed to cost $150,000, and to have a lifetime of 10 years [86]. The 3DLRFD requires low maintenance ($300/year), incurring a total cost of $15,300/year or 153 s$/year.

C. Solution Measurement and Monitoring System

The SMMS is assumed to monitor 12 critical tank and vessels, as it does at Rokkasho [84]. The system uses sensitive dip-tube pneumatic pressure gauges and temperature gauges to monitor pressure, volume, and temperature, and to derive density. The cost of the hardware for the IAEA-installed 12-critical-vessel system at Rokkasho was approximately 2 million dollars, with an integrated software cost of approximately 1.5 million dollars [86]. To estimate a cost for the SMMS at the reprocessing facility modeled in this work, the combined Rokkasho SMMS cost of 3.5 million was scaled down according to annual throughput. This scaling assumes that the for a smaller facility, like the facility modeled here, there are fewer process vessels, meaning less measurement hardware (i.e. gauges and wiring) is required for the system. Further, because there are fewer processes vessels and fewer instruments, less data will be collected, thus requiring less data processing capability and storage. Because Rokkasho has a nominal annual throughput about four times larger than the facility modeled here, it was assumed that the system incurs a capital cost around $875,000, and the system is assumed operable for 20 years, incurring an annual capital cost of $43,750. This system is assumed to require high maintenance ($4,375/year), making the total annual cost $48,125, or 481.25 s$. Because this system transmits information continuously and remotely, inspection time is not required for this safeguard; however, the attacker does need to purchase assessment time, at 0.6 s$ per day.

D. Destructive Analysis

As noted in the GCEP cost section, the estimated cost for a thermal ionization mass spectrometer (TIMS) is approximately $750,000. Unlike for the enrichment facility, however, where this machine is used by many front-end fuel cycle facility, this piece of equipment is located in an on-site laboratory at the reprocessing facility, meaning it is used solely by the reprocessing facility. The equipment is assumed to have a serviceable life of 10 years, incurring an annual cost of $75,000. Low maintenance is assumed ($1500/year) for a total annual cost of $76,500 or 765 s$.

DA is an additional inspection activity, which costs the defender 20% of the base inspection cost per day (recall that base inspection cost varies depending on inspection frequency). DA also requires analysis, which costs the defender 2 s$ per batch of samples. Table 5-VII summarizes all costs for all safeguards, while Table 5-VIII illustrates the cost assessment for a sample defender strategy where the defender has purchased each safeguard, but has chosen to play the most basic version of each safeguard. Parameters for this strategy are given in Table 5-IX.

Table 5-VII. Summary of reprocessing safeguards costs

Safeguard		**Capital Cost (s$/year)**	**Fixed O&M (s$/year)**	**Variable O&M (s$/year)**	**Total Fixed Cost (s$/year)**
Base Insp.	C/S-video	20.9	2.09	5/insp 6.03/insp	22.99
	C/S- drd	105	2.10	0	107.1
	DIV	9	0.18	0	3 (150)
SMMS		437.5	43.75	0.60/day	481.25
DA		750	15	1/insp 1.21/insp 2/batch	765

Table 5-VIII. Sample safeguarding strategy cost at reprocessing facility

Safeguard		**Capital Cost (s$/year)**	**Fixed O&M (s$/year)**	**Variable O&M (s$/year)**	**Total Cost (s$/year)**
Base Insp.	C/S-video	20.9	2.09	307.53	330.52
	C/S- drd	105	2.10	0	107.10
	DIV	0	3	0	3
SMMS		437.5	43.75	216	697.25
DA		750	15	61.51 102	928.51
Total		**1313.4**	**65.94**	**687.04**	**2066.38**

Table 5-IX. Parameters for sample reprocessing strategy

Parameter	Value
Basic insp. freq.	7 $days^{-1}$
Basic insp. team size	small
FAP- drd	0.05
3DLRFD?	NO
FAP- SMMS	0.05
DA freq.	7 $days^{-1}$

5.6 PAYOFFS

The general method for calculating payoffs for a given defender-attacker strategy pair is presented in Section 4.7 Payoffs. Calculations for the FOM values for the two materials at the reprocessing facility are described below.

5.6.1 FOM Calculation- Chopped spent fuel pieces

A FOM value cannot be calculated for chopped spent fuel (SF) pieces, as spent fuel has an infinite bare-sphere critical mass [87]. A value of 0.50 was assigned to SF pieces for the purposes of this work. Implicit in the use of this value is the assumption that SF is more attractive to an adversary than natural uranium but less attractive than separated TRU. In practice the value of spent fuel to an attacker depends on the attacker's capability. Thus in future work two sets of analyses will be performed: one with the FOM of SF equal to 0.50, to simulate an adversary with little to no clandestine reprocessing capability; and one with the FOM of SF equal to the FOM of TRU, to simulate an adversary with ample clandestine reprocessing capability for whom the additional processing of spent fuel is a trivial barrier to weaponization. For the purposes of this work, the former adversary is assumed and a FOM of 0.50 is used for chopped spent fuel pieces.

5.6.2 FOM Calculation- TRU solution

The spent fuel vector used to estimate the FOM of the TRU solution is given in Table 5-X [88]. The relative abundance is the weight fraction of TRU solution each isotope comprises. This information was obtained from an ORIGEN run that generated weight fractions for each isotope of interest after a ten-year cooling period. The fresh fuel modeled was an 8x8 BWR

assembly with 4.4% enrichment and 40 MWd/kg burnup. Table IV also provides the density of each isotope used in the calculations. These densities are for the solid allotrope of the isotope at room temperature, which is the form the isotopes would be in in solution at the reprocessing facility.

Table 5-X. Spent fuel characteristics used to estimate TRU FOM

Isotope	Relative Abundance	Density (g/cc) at r.t.
Np-237	0.0806	20.5
Pu-238	0.0301	19.8
Pu-239	0.477	19.8
Pu-240	0.126	19.8
Pu-241	0.147	19.8
Pu-242	0.0695	19.8
Am-241	0.0467	12
Am-242m	0.0003	12
Am-243	0.0178	12
Cm-243	0	13.5
Cm-244	0.0052	13.5

Based on the spent fuel characteristics given above, the bare-sphere critical mass (BSCM) and decay power of the TRU were calculated using the metrics calculator spreadsheet described in Section 4.7.1. These values are given in Table 5-XI. The dose rate of TRU material ($\dot{D}_{TRU}$) is estimated based on the activity in Ci/kg for the TRU material (A_{TRU}) and the ratio of dose rate to activity for 90% enriched HEU, as shown in Equation 5.10. Recall that the dose rate for HEU was determined using MCNP calculations. The activity, dose rate, and activity: dose rate ratio for both HEU and TRU are given in Table 5-XII. The dose rate for TRU is in italics to indicate that the quantity is derived from the others in the table according to Equation 5.10.

$$\frac{\dot{\boldsymbol{D}}_{\boldsymbol{HEU}}}{\boldsymbol{A}_{\boldsymbol{HEU}}} = \frac{\dot{D}_{TRU}}{\boldsymbol{A}_{\boldsymbol{TRU}}} \tag{5.10}$$

Where:

$\dot{D}_{HEU}$- dose rate of HEU for 0.2M at 1 m [rad/hr]
A_{HEU}- activity of HEU [Ci/kg]
$\dot{D}_{TRU}$- dose rate of TRU for 0.2M at 1 m [rad/hr]
A_{TRU}- activity of TRU [Ci/kg]

Table 5-XI. Inputs used to calculate TRU FOM

Characteristic	Value
BSCM (kg)	16.3
Decay power (W/kg)	33.5
Dose rate (rad/hr)	0.0155

Table 5-XII. Values used to determine dose rate of TRU material

Material	Activity (Ci/kg)	Dose Rate (rad/h of 0.2M at 1 m)	Ratio (Activity: Dose rate)
HEU	1.96×10^{-3}	1.84×10^{-9}	9.39×10^{-7}
TRU	1.65×10^{4}	*0.0155*	9.39×10^{-7}

Inserting the values given in Table 5-XI into Equation 4.28, the FOM for TRU is calculated as 1.85. This value agrees well with the literature value. **Error! Reference source not found.** shows the FOM as a function of burn-up for several types of material, including TRU, ten years after reactor discharge [69]. Based on the figure, the FOM for TRU solution can be estimated at approximately 1.9. Thus the calculated value of 1.85 used in this model agrees to two significant figures with the literature value.[23]

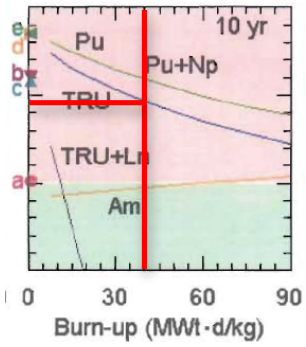

Figure 5-5. FOM as a function of burn-up 10 years after reactor discharge (red lines added)

[23] A value of 1.8 was used for reprocessing model results, but the value was updated to 1.85 for the integrated model and results

RESULTS

Chapter 6: Single Facility Results

This section presents the results for the stand-alone enrichment and reprocessing facilities. The chapter is divided into two major sections: enrichment results and reprocessing results. The results from the enrichment model are further subdivided into alpha sensitivity, budget sensitivity, background DP sensitivity and convergence. The reprocessing section presents the results of the alpha sensitivity analysis and the budget sensitivity analysis.

6.1 ENRICHMENT MODEL RESULTS

In order to validate the detection probabilities and payoffs generated by the simulation model, results for each defender-attacker strategy pair were compared against results produced from hand calculations. Validation was done in two rounds—the first round was a comprehensive validation that checked to ensure the simulation was working properly by testing every permutation of each individual safeguard against every permutation of each attacker option. The second round tested the cumulative detection probability calculations by testing defender strategies with multiple active safeguards. Edits were made to code as needed to ensure that model calculations produced the expected results.

6.1.1 Validation

Initial validation was performed to verify that the simulation model generated detection probabilities as intended. Each safeguard was tested independently against each attacker option, including every permutation of each safeguard against every permutation of each attacker option. Table 6-I shows the total number of safeguards, attacker options, and permutations of each in the model when the validation was conducted. Not all safeguards are effective against all attacker strategies, thus eliminating the number of safeguard-attacker option pairs that needed to be tested. Considering only viable safeguard-attacker options pairs, a total of 2,214 simulation results were generated and validated against hand calculations. Hand calculations were performed as evaluations in a separate Excel spreadsheet. Edits were made as needed if discrepancies arose, and the end result was that in all cases, the hand calculations and the values

generated by the simulation model produced the same DP value. This exercise confirmed that the simulation model performs detection probability calculations as expected.

Table 6-I. Scope of validation

Safeguard	Permutations	Attack Option	Permutations
Inspection	8	Cylinder theft	4
Passive seals	4	Some material from a cylinder	40
NDA	4	Some material from a cascade	30
DA	4	Cascade re-piping	27
Video- transmitted	2	Cascade recycle	45
Active seals	2		
CEMO	4		

While the exhaustive initial validation tested to ensure that the simulation model worked properly for a single safeguard active against a single attacker option, the secondary validation was conducted to ensure that the simulation model combined DPs correctly for defender strategies where multiple safeguard are active. To perform this check, five defender strategies comprised of multiple active safeguards were tested against each attacker option. Note that each defender and attacker strategy is assigned a strategy number; these numbers are used to uniquely identify each defender and attacker strategy in the model and have no physical meaning. Table 6-II provides parameter descriptions for each of the five defender strategies used in the validation. Because many of the safeguards require that the defender purchase inspections before purchasing said safeguard (e.g. the defender cannot purchase NDA without first purchasing inspections), inspections were active in all five defender strategies. All of the safeguards were active in at least one of the strategies, and the last strategy tested featured all nine safeguards.

The attacker strategies against which the defender strategies were validated are given in Table 6-III.The duration and frequency of the attacker options was intentionally varied to test over a range of scenarios. As before, the simulation output was compared to hand calculations performed in a separate Excel spreadsheet for each defender-attacker strategy pair. The simulation model and calculated payoff results were equal for all strategy pairs shown.

Table 6-II. Defender strategy descriptions—validation

Strategy	Active safeguards	FAP	Number[a]	Count time (s)	Frequency (days^{-1})	Team size
D202905	Inspection	0.01	---	---	7	small
D206550	Inspection	0.01	---	---	7	small
	Passive seals	---	0.5	---	7	---
D208170	Inspection	0.01	---	---	7	small
	Passive seals	---	0.5	---	7	---
	NDA	0.01	---	---	28	---
	DA	---	0.33	---	28	---
D203139	Inspection	---	0.33	---	7	small
	Video-transmitted	---	---	---	---	small
	Active seals	---	1.00	---	---	---
	CEMO	0.01	---	300	---	---
D202908	Inspection	---	0.33	---	7	small
	Visual inspection	---	---	---	30	---
	ES	---	6	---	90	---
D208407	Inspection	0.01	---	---	7	small
	Passive seals	---	0.5	---	7	---
	NDA	0.01	---	---	28	---
	DA	---	0.33	---	28	---
	Video-transmitted	---	---	---	---	small
	Active seals	---	1.00	---	---	---
	CEMO	0.01	---	300	---	---
	Visual inspection	---	---	---	30	---
	ES	---	6	---	90	---

Table 6-III. Attacker strategy descriptions—validation

Strategy	Attacker option	Duration (days)	Frequency (days^{-1})	Items	Area	Mass (kg)	x_p
A2	Cylinder theft	---	---	2	feed	---	---
A76	Material theft- cylinder	30	7	2	feed	110	---
A196	Material theft- cascade	360	30	0.5	product	0.010	---
A210	Re-piping	30	1	0.1	---	---	0.197
A260	Recycle	30	7	0.5	---	---	0.90
A317	Undeclared feed	360	7	0.5	---	---	---

6.1.2 Defender strategy cost distribution

The cost of defender strategies ranges from 0 to 5900 s$. Figure 6-1 is a density function of defender strategy cost, showing how many of the 246,645 defender strategies fall in each 100 s$ increment. This figure was used to guide selection of defender budgets for model runs.

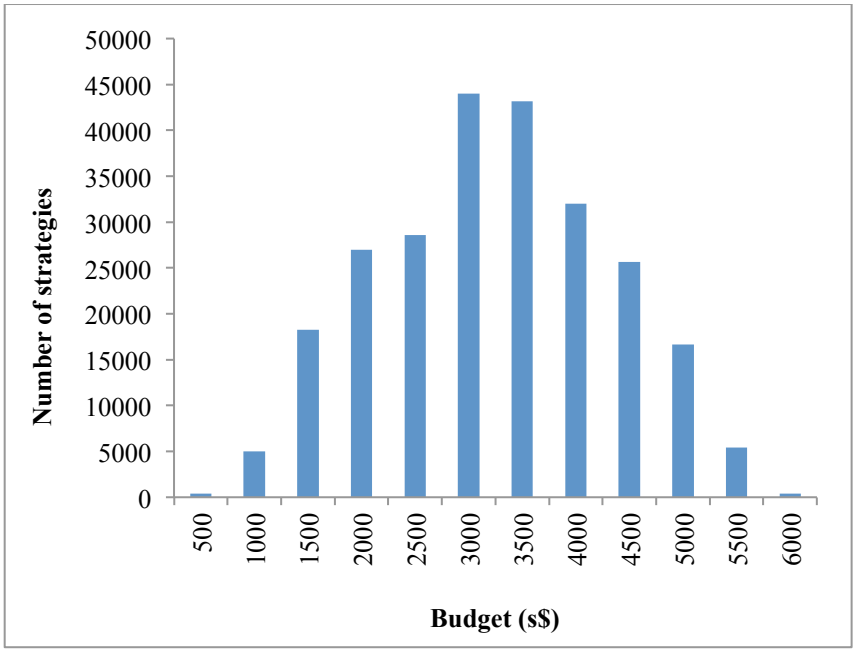

Figure 6-1. Defender strategy cost distribution

6.1.3 Alpha sensitivity

As described in Section 4.7.2, the equilibrium payoff is the scenario detection probability weighted by material quantity and attractiveness, where Figure of Merit metric is used to represent material attractiveness . Both a breakout-willing attacker and risk-averse attacker are modeled. Figure 6-2 shows the variation in the equilibrium payoff value as a function of alpha for three different budgets for the breakout-willing adversary. Additionally, plotted along the secondary axis is the 'normalized payoff', which normalizes the payoff value by the breakout scenario. This payoff ranges from zero to one, and takes the value one only when the attacker obtains the best possible material and the scenario DP is one. There are two distinct regions in the figure: (1) the region where alpha is greater than or equal to 0.3, and the payoff values are the same for all budgets, and (2) the region below alpha = 0.3, where the payoffs vary across the budgets. In the high-alpha region, the attacker is incentivized to obtain as much high-quality

material as possible even at the expense of certain detection, which drives him to play highly visible strategies with long durations. In each of these trials, the attacker chooses to dedicate 50% of the facility's enrichment capacity to recycle material through the cascade, and he perpetrates this attack daily for an entire year. For all three defender budgets shown in Figure 6-2, the DP against this attacker strategy is 1; thus, the equilibrium payoff is the same for all defender budgets.

In the low-alpha region, particularly when alpha = 0, it is clear that the defender is able to buy additional detection capability with a higher budget. For the case where alpha equals zero, the payoff is the overall scenario detection probability. Here the attacker plays a very conservative strategy, seeking only to minimize detection, without regard for the quantity or quality of material obtained. As alpha increase from zero to 0.2, the attacker shifts towards strategies that are easier to detect but provide a better material payoff, and the defender adapts her strategy accordingly. The difference in payoff between the three budgets decreases as alpha increases because as the attacker becomes less risk averse, the ability to buy extra detection becomes less consequential. Based on the results of this analysis, alpha was assigned a value of 0.19 for the remainder of the model runs and analyses.

Figure 6-3 is the same plot as Figure 6-2, but shows the results for a risk-averse adversary. This figure displays the same general trend as alpha increases, but it does not show the same stark contrast between low-alpha and high-alpha values as for the risk-preferring adversary, because in this case the adversary does not switch to an aggressive breakout-type strategy at high alpha values. The risk-averse adversary does switch to a more aggressive strategy of longer duration, but he still avoids strategies that will result in a DP of 1. Thus even when the attacker values quantity and quality of material, he still selects strategies with low enough overall detection probabilities that the defender's budget does affect the payoff. It is apparent from the figure that as alpha increases, the difference in payoff between the different budgets decreases, which occurs because as alpha increases, the attacker selects strategies designed to target higher value material, and these strategies are generally easier to detect and thus less sensitive to defender investment choices. This is particularly true at alpha = 0.30, where the payoff for 1500 s$ is only about 3% higher than the payoff for 200 s$. This is a result of the

game theoretic nature of the model—as the defender's budget increases and she is able to purchase more safeguards to detect material theft from the cascade, the attacker also changes his strategy from a mixed strategy comprised of material theft from the cascade and undeclared feed to a pure strategy of undeclared feed. The net result is only a small increase in overall payoff, despite the defender playing a much better strategy.

The hollow markers in both plots describe the normalized payoff to the attacker, or the share of his maximum possible utility. It can be seen that in the first plot there is a sharp rise in the attacker's utility from alpha = 0 to alpha = 0.1 as the attacker switches from a strategy that focuses solely on avoiding detection to a strategy that is incentivized by material value. As with the non-normalized payoff, for alpha ≥0.3, the attacker's utility is approximately constant because he is playing the same strategy against the same defender strategy each time. For the scenario with the risk-averse adversary shown in the second plot, the trend is nearly the opposite. For low alpha values all of the attacker strategies have similar utilities, though there is a slight increase as alpha increases, because the attacker prioritizes avoiding detection.

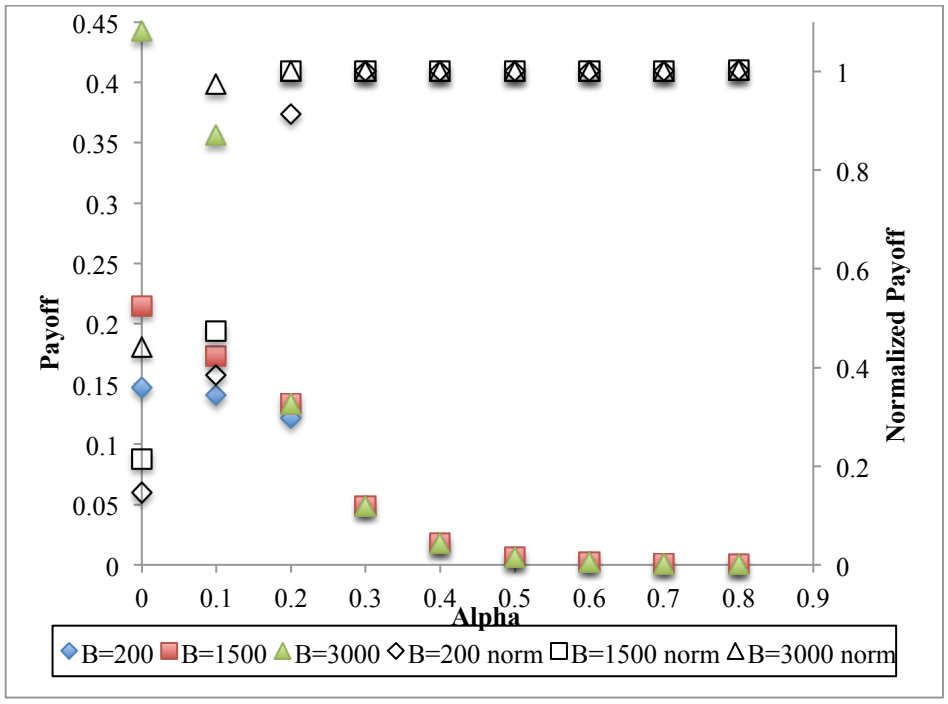

Figure 6-2. Payoff as a function of alpha for the breakout-willing attacker

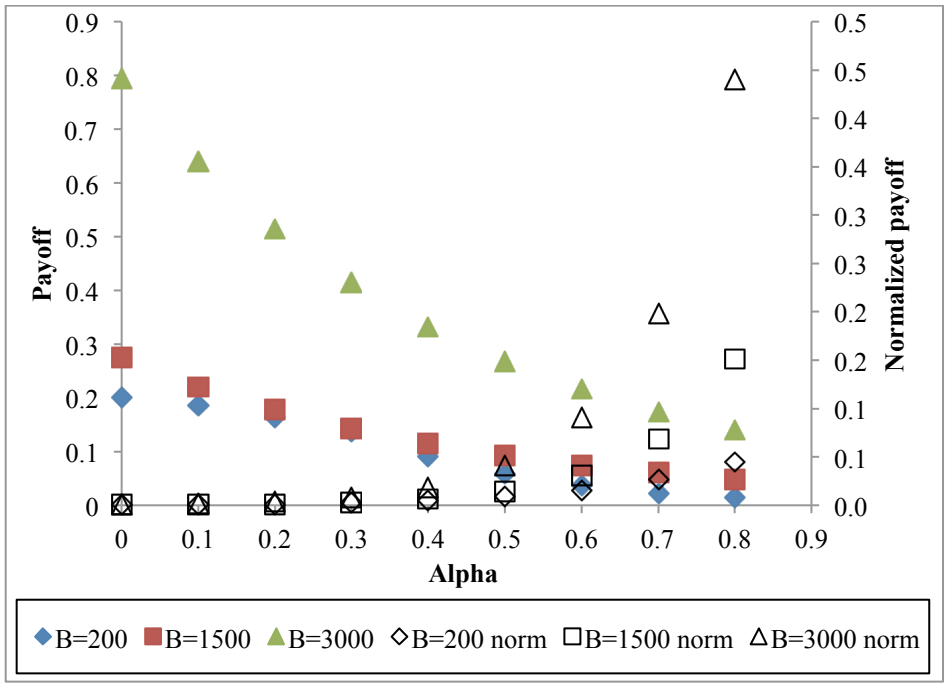

Figure 6-3. Payoff as a function of alpha for the risk-averse attacker

Figure 6-4 and Figure 6-6[24] show the variation in attacker and defender strategies as a function of alpha for B = 200 for the risk-preferring attacker, and Table 6-IV provides additional detail about each attacker strategy. In the low alpha region, both the defender and attacker play mixed equilibrium strategies. The fraction of each pure strategy played is given on the vertical axis. At alpha = 0 and alpha = 0.1, the defender plays a mixed strategy featuring both active seals (D90), and an inspection with NDA (D204120), while the attacker plays a mixed strategy of producing undeclared product from undeclared feed and stealing material directly from the cascade. The mixed strategy here represents randomization— the defender plays D90 31.5% of the time, meaning almost a third of the active seals applied at the facility are real seals that can relay information to a person waiting to assess an alarm, while the other two-thirds are dummy seals. The attacker can see the seals on the cascades, but cannot discriminate between real and dummy seals. The defender also plays the inspection + NDA strategy 68.4% of the time, meaning the defender randomly conducts only 68% of her permissible inspections.

[24] Note that results were generated with discrete alpha values and Figure 6-4 and Figure 6-6 show interpolations between these values. Behaviors between alphas may not be linear, as implied by the figures.

Similarly the attacker plays a mixed equilibrium strategy, which is best interpreted in the context of multiple attacks or ongoing attacks in which the attacker may shift between strategies. Over the course of an extended period, 39% of the time the attacker will feed undeclared feed through the cascade, and the other 63% of the time he will divert material directly from the cascade.

In both cases he selects these strategies for low alpha values because they are one-time attacks with low detection probabilities. The defender uses active seals to counter material theft from the cascades, and purchases an inspection to detect undeclared feed. As alpha increases from 0 to 0.1, the attacker increases the frequency with which he attacks the cascades and increases the fraction of the cascades dedicated to undeclared production, because both of these changes result in additional material production. At alpha = 0.3, the attacker commits to a pure strategy of recycling material through the cascade in a frequent and lengthy misuse. Likewise the defender commits to the inspection + NDA strategy because NDA is effective in detecting the overly enriched material produced in the attacker's strategy. The strategies for B = 1500, B = 3000, and B = 6000 demonstrate similar trends, with the attacker transitioning from undeclared product in the low-alpha region to recycling in the high-alpha region. As in this example, neither the defender nor attacker strategies show any variation from alpha = 0.3 to alpha = 0.8.

Figure 6-5 and Figure 6-7 are the analogous plots for the risk-averse adversary. The general trends shown in these plots mirror those of the risk-preferring adversary, though there are some notable differences. At low alpha values for both the attacker and defender strategies, material attractiveness and quantity do not strongly affect the payoff, so the risk-averse adversary chooses the same relatively low DP-strategy options as the risk-preferring adversary, but plays a different fraction of the strategies. Notably the risk-averse adversary plays a smaller fraction of material theft from the cascade, because this strategy is more easily detected than undeclared feed. The risk-averse attacker also continues to play mixed strategies at higher alpha values before switching to a pure strategy. While the risk-preferring attacker switches to an aggressive pure recycle strategy at for alpha = 0.3, the risk-averse attacker continues to play mixed strategies until alpha = 0.40, at which point he shifts to a more aggressive undeclared feed strategy that still has a non-zero evasion probability. The pure strategy played at high alpha

values for the risk-averse attacker, A320, has a DP of around 0.443, while the strategy played by the risk-preferring attacker, A276, has a DP of 1. This result is consistent with the preferences of both types of attackers as characterized by the payoff function.

The defender strategies played do not change based on the attacker's risk preference, though the fraction of each strategy played does. The defender plays a larger fraction of D204120 (inspection + NDA) against the risk-averse attacker, because this strategy is effective against undeclared feed, of which the attacker is plays more. The defender also does not shift to a pure strategy against the risk-averse attacker until alpha > 0.50, which mirrors the attacker's behavior.

Table 6-IV. Attacker strategy descriptions—enrichment

Strategy	Parameter 1	Parameter 2	Parameter 3	Parameter 4
A300- udfeed	dur = 7 days	freq = 7 $days^{-1}$	fraction = 0.0167	
A156- matcasc	dur = 7 days	freq = 7 $days^{-1}$	fraction = 0.0167	mass = 0.010 g
A302- udfeed	dur = 7 days	freq = 1 $days^{-1}$	fraction = 0.50	
A151- matcasc	dur = 7 days	freq = 1 $days^{-1}$	fraction = 0.0167	mass = 0.100 g
A276- recycle	dur = 360 days	freq = 1 $days^{-1}$	fraction = 0.50	x_p = 0.197
A320- udfeed	dur = 360 days	freq = 30 $days^{-1}$	fraction = 0.50	

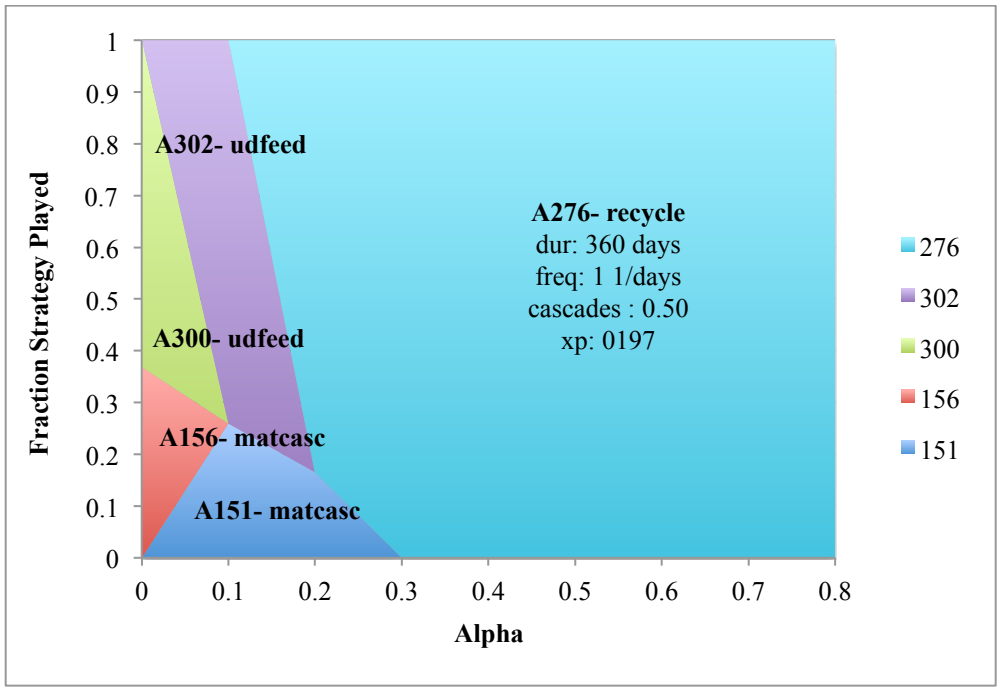

Figure 6-4. Attacker strategy as a function of alpha for breakout attacker (B =200)

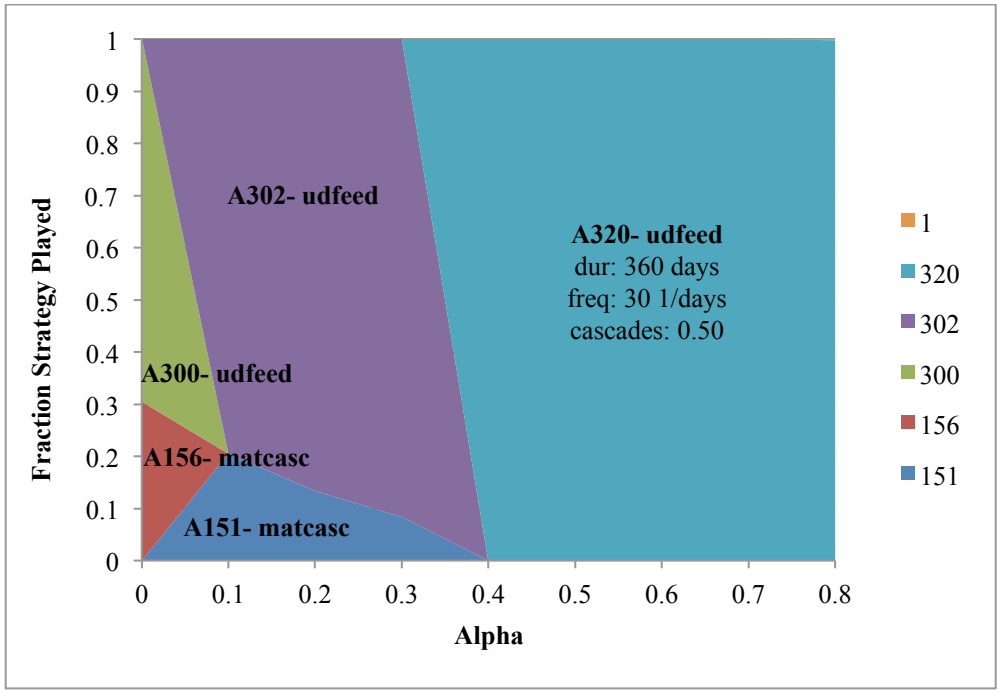

Figure 6-5. Attacker strategy as a function of alpha for risk-averse attacker (B =200)

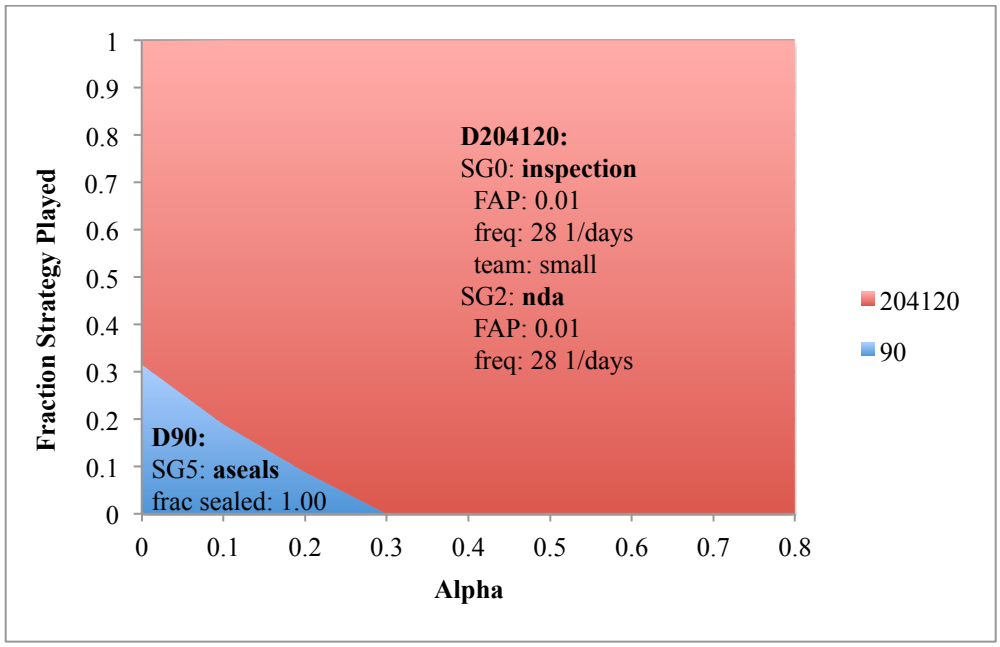

Figure 6-6. Defender strategy as a function of alpha for breakout attacker (B = 200)

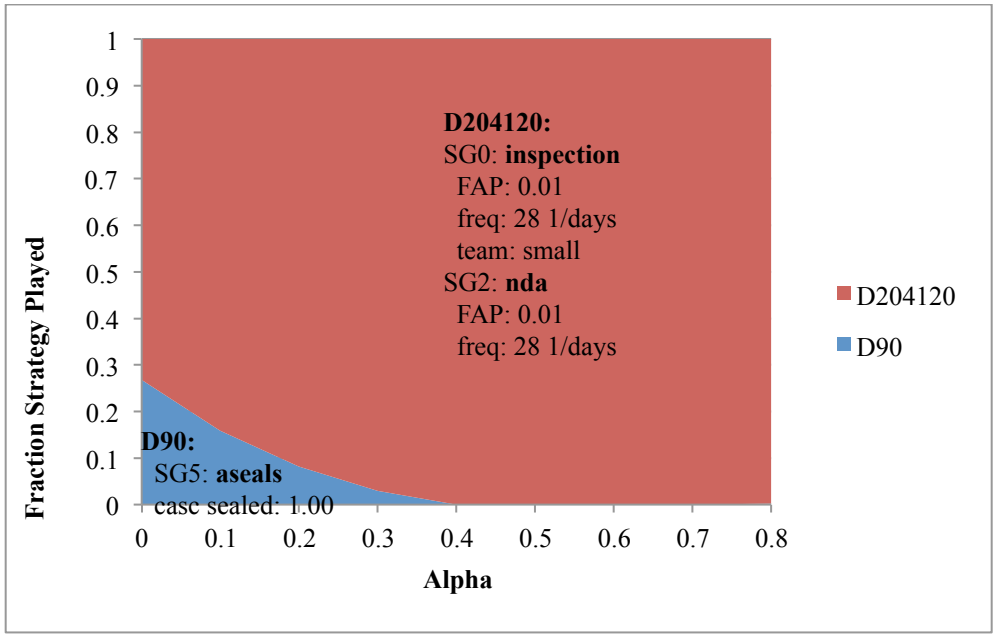

Figure 6-7. Defender strategy as a function of alpha for risk-averse attacker (B = 200)

While the figures above show the optimal payoffs and strategies for each alpha value, Figure 6-8 shows how *suboptimal* the non-optimal strategies are in each alpha region against the

breakout-willing adversary. These value are shown for B = 3000. Table 6-V enumerates the payoffs and defender/attacker strategies for each alpha value. For example, for B = 3000, defender strategy D225991 is optimal at alpha = 0.1. Figure 6-8 shows how the payoff for this strategy compares to the payoff for other strategies in different alpha region. For each data point, the payoff is for the strategy pair comprised of the indicated defender strategy and the optimal attacker strategy in that region (i.e. the D225991 point at alpha = 0.2 is for the D225991-A276 strategy pair, because A276 is the dominant attacker strategy in that alpha region). Table 6-VII provides details for the defender strategies listed in Table 6-VI. As in Figure 6-2, at alpha greater than or equal to 0.2, all of the defender strategies result in the same payoff value, because the payoff is being dominated by the aggressive attacker strategy. At lower alpha values, it is clear that defender strategy D102870 is suboptimal. This strategy features weekly inspections with a large team and weekly DA sampling. While this strategy is highly effective for high alpha values, where the attacker recycles material through the cascade to produce highly enriched material over an extended period of time, subjecting himself to many inspections, it is relatively ineffective against the one-time production of undeclared product from undeclared feed, especially owing to the long analysis time requires, which delays detection by 14 days. Undeclared production can be detected using only two safeguards: review logged video images during inspection and special inspections inside the cascade hall. Consequently any strategy that does not employ visual inspection is of limited utility against undeclared production. Further, the size of the inspection team only affects DP by reducing the human reliability effect described in Section 2.4 Human Reliability Analysis; that is, subsequent inspections are more effective for large inspections teams. Thus for attacker strategies of short duration, where the defender only conducts one or two inspections over the course of the simulation, the size of the team does not affect the payoff significantly. Combined these two factors make D102870 a suboptimal defender strategy when played against attacker strategies A300 or A302.

The value lost plot reveals a surprising result, namely that defender strategies D1846 and D225991 appear to be equally effective for alpha = 0 and alpha = 0.1, but the defender plays a pure strategy of D1846 for alpha = 0 and a pure strategy of D225991 for alpha = 0.1. Table 6-VIII shows the first five defender and attacker moves for both the alpha = 0 and alpha = 1

trials. The table shows that the first two defender and attacker moves are identical for the two trials, but in the second round, the pure strategy the attacker plays differs, because for the alpha = 0 trial the attacker seeks only to minimize detection, and in the alpha = 0.1 trial the attacker wishes to obtain more material. Recall that the strategy the defender plays in the third round is the pure strategy that will optimize her payoff in the next round against the attacker's mixed strategy history. Thus for alpha = 0, the defender is playing against an attacker who plays strategy A3 one-third of the time (cylinder theft from storage), strategy A198 one-third of the time (re-piping), and strategy A156 one-third of the time (material theft from cascade). Her best myopic response is to play D1846, which contains a suite of safeguards, including DA to counter the re-piping strategy and active seals to counter the material theft from the cascade. For the case of alpha = 0.1, the defender is playing against an attacker who plays strategy 3 one-third of the time, strategy A198 one-third of the time, and strategy A302 one-third of the time. In this case the defender does not need to purchase active seals, but can instead spend more money on a larger inspection team, which will help detect the cylinder theft and undeclared feed. Thus both the defender and attacker select strategies to optimize their utilities against the other players' mixed strategy histories.

Figure 6-9 shows the value lost plot for defender strategies at 3000 s$ against the risk-averse attacker. The plot shows that for a given alpha values, all of the defender strategies are equally effective against the optimal attacker strategy. Table 6-VI shows the defender and attacker strategies for each alpha value, and Table 6-VII gives details about the three defender strategies shown in Figure 6-9. Because payoff 2 incentivizes the attacker to prioritize avoiding detection, he chooses strategies that are difficult to detect, which gives the defender a limited range of effective strategies to play in response. All three defender strategies played have the same parameter specifications for inspection and visual inspection, which are the only two safeguards effective against undeclared feed, which is why both strategies yield the same detection probability for a given alpha.

While all three defender strategies result in the same payoff against the pure equilibrium strategy shown below, the defender switches between the strategies to deter the attacker from employing better strategies. The strategies shown in Table 6-VI are pure equilibrium strategies,

but in fact the attacker plays a very small fraction of other strategies for each alpha value. For alpha = 0.1-0.5, the attacker plays very small fractions of strategies A231 and A256, both of which are recycle strategies with a large fraction of the cascade dedicate to the misuse. In response to this, the defender plays strategy D499, because this strategy includes environmental sampling, which is an effective method to detect overly enriched product when a large fraction of the cascades are used (recall that the DP depends on the number of samples taken and the number of cascades dedicated). At alpha = 0.6, the attacker plays a small percentage of A225, which is a recycle strategy that only uses one cascade. In response to this attack strategy, the defender switches to strategy D1711, which includes DA to detect overly enriched product. Finally at alpha = 0.8, the attacker plays strategy A0, which is cylinder theft. This causes the defender to switch to strategy D1846, which contains transmitted video, which is capable of detecting cylinder theft. This result suggests that the optimal defender strategies are not strongly sensitive to alpha, which is consistent with an attacker who prioritizes avoiding detection over obtaining high value material.

Table 6-V. Equilibrium strategies and payoffs for the breakout attacker (B = 3000)

Alpha	Defender Strategy	Attacker Strategy	Payoff
0	D1846	A300	0.4425
0.1	D225991	A302	0.3560
0.2	D102870	A276	0.1336
0.3	D102870	A276	0.04887
0.4	D102870	A276	0.01787
0.5	D102870	A276	0.006531
0.6	D102870	A276	0.002388
0.7	D102870	A276	0.000873
0.8	D102870	A276	0.000320

Table 6-VI. Equilibrium strategies and payoffs for the risk-averse attacker (B = 3000)

Alpha	Defender Strategy	Attacker Strategy	Payoff
0	D1711	A300	0.4425
0.1	D499	A302	0.3560
0.2	D499	A302	0.1336
0.3	D499	A302	0.04887
0.4	D499	A302	0.01787
0.5	D499	A302	0.006531
0.6	D1711	A302	0.002388
0.7	D1711	A302	0.000873
0.8	D1846	A302	0.000320

Table 6-VII. Defender strategy descriptions

Strategy	Active SGs	Parameter 1	Parameter 2	Parameter 3
D1846	Inspection	freq = 7 $days^{-1}$	team size = small	FAP = 0.01
	DA	freq = 7 $days^{-1}$	cyl. sampled = 3	
	Video- trans.	team size = small		
	Active seals	frac. sealed = 1.00		
	Visual insp.	freq = 7 $days^{-1}$		
D225991	Inspection	freq = 28 $days^{-1}$	team size = large	FAP = 0.01
	NDA	freq = 28 $days^{-1}$	FAP = 0.01	
	Visual insp.	freq = 7 $days^{-1}$		
D102870	Inspection	freq = 7 $days^{-1}$	team size = large	FAP = 0.01
	DA	freq = 7 $days^{-1}$	cyl. sampled = 3	
D1711	Inspection	freq = 7 $days^{-1}$	team size = small	FAP = 0.01
	DA	freq = 7 $days^{-1}$	cyl. sampled = 3	
	Active seals	frac. sealed = 1.00		
	Visual insp.	freq = 7 $days^{-1}$		
D499	Inspection	freq = 7 $days^{-1}$	team size = small	FAP = 0.01
	Active seals	frac. sealed = 1.00		
	Visual insp.	freq = 7 $days^{-1}$		
	ES	freq = 7 $days^{-1}$		

Table 6-VIII. Defender and attacker strategy histories

	Alpha = 0		Alpha = 0.1	
Round	**Defender play**	**Attacker play**	**Defender play**	**Attacker play**
0		3		3
1	101655	198	101655	198
2	102870	156	102870	302
3	1846	300	225991	302
4	1846	300	225991	302
5	1846	300	225991	302

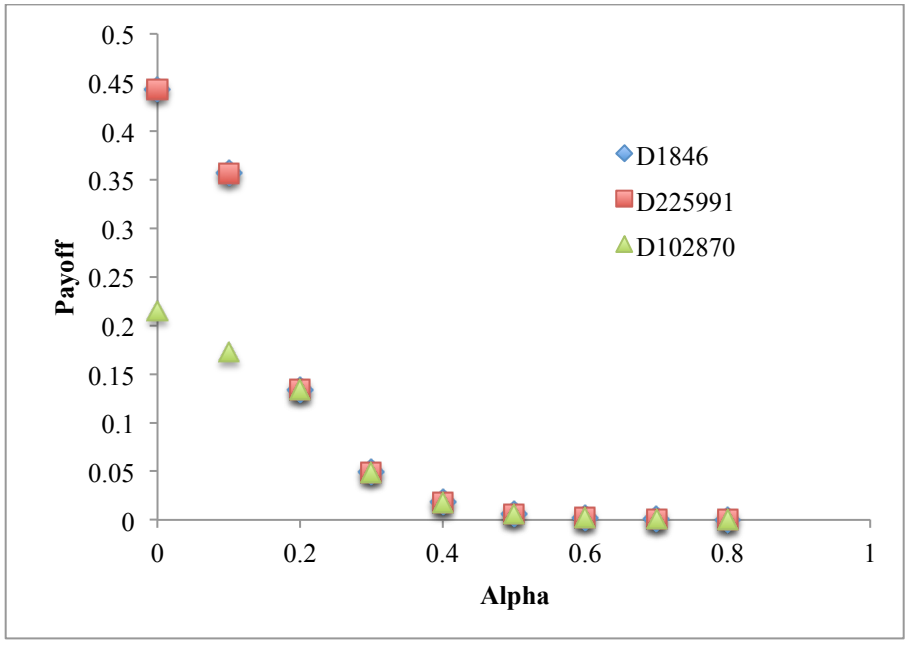

Figure 6-8. Value lose plot for breakout attacker (B = 3000)

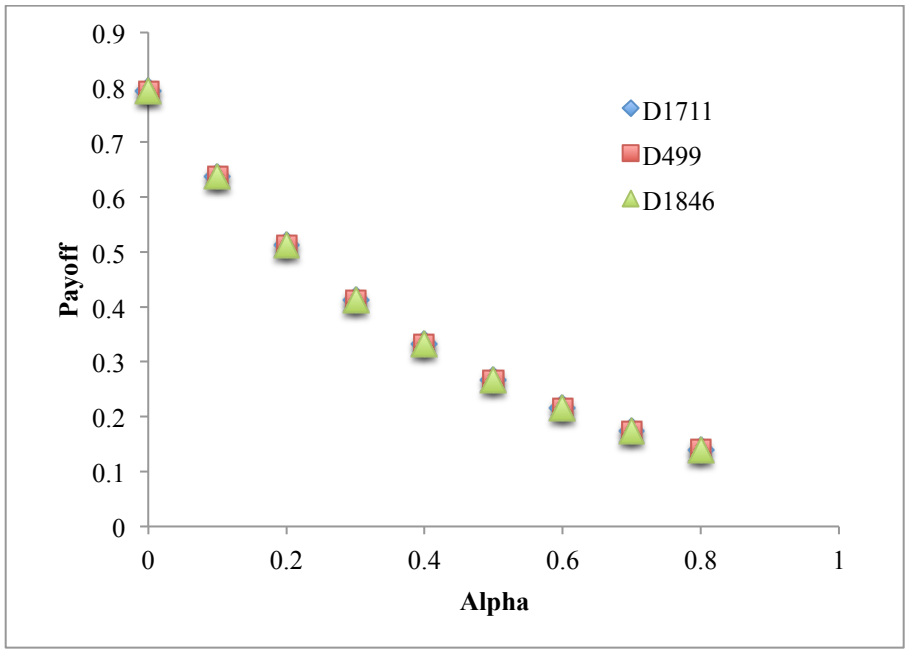

Figure 6-9. Value lost plot for risk-averse attacker

6.1.4 Budget Sensitivity

Figure 6-10 displays the efficient frontier, the optimal defender and attacker strategy for each budget. Two sets of results are pictured: alpha = 0.19 and alpha = 0, where the payoff equals the DP. Table 6-IX gives details about the defender and attacker strategies at the nodes labeled on the curves. For each budget, the nodes represent the most cost efficient defender strategy; that is, the strategy for which the defender gets the largest payoff increase per s$ spent.

For the weighted payoff curve where alpha = 0.19, the defender budget of 1530 s$ allows the defender to buy safeguards leading to the maximum possible detection probability. Past this point, spending additional money does not buy the defender more detection probability against this risk-preferring attacker, because the payoff above this budget is dominated by the aggressive attacker strategy that seeks high value material, even if detection is certain. As described above, once the defender budget is sufficiently high that the attacker no longer can easily evade detection by choosing conservative strategies, the attacker instead changes tack and attempts to

maximize his utility by obtaining large quantities of high value material,[25] even at the expense of adapting an easily detectable strategy. Thus for budgets over 1530 s$, the DP is effectively 1, and no change in defender strategy can affect the equilibrium payoff.

The curve for alpha = 0 is plotted on the right-hand vertical axis. These values are higher because they are not divided by a factor related to material quantity and FOM. The general shape of this curve mirrors that of the weighted payoff curve—there is an increase in payoff at 500 s$, and again for B > 2000, at which point the payoff reaches its maximum value. The alpha = 0 curve does have an additional feature, however, which is an additional increase in payoff from 1530 s$ to 2000 s$. This feature is not present in the alpha = 0.19 curve because for alpha = 0.19, at 1530 s$ the attacker switches to an aggressive, easily detected strategy. For both alpha values, budgets between 1520 and 1530 s$ were tested in one dollar increments to see if any additional, small steps existed, and the results indicated that they do not. The payoff remains constant from 500 s$ to 1530 s$, and then a discreet jump occurs at this budget. It should be noted in the regions of constant payoff from 500-1530 s$ and >2000 s$, the defender strategies do change.

As shown in Figure 6-1, most of the defender strategies cost between 1500 and 4000 s$. Because so many different strategies exist at this price point, even small increases in budget allow the defender to purchase additional capability to bolster the DP. The maximum DP is reached at B = 2000, because there are no additional safeguards the defender can buy that will are effective against this type of attacker strategy. The attacker strategy played in this case, production of undeclared product from undeclared feed, is a strategy to which the defender is quite vulnerable because it is difficult to detect; however, the strategy does not yield very high value material, which is why the attacker switches away as the material quality plays a more significant role in determining the payoff (as alpha increases from 0).

Figure 6-11 shows the efficient frontier against a risk-averse attacker. The similar shapes of the alpha = 0 and alpha = 0.25 curves follow from increases in payoff at the same budgets, as the defender chooses broadly the same safeguards sets at these two alpha values. In general the magnitude of the increase in payoffs at a given budget is the same, as well, with the exception of

[25] In this context, maximizing the attacker utility actually means achieving the lowest possible payoff, as the attacker is the minimizing player.

the increase in payoff that occurs at 500 s$. At this budget there is a sizable increase in payoff for alpha = 0, but only a very small increase for alpha = 0.25. The increase for alpha = 0.25 is small because there is little change in the attacker's strategy from 200 s$ to 500 s$. The attacker goes from playing 302 about 90% of the time to playing it 100% of the time. Likewise the defender shifts from playing mostly D204120 (inspection + NDA) to playing D204210 (inspection + NDA + active seals). The defender switches to this strategy to force the attacker away from stealing material from the cascade (A151), which yields more material from the attacker, but can be detected with a high probability by active seals. While this change in defender strategy force the attacker away from strategy A151, it does not increase the defender's ability to detect undeclared feed. Thus the small increase in detection probability seen at 200 s$ is from the change in the defender's membership in these strategies—at 200 s$, she plays D204120 about 95% of the time, and at 500 s$, she always plays D204210.

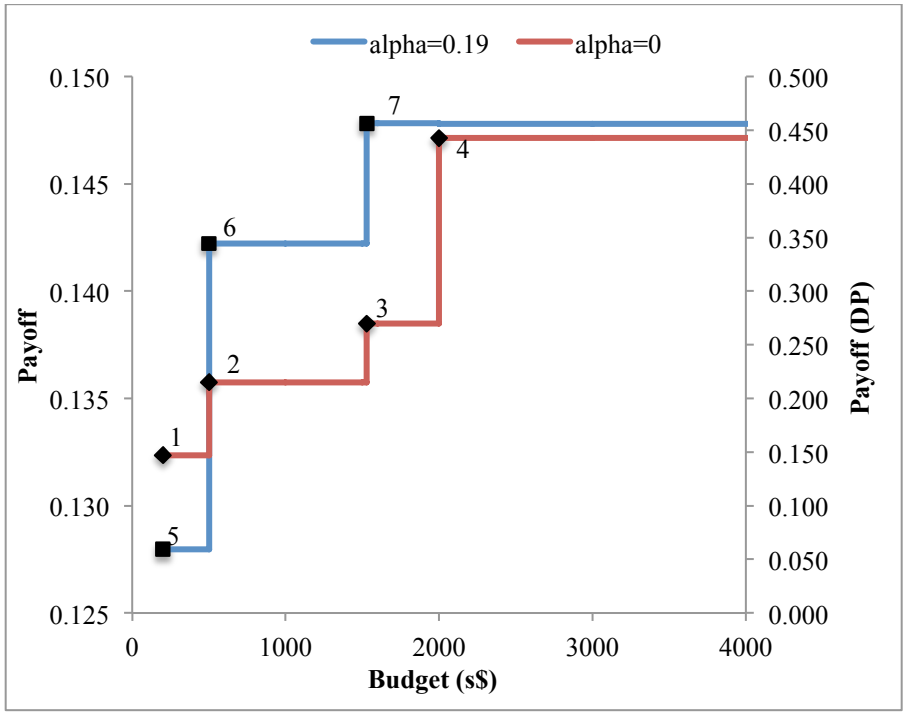

Figure 6-10. Efficient frontier for breakout-willing attacker

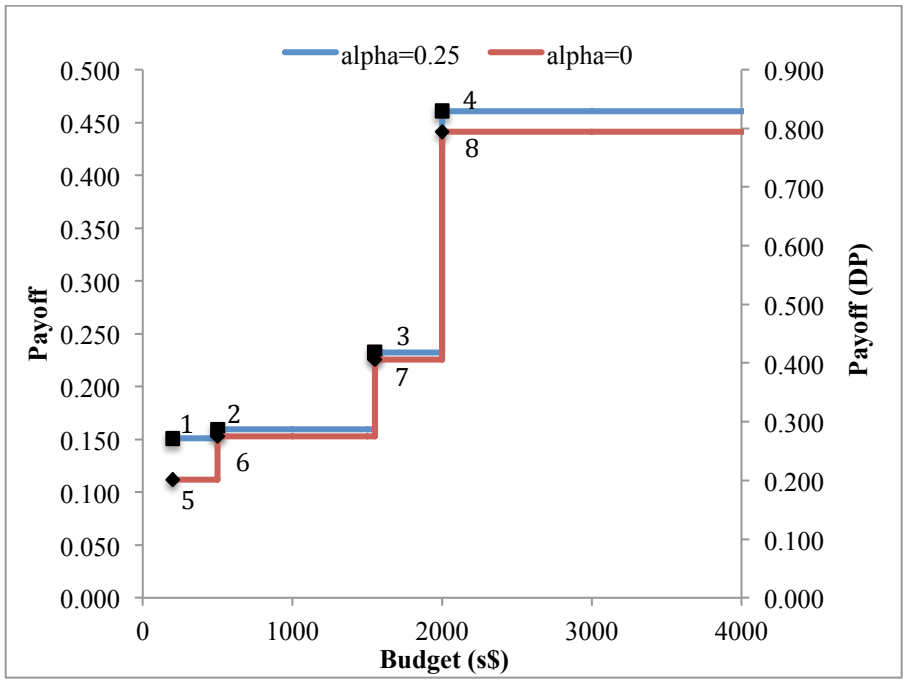

Figure 6-11. Efficient frontier for risk-averse attacker

Table 6-IX. Equilibrium strategies for risk-preferring attacker

Node	Budget	Defender Strategy	Attacker Strategy	Payoff
1	200	90- 0.315 204120- 0.684	156- 0.368 300- 0.632	0.1470
2	500	205560	300	0.2150
3	1530	1- 0.730 226080- 0.09 226215- 0.159	0- 0.069 300- 0.928	0.2697
4	2000	225991	300	0.4425
5	200	96- 0.102 204120- 0.898	151- 0.179 302- 0.817	0.1280
6	500	205560	302	0.1422
7	1530	1- 0.175 1851- 0.824	276	0.1480

Table 6-X. Equilibrium strategies for risk-averse adversary

Node	Budget	Defender Strategy	Attacker Strategy	Payoff
1	200	90- 0.053 204120- 0.947	151- 0.106 302- 0.894	0.1508
2	500	204210	302	0.1594
3	1550	1- 0.941 226086- 0.059	299- 0.049 302- 0.951	0.2326
4	2000	204211	302	0.4608
5	200	96- 0.268 204120- 0.732	151- 0.304 302- 0.696	0.2013
6	500	1710	300	0.2753
7	1550	1- 0.993 226215- 0.011	300	0.4064
8	2000	204211	300	0.7939

Figure 6-12 and Figure 6-13 plot the consequence and difficulty of twenty attacker strategies for a risk-averse attacker, where consequence is defined as the product of FOM and quantity of uranium, and scenario difficulty is the detection probability for a given scenario. In both plots, the hollow markers indicate the attack scenarios against a defender with a lower budget, and the purple markers illustrate attack scenarios against a defender with a higher budget. The attacker's ultimate objective is to obtain the most high value material possible with the lowest detection probability possible; that is, to choose the highest consequence, lowest difficulty attack. The attacks to which the defender is most vulnerable are circled in red on both plots.

It is clear from the plot that increasing the defender's budget greatly increases the scenario difficultly for all attacker strategies, though it does not increase the difficulty uniformly. This is because based on available safeguards options, some attack scenarios, like introduction of undeclared feed to produce undeclared product, remain easy to evade, even when the defender has unlimited resources. Fortunately for the defender, many of these scenarios yield very little consequence, as the attacker obtains low-enriched product. Note that in both plots the injection of extra money allows the defender to increase the scenario difficulty for the most attractive attack options. Thus with sufficient resources, the defender can make all of the attacker's options unattractive.

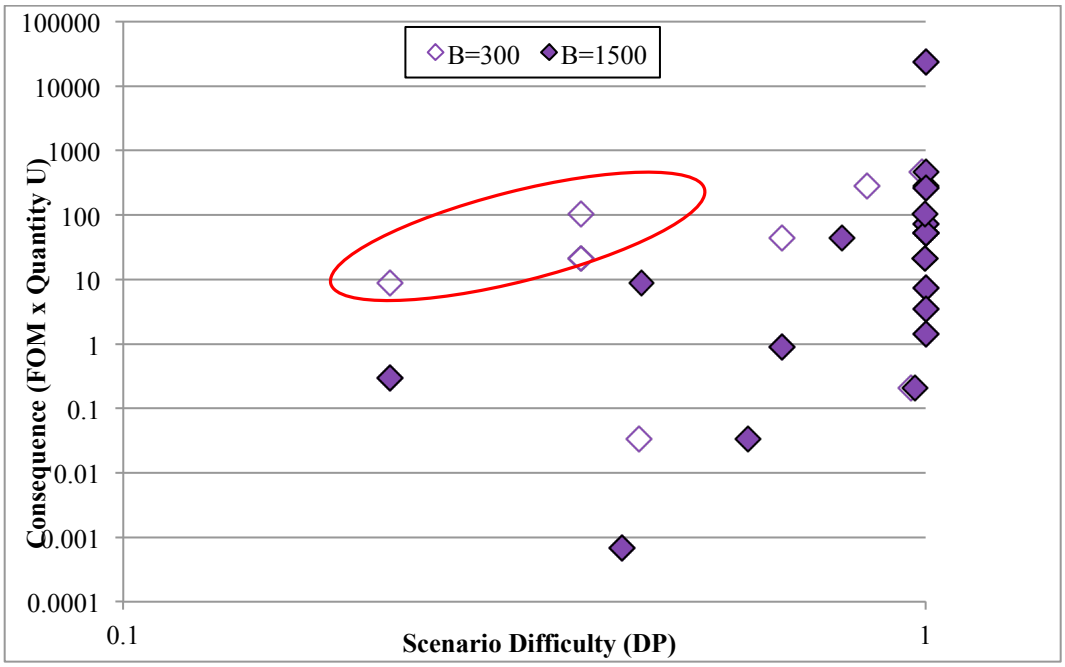

Figure 6-12. Consequence vs. difficulty for select attack scenarios (B = 300, 1500 s$)

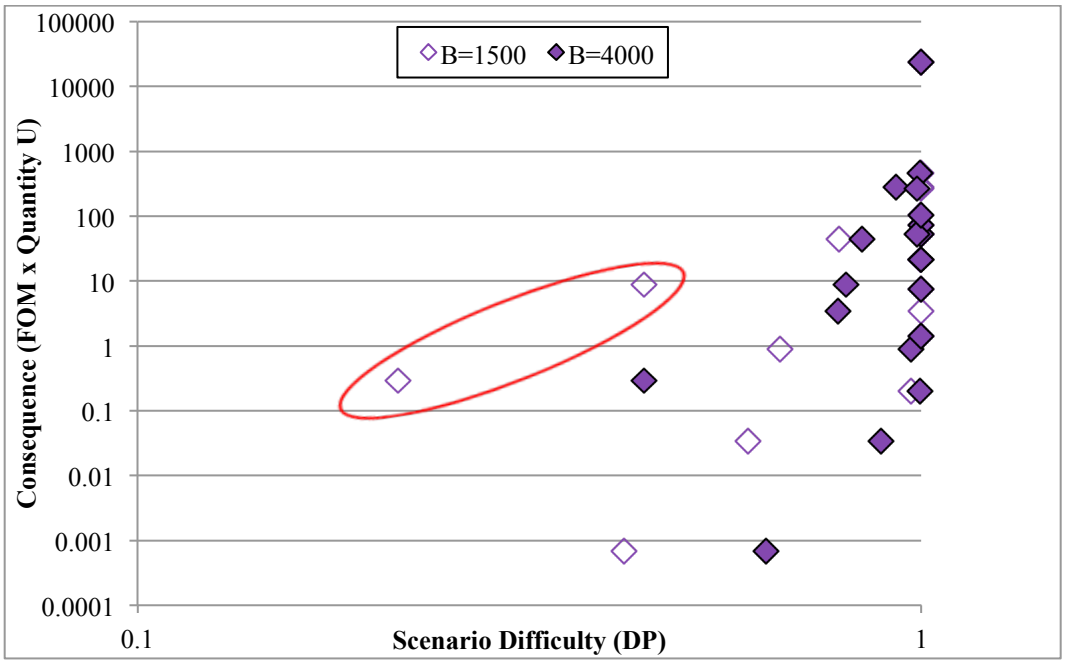

Figure 6-13. Consequence vs. difficulty for select attack scenarios (B=1500, 4000 s$)

6.1.5 Exogenous DP sensitivity

As mentioned in the methodology section, a daily background detection probability can be applied in the simulation model to serve as a proxy for exogenous detection means not explicitly modeled, including intelligence, which offers additional detection to the defender. If provided by a third party, intelligence information can be cost-free to the defender. Intelligence has a non-uniform probability of detecting different types of attacks; thus, the background DP is applied non-uniformly across the attacker options. To test the sensitivity of the equilibrium strategies to the background DP, the background DP against undeclared production was systematically varied from 0.001 to 0.1, and changes in payoff and defender and attacker strategy were recorded. Payoff function 1 was used for this analysis. The background DP for all other strategies was held at zero and alpha is set to zero for these trials, meaning the payoff equals the scenario DP. This trial was designed to mimic the real-world situation where intelligence collection may be able to detect unusual cylinder traffic into and out of a facility, as would be necessary for producing undeclared product from undeclared feed, even with no knowledge of operations inside the facility. Figure 6-14 displays the change in payoff for three different budgets as a function of background DP, and Figure 6-15 and Figure 6-16 show the changes in defender and attacker strategy as a function of background DP for B = 200.

Figure 6-14 shows that an increase in background DP results in a significant increase in the equilibrium payoff for value of DP less than or equal to 0.01. When the background DP is increased from 0.01 to 0.05 there is little incremental increase in the overall DP, because at this point the attacker has already shifted strategies to a different option that is unaffected by background DP. For background DP values less than 0.01, the attacker's best option is still undeclared product, despite the increase in DP due to the background DP.

The slopes of the regressions indicate that the incremental increase in payoff per unit background DP is greatest for B = 1500. At high budgets, like B = 4000, the defender is able to buy significantly more DP, so the baseline DP is much higher than for the B = 1500 case. Thus the relative difference made by the injection of additional DP is smaller for B = 4000 than for B = 1500. Conversely for B = 200, the baseline DP is so low that it is very easy for the attacker to pick an effective strategy that minimizes the equilibrium payoff to the defender. Thus even with

the additional DP provided by the background DP, the incremental increase in payoff is not as great because the attacker has a suite of attractive options from which to pick.

While the incremental increase in payoff is not as large for the low budget as it is for the intermediate budget, the sensitivity of strategy selection is much greater in the low budget case. Figure 6-15 and Figure 6-16 show the equilibrium defender and attacker strategies as a function of background DP. Figure 6-15 shows that even a 0.1% daily background DP changes the fraction of the pure strategies played in the equilibrium mixed strategy, and a daily background DP of 0.5% changes the strategies that comprised the equilibrium mixed strategy. This change in defender strategy occurs in response to anticipated changes in attacker strategy, displayed in Figure 6-16. With the introduction of any background DP, the attacker begins to shift away from undeclared production, because this is the only attacker option to which the background DP applies and by 1% daily background DP, the attacker moves away from undeclared production entirely. This result has big implications for the selection of inspection strategies at low budgets; namely that the optimally efficient inspection strategy in the absence of intelligence information is not necessarily the optimally efficient inspection strategy if intelligence information is available. Thus a cost-constrained must consider available reliable exogenous sources of detection in order to employ an optimally efficient strategy.

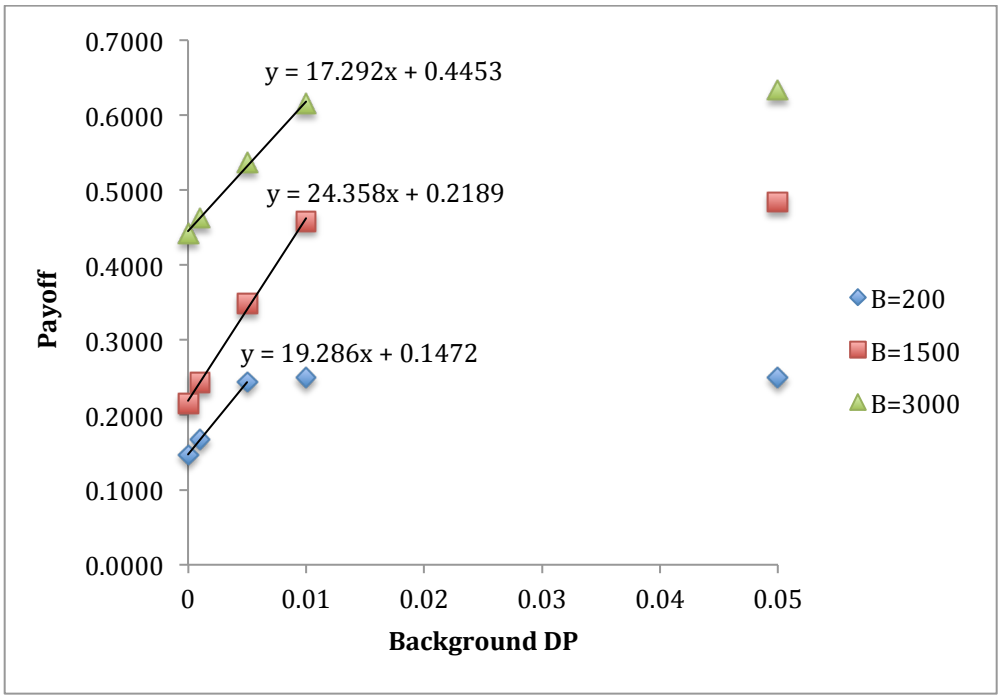

Figure 6-14. Payoff as a function of background DP

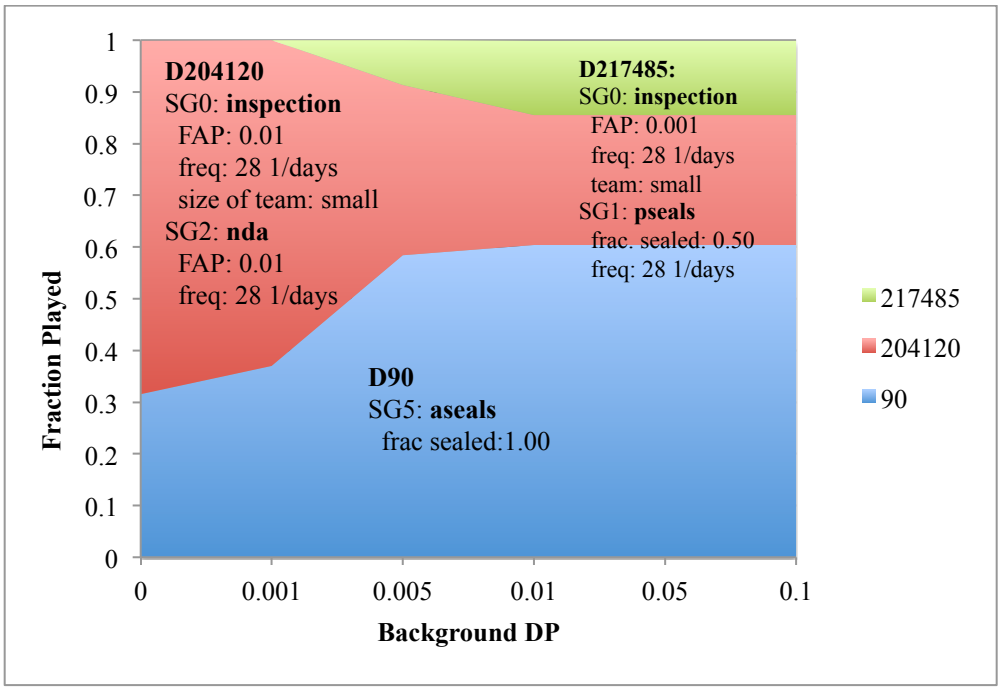

Figure 6-15. Defender strategy as a function of background DP for B = 200

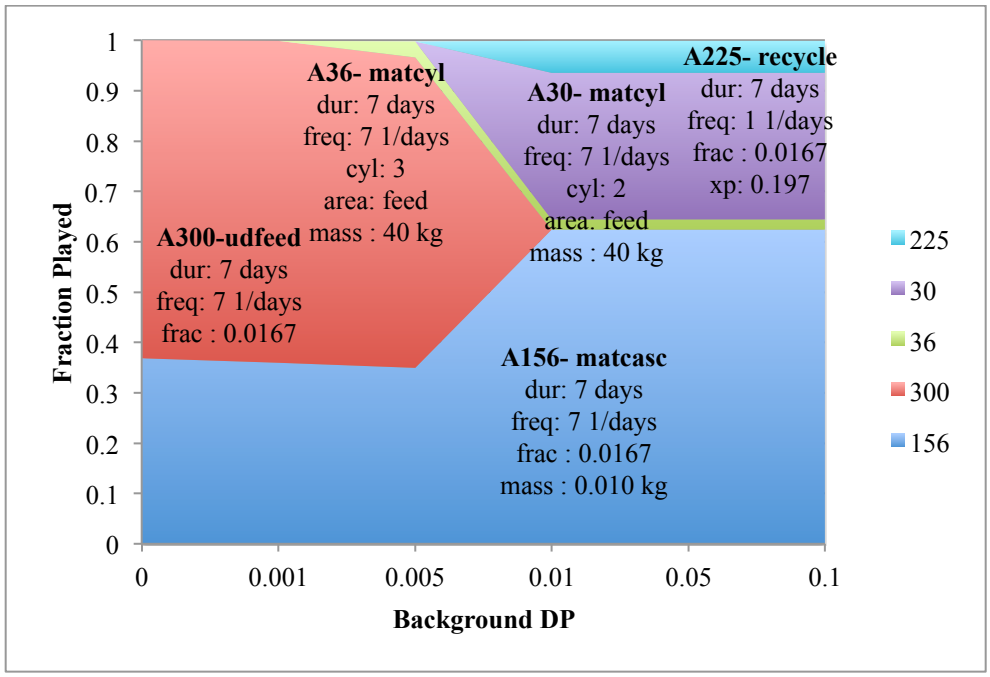

Figure 6-16. Attacker strategy as a function of background DP for B = 200

6.1.5 Convergence

To test the convergence speed of the fictitious play code used in this work, a series of trials were run, varying the ϵ value used (calculated using Equation 3.13 and recording the time and number of iterations required for the run. The series of trials were run at B = 200, B = 1550, and B = 3000, in order to observe any differences that may arise from the mixed equilibrium strategy at B = 200 and B = 1550 and the pure equilibrium strategy at B = 3000. The runs were conducted with alpha = 0.19, and ϵ was varied logarithmically from $\epsilon = 1\text{x}10^{-2}$ to $\epsilon = 1\text{x}10^{-5}$. Results are shown in Table 6-XI below. The last column gives the number of times the simulator was called to calculate a payoff value.

Table 6-XI. Convergence results for B = 200, 1550, 3000

B	m+n	ϵ	Iterations	Time (s)	Sim. Calls
200	334	0.1	84	3.344	266 828
		0.01	733	9.225	266 828
		0.001	7 057	66.58	266 828
		0.0001	30 872	283.8	266 828
		0.00001	37 206	342.8	266 828
1550	26 789	0.1	123	36.84	971 980
		0.01	1408	49.13	971 980
		0.001	14 425	168.0	971 980
		0.0001	41 903	421.9	971 980
		0.00001	46 804	467.1	971 980
3000	123 601	0.1	71	49.57	987 401
		0.01	755	54.51	987 401
		0.001	7 602	117.2	987 401
		0.0001	21 576	247.1	987 401
		0.00001	24 292	272.1	987 401

The data show that for all runs, the number of calls to the simulator remains constant as the convergence criterion becomes more stringent, indicating that no new payoff values are being calculated. Instead, the needed payoff values are calculated upfront and then used repeatedly to calculate the membership of each strategy component in the ϵ-approximate equilibrium. This characteristic of the FP algorithm proves advantageous as the simulation call becomes more computationally expensively, as achieving great accuracy requires more iteration through the FP process, but not more calls to the simulator. At B = 6000, where the defender can choose from the entire set of defender strategies, and ϵ = 0.001, the value used in most of the analyses, a simulation call takes an average of 6.480×10^{-5} seconds to complete. Because the payoff matrix is comprised of 246,645 defender strategies and 321 attacker strategies, a total of 79.2 million simulation calls would be required to pre-populate the matrix and solve the game using

conventional linear programming methods. The pre-population of the payoff matrix would thus take just over 5,130 seconds, or a little over 85 minutes per run (excluding trivial time required to initialize defender and attacker strategies and solve the linear programming problem). As the data in Table 6-XI shows, the time required for a run using the FP algorithm is on the order of 100 seconds, making this method approximately 50 times faster than the traditional approach.

A second result is the lack of dependence of number of iterations on the dimensions of the payoff matrix, as shown in Figure 6-17. Here budget is used as proxy for the size of the payoff matrix, as the defender has more viable strategies at higher budgets. Brown conjectured that the order of convergence for the FP algorithm should be independent of the dimensions of the payoff matrix, and thus the computation time should scale linearly with dimensionality of the matrix, and the data in Table 6-XI and Figure 6-17 support this conjecture [31]. The data show that while more iterations are required to solve the game for B = 1550 versus B = 200, B = 3000 requires the fewest iterations of all the trials. This suggests that the number of iterations needed is not a function of dimensionality, but of the number of attractive strategies available to the defender at a given budget. At B = 1550 the defender has not only many strategies to choose from, but many strategies that are comparable, but slightly different, in effectiveness. At B = 200 the defender has significantly fewer strategies to choose from, and at B = 3000 many of the less expensive defender strategies are deeply suboptimal, so the number of iterations required to determine the ideal strategy is limited. Note that while the number of iterations does not change as the dimensionality increases, the computation time and number of simulation calls do, simply because more payoff values must be calculated due to the increased number of defender options.

Figure 6-17 shows that the number of iterations required is initially inversely proportional to the convergence tolerance, ϵ. This relationship no longer holds true for $\epsilon < 0.001$, which occurs because the convergence is not strictly asymptotic and upper and lower bound on the equilibrium value approach at different rates.

A goal of this analysis was to verify that the convergence rate of the FP algorithm used is consistent with the rate reported in the literature, specifically the condition on k in Equation 3.12. Figure 6-18 shows a plot of *iterations* vs. $1/\epsilon$ for B = 200, 1550, and 3000. Also shown on the graph is a power law fit to all three sets of data. The fits show that the curves have the correct

general shape. The exponent value is nearly independent of ϵ for smaller ϵ values, but decreases as m+n increases (increasing budget), which is consistent with this exponent being bounded from below by m+n, as dictated by Equation 3.12.

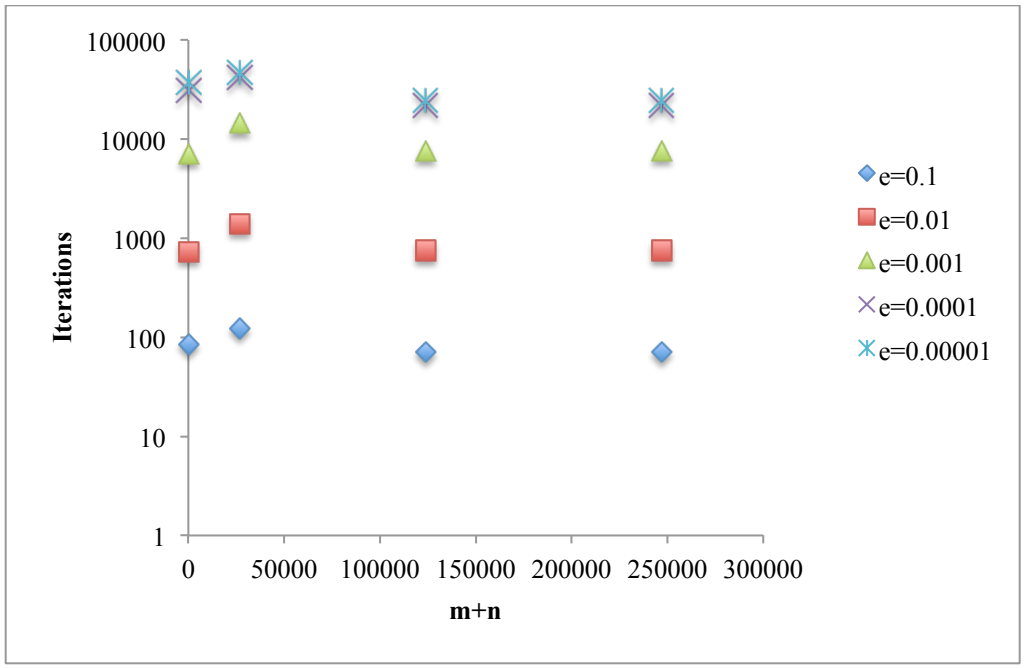

Figure 6-17. Iterations as a function of dimensionality

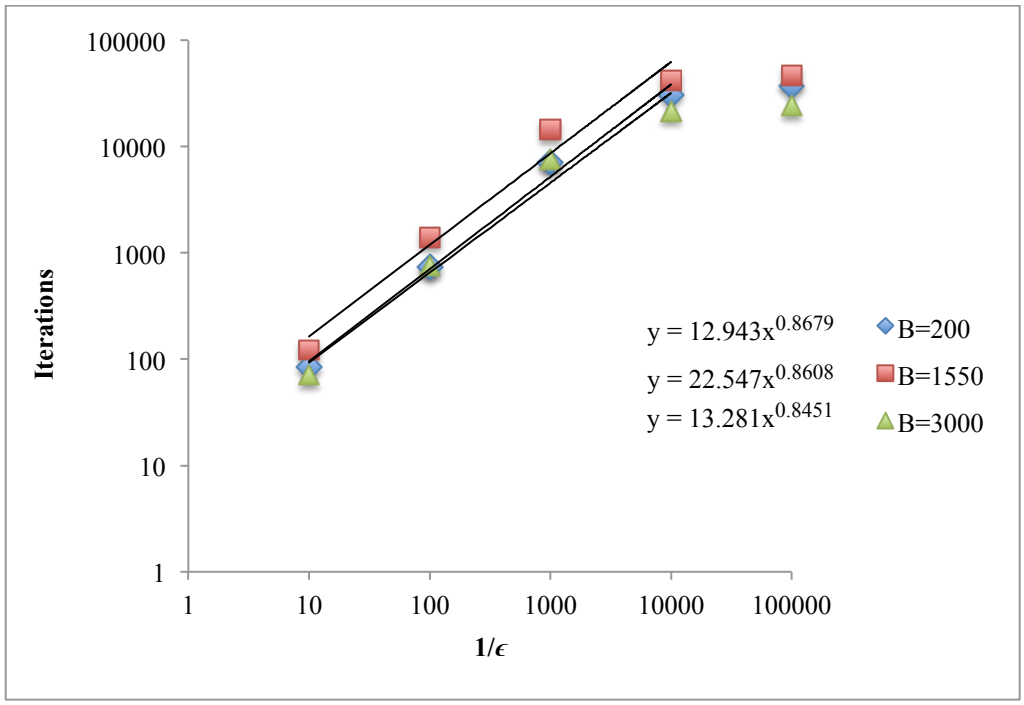

Figure 6-18. Iterations as a function of 1/ ϵ

6.2 Reprocessing Model Results

This section gives the reprocessing model results, including alpha and budget sensitivity results for both types of attackers.

6.2.1 Defender strategy cost distribution

Defender strategies at the reprocessing facility require budgets ranging from 0 to 9,000 s$. Note that this range is higher than for the enrichment facility, where the costs range from 0 to 5900 s$. Figure 6-19 shows the cost distribution for defender strategies. There are a total of 303 unique strategies available to the defender at the reprocessing facility.

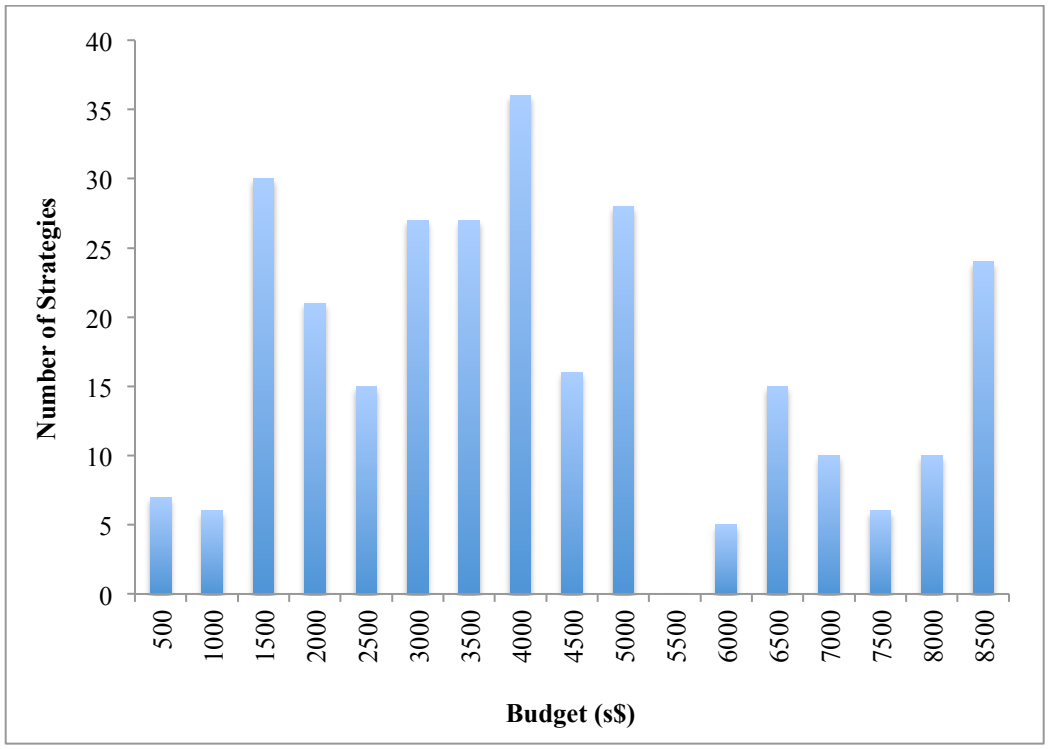

Figure 6-19. Defender strategy cost distribution

6.2.2 Alpha sensitivity

Two different types of adversaries are modeled: the risk-preferring adversary, who selects aggressive strategies to obtain high value material; and the risk-averse adversary, who seeks to avoid detection at all costs. The risk-preferring adversary is modeled using payoff 1, and the risk-averse adversary is modeled using payoff 2. Both payoffs are dependent on the parameter alpha, which characterizes the weight the attacker ascribes to material attractiveness. Higher alpha values correspond to an attacker who is incentivized to attain large quantities of high value material, even at the expense of selecting a risky strategy with a high detection probability.

Risk-Preferring Attacker

Figure 6-20 shows the change in payoff as alpha is varied from 0 to 0.7 for the breakout-willing attacker. The payoff is plotted at three different budgets: 1000 s$, 2000 s$, and 4000 s$. Also plotted is the normalized payoff. Recall that the defender seeks to maximize payoff, while the attacker seeks to minimize it. Recall also that the normalization rescales the payoff function

to take the value of 1.0 at any alpha for 'breakout' outcome where the adversary seeks to attain the most high-quality material at the expense of certainly being detected. At alpha equals zero the attacker places no value on material attractiveness, so the payoff equals the detection probability. Thus at higher budgets the payoff is higher, because the defender is able to purchase better safeguards to increase the DP. For all alpha values above zero, however, the normalized payoff is the same for all three budget levels. The reason for this is easily understood from the normalized payoffs. For any alpha level above zero, it can be seen that the normalized payoff levels off at one, which means the attacker is obtaining the best possible material, the DP is one, and the 'breakout' scenario mentioned above is reached. Thus increases in defender budget do not affect the payoff, because the DP is already one, so the defender is not able to purchase anything additional to further increase the payoff. This occurs because the payoff function used for the risk-preferring adversary encourages him to seek high-value material irrespective of the DP this strategy incurs. Defender investments only serve to ensure that the adversary is forced into the 'breakout' scenario where he must accept certain detection.

This effect is seen clearly in Figure 6-21, which plots attacker strategy as a function of alpha at B = 2000 s$. Figure 6-22 shows the defender strategy as a function of alpha for the same budget. As described above, Figure 6-21 shows that the attacker chooses very conservative strategies with low detection probability for alpha equals zero when he values all target materials equally, and then immediately shifts to the most aggressive strategy when higher alpha values encourage him to obtain higher-quality material. At alpha equals zero, the attacker plays a mixed strategy of diverting chopped spent fuel from the front-end accountancy tank and diverting TRU solution from the TRU product tank. In both diversion scenarios, he chooses the minimum possible diversion period (7 days) with the least frequent possible diversions (every 7 days), such that there is only one diversion event that occurs for both strategies. The attacker prefers a single diversion event where a small amount of material is removed over a series of diversions because this reduces his likelihood of being detected. Likewise the defender also plays a mixed strategy, employing dual C/S, design information verification, and the SMMS system. The strategy uses the 3DLRFD to bolster the DIV DP, but randomizes the location in which DIV is conducted

between the front-end and the back-end to optimize the probability of detecting either a front-end or back-end diversion.

At non-zero alpha values, the attacker switches to diverting a large quantity of TRU material in daily diversions over a year. Because the attacker is playing such an aggressive strategy, the payoff is not sensitive to the defender's strategy. The defender is able to choose from a host of strategies options, all of which yield the same DP of 1. Above alpha equals 0.3, the defender chooses a strategy well below budget that features only one safeguard, but still results in a scenario DP of 1. This transpires because there are no strategies available to the attacker that would allow him to obtain desirable material with a sub-unity DP. Therefore, faced with the choice of diverting material of low value while remaining undetected and obtaining useful material while certainly being detected, the attacker now values the material sufficiently to prefer the latter 'breakout' scenario. Table 6-XII gives the parameter details for the defender strategies played at B = 2000.

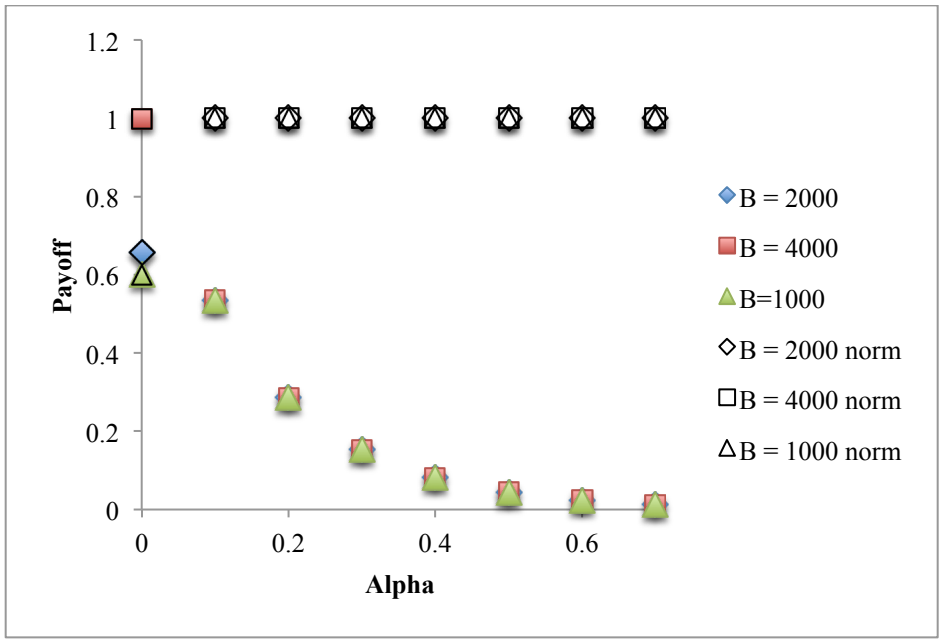

Figure 6-20. Payoff as a function of alpha for the breakout-willing attacker

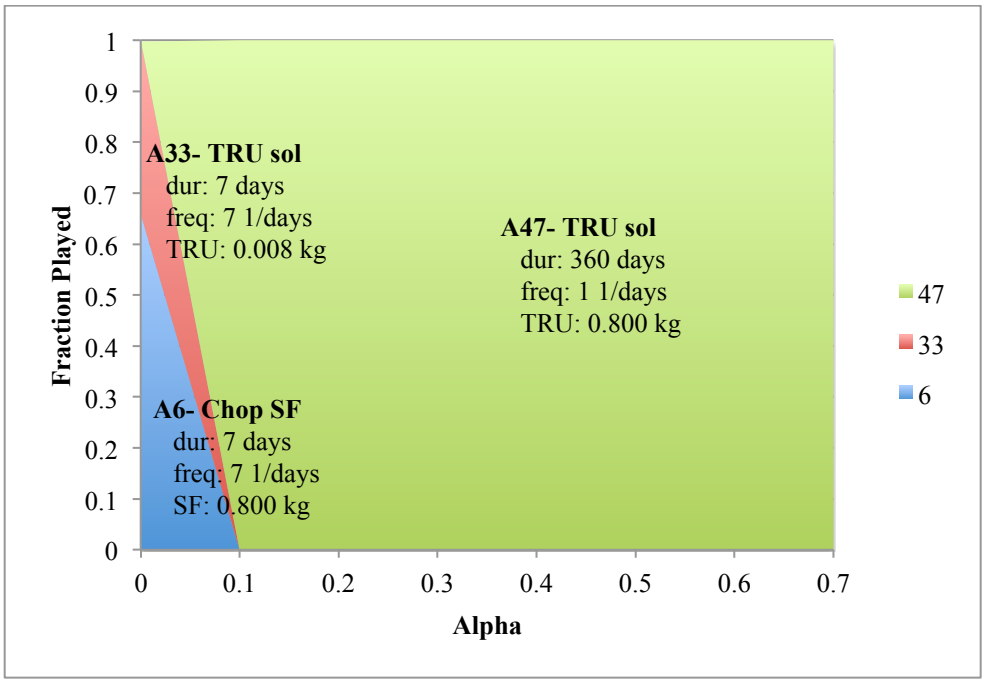

Figure 6-21. Attacker strategy as a function of alpha for breakout-willing attacker

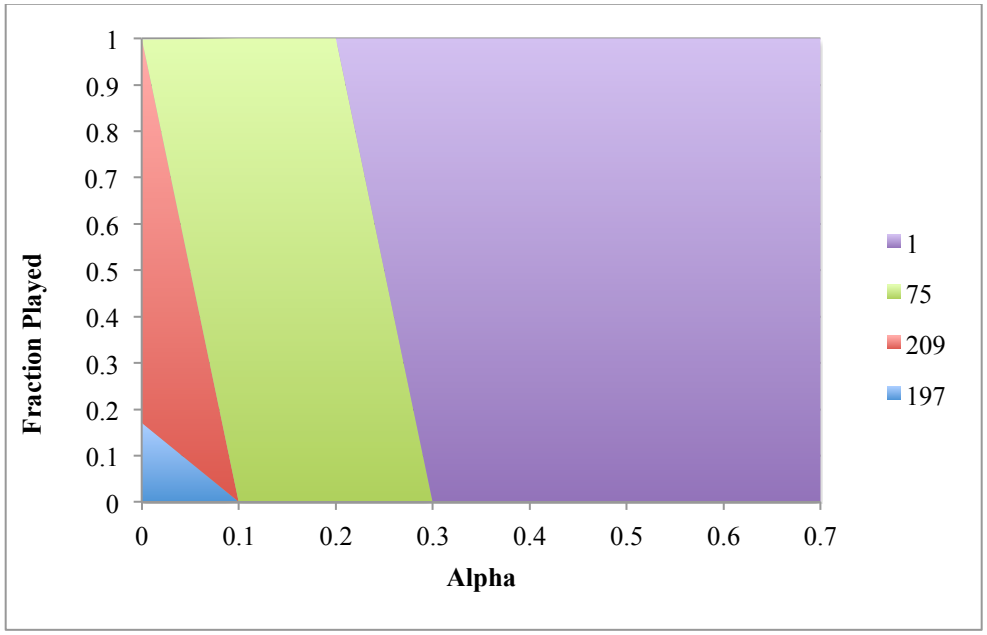

Figure 6-22. Defender strategy as a function of alpha for the breakout-willing attacker. See Table I for explanation of strategies.

Table 6-XII. Defender strategies played at B = 4000

Strategy	Active SGs	Parameter 1	Parameter 2	Parameter 3
D209	Dual C/S	freq = 7 days^{-1}	team size = small	FAP = 0.05
	DIV	area = back-end	3DLRFD	
	SMMS	freq = 1 days^{-1}	FAP = 0.05	
D197	Dual C/S	freq = 7 days^{-1}	team size = small	FAP = 0.05
	DIV	area = front-end	3DLRFD	
	SMMS	freq = 1 days^{-1}	FAP = 0.05	
D75	Dual C/S	freq = 1 days^{-1}	team size = small	FAP = 0.01
	DIV	area = back-end	no 3DLRFD	
D1	SMMS	freq = 1 days^{-1}	FAP = 0.05	

Risk-Averse Attacker

Figure 6-23. Payoff as a function of alpha for the risk-averse attacker shows the payoff as a function of alpha for the risk-averse attacker, and Figure 6-24 shows the normalized payoffs as a function of alpha. As for the risk-preferring attacker, the payoff is shown at three budgets: 1000 s$, 2000 s$, and 4000 s$. Figure 6-24 shows attacker behavior that differs from that of the risk-preferring adversary; namely, the attacker does not immediately switch to the breakout scenario for B = 1000 or 2000 s$. Instead, the figure shows a trend of increasing normalized payoff as alpha increases. The normalized payoff increases with increasing alpha because as alpha increases, the attacker is incentivized to pursue strategies that yield more high-value material, and these strategies are inherently easier to detect, resulting in a higher DP.

The normalized payoffs for B = 4000 resemble those seen for the risk-preferring adversary. For any value of alpha greater than zero, the attacker switches to the most aggressive 'breakout' strategy. This occurs because the defender's high budget allows her to purchase highly effective strategies, so for any attacker strategy, save the most conservative one, the DP equals one. Consequently, if the attacker cares at all about the value of the material he obtains, he will have no chance of evading detection. Because he has no chance of evading detection, even

the risk-averse attacker will be forced into 'breakout' where he chooses to maximizes his material utility while accepting the inevitability of detection.

Figure 6-25 shows the risk-averse attacker's behavior as a function of alpha for B = 2000 s$. Note than unlike the risk-preferring attacker, the risk-averse attacker does not switch to a breakout strategy until alpha = 0.6, because he is much more concerned with evading detecting than the risk-preferring attacker. At very low alpha values (alpha = [0,0.2]), the attacker plays a mixed strategy comprised of the two most conservative possible pure strategies. The mixed strategy diverts material from both the front-end and the back-end, and in both cases the minimal amount of period is diverted in a one-time attack. For intermediate values of alpha (alpha = [0.3,0.5]), the attacker switches to a mixed strategy comprised of two different pure strategies, A30 and A34, both of which involve the diversion of TRU solution. The attacker shifts from a mixed strategy where both SF pieces and TRU are stolen to one where only TRU is stolen because the higher alpha values incentivize the attacker to seek higher-value material. The mixed strategy played at intermediate alpha values is less conservative than the ones played at low alpha values—the attacker randomizes between stealing the minimal amount of material more frequently and stealing a larger amount of material as infrequently as possible. For high alpha values (alpha = [0.6,0.7]), the attacker's behavior is dominated by desire for high-value material, and the risk-averse attacker behaves in the same manner as the risk-preferring attacker, which is to shift to a breakout strategy of divert large quantities of TRU solution daily over the course of a year.

Figure 6-26 shows the defender's strategy against a risk-averse attacker as a function of alpha at B= 2000 s$. As she did against the risk-preferring attacker, the defender initially plays a mixed strategy that randomizes between front-end and back-end DIV, which is intended to counter the attacker's randomization between front-end and back-end attacks. As alpha increases and the attacker becomes increasingly motivated by material value, the fraction of strategy A57 played by the defender decreases, because this strategy is most effective for detecting front-end attackers, and the attacker is increasingly unlikely to launch a front-end attack to obtain SF pieces as he becomes more driven by material value. At high alpha values, the attacker switches to the breakout scenario, as described above, and attacker switches to a pure strategy comprised

of dual C/S, DIV, and SMMS. Interestingly, for the breakout scenario the defender decreases the frequency with which she inspects, and instead buys the SMMS. The SMMS has a probability of alarming in response to a back-end diversion on any day where a diversion occurs. Thus this safeguard is quite effective against a daily attacks with a long duration, because even if the per-attack DP is relatively low, the cumulative DP over the course of the scenario is one.

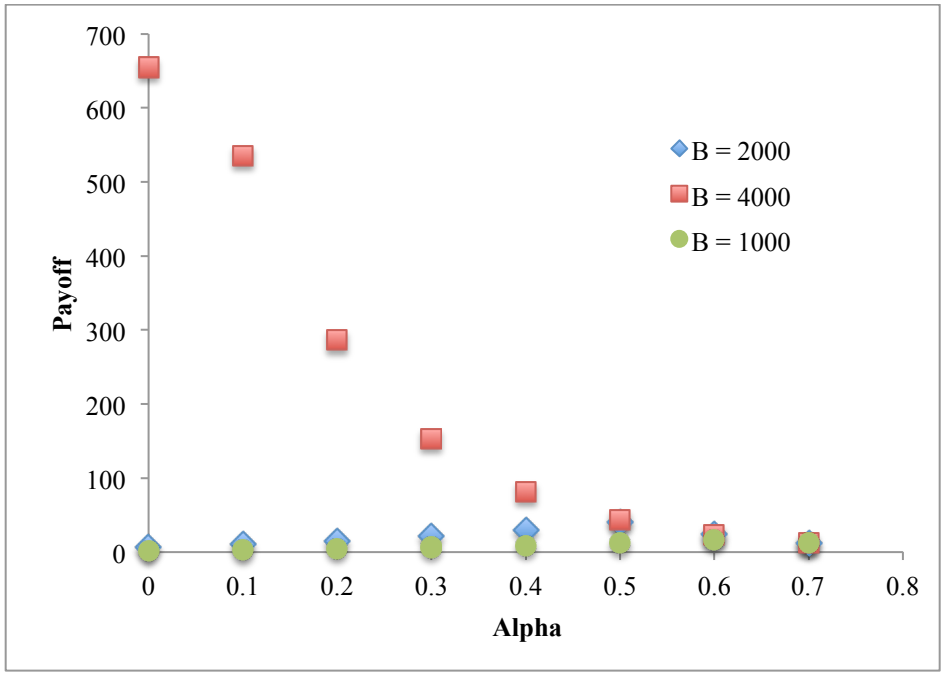

Figure 6-23. Payoff as a function of alpha for the risk-averse attacker

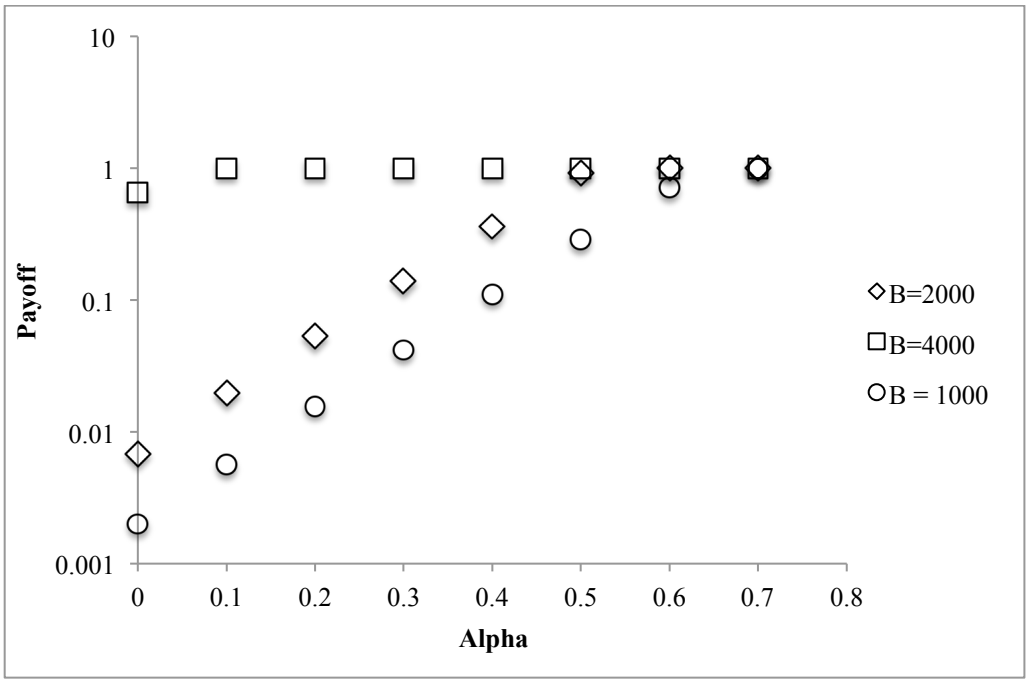

Figure 6-24. Normalized payoff as a function of alpha for the risk-averse attacker

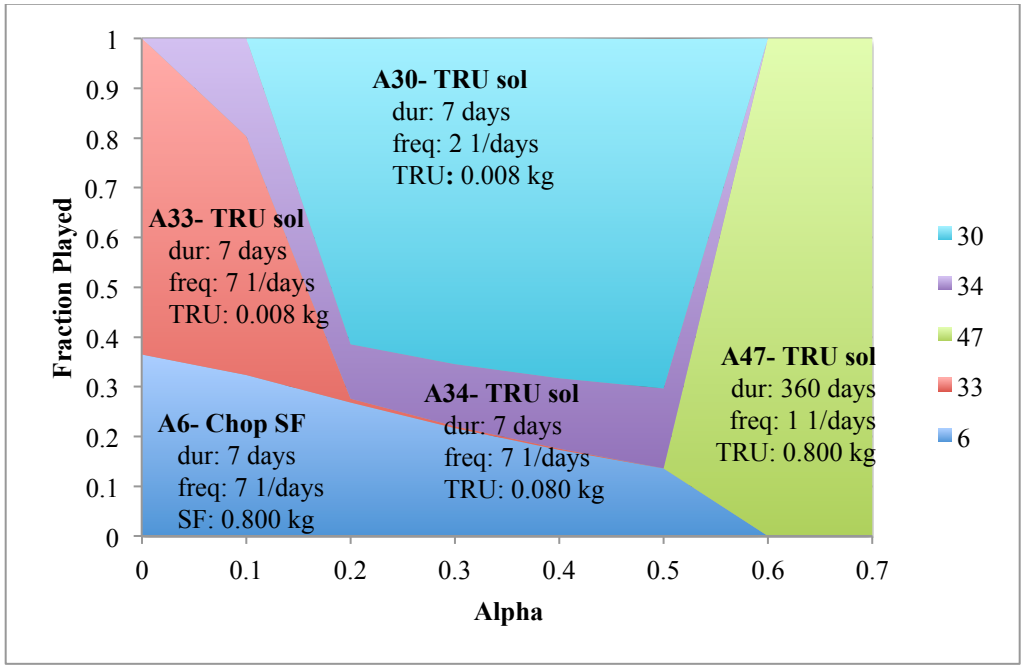

Figure 6-25. Attacker strategy as a function of alpha for the risk-averse attacker

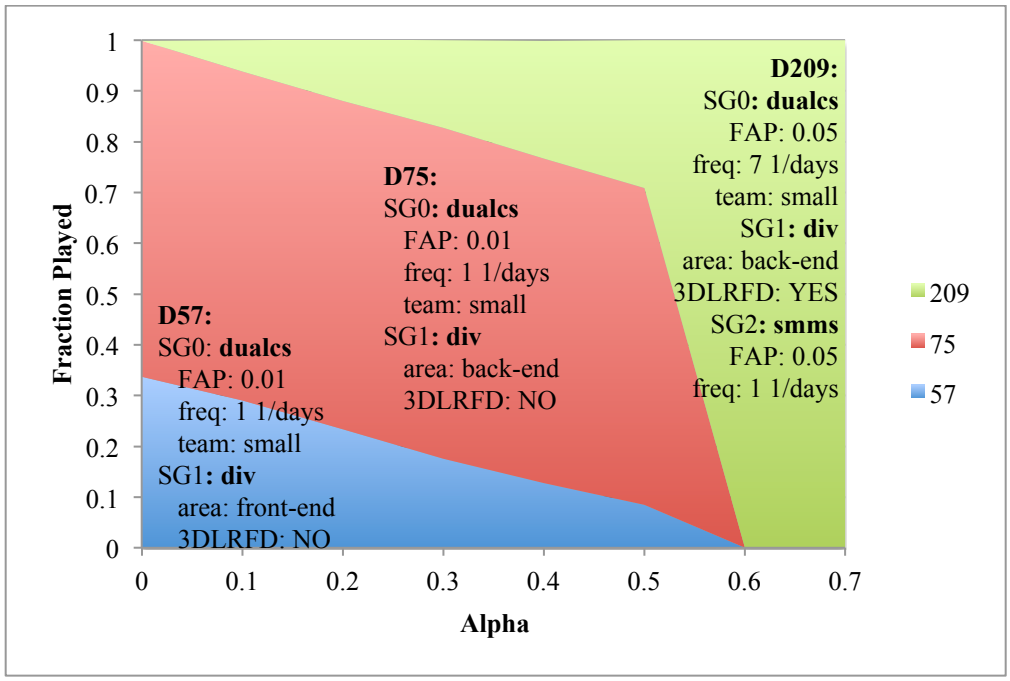

Figure 6-26. Defender strategy as a function of alpha for the risk-averse attacker

6.2.3 Budget sensitivity- Efficient Frontier

Figure 6-27 shows the efficient frontier for payoff 1 and 2 at alpha equals zero (payoff equals DP). It is evident from the figure that for any budget greater than 3500 s$, the defender cannot improve her payoff against the risk-preferring attacker (payoff 1) because the DP at 3500 s$ is one; thus additional investments do not affect the defender's payoff. Similarly for the defender against the risk-averse attacker, budget increases above 4000 s$ do not affect the payoff, because at this budget the maximum payoff has been reached. Note that the budget values the yield a DP of one for the defender are very close in value in this figure, which is because alpha equals zero. Here neither attacker places any value on the type or quantity of material obtained, so the strategies for the two types of attacker are more similar than for non-zero alpha values.

The regions in Figure 6-27 that show large payoff increases correspond well with the budget ranges featuring a large number of strategies available to the defender. For the risk-preferring attacker, large increases in payoff occur in regions from 500-1500 s$ and from 3000-4000 s$. It is apparent in Figure 6-27 that these intervals correspond to the budget intervals with

the largest number of strategies available to the defender. Thus the significant increase in payoff occurs because the defender is able to afford some new safeguard or safeguarding parameter that significantly increases her detection probability. For example, payoff 1 increases from 0.424 to 0.657 from 500 s$ to 1500 s$. At 500 s$, the defender plays a pure strategy of routine inspections with a frequency of every seven days, and without purchasing the 3DLRFD. At 1500 s$, the defender plays a mixed strategy of two different routine inspections, one that performs DIV on the front-end of the facility with a 3DLRFD, and other that performs DIV on the back-end of the facility with a 3DLRFD. AT 1500 s$ the defender is also able to purchase the SMMS system as part of her mixed strategy. By comparison the increase in payoff between 1500 s$ and 2000 s$ is relatively small, because in this case the defender is not able to play a new strategy; instead she plays different fractions of the same two pure strategy to constitute her mixed strategy.

The same result is seen for the risk-averse attacker on the interval from 2000 s$ to 3500 s$, where two major step increases in payoff are seen (from 2000 to 2500 and from 2500 to 3500 s$). The increase from 2000 to 2500 s$ occurs because the defender is able to purchase the 3DLRFD and accept a higher false alarm probability (which increases detection probability but costs more), and the increase from 2500 to 3500 s$ occurs because the defender can afford to purchase DA sampling and the SMMS system at the higher budget. The small increase in payoff between 3500 and 4000 s$ occurs because the defender is able to purchase a new pure strategy that includes *both* DA sampling and the SMMS system. Note that at 3500 s$, the defender plays a mixed strategy comprised of two pure strategies, one of which has a DA component and one of which has an SMMS component. The ability to play a pure strategy with both of these components does increase the defender's DP, but not drastically, suggesting that randomizing between DA sampling and the SMMS system, in concert with routine inspections, is nearly as effective as doing both on a regular schedule.

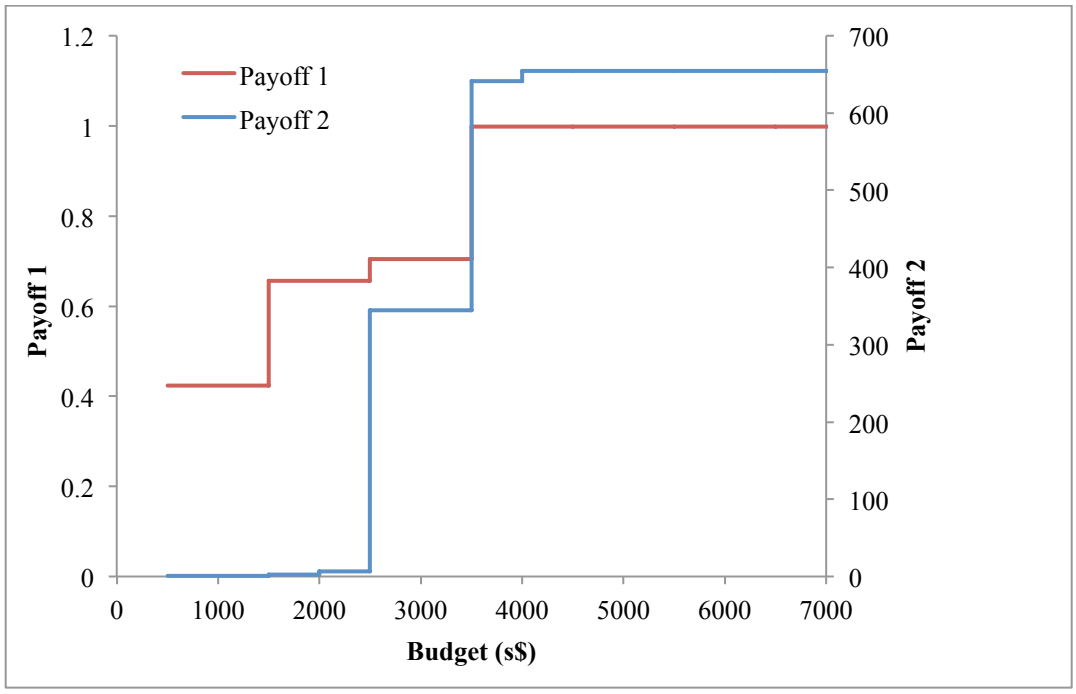

Figure 6-27. Payoff 1 and 2 as a function of budget at alpha = 0

Figure 6-28 shows normalized payoffs 1 and 2 as a function of budget at alpha = 0.2. Recall from previous discussion that the normalized payoff takes a value of 1 if two conditions are met: (1) the DP is 1, and (2) the attacker obtains the maximum quantity of highest value material. Note that Figure 6-28 gives the log of the normalized payoff along the y-axis. For the risk-preferring attacker, the payoff is always 1, irrespective of the budget. This is because at alpha = 0.2, the risk-preferring attacker is sufficiently incentivized to pursue the breakout strategy—the scenario in which he seeks the maximum amount of high-value material despite facing certain detection. Because this strategy is so overt, the DP is 1, even at very low budgets, resulting in a normalized payoff of 1. Conversely, the risk-averse attacker pursues more conservative strategies up to a defender budget of 2500 s$, because the risk-averse attacker wishes to avoid certain detection if possible. Above a budget of 2500 s$, however, the defender's resources are sufficient to detect even the attacker's more conservative strategies with a probability of 1; thus the attacker resigns himself to the certainty of detection. Faced with certain detection and obtaining a small amount of material, or certain detection and obtaining a large

amount of high-value material, the attacker chooses the latter and switches to the breakout strategy.

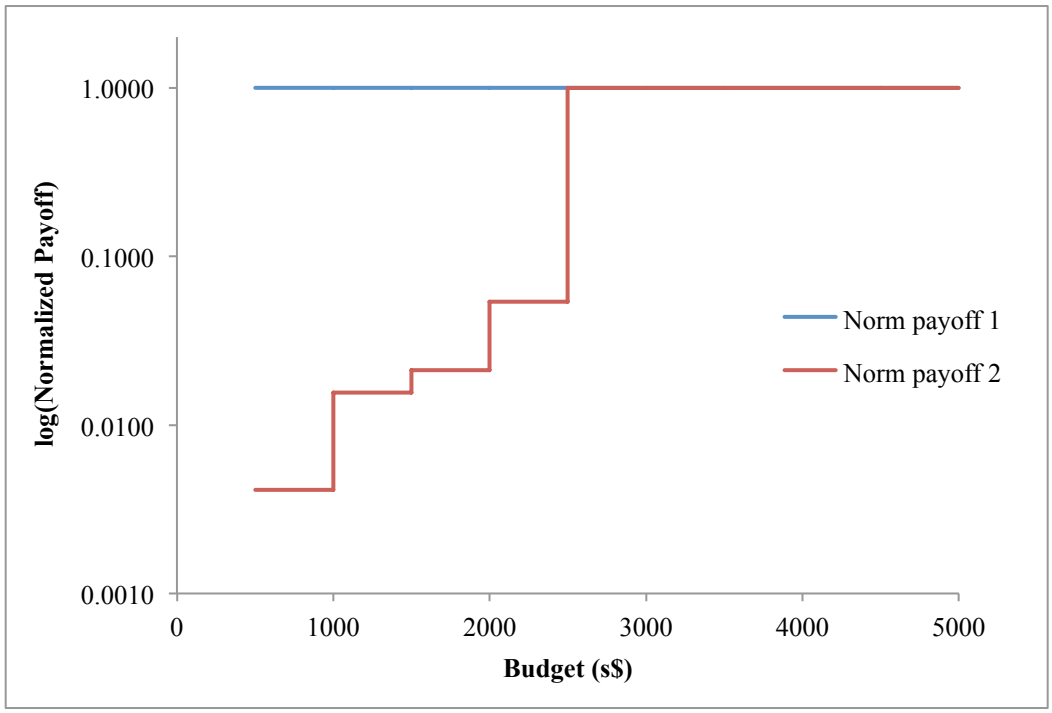

Figure 6-28. Normalized payoff 1 and 2 as a function of budget for alpha = 0.2

Chapter 7: Integrated Facility Model Results

This chapter provides results for the integrated, two-facility model. In this model the attacker has the option of attacking either the enrichment or reprocessing facility. As with the single-facility models, the defender's strategy options include every allowable permutation of safeguards, ranging from only enrichment or reprocessing safeguards to full suites of safeguards at both facilities. Minor changes were made to enrichment and reprocessing simulations when implementing them in the integrated model; details about these changes can be found in Appendix B: Implementation. The results of this section provide insight into the optimal resource allocation strategy across multiple facilities, and how this strategy is affected by adversary characteristics.

There are a total of 1,668,924 unique defender strategies available in the integrated facility model, along with 375 attack strategies. Note that while the defender can allocate safeguarding resources across both facilities, the attacker can still only attack one of the two facilities, though the attacker can play a mixed strategy with membership in both facilities. The defender strategies range in cost from 0- 1400 s$. Figure 7-1 shows the defender strategy cost distribution for the integrated model.

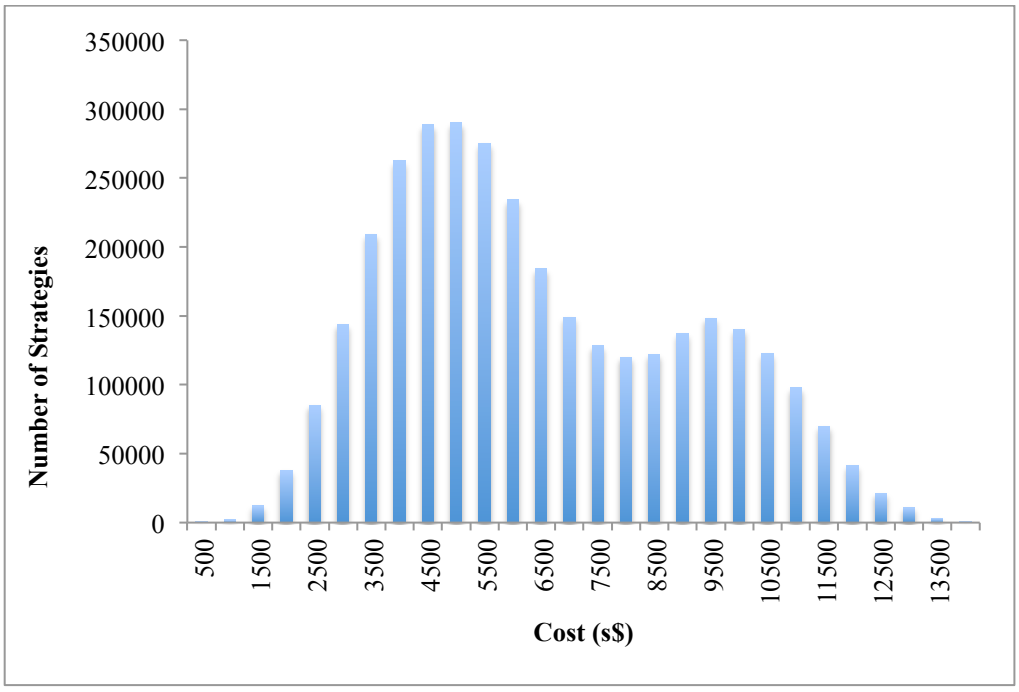

Figure 7-1. Defender strategy cost distribution for integrated model

7.1 Alpha Sensitivity

As for the single facility model analyses, an alpha sensitivity study was conducted by varying alpha from 0 to 0.5 for both the breakout-willing and risk-averse attacker. The results for the two types of attackers are presented below.

7.1.1 Breakout-willing Attacker

Figure 7-2 shows the payoff and normalized payoff for the breakout-willing attacker as a function of alpha at three budget levels. These results exhibit the same characteristic behavior seen for the breakout-willing attacker in the single facility models; namely, for any alpha value greater than or equal to 0.2, the payoff is the same for all three budgets, and the normalized payoff equals 1. This occurs because once the attacker is sufficiently motivated by material value (here alpha = 0.2), he resorts to the breakout strategy in this face of even moderate safeguards. Under this strategy, he seeks to obtain the maximum quantity of high value material, despite

knowing he will be detected for certain; once defender investment in safeguards suffices to push him into breakout, further defender investment ceases to change the attacker's behavior. The largest difference in normalized payoff between the three budgets occurs at alpha = 0.1, because at this budget the attacker begins to be motivated by material utility, and plays a more risky strategy than at alpha = 0, where he sought only to evade detection, but he has not yet resorted to the breakout strategy. Thus for this somewhat material-motivated attacker, the defender's budget has the greatest impact on the normalized payoff because the attacker still behaves evasively, responding to expected defender safeguards investments by switching to lower-risk strategies at the expense of material utility.

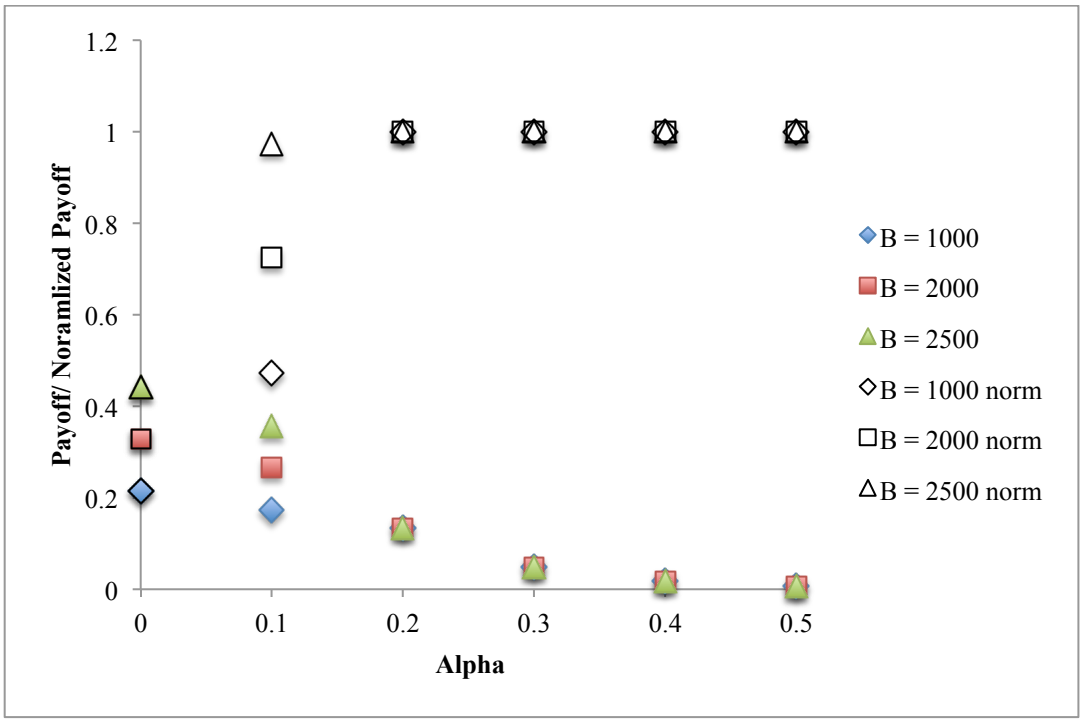

Figure 7-2. Payoff as a function of alpha for the breakout-willing attacker

Figure 7-3 shows the breakout-willing attacker's strategy as a function of alpha at B = 2000. As mentioned above, at alpha = 0 the attacker, while determined to mount his attack, is

indifferent to the type of material he obtains and seeks only to evade detection. Thus at alpha = 0, the attacker plays a mixed strategy comprised of three pure strategies, all of which have low DPs. The three strategies he may choose are the production of undeclared feed at the enrichment facility, the diversion of chopped spent fuel pieces from the front-end of the reprocessing facility, and the diversion of TRU solution from the back-end of the reprocessing facility. In all three cases, he perpetrates a one-day attack, diverting or producing the smallest possible quantity of material, in order to minimize his DP. Note that in this case the attacker plays a mixed strategy that randomizes between attacking the enrichment facility and the reprocessing facility. This strategy is consistent with the paradigm that the attacker can attack only one facility; the mixed strategy means that he will *either* attack the enrichment facility or the reprocessing facility, and his likelihood of choosing to attack either facility is described by the membership of that pure strategy in the mixed strategy. In this case, the attacker may choose produce undeclared feed (74% chance), divert chopped spent fuel pieces (17% chance), or divert TRU solution (9% chance).

As alpha increases from 0 to 0.1 and the attacker begins to place some value on material type and quantity, he shifts to a more aggressive mixed strategy that continues to include targets in both the enrichment facility and the reprocessing facility. It is important to note that the presence of both facilities in the attacker's strategy list is an expected, and desirable, outcome of the game. As the budget is increased, the defender is allocating investments in such a way as to make all potential targets within both facilities equally (un)desirable to the attacker. Therefore, the defender will invest in the more vulnerable facility until its vulnerability drops to equal that of the easiest-to-attack target in the other facility. As budget continues to increase from that point, the defender will divide his resources between the two facilities to maintain parity between potential targets across the facilities.

Returning to the alpha = 0.1 case, the attacker plays an aggressive strategy of diverting TRU solution daily for a year at the reprocessing facility, but he plays this strategy only about a quarter of the time, and plays a more conservative undeclared feed production strategy the remain three-quarters of the time. The undeclared production strategy employed at alpha = 0.1 is more aggressive than the limited one-time attack that occurs at alpha = 0, though still a one-time attack with a relatively low DP. At alpha = 0.2 and above, the attacker switches to the breakout strategy, which is to recycle material through the cascade at the enrichment facility to produce HEU. This strategy produces the highest material utility of any of the strategies at both facilities, as it produces the largest quantity of high-value material. This makes it the most attractive option to a breakout-willing attacker once the facilities are sufficiently well safeguarded to make his detection likely.

Defender strategy as a function of alpha at B = 2000 is shown in Figure 7-4. A detailed description of each of the defender strategies played is given in Table 7-I. At alpha = 0, the defender counters the attacker's mixed strategy by playing a mixed strategy that is comprised of three pure strategies. Two of the pure strategies played feature five safeguards spread across the two facilities—inspection and NDA at the enrichment facility, and dual C/S, DIV, and SMMS at the reprocessing facility. The only difference between these two pure strategies that are part of the mixed strategy is the area in which design information verification is conducted at the reprocessing facility. Just as the attacker may choose to divert chopped spent fuel pieces from the front-end (17%) or TRU solution from the back-end (9%), the defender randomizes between conducting DIV in the front-end (8%) and conducting DIV in the back-end (42%). In practice, this would mean that upon each inspection, the defender would sometimes (8%) choose to conduct front-end DIV but more often (42%) in the back-end. The attacker knows is aware of this defender behavior, but does not know which option will actually be chosen in advance of each inspection. Here the defender focuses his resources in the back-end because the TRU

diversion is more difficult to detect with dual C/S than the chopped SF piece diversion, so DIV adds a needed additional detection measure.

The third pure strategy that has membership in the defender's mixed equilibrium strategy at B = 2000 is a suite of enrichment safeguards. This strategy features, among other safeguards, inspection and visual inspection, which are effective in detecting undeclared production using undeclared feed. The defender plays this strategy with a membership of 50% in order to counter the attacker's preferred strategy, undeclared production, which the attacker plays a large percentage of the time due to the difficultly in detecting it. The fact that the defender's mixed strategy is comprised in part of this enrichment-only strategy represents a shortcoming of the simultaneous play game model for this application. In reality, an inspectorate like the IAEA could not safeguard only one facility without the attacker being able to observe this behavior and change his strategy accordingly, because in reality certain elements of the defender's strategy are transparent to the attacker, such as the installation of equipment. Section 8.2 Future Work discusses a method for addressing this shortcoming by incorporating a hybrid Cournot-Stackelberg game. For the purposes of this work, this mixed strategy result should be interpreted as the defender playing a combination of the component pure strategies, not strictly randomizing between the pure strategies.

At alpha = 0.1, the defender continues to play a mixed strategy, randomizing between an enrichment-only safeguarding strategy and a strategy that allocates resources across both facilities. The defender reduces the frequency with which she inspects the enrichment facility, because the attacker is playing slightly more aggressive strategies that are easier to detect, so less frequent inspection is still effective. Additionally the defender shifts to performing DIV on only the back-end of the reprocessing facility, because once the attacker differentiates between different material qualities chopped spent fuel pieces are far less attractive to him. At alpha = 0.2, the defender plays a pure strategy with two safeguards at each facility. She employs

inspection and NDA monthly at the enrichment facility, both of which are effective against HEU production, and she plays dual C/S and DA sampling at the reprocessing facility. The investment made in reprocessing safeguards is just sufficient to deter the attacker from perpetrating an attack at the reprocessing facility. Against the breakout-willing attacker, the defender chooses a relatively limited suite of safeguards at high alpha values, because the attacker switches to the breakout strategy, which is highly visible and easy to detect. Similarly for a fixed alpha value, the suite of safeguards selected by the defender does not change with additional investments above B = 4000 s$, because at and above this investment level the attacker commits to a single strategy.

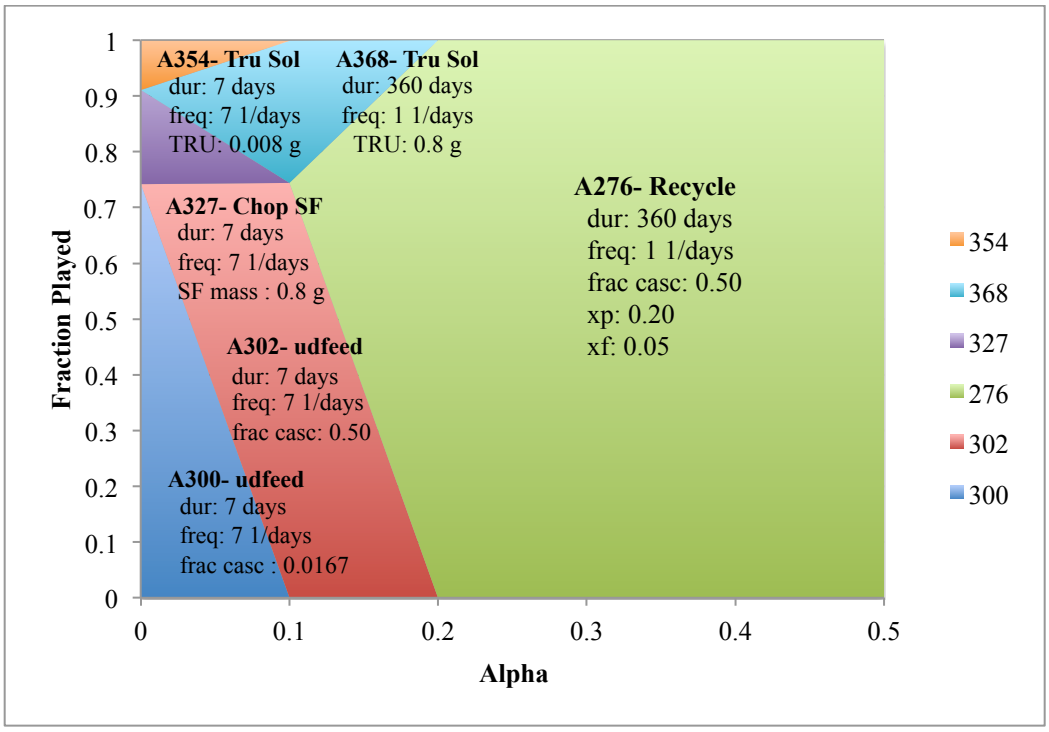

Figure 7-3. Breakout-willing attacker strategy as a function of alpha

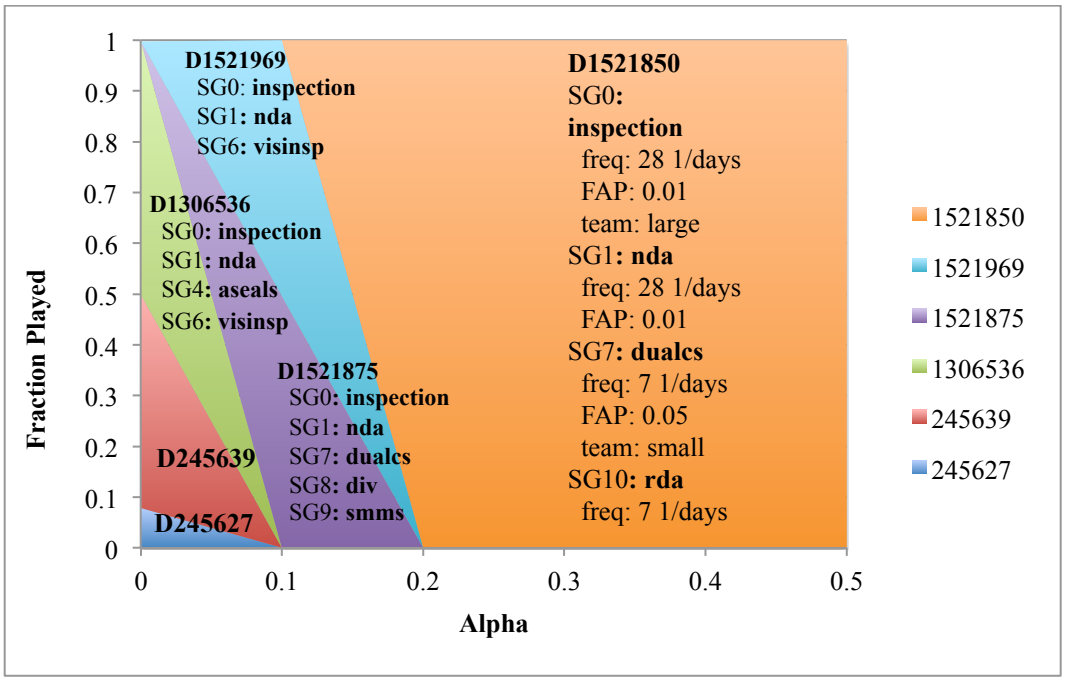

Figure 7-4. Defender strategy as a function of alpha against breakout-willing attacker

Table 7-I. Integrated model defender strategy descriptions

Strategy	Active SGs	Parameter 1	Parameter 2	Parameter 3
D245627	Inspection	freq = 7 days^{-1}	team size = small	FAP = 0.01
	NDA	freq = 28 days^{-1}	FAP = 0.01	
	Dual C/S	freq = 7 days^{-1}	team size = small	FAP = 0.05
	DIV	3DLRFD = yes	area = front-end	
	SMMS	freq = 1 days^{-1}	FAP = 0.05	
D245639	Inspection	freq = 7 days^{-1}	team size = small	FAP = 0.01
	NDA	freq = 28 days^{-1}	FAP = 0.01	
	Dual C/S	freq = 7 days^{-1}	team size = small	FAP = 0.05
	DIV	3DLRFD = yes	area = back-end	
	SMMS	freq = 1 days^{-1}	FAP = 0.05	
D1306536	Inspection	freq = 28 days^{-1}	team size = small	FAP = 0.01
	NDA	freq = 28 days^{-1}	FAP = 0.01	
	Active seals	frac. sealed = 1.00		

	Visual insp.	freq = 7 days^{-1}		
	Inspection	freq = 28 days^{-1}	team size = large	FAP = 0.01
	NDA	freq = 28 days^{-1}	FAP = 0.01	
D1521875	Dual C/S	freq = 7 days^{-1}	team size = small	FAP = 0.05
	DIV	3DLRFD = yes	area = back-end	
	SMMS	freq = 1 days^{-1}	FAP = 0.05	
	Inspection	freq = 28 days^{-1}	team size = large	FAP = 0.01
D1521969	NDA	freq = 28 days^{-1}	FAP = 0.01	
	Visual insp.	freq = 7 days^{-1}		
	Inspection	freq = 28 days^{-1}	team size = large	FAP = 0.01
	NDA	freq = 28 days^{-1}	FAP = 0.01	
D1521850	Dual C/S	freq = 7 days^{-1}	team size = small	FAP = 0.05
	DA- repr.	freq = 7 days^{-1}		

7.1.2 Risk-Averse Attacker

The results presented above for the breakout-willing attacker indicate that the normalized payoff for the game is 1 at alpha $\geq$ 0.2, where even a minimal defender budget is sufficient to drive the attacker to accept certain detection by choosing the breakout strategy. Figure 7-5, which shows the normalized payoff as a function of alpha for the risk-averse attacker, highlights his very different behavior. It can be seen in Figure 7-5, even at alpha = 0.5, the normalized payoff only reaches a maximum value of 0.39, because the risk-averse attacker does not resort to the breakout strategy. It is also apparent that as alpha increases, the difference in normalized payoff between B = 2000 and B = 2500 decreases. This occurs because as alpha increases, the attacker's strategy becomes increasingly aggressive as he becomes more material-motivated. He shifts towards strategies that are easier to detect, although never to the extent of the breakout-willing attacker; the risk-averse attacker will never accept a breakout scenario where his detection is certain. As the attacker's preferred strategies become more aggressive, the difference in the amount of detection that can be bought at 2500 s$ and 2000 s$ decreases.

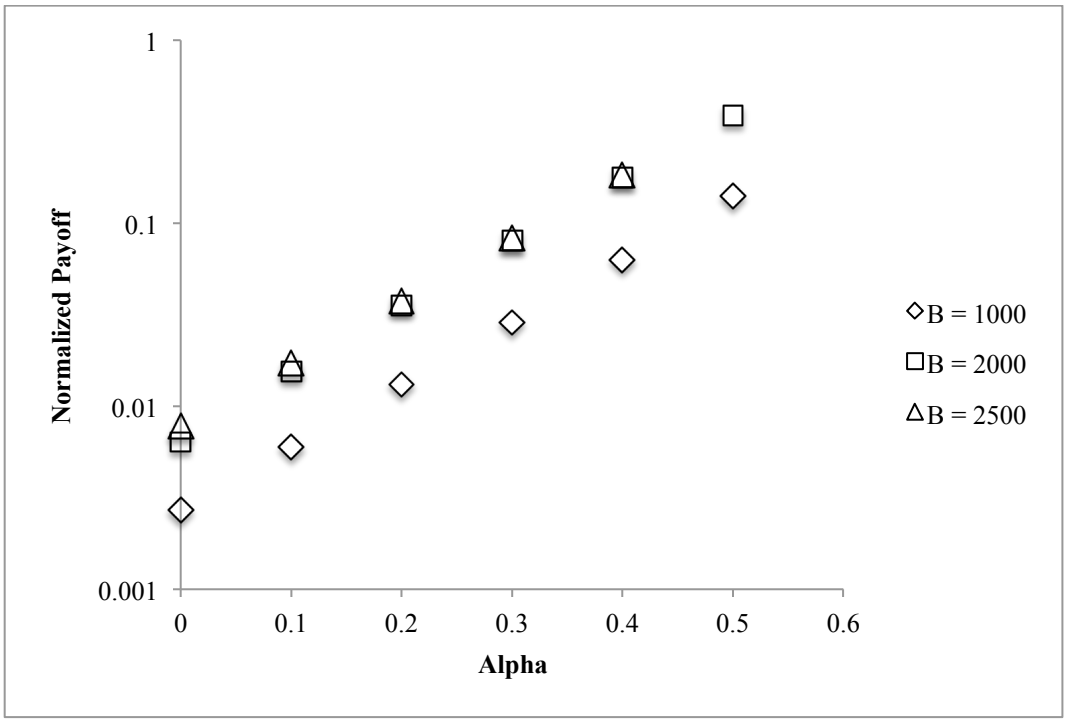

Figure 7-5. Normalized payoff as a function of alpha for the risk-averse attacker

Figure 7-6 shows the attacker strategy as a function of alpha. As expected, at alpha = 0 the attacker plays a mixed strategy similar to the one played by the breakout-willing attacker, because at this alpha value his only consideration is minimizing DP. As alpha increases, the attacker shifts towards playing various mixed strategies, all of which are dominated by strategy A302, the one-time production of undeclared product from undeclared feed. While short in duration, this strategy does commit half of the cascades to the misuse, meaning it makes a relatively large quantity of material and is relatively visible. It is interesting to note that at alpha = 0.5, the attacker plays a small fraction of a very aggressive TRU solution diversion strategy at the reprocessing facility. This strategy selection can best be understood by looking at the attacker strategy in concert with the defender strategy. Figure 7-7 shows the defender strategy as a function of alpha. Note that between alpha = 0.1 and alpha = 0.4, the defender dedicates an increasing fraction of her resources to strategy D1521969. As shown in Table 7-I, this strategy is

comprised exclusively of enrichment safeguards, including inspection and visual inspection. Accordingly, this strategy is designed to detect the production of undeclared material from undeclared feed, which is why the defender increasingly relies upon it as the attacker plays this strategy a larger fraction of the time.

The results do show, however, that if the defender commits too many of his resources to one facility, it leaves the other facility vulnerable to attack. This explains the defender and attacker behavior seen at alpha = 0.5, where the attacker plays a small share of an aggressive attack at an enrichment facility, and the defender counters by diverting additional resources from the enrichment-only strategy to strategies that include safeguards at both facilities.

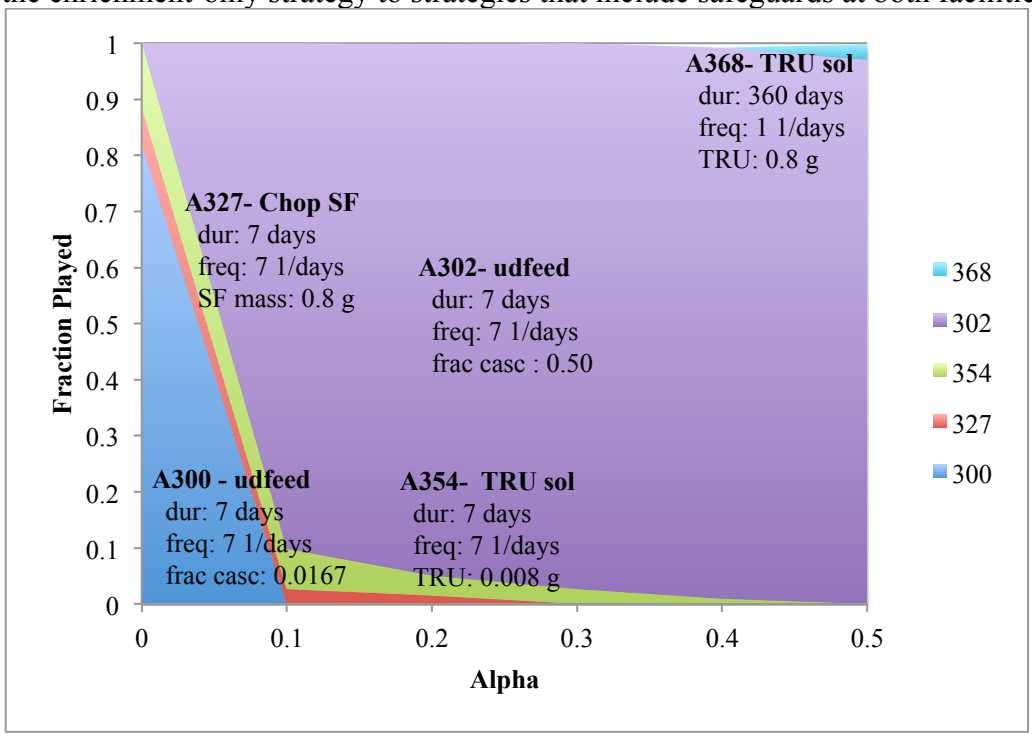

Figure 7-6. Risk-averse attacker strategy as a function of alpha

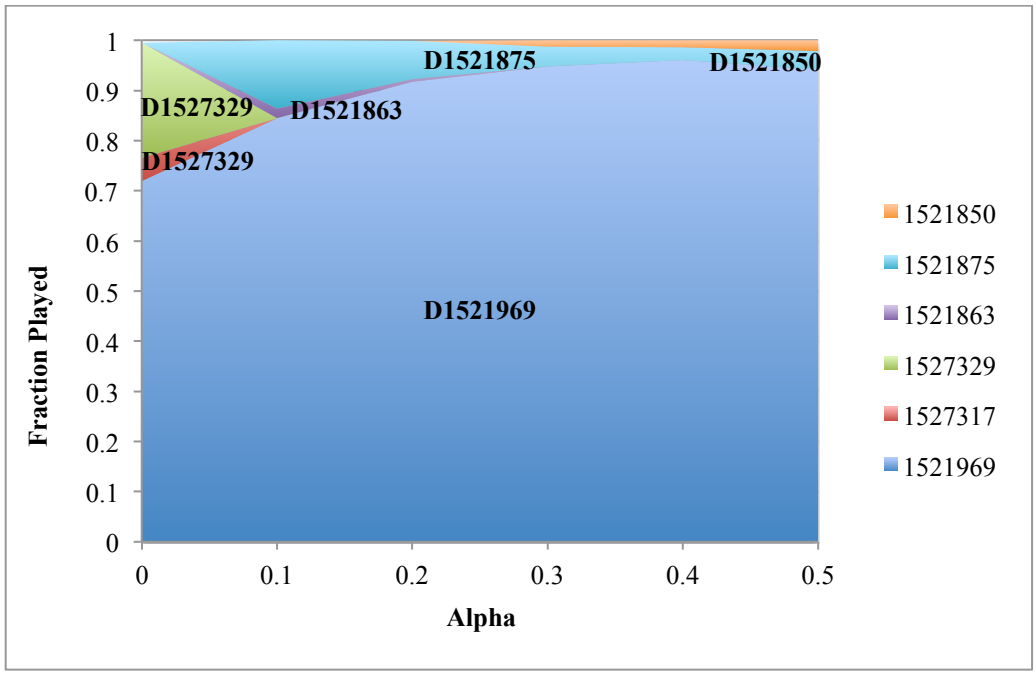

Figure 7-7. Defender strategy as a function of alpha against risk-averse attacker

7.2 Optimal Resource Allocation across System of Facilities

One of the valuable outputs generated by this model is the optimal allocation of defender resources across two facilities. This section presents the efficient frontier for the integrated model and compares it to the efficient frontiers for the stand-alone enrichment and reprocessing models. Additionally, it presents results verifying that the investment portfolios output by the integrated model are optimally distributed between the two facilities.

7.2.1 Efficient Frontier

Figure 7-8 features the efficient frontier for the integrated, two-facility model alongside the efficient frontiers for the enrichment and reprocessing stand-alone models.

The values plotted are the normalized payoff for the risk-averse attacker with some material motivation (alpha = 0.1). The figure shows that at the enrichment facility, only an investment increase from 1000 to 2000 s$ results in an increased payoff for the defender, because of the low-risk nature of the attacker's strategy. Here the attacker is producing undeclared product from

undeclared feed, which is a strategy against which relatively few safeguards are effective. As such, even if the defender has a large number of resources to invest detection of this strategy is not certain. Conversely, at the reprocessing facility, the strategies available to the attacker are generally easier to detect, so the payoff is far more sensitive to the defender's budget. Even the risk-averse attacker with minimal material motivation resorts to the breakout strategy at the reprocessing facility, because beyond a certain defender investment level he is unable to evade detection, no matter the attacker strategy he selects.

The efficient frontier for the integrated facility model shares features with both of the stand-alone facility efficient frontier plots. Each increase in payoff in the integrated facility efficient frontier corresponds to a similar increase in an individual facility payoff increase. The increase in payoff between 1000 and 2000 s$ corresponds well with the increase in payoff seen at the enrichment facility over this interval, and the small increase seen from 2000 to 2500 s$ dollars can be attributed to the large increase in the reprocessing facility payoffs over this interval. It is clear from the figure that the efficient frontier for the integrated model is dominated by the enrichment facility strategies upon which the attacker focuses. This occurs because the defender primarily allocates her resources defending the enrichment facility, as the reprocessing facility is in fact easier to safeguard given a moderate total budget. Then the attacker preferentially attacks the enrichment facility, as is explained in detail in Section 7.7.2.

The figure also shows that the payoff for the integrated facility is always as low as, or lower than, the payoff for either of the single facilities. This is because for a given budget level, the defender must defend two facilities in the integrated model, versus only one in a single facility model. Further, in the integrated model, the attacker is able to determine which facility is more vulnerable and attack that facility. Thus the system is as vulnerable as the most vulnerable facility, which is why the defender invests her resources in a manner such that both facilities are equally unattractive targets. Note that in this case that is not possible, even at high defender

budgets, because of modeling assumptions made about the detectability of attacks at the enrichment and reprocessing facilities. In this case, even if the defender has unlimited resources, the risk-averse attacker is still able to perpetrate an attack at the enrichment facility with DP < 1, which is why the payoff is lower at the enrichment facility than the reprocessing facility.

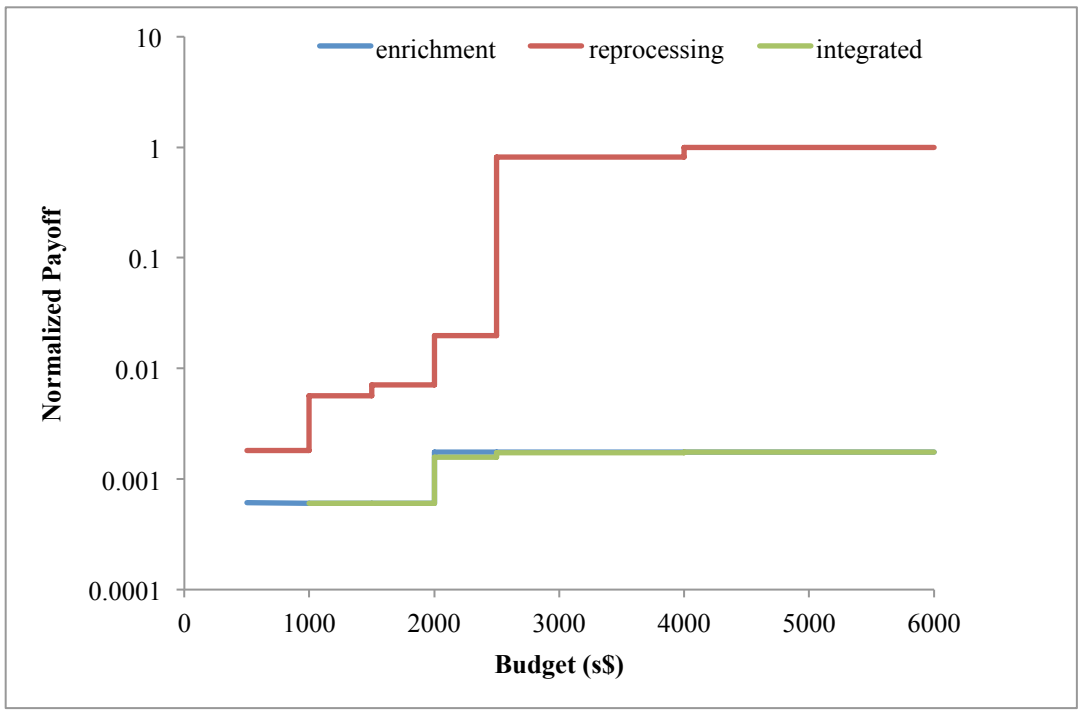

Figure 7-8. Efficient frontiers for enrichment, reprocessing, and integrated facility models

7.2.2 Optimality of Investment Distribution

To investigate the allocation of resources between the two facilities, a sensitivity analysis was performed by sweeping across a range of resource splits and comparing the results to those output by the integrated model. The integrated model was run with a defender budget of 2500 s$, and at this budget, the defender plays pure strategy D1522158, which is comprised of inspection, NDA, visual inspection, dual C/S, and DIV.

Table 7-II describes strategy D1522158 in detail and also provides a cost-breakdown for all of the safeguards purchased. This resource allocation is specific to this model and results from modeling assumptions made, as described in greater detail below. Based on the costs shown in

the table, the defender allocates about 1986 s$, or approximately 81% of the investment, to defending the enrichment facility, 472 s$ to the reprocessing facility, and has 42 s$ left over. Any allocation other than this 1986-472 split should be sub-optimal and result in a lower payoff to the defender. Note that though the defender has a total budget of 2500 s$, she only invests 2458 s$ in her defense strategy. In practice the defender rarely uses the entire budget allocated to her, because her investment options are discrete in nature, so she allocates resource until there is no slack in her budget; that is, until the purchase of an additional useful safeguard would exceed her budget. Note that this analysis was conducted to demonstrate the ability of the model to allocate across multiple facilities, and the results should not be interpreted as a global statement about the relative vulnerability of enrichment facilities versus reprocessing facilities. This point is discussed in greater detail below.

Table 7-II. Defender strategy selection at B = 2500 s$

Strategy	Active SGs	Parameter 1	Parameter 2	Parameter 3	Cost
D1522158	Inspection	freq = 28 days^{-1}	team size = large	FAP = 0.01	426.39
	NDA	freq = 28 days^{-1}	FAP = 0.01		30.07
	Vis. Insp.	freq = 7 days^{-1}			1530.00
	Dual C/S	freq = 7 days^{-1}	team size = small	FAP = 0.05	468.62
	DIV	3DLRFD = no	area = front-end		3.00

In order to show that this cost split is optimal, the stand-alone enrichment and reprocessing models were run with the defender budgets set to their respective shares of the total budget. For the 1986-472 split described above, the reprocessing model was run with B = 472, and the enrichment model was allocated the balance of the total budget, or B = 2028. Each model generated an equilibrium payoff, and the lower of the two payoffs was recorded. The lower payoff was used because it represents the more vulnerable point in the two-facility system. Runs were conducted varying the percentage of the total budget invested in the reprocessing facility from 0 to 100%. Figure 7-9 shows the results of this test. Along the x-axis, the reprocessing investment varies from 0 s$ (0% of total budget) to 2500 s$ (100% of total budget). The y-axis

shows the payoff at the more vulnerable of the two facilities. These data were collected for the risk-averse attacker who is somewhat motivated by material utility (alpha = 0.1).

Because the attacker is an intelligent adversary, it is assumed that he can preferentially attack the more vulnerable of the two facilities, meaning the system defense is only as effective as its least effective element. Thus the defender makes defense investments with the goal of making both facilities equally unattractive targets for the attacker. It is clear from Figure 7-9 that if the defender over-invests in one facility, like investing 2050 s$ at the enrichment facility and the remaining 450 s$ at the reprocessing facility, the system payoff is quite low, because the defender leaves one facility very vulnerable (in this case, the reprocessing facility). Figure 7-9 also illustrates the optimal resource allocation output by the integrated facility model. The red circle shows the payoff for a reprocessing budget of 472 s$, which was the amount of money allocated to defending the reprocessing facility in the equilibrium strategy output by the integrated model. It can be seen from the figure that if the defender invests even one dollar less in the reprocessing facility, the system payoff drops appreciably. It is apparent from the figure that there is a small cluster of data points, ranging from 472 s$-500 s$, for which the system payoff is optimal. These budgets are effectively equivalent due to the discretized nature of the budget discussed previously. The figure clearly shows, however, that any cost split between facilities besides the 1986-472 split output by the integrated facility model results in a lower system payoff, and is thus suboptimal.

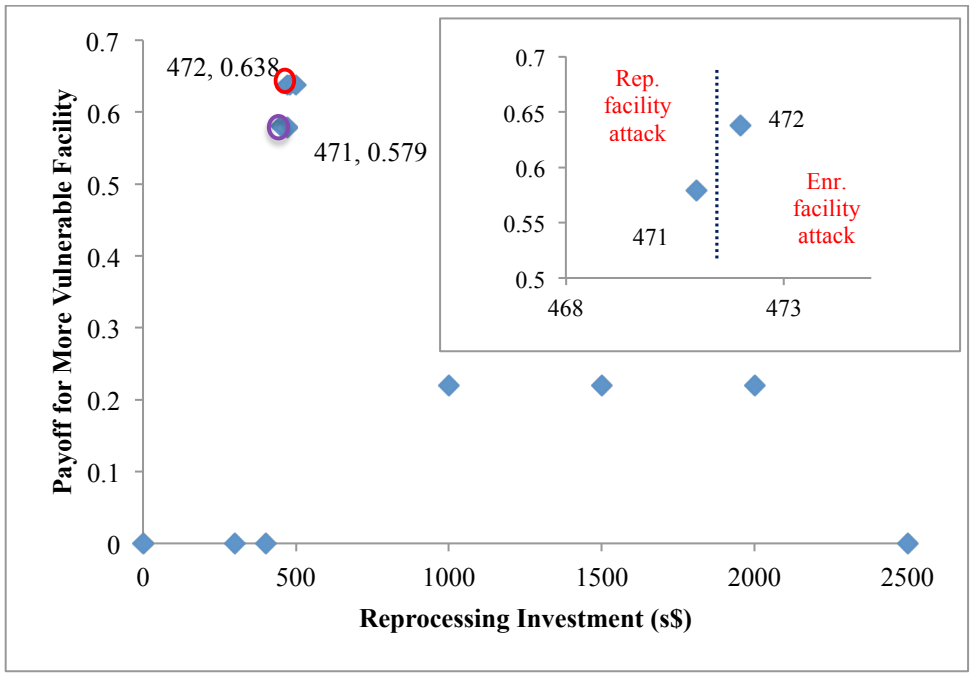

Figure 7-9. Payoff at more vulnerable facility as cost share across facilities is varied

The results presented above indicated that the defender should allocate approximately 80% of her resources to the enrichment facility and the remaining 20% to the reprocessing facility. This basic finding—that the defender should be investing more heavily in defending the enrichment facility—is seen for both types of attackers and over a range of material motivations (over a range of alpha values). It should be noted that this result is specific to this model because of the different level of detail with which the two facilities were modeled. The enrichment facility was modeled in much greater detail, and thus included a menu of varied attacker options which resulted in some attacks with high DPs and others with low DPs. The reprocessing facility model is underdeveloped relative to the enrichment facility, particularly the attacker options at the reprocessing facility. The result of this small set of available attacker options at a small facility is that detection probabilities at the reprocessing facility are artificially high, making the reprocessing facility appear unrealistically vulnerable in comparison to the enrichment facility.

The breakout strategy, wherein the attacker seeks to obtain the maximum quantity of high value material, even knowing he will certainly be detected, occurs in this model at the enrichment facility. If that attacker chooses to recycle material through the cascade daily for an entire year, dedicating half of the plant's cascades to the misuse, the attacker achieves a material utility ($FOM \cdot Q$) of 24,446. By comparison, the attacker strategy at the reprocessing facility that yields that largest quantity of high value material has a material utility of only 518. For the system of the two facilities, a breakout attacker will thus target the enrichment facility simply because he can obtain higher-quality material more quickly there. If the size of the reprocessing facility were scaled up, or it were producing Pu rather than TRU, the breakout might instead take place there. The attacker's choice of the enrichment facility for breakout is a result of model and scenario assumptions.

A similar inclination towards the enrichment facility can be seen for the risk-averse attacker with little to no material motivation. Across the two facilities, the attacker strategy with the lowest DP occurs at the enrichment facility, with a one-time attack producing undeclared product from undeclared feed using only cascade. Accordingly, in this model, both a highly aggressive breakout attacker and highly risk-averse attacker preferentially attack the enrichment facility, as do attackers possessing intermediate characteristics. As a result, the defender invests the majority of her resources in defending the enrichment facility, in particular because this optimizes her payoff against the risk-averse attacker seeking to evade detecting by perpetrating a very limited attack at the enrichment facility.

These system-level resource allocation results are best not interpreted in a literal, immediately real-world relevant sense, but instead should be analyzed for their underlying implications. Specifically, these results suggest that the defender should allocate resources in such a manner so as to make all facilities equally unattractive to an adversary. Further, in order to achieve this objective, the defender must consider adversary-specific characteristics, such as

risk-preference and material motivation. The defender gains more by investing in the facility that would otherwise be more attractive to the risk-averse attacker, because this attacker can theoretically be deterred and his strategy can be influenced by additional detection capability. Against a breakout-willing attacker, conversely, the defender does best to allocate only the minimal resources required to detect an aggressive attack, as this type of attacker's behavior is dominated by desire for high-value material and cannot be significantly influenced by defender strategy. The best outcome for the defender is to force such an adversary into a breakout strategy.

CONCLUSIONS AND FUTURE WORK

Chapter 8: Conclusions and Future Work

8.1 CONCLUSIONS

This work presents a computational model that employs a novel methodology to find optimal inspector and proliferation strategies at and across nuclear fuel cycle facilities. The methodology couples a game theoretic solver with a probabilistic simulation model of a gas centrifuge enrichment plant and an aqueous reprocessing facility. The game calls the simulation model to generate payoff values for given inspector-proliferator pairs, and the simulation model calculates the payoffs by weighting the detection probability for the pair by the quantity and quality of material obtained in the scenario. These payoff values are returned to the game and used to populate the payoff matrix. The game is solved using the fictitious play algorithm, and the model outputs the equilibrium defender and attacker strategies as well as the equilibrium value. This document describes the methodology in detail, including the theoretical underpinnings of the game theoretic optimization, the mechanics of the simulation model, and specific inputs to the simulation model. Additionally this work presents results obtained using the model, namely the optimal inspector and proliferator strategies at a GCEP, a reprocessing facility, and across the system of the two facilities. The numerical values presented here are notional and intended to illustrate the methodology, and as such should not be interpreted literally; however, the methodology has been developed such that a user could input facility-specific assumptions and detection probability algorithms to generate realistic results.

One of the more compelling results presented here is the visual representation of scenario payoff as a function of budget, presented as a so-called “efficient frontier”. The efficient frontier traces the optimally efficient strategy at any budget, such that a rational actor should never select a strategy off of this frontier. Further because of the game theoretic framework used, this

analysis anticipates and accounts for changes in attacker strategy based on defender budget level, and calculates optimal defense strategies given changing adversary behavior. For both stand-alone facility models and the integrated facility model, the efficient frontier plots show large increases in payoff at certain budgets, and show regions of plateau in other budget intervals. This plot conveys information about when additional investment provides diminishing returns, as is the case in the plateau regions where additional investment does not result in increased payoff, and when additional investment can elevate the defender above a cost threshold and allow her to purchase some advantageous symbiotic safeguards combination that will result in increased detection capability. Understanding where on the efficient frontier the defender is operating can serve as a guide for rational decision making by providing information about whether additional resource investment should be expected to increase payoff, and at what level additional resources need to be invested in order to affect the payoff.

While the efficient frontier illustrates the optimal strategy for a defender at a given budget level, this result is highly sensitive to the type of attacker against which the defender is defending. This sensitivity is particular to the game theoretic approach and requires that assumptions be made about attacker capability and motivation, which is a potential weakness of this methodology. In order to determine the robustness of the results for a range of attacker capabilities and motivations, the model could be run stochastically with a distribution placed on attacker capability. Note also that because of the zero-sum nature of the game, changing assumptions about payoff for the attacker also changes these payoffs for the defender. This too is a limitation of this model, because though different attackers may value material differently, presumably defender valuation of material is immutable. In this work a single attacker risk preference and material motivation was assumed for each run, with attacker material motivation serving as a proxy for state capability. A state that has clandestine enrichment or reprocessing capability may be able to use material with lower intrinsic material attractiveness to achieve its

objectives than a state with no clandestine facilities, which needs to obtain directly weapons useable material. The relationship between state risk preference and optimal defense strategy is examined here by modeling two different types of attackers—a breakout-willing attacker and a risk-averse attacker. The results indicate that even a risk-averse attacker who is highly motivated by material can be contained and prevented from pursuing the breakout strategy. Conversely, a breakout-willing attacker with relatively low material drive will resort to the breakout strategy even at low defender budgets, at which point he will be detected for certain even with very limited defense strategies. Thus additional defense investments against this type of attacker are wasteful, because they do not buy any additional detection.

In addition to being highly sensitive to attacker risk preference and material motivation, defender strategies are sensitive to exogenous sources of detection probability, particularly at low budgets. The results presented in this work show that at low defender budgets at the enrichment facility, even a daily exogenous DP of 0.1% for detecting the production of undeclared feed altered the defender's optimal strategy at the facility. This result suggests that inspectorates like the IAEA, which is estimated to receive approximately 10% of its information from third-party intelligence,[26] should consider what types of attacks intelligence and other exogenous sources of DP are capable of detecting and how much additional detection capability exogenous sources provide. The inspection strategy that is optimal in the absence of exogenous detection sources may not be optimal in the presence of such sources, particularly at low defender budgets or if the exogenous sources provide DP against the most vulnerable proliferation pathways.

The model also outputs the optimal defense resource allocation strategy across multiple facilities. The results of this work confirm the intuitive notion that the attacker does at least as well, if not better, when he can choose between attacking either of two facilities. For a given

[26] Remarks made by high-level IAEA official in an off the record session

budget, the defender is better able to defend one facility than two, because he can invest all his resource at the single facility rather than allocate them across the two facilities. Thus the attacker's evasion probability is slightly higher in the case of the integrated facility model than it is for even the more vulnerable of the two stand-alone facilities. Because the attacker is always able to attack the more vulnerable facility in the two-facility system, the defender's investment strategy seeks to make both facilities equally unattractive targets for the attacker. As the model results show, if the defender over-invests in either facility, the intelligent adversary is able to take advantage of vulnerabilities at the under-defended facility. The results from this work also verify that the defense investment distribution across the two facilities output by the model is optimal, and venturing away from this distribution to any other cost-sharing paradigm results in a lower overall system payoff for the defender.

The ability of this model to find optimal defender strategies across multiple facilities represents a novel contribution. While traditional proliferation pathway analyses and safeguarding analyses find optimal inspector and proliferator strategies at an enrichment facility or a reprocessing facility, these analyses have limited meaning in real-world situations where an adversary can shift his strategies between facilities and the defender needs to allocate resources efficiently across facilities. The ability of this model to view states' fuel cycles from a systems level and to optimize accordingly make is a useful tool for guiding and supporting the IAEA's emphasis on the state-level approach and information-driven safeguards. This tool can provide a systematic basis for allocating safeguarding resources across multiple facilities in a state, which is of particular utility to the IAEA due to the cost constraints under which it operates, requiring that its strategy become increasingly efficient without compromising effectiveness.

While the results generated by this model represent a new, multi-facility approach to safeguards analysis, the true novelty of the tool lies in the methodology itself. Many proliferation pathways analysis tools use probabilistic risk assessment techniques to analyze vulnerable

proliferation pathways and calculate detection or success probabilities. While PRA-type techniques have utility for many types of analyses, such as safety analyses, techniques of this type may not be as useful for adversarial situations, where the attacker's behavior is governed by rational decision making, rather than chance. For strategic interactions, like those between the IAEA and a state, game theory offers the advantage of more faithfully capturing the behavior of an intelligent adversary who is able to optimize his strategy in the context of the defender's strategy options and resources. The coupling of a game theoretic solver to a probabilistic simulator brings to bear in this model the strengths of both types of techniques. The game theoretic solver performs the prescient optimization required for adversarial decision-making, and the simulation model informs the game with realistic payoff values without placing burdensome restrictions on the complexity of the model. The result of this coupling is a tool capable of generating meaningful output with real-world applicability.

8.2 Future Work

A significant potential application for the model developed in this work is for marginal cost analysis, particularly in the arena of safeguards investment decision making. This model could be used to perform cost sensitivity analysis for a new type of safeguard tool or technique, by determining cost above which the defender no longer selects it because the detection probability to cost ratio is too low. In order to do cost sensitivity analysis with this tool, the model would be populated with the estimated detection capability of a novel safeguarding tool or a tool under consideration, and the cost at which the defender selects the safeguards could then be calculated and compared to the projected cost for development or deployment of the tool. In this way, the model can be used to guide safeguards R&D investment decision making. In a similar vein, the model could also provide an estimate for the "value" of intelligence in a specific threat environment, a piece of information that has the potential to affect policy decision making.

One of the more pressing policy questions surrounding states that may or may not have proliferant aims is whether the state can be deterred from proliferating, and if so, at what cost. The model presented in this work can be used to draw a quantitative relationship between attacker characteristics and "deterrence budget", or the investment level required by the defender to deter a state from perpetrating an attack. While the model currently does not feature a "no action" option for the attacker, such an option could easily be incorporated. A risk tolerance could be assumed for an attacker by establishing some DP above which he chooses the "no action" option, because he would rather do nothing than accept that risk of detection. A functional relationship between the attacker's risk tolerance the budget required to force him to the no action option could then be determined. Such an analysis would provide policy makers unique insight into how safeguards investments do or do not affect the decision made by a state to pursue an illicit weapons program.

While the methodology presented here allows for the generation of realistic and policy-relevant results, like those discussed above, it does have some shortcomings that limit its direct applicability to real-world situations. Specifically, the use of a Cournot game limits the fidelity with which some safeguarding strategies can be modeled. A Cournot game was used because it more faithfully captures the impact of random inspections, which are one of the foundational elements of IAEA safeguarding strategies; however, a sequential play game is a better approximation for certain types of safeguards, like CEMO or seals, where the attacker has *a priori* knowledge that the defender is playing a certain strategy or strategy element, because he can observe it once it is installed. In order to accommodate both sequential and simultaneous elements into the model, a hybrid Cournot-Stackelberg game could be modeled. In such a model, the defender would play certain elements that are transparent to the attacker, like routine inspections or the installation of a large piece of equipment, and then having observed those elements, the attacker would commit to a strategy and the defender would simultaneously

commit the remainder of her resources. Adapting the methodology to feature a hybrid game would make the output more realistic and physically meaningful in cases where some of the defense strategy has mixed Cournot and Stackelberg elements, such as a strategy that features both random inspections and the installation of permanent equipment.

Appendix A: IAEA Gas-Centrifuge Enrichment Plant Safeguards

Physical Inventory

Physical inventories are conducted to count and verify feed and product cylinders in storage yards, connected to cascades, and in process vessels.

Mass Balance Verification- Load-Cell Based Weighing System

During inventory, the mass balance of both uranium and ^{235}U are verified, and missing mass is calculated using Equation A.1. Any non-zero mass difference (i.e. $\frac{dm}{dt} \neq 0$) is cause for further investigation [45].

$$\frac{dm}{dt} = \dot{m}_{feed} - (\dot{m}_{tails} + \dot{m}_{product}) = 0 \qquad \text{A.1}$$

The load-cell based scale used for this safeguard operates in two load ranges: up to 5000 kg and up to 20,000 kg. It determines the gross weight of bulky, massive objects like UF_6 shipping cylinders. Gross weights can be determined with an accuracy of better than 1% [41].

The inspector and operator agree to a specified "residence time," during which feed and product cylinders must remain in storage and cannot be introduced into the cascade or shipped to customers. After the residence time the operator may move or ship the cylinder, whether the IAEA has verified the material or not. Around fifteen days is a standard residence time for product cylinders [89].

Video surveillance- reviewing logged images

Optical surveillance is used in storage areas where human presence and activities are relatively rare events. Multiple cameras are used to ensure that the entire area falls under the field of view. Image recording can either be done periodically, with the period less than the minimum time needed to remove material, or can be triggered by motion or scene change. Two images should be recorded in rapid succession, so that the direction of motion can be determined. Images can either be logged for examination by inspectors at a later date, or transmitted remotely to the IAEA. Data encryption and authentication are done to prevent tampering with the transmitted signal.

Seals

Seals are attached to single items to ensure that material is not introduced or removed. IAEA equipment that is left at the facility is also sealed to prevent tampering. Seals can be either single-used items, which are replaced each time they are checked, or seals that are verifiable in situ. All seals are uniquely identifiable. Passive single-use seals (CAPS) are identifiable by a unique pattern of random scratches on the inside surface of the metal cap. During seal verification, CAPS are detached and sent to IAEA Headquarters for verification, where the integrity of the seal is checked and pattern of scratches is checked against the original pattern to ensure that the attacker has not replaced the seal [41].

Unlike passive seals, active seals can be verified in situ during inspections, and can also transmit a signal if they have been tampered with. Active seals can be fiber optic, ultrasonic, or electronic [41]. These seals are re-useable and can be used for multiple years if they are not tampered with, though the batteries generally need to be replaced every two-four years [90].

Non-Destructive Assay (NDA)

NDA determines enrichment at the gross and partial- defects level.[27] A germanium detector coupled with a multi-channel analyzer is generally used to determine the enrichment of a UF_6 shipping cylinder. The thickness of the cylinder is first determined using an ultrasonic thickness gauge, in order to account for gamma attenuation in the cylinder walls. Results can have an accuracy of 1-2%, provided that the steel wall is less than 10 mm thick [41]. An NaI detector is generally used for NU feed and DU tails, with errors between 10-20% for NU and 25-50% for DU [30].

Destructive Analysis (DA)

Destructive analysis is used to determine enrichment at the bias-defects level [91].[28] In order to perform DA, the inspector takes independent samples at the facility and conditions them on-site to ensure that they are in a chemical form suitable for transport. The samples are then

[27] The 2001 IAEA Safeguards Glossary defines a gross defect as "an item or batch that has been falsified to the maximum extent possible so that all or most of the declared material is missing." A partial defect is "an item or batch that has been falsified to such an extent that some fraction of the declared amount of material is actually present."

[28] A bias defect refers to "an item or batch that has been slightly falsified so that only a small fraction of the declared amount of material is missing".

packaged and sealed and shipped to the IAEA Safeguards Analytical Laboratory (SAL). The samples are either analyzed at SAL or a laboratory in the Network of Analytical Laboratories (NWAL) using a variety of analytical techniques.

To determine isotopic uranium concentrations in UF_6 samples, two primary techniques are used: Thermal Ionization Mass Spectrometry (TIMS) and high-resolution gamma spectrometry. TIMS is performed with total sample evaporation on a filament, which results in a relative error of 0.05% for isotope ratios of 0.05-20. Gamma ray spectrometry with an NaI detector is used as a complementary quantification measure. For this technique, the UF_6 sample is dissolved and the gamma emission from the 186 keV peak counted. The sample is compared against five standard uranium solutions with known uranium concentrations. Errors for this technique range from 0.5% for natural uranium to 0.2% for enriched uranium [41].

CEMO

The continuous enrichment monitor (CEMO) is mounted to the low-pressure end of a header pipe and sealed. The unit is attached to the aluminum pipe walls, which are about 5 mm thick [92]. Pressure at this point is around or less than 10 torr [54], [93], [94]. Eight NaI detectors measure the intensity of the 186-keV ^{235}U gamma peak to determine the total mass of ^{235}U. A ^{109}Cd source is used to determine process gas pressure (through absorption of Ag K-alpha x-rays). Using the two measurements, gas enrichment is measured. Two operating parameters must be met in order or CEMO to operate effectively:

(1) $D * P > 30$ cm.torr
(2) $D * E * P > 10$ cm.%.torr

Where D [cm] is the pipe inner diameter, E [% ^{235}U] is enrichment, and P [torr] is pressure.

CEMO is designed to give a "go-no go" message confirming that the enrichment of the gas is below 20%. It is checked during inspections and gives a data summary to the inspector with information about any anomalies, as well as enrichment and pressure trends since the last inspection. The CEMO also send status updates to the IAEA. A daily message is sent to the IAEA about the state of health of the machine and indicating that no safeguard situation has arisen requiring inspector presence [95]. If there are two consecutive enrichment readings above 20%, a message is sent to the IAEA: "Inspector presence necessary" [92].

Limited Frequency Unannounced Access (LFUA) Visits

Inspectors perform limited inspections annually to inspect cascade halls. These inspections are performed on a random basis, and access must be provided to the inspectors within two hours of the request. LFUA visits occur 4-12 times/year. Activities during an LFUA visit include visual observation, NDA measurements on header pipes, DA on UF_6 samples from the cascade (rare event) and environmental sampling (ES) [30].

Visual Observation

During special inspections, inspectors visually inspect the cascade halls. They look for the presence of unreported feed/withdraw (F/W) equipment or any extraneous cylinders in the area, like small 5A cylinders that can be used to remove small product quantities. Inspectors also compare cascade piping connections and valve settings with design specifications to detect any cascade re-piping [58], [63].

Environmental Sampling

Environmental sampling gives information about past and current activities at a facility. This technique is used in cascade halls during a special inspection. Inspectors take swipes on 10x10 cm cotton swipes prepared in an ultra-clean lab and send them to Vienna for analysis [96]. Low-level gamma spectrometry with a germanium detector and X-ray fluorescence spectrometry are used as preliminary screening tests. Both of these techniques can identify the presence of U or Pu in a sample and can give information about the activity of the sample. The gamma counting takes a total of 15 hours (1 hr for each of 15 samples) and the x-ray fluorescence takes 4-5 hours. After initial screening, samples are distributed to NWAL laboratories for further analysis. Isotopic analysis is done using TIMS, as described for destructive analysis; however, for ES much greater sensitivity is needed, in the 10^{-9} and 10^{-12} g ranges. A Scanning Electron Microscope is used to obtain information about the size and morphology of U and Pu particles, which gives information about the process that created the particles [41].IAEA inspectors take six ES samples from various places at the facility when they perform this safeguard [97].

Appendix B: Implementation

B.1 Strategy Generation and Storage

The defender strategies are stored using a data structure named "safeguards", which holds parameter information about each safeguarding option, including, name, whether the safeguard is active (meaning it has been purchased by the defender), the false alarm probability, the number of items to which it applies, count time, frequency and dependency. Note that all of these parameters do not apply to each safeguard, in which case the parameter specification is set to a designated "EMPTY" value.

Defender strategies are stored in a separate "dstrategy" structure that holds a unique ID for each strategy, as well as the array of safeguards that characterizes that strategy. The enumeration of defender options is stored in an array holding all of the "dstrategy" structures. Analogous structures are used to store attacker strategy information. The analogue to the "safeguards" structure is the "aoptions" structure, which stores the name of the option, whether it is active, the duration, the frequency, the number of items attacked, the area (feed or product storage), the amount of material taken in each attack, the product assay and the feed assay

Each attacker strategy is stored in an "astrategy" structure; however, this structure differs in that each strategy does not hold an array of "aoptions", as only one attacker option is active in each attacker strategy. The universe of attacker strategies is again stored in an array of "astrategy" structures.

B.2 Integrated Model Implementation

Minor adaptations were made to the enrichment and reprocessing simulations models in the integrated model. These changes include:

- Passive seals and environmental samplings were eliminated from the menu of defender options at the GCEP
- All inspection strategies include a GCEP inspection

- The FAP for GCEP inspections was fixed at 0.01
- The count rate for CEMO was fixed at 300 s

References

[1] B. Obama, “Remarks of President Barack Obama,” Prague, 05-Apr-2009.

[2] P. Kerr, “ElBaradei: IAEA Budget Problems Dangerous,” *Arms Control Association*. [Online]. Available: http://www.armscontrol.org/print/2465. [Accessed: 29-Aug-2008].

[3] “IAEA Regular Budget for 2012,” *International Atomic Energy Agency*. [Online]. Available: http://www.iaea.org/About/budget.html. [Accessed: 22-Sep-2012].

[4] National Research Council and Committee to Review the Department of Homeland Security's Approach to Risk Analysis, “Review of the Department of Homeland Security's Approach to Risk Analysis,” pp. 1–161, Dec. 2010.

[5] L. A. T. Cox Jr, “Game Theory and Risk Analysis,” *Risk Analysis*, vol. 29, no. 8, pp. 1062–1068, Aug. 2009.

[6] K. Budlong Sylvester and J. Pilat, “The Evolution of Information-Driven Safeguards (ppt),” pp. 1–12, 2010.

[7] US Committee on the Internationalization of the Civilian Nuclear Fuel Cycle, National Research Council US Committee on the Internationalization of the Civilian Nuclear Cycle, and Russian Academy of Sciences US Committee on the Internationalization of the Civilian Nuclear Fuel Cycle, *Internationalization of the nuclear fuel cycle: goals, strategies, and challenges*. 2008.

[8] D. Engi and D. Boozer, “Use of ISEM in studying the impact of guard tactics on facility safeguards system effectiveness.[Insider Safeguards Effectiveness Model],” 1977.

[9] A. Pritsker and N. Hurst, “GASP IV: a combined continuous-discrete FORTRAN-based simulation language,” *Simulation*, vol. 21, no. 3, p. 65, 1973.

[10] J. Matter, “SAVI: A PC-based vulnerability assessment program,” 1988.

[11] J. Matter, R. Al-Ayat, and T. Cousins, “A demonstration of ASSESS: Analytic System and Software for Evaluating Safeguards and Security,” 1989.

[12] “ATLAS (Adversay Time-Line Analysis System).” 25-Jun-2003.

[13] F. Durán, “Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Materials ,” *Dissertation*, p. 118, Aug. 2010.

[14] H. A. Dayem, “Modeling and Simulation for the Design and Evaluation of Advanced Materials Accounting Systems,” pp. 1–9, 1979.

[15] B. Cipiti and O. Zinaman, “Separations and safeguards model integration.,” 2010.

[16] B. B. Cipiti, F. A. Durán, B. Middleton, and R. Ward, “Fully Integrated Safeguards and Security for Reprocessing Plant Monitoring,” *SAND2011-7292, Sandia National Laboratories (October 2011)*.

[17] H. L. HA Elayat and W. O'Connell, “Systems Analysis of Safeguards Effectiveness in a Uranium Conversion Facility,” pp. 1–11, Jun. 2004.

[18] H. Elayat, W. O'Connell, and B. Boyer, “Gas Centrifuge Enrichment Plant Safeguards System Modeling,” 2006.

[19] M. Yue, L. Cheng, and R. Bari, “A Markov Model Approach to Proliferation-Resistance Assessment of Nuclear Energy Systems,” *Nuclear technology*, vol. 162,

no. 1, pp. 26–44, 2008.
[20] D. Bley, U. S. BCI, J. Cazalet, F. CEA, G. Renda, G. Rochau, U. S. SNL, M. Senzaki, I. Therios, and M. Zentner, "Evaluation methodology for proliferation resistance and physical protection of Generation IV nuclear energy systems: an overview," 2006.
[21] J. Watson, *Strategy: An Introduction to Game Theory*, 2nd ed. New York: W.W. Norton & Company, 2008.
[22] R. Avenhaus and M. J. Canty, *Compliance Quantified: An Introduction to Data Verification*. New York: Cambridge University Press, 1996.
[23] V. Bier, S. Oliveros, and L. Samuelson, "Choosing What to Protect: Strategis defense allocation against an unknown attacker," pp. 1–36, Dec. 2004.
[24] D. Kilgour and R. Avenhaus, "The Optimal Distribution of IAEA Inspection Effort: Final Report," The Division, Jun. 1994.
[25] G. Brown, W. Carlyle, R. Harney, E. Skroch, and R. Wood, "Interdicting a nuclear-weapons project," *Operations research*, vol. 57, no. 4, pp. 866–877, 2009.
[26] G. D. Wyss, J. P. Hinton, K. Dunphy-Guzman, J. Clem, J. Darby, C. Silva, and K. Mitchiner, "Risk-Based Cost-Benefit Analysis for Security Assessment Problems," *International Meetings on Probabilistic Safety Assessment and Management*, pp. 1–12, Mar. 2010.
[27] G. D. Wyss, J. F. Clem, J. L. Darby, K. Dunphy-Guzman, J. P. Hinton, and K. W. Mitchiner, "Risk-based cost-benefit analysis for security assessment problems," pp. 286–295, 2010.
[28] "Human Reliability Analysis," *NOPSEMA*, 25-Jun-2012. [Online]. Available: http://www.nopsema.gov.au/resources/human-factors/human-reliability-analysis/. [Accessed: 25-Jun-2013].
[29] J. Robinson, "An Iterative Method of Solving a Game," *The Annals of Mathematics*, vol. 54, no. 2, pp. 296–301, Sep. 1951.
[30] B. Boyer, "Safeguards Approaches for Gas Centrifuge Enrichment Plants," *ppt*, pp. 1–37, Sep. 2008.
[31] G. W. Brown, "Some Notes on Computation of Game Solutions," p. 78, 1949.
[32] A. Washburn, "A new kind of fictitious play," *Naval Research Logistics*, vol. 48, pp. 270–280, 2001.
[33] C. Daskalakis, "Topics in Algorithmic Game Theory." 10-Feb-2010. [Online]. Available: http://people.csail.mit.edu/costis/6896sp10/lec3.pdf.
[34] H. Shapiro, "Note on a Computation Method in the Theory of Games," *Communications of Pure and Applied Mathematics*, vol. XI, pp. 587–593, Nov. 1958.
[35] J. Szep and F. Forgo, *Introduction to the Theory of Games*. Hingham, MA: D. Reidel Pub. Co., 1985.
[36] D. Gordon, J. Sanborn, J. Younkin, and V. DeVito, "An Approach to IAEA Material-Balance Verification at the Portsmouth Gas Centrifuge Enrichment Plant," *Proceedings of the Fifth Annual Symposium on Safeguards and Nuclear Material Management*, p. 39, 1983.
[37] B. D. Boyer, H. Erpenbecka, K. Millera, K. Ianakieva, B. Reimolda, S. Warda, and

J. Howellb, “Gas centrifuge enrichment plants inspection frequency and remote monitoring issues for advanced safeguards implementation,” 2010.
[38] G. G. Thoreson and E. A. Schneider, “Efficient calculation of detection probabilities,” *Nucl Instrum Meth A*, vol. 615, no. 3, pp. 313–325, Apr. 2010.
[39] A. D. Swain and H. E. Guttman, “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,” Aug. 1983.
[40] P. Newman, S. Rhoades, and R. Smith, “Allocating audit resources to detect fraud,” *Review of Accounting Studies*, vol. 1, no. 2, pp. 161–182, 1996.
[41] IAEA, “Safeguards Techniques and Equipment,” *International Nuclear Verification Series*, vol. 1, pp. 1–92, Aug. 2003.
[42] R. Poyser, “Areva,” pp. 1–24, Jun. 2012. [Online]. Available: http://tinyurl.com/ll4r36u.
[43] G. Eccleston and E. Wonder, “Uranium Hexfluoride (UF6) Cylinders Monitoring Needs,” *Discussions with NMMSS Users Group Meeting*, pp. 1–25, 2010.
[44] D. Kovacic, S. Hayes, D. Burk, M. Whitaker, and J. Morgan, “UF6 Cylinder Tagging System for a Uranium Enrichment Plant,” *ORNL/TM-2006/98*, 2006.
[45] B. D. Boyer, K. Erpenbeck, K. Miller, K. Ianakiev, B. Reimold, S. Ward, and J. Howell, “Gas Centrifuge Enrichment Plants Inspection Frequency and Remote Monitoring Issues for Advanced Safeguards Implementations,” pp. 1–20, Oct. 2010.
[46] C. Sacchi and C. Regazzoni, “A distributed surveillance system for detection of abandoned objects in unmanned railway environments,” *Vehicular Technology, IEEE Transactions on*, vol. 49, no. 5, pp. 2013–2026, 2000.
[47] M. L. Garcia, *Design and Evaluation of Physical Protection Systems*, 2nd ed. Butterworth-Heinemann, 2007.
[48] R. Johnston, “Assessing the Vulnerability of Tamper-Indicting Seals,” *Port Technology International*, 2005.
[49] R. Johnston, A. Garcia, and A. Pacheco, “Efficacy of tamper-indicating devices,” *Journal of Homeland Security*, 2002.
[50] R. Johnston, A. Garcia, and W. Grace, “Vulnerability assessment of passive tamper-indicating seals,” *JNMM*, vol. 23, no. 4, 1995.
[51] J. Wieman, “Practical Uncertainty limits in Gamma-Ray Enrichment Measurements on Low Enriched Uranium Hexafluoride.”
[52] H. Smith Jr, “The Measurement of Uranium Enrichment,” *Passive Nondestructive Assay of Nuclear Materials*, vol. 7, 1991.
[53] M. Wiggs, “Measurement of Germanium Detector Efficiency,” pp. 1–9, Sep. 2009. [Online]. Available: http://physics.nd.edu/assets/25222/wiggs_marcus_germanium_detect.pdf.
[54] D. Close, J. Pratt, H. Atwater, J. Malanify, K. Nixon, and L. Speir, “Measurement of uranium enrichment for gaseous uranium at low pressure,” 1985.
[55] R. Harray, J. Aaldijk, and J. Braak, “Some Measurements for Centrifuge Enrichment Plant Safeguards,” *Proc. Third Annu. ESARDA Symp. Safeguards Nucl. Mater. Manage*, pp. 6–8.
[56] K. Ianakiev, B. Boyer, A. Favalli, J. Goda, T. Hill, D. MacArthur, C. Moss, M. Paffett, C. Romero, and M. Smith, “Improving Accuracy and Reliability of 186-keV

Measurements for Unattended Enrichment Monitoring," *Pacific Northwest Conference on Global Nuclear Security11–16 April*, 2010.
[57] L. Demsetz, J. Cabrera, and B. University of California, "Detection Probability Assessment of Visual Inspection of Ships," 1999.
[58] J. M. Whitaker, "Safeguarding Uranium Enrichment: The Challenge of Large Gas-Centrifuge Facilities," *2010 NNSA Intern Videoconference Series*, pp. 1–29, Aug. 2010.
[59] O. Heinonen. Personal communication, Cambridge (12-Dec-2012).
[60] IAEA, "IAEA Safeguards Analytical Laboratories," pp. 1–2, Nov. 2012.
[61] *Bureau of Labor Statistics*. [Online]. Available: http://www.bls.gov. [Accessed: 26-Jun-2013].
[62] J. Garner. "Quick safeguards question." Personal e-mail (06-Feb-2013).
[63] B. D. Boyer, "IAEA Verifications at an Uranium Enrichment Plant," pp. 1–25, Aug. 2009.
[64] Motorola, "Video Surveillance Economics," pp. 1–6, Aug. 2008. [Online]. Available: http://tinyurl.com/lm29cex.
[65] *Amptek*. [Online]. Available: http://www.amptek.com. [Accessed: 26-Jun-2013].
[66] C. Lythgoe, "Thermal Ionisation Mass Spectrometry," pp. 1–27, Dec. 2006.
[67] "Annual Report 2009," *International Atomic Energy Agency*, 26-Jun-2010. [Online]. Available: http://www.iaea.org/Publications/Reports/Anrep2009/table_a5.pdf. [Accessed: 26-Jun-2013].
[68] M. Wolfe, "Electronic Cargo Seals: Context, Technologies, and Marketplace," *Intelligent Transportation Systems Joint Program Office, FHWA, USDOT, July*, vol. 12, 2002.
[69] C. Bathke, "The Attractiveness of Materials in Advanced Nuclear Fuel Cycles for Various Proliferation and Theft Scenarios," *ppt*, p. 16, 2009.
[70] B. B. Cipiti. "MPACT Report." Personal e-mail (25-Mar-2013).
[71] T. Todd, "Spent Nuclear Fuel Reprocessing," pp. 1–59, Feb. 2008.
[72] P. Durst, I. Therios, R. Bean, A. Dougan, B. Boyer, Pacific Northwest National Laboratory US, and United States Dept of Energy, *Advanced Safeguards Approaches for New Reprocessing Facilities*. 2007.
[73] C. Pereira, "UREX+ Process Overview," pp. 1–55, Mar. 2008.
[74] T. L. Burr, C. A. Coulter, and L. E. Wangen, "Benchmark data for a large reprocessing plant for evaluation of advanced data analysis algorithms and safeguards system design," 1998.
[75] A. Tanskanen, "Assessment of the neutron and gamma sources of the spent BWR fuel," *Interim report on Task FIN JNT A*, vol. 1071, 2000.
[76] Croff, "Reactors and Fuels," pp. 1–56, Dec. 2008.
[77] C. Creusot, B. Chesnay, S. Johnson, S. Nakano, Y. Yamauchi, Y. Yanagisawa, J. Goncalves, and V. Sequeira, "Innovative Approaches to DIE/DIV Activities at the Rokkasho Reprocessing Plant," 7th International Conference on Facility Operations-Safeguards Interface, Mar. 2004.
[78] E. M, M. Chesnay, C. Creusot, J. Damico, S. Johnson, J. Wuester, S. Masuda, and M. Kajii, "A.1.1 Solution Monitoring Applications for Rokkasho Reprocessing

Plant," 7th International Conference on Facility Operations- Safeguards Interface, Mar. 2004.
[79] S. J. Johnson, R. Abedin-Zadeh, C. Pearsall, K. Hiruta, C. Creusot, E. MM, E. Kuhn, B. Chesnay, N. Robson, and H. Higuchi, "Development of the safeguards approach for the Rokkasho reprocessing plant," 2001.
[80] S. Johnson, E. MM, and M. Schanfein, "Report on the NGS3 Working Group on Safeguards by Design for Aqueous Reprocessing Plants," 2011.
[81] M. Collins, "Hybrid K-Edge Densitometer Simulation Module for Safeguards Performance Modeling," *NEAMS PI Meeting*, pp. 1–14, Oct. 2010.
[82] G. A. Warren, K. Anderson, A. M. Casella, Y. Danon, M. Devlin, A. Gavron, R. C. Haight, J. T. Harris, G. Imel, J. Kulisek, J. M. O'Donnell, T. Stewart, and A. Weltz, "Lead Slowing-Down Spectrometry Time Spectral Analysis for Spent Fuel Assay: FY12 Status Report," Oct. 2012.
[83] A. H. Liu, "Simulation and implementation of distributed sensor network for radiation detection," *Dissertation*, 2010.
[84] T. Iwamoto, "Hold-up Measurement in a Reprocessing Facility," pp. 1–17, Nov. 2006. [Online]. Available: http://www.inmm.org/holdup_workshop/2C%20Iwamoto.pdf.
[85] R. M. Van Genhoven, R. T. Kouzes, and D. L. Stephens, "Alternative Neutron Detector Technologies for Homeland Security," PNL-18471, Jun. 2009.
[86] S. Johnson. "Follow-up questions." Personal e-mail (April 26, 2013).
[87] S. E. Bays, S. J. Piet, N. R. Soelberg, M. J. Lineberry, and B. W. Dixon, "Technology Insights and Perspectives for Nuclear Fuel Cycle Concepts," *Fuel Cycle Research & Development, INL/LTD-10-19977*, 2010.
[88] G. Radulescu, I. C. Gauld, and G. Ilas, "SCALE 5.1 Predictions of PWR Spent Nuclear Fuel Isotopic Compositions," *ORNL/TM-2010/44, Oak Ridge National Laboratory, Oak Ridge, Tennessee*, 2010.
[89] B. Boyer, D. Gordon, and J. Jo, "Use of Mailbox approach, video surveillance, and short-notice random inspections to enhance detection of undeclared LEU production at gas centrifuge enrichment plants," 2006.
[90] R. Tzolov, M. Goldfarb, and L. Pénot, "Development and evaluation of new electronic seals at the IAEA," *Symposium on International Safeguards, Verification and Nuclear Material Security*, vol. 29, 2007.
[91] "IAEA Safeguards Glossary," pp. 1–230, May 2002.
[92] K. Ianakiev, B. Alexandrov, B. Boyer, T. Hill, D. MacArthur, T. Marks, C. Moss, B. Nolen, M. Paffett, and G. Sheppard, "New generation enrichment monitoring technology for gas centrifuge enrichment plants," *Nuclear Science Symposium Conference Record, 2008. NSS'08. IEEE*, pp. 3055–3059, 2008.
[93] D. Close and J. Pratt, "Verification of Uranium Enrichment in Gaseous Centrifuge Header Pipers with a Diameter of 44.5 mm,"," *ESARDA*, vol. 21, p. 161, 1987.
[94] A. Lebrun, "Design, modeling and viability analysis of an online uranium Enrichment Monitor," *Nuclear Science Symposium and …*, 2011.
[95] S. Baker, B. Dekker, P. Friend, and K. Ide, "The Introduction of a Continuous Enrichment Monitor for Safeguards Applications in Centrifuge Enrichment Plants,"

ESARDA, pp. 1–5, 1995.

[96] W. Bush, G. EKENSTAM, J. Janov, E. Kuhn, and M. Ryjinski, “IAEA Experience with Environmental Sampling at Gas Centrifuge Enrichment Plants in the European Union.”

[97] M. Zendel, D. L. Donohue, E. Kuhn, S. Deron, and T. Bíró, “Nuclear Safeguards Verification Measurement Techniques,” no. 63, Boston, MA: Springer US, 2011, pp. 2893–3015.

VITA

Rebecca Ward, the daughter of Rita Mendl and David Ward, was born and raised in Maryland. She attended McDaniel College in Westminster, MD, where she played varsity soccer and graduated Summa Cum Laude with B.A. degrees in Chemistry and Physics in 2006. After college Rebecca taught Physics and coached soccer and lacrosse for two years at Pope John Paul II High School in Hendersonville, TN. In 2008, Rebecca began her graduate studies in the Nuclear and Radiation Engineering program at the University of Texas at Austin, earning her Master's degree in 2010 and continuing on to complete her Doctorate of Philosophy in 2013. During her final year of graduate work, Rebecca served concurrently as a Stanton Nuclear Security Fellow at the Belfer Center for Science and International Affairs at the Harvard Kennedy School. Rebecca is the proud dog mom of Ollie, who is probably the cutest dog who ever lived.