PHYSICAL SECURITY SYSTEM SENSITIVITY TO DBT PERTURBATIONS

A Thesis

by

CURTIS ALAN CONCHEWSKI

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

August 2012

Major Subject: Nuclear Engineering

Physical Security System Sensitivity to DBT Perturbations

PHYSICAL SECURITY SYSTEM SENSITIVITY TO DBT PERTURBATIONS

A Thesis

by

CURTIS ALAN CONCHEWSKI

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Approved by:

Co-Chairs of Committee,	David Boyle
	William Charlton
Committee Member,	Quan Li
Head of Department,	Yassin Hassan

August 2012

Major Subject: Nuclear Engineering

ABSTRACT

Physical Security System Sensitivity to DBT Perturbations. (August 2012)

Curtis Alan Conchewski, B.S., Texas A&M University

Co-Chairs of Advisory Committee: Dr. David Boyle
Dr. William Charlton

This thesis examines how perturbing selected adversary capabilities in a design basis threat (DBT) may affect the assessment of a facility's security system performance. We found that using a strictly defined DBT to design and analytically test facility security systems can lead to invalid assessments that security measures are meeting standards. Design Basis Threats are intended to represent the most severe yet realistic attack a facility might face. However, the static nature of the standard DBT makes it unable to test the performance of a facility security system in the case where a specialized adversary may possess different capabilities than defined in the DBT. Our analysis of security system performance for various modeled facilities revealed significant vulnerabilities to certain perturbations of adversary capabilities. These vulnerabilities went undetected when the original strictly defined graded DBT was used in the assessment procedure. By maximizing one adversary capability at the expense of others, a specialized adversary force was able to efficiently defeat each facility.

To address this problem, we proposed employing a so-called "point-based" DBT as an alternative to the existing strictly defined DBT. In a point-based DBT, multiple scenarios are assessed that test different sets of adversary capabilities to better uncover

and understand any security system vulnerabilities that may exist. We believe the benefit of identifying these site-specific security vulnerabilities will outweigh the additional cost of generating a point-based DBT, especially if the vulnerabilities are identified during the initial design of the security system.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Page

1. INTRODUCTION

Most security systems for high value nuclear targets are designed using specific threat definitions as suggested by the IAEA. Security designers use these threat definitions to test a facility's physical security system to ensure adequate protection is in place. The design basis threat (DBT) is often an amalgamation of current threats due to our inability to accurately define an actual future adversarial actor. We hypothesized that using a DBT with explicitly defined threat capabilities can result in exploitable security vulnerabilities when the threat is incorrectly defined. This thesis analyzes the sensitivity of several physical security systems to DBT perturbations, based on how the security system's performance changes against the perturbed threat. Multiple facility security systems were modeled with features capable of defeating the initial DBT. Elements of this DBT were then perturbed, enabling determination of the threat characteristics most important to correctly define and the consequences of small variations in the threat. Following this work's analysis of the current DBT system, two end-products are discussed: a tabulation of the DBT characteristics that produce the greatest change in security performance when altered and an alternative point-based approach to the current DBT methodology.

This thesis follows the style of *Nuclear Science and Engineering.*

1.1 Design Basis Threat Background

To ensure that high consequence nuclear material is adequately protected, the IAEA recommends the use of a design basis threat (DBT). This recommendation is found in INFCIRC/225/Rev5 [1], which requires the use of a design basis threat (DBT) or a threat assessment devised by the State's competent authority. A DBT is a state-designed adversarial threat which the security systems at applicable facilities must be capable of defeating. Adversary characteristics such as the number of attackers, financial backing, equipment, weapons, training, insider support, motivation, and employed tactics are all explicitly defined in a "strictly defined" DBT. In the United States, multiple agencies contribute to and help construct the DBT based on input from the intelligence community's assessment of credible threats. An accurate DBT allows for the efficient implementation of security features, allocation of resources, and confidence in the security system as a whole. Due to the continuously changing range of threats that possess the motivation and capability of striking US assets, it is impossible to guarantee that the most likely threat is encompassed by the current DBT. Since an actual attack is unlikely to look exactly like the adversary in the DBT, it is important that the physical security system be able to handle threats with characteristics that differ from those defined in the DBT.

While it is possible for a state to develop either a separate DBT for each facility or a single state-wide threat assessment, it is more common to use a "graded" DBT system (sometimes referred to as a tiered DBT). For this approach, the state's competent

authority divides its facilities into several grades based on the category of material contained or the consequences of a successful adversary action. A DBT is then designed for each grade rather than for each facility. The use of a graded system instead of a single nationwide DBT has the benefit of balancing risk amongst different categories of facilities. A hospital with medical sources need not be capable of defeating the same highly trained adversary force that comprises the DBT of a highly enriched uranium (HEU) storage facility. With a graded DBT, the hospital is placed on a lower grade than the HEU depot. A balance of risk between the facilities is established with the graded DBT, as the HEU depot's higher consequence level is offset by the enhanced security features necessary to defeat the higher grade DBT. Facility risk is proportional to the probability and consequences of a successful adversary attack. The mechanics behind how risk is calculated and used are discussed in Section 2.

The graded DBT system is commonly used based on the belief that it is the most efficient middle ground between use of a statewide DBT and separate DBTs for each nuclear asset. Questions about the validity of this belief motivated this thesis.

1.2 Background and Literature Review of Nuclear Security

The basics of nuclear material physical protection methods are established and mandated in INFCIRC/274/Rev1 [2], which requires compliant parties to provide a sufficient level of protection for nuclear assets. The jurisdiction of required State protection is expanded to include all in-state transportation and transit out of country until the new host country takes charge. This document also breaks down what types and

quantities of material constitute the three IAEA categories of nuclear material that must be protected. Category I material includes unirradiated plutonium (as long as the ^{238}Pu concentration is less than 80%), unirradiated HEU, and unirradiated ^{233}U. This category requires the most stringent security, including storage in a designated protected area, constant surveillance with guards in close communication to the response force, access restricted to only those with special clearance, and special measures to ensure detection and prevention of an assault. This is the level of material that represents the target throughout the thesis work and normally calls for the highest grade of a graded DBT.

More specific recommendations on how this level of security should be established are found in INFCIRC/225/Rev5 [1]. This document provides an in-depth look at the State's responsibility: international transport, physical protection, risk management, defense in depth, security culture, quality assurance, and confidentiality. The physical protection responsibilities include planning and preparing a response force to deal with the threats of theft and sabotage, as well as requirements for each category of material to prevent or mitigate these threats. This information circular also introduces the concept of a design basis threat as a follow-up to a threat assessment for high value material or targets. The IAEA describes the basics of an effective protection system as a function of detection, delay, and response. The detection, delay, and response format with an evolving DBT forms the backbone of physical security design in most nuclear countries and for multiple agencies within the United States.

The IAEA goes into further detail of how to construct and use a DBT in their Nuclear Security Series No.10, "Development, Use and Maintenance of the Design Basis Threat" [3] implementation guide. Whereas other IAEA documents mentioned the benefits of or the need to use a DBT, this document is entirely focused on the DBT concept and goes through each step of its establishment, use, and upkeep. The DBT is stated to be "a comprehensive description of the motivation, intentions, and capabilities of potential adversaries against which protection systems are designed and evaluated. Such definitions permit security planning on the basis of risk management. A DBT is derived from credible intelligence information and other data concerning threats, but it is not intended to be a statement about actual, prevailing threats." This last part is important in its acknowledgement that, based on the realistic limitations of intelligence collection, the DBT will never precisely represent the actual threat facing the facility, and in fact, is not intended to. It is unlikely for any one adversary group to possess all the capabilities of the DBT, which are compiled from analysis of all possible adversaries with the capability and motivation to attack the facility. A more detailed look into the role of intelligence with regards to nuclear security can be found in the *Nonproliferation Review* article, "Indispensable Intelligence and Inevitable Failures" by Torrey Froscher[4]. Froscher's assertion that the intelligence that leads to the characteristics of the DBT can never be exact or complete, demonstrates the value of this thesis which seeks to understand and limit security system performance sensitivities to the DBT.

To understand how perturbations of the DBT can affect the physical security system's performance, it is necessary to understand the security system design. A

thorough and commonly used top level perspective is given in Mary Lynn Garcia's "Design and Evaluation of Physical Protection Systems," [5]. Garcia establishes the reasoning and mathematics behind detection and delay and explains the concept of risk as calculated in terms of physical protection system (PPS) properties, attack probability, and consequence. An interesting discussion about the definition of risk and the difficulty of conducting cost-benefit analysis of physical security is found in Sandia's "Risk-Based Cost-Benefit Analysis for Security Assessment Problems," [6]. This book delves further into using game theory to depict the probability of attack and presents deterrence and devaluation as forms of dissuasion that seek to influence the adversary's decision making process. Probability of attack and the value of deterrence are notorious for being difficult, if not impossible, to quantify accurately due to the need to understand the adversary's motivation, values, and decision making process. Instead, Sandia believes security investment should be based on consequence and attack scenario difficulty. The attack scenario consists of two main phases: preparation and execution. Both phases have multiple steps the attackers must perform which the host government could discover and compromise. Sandia further discusses how threat assessment is highly based on the target, which is in some contrast to the state level or graded DBT approach commonly used.

The need to ensure the highest degree of security for nuclear assets has been repeatedly brought to the public's attention through congressional testimonies and oversight reports. The GAO's testimony to Congress on the NRC in 2007 [7] revealed differences between the NRC's and the DOE's DBT, despite both protecting high

consequence material such as HEU. An additional critique in the same testimony included the perception that the NRC's DBT was based as much on recommendations from vendors as it was from security experts. Several adversarial capabilities the experts recommended were removed based on financial concerns. Possible deficiencies in the NRC's DBT were again brought to public attention in August 2010 in the CRS Report for Congress [8]. The main deficiency sited was vulnerability to aircraft crashes in older nuclear power plants. It is our belief that further development of physical security design could help persuade public interest groups that the safety of the public is still considered a top priority. The departments and agencies responsible for our nuclear infrastructure could demonstrate this development by reducing PPS sensitivity to the DBT.

While the author is familiar with DOE building practices with regards to physical security, DOD methods were extrapolated from a current DOD security engineering planning manual [9]. This document explains basic scenario considerations and the facility features designed to counter the adversary's actions or mitigate consequences.

A reasonably current (2004) listing of existing terrorist threats, including capabilities and intent, created by the RAND Corporation [10], was consulted to determine which DBT capabilities to perturb in this thesis. This RAND document also discusses the capability-versus-intent plot often used to show the highest current threats to the United States as well as which groups could become threats with shifts in funding or ideology.

We researched the security designing methods employed in several non-nuclear industries to take advantage of modern PPS features used to protect other vital infrastructure systems. The article, "Infrastructure Vulnerability Assessment Model (I-VAM)," [11] in *Risk Analysis,* provided insight into a security approach called I-VAM. The article provides additional discussion on the meaning of vulnerability and risk as well as a basic way to quantify deterrence that is not present in INFCIRC/225 based models. Later in the article, the I-VAM method is demonstrated on a medium-sized clean water system (source, treatment, storage, and distribution) to quantify its vulnerability. Another industry responsible for protecting large-footprint high consequence facilities often found in less than secure environments is the petroleum industry. A vulnerability assessment of a hypothetical refinery and the basics of conducting a risk assessment are found in a *Journal of Petroleum Science and Engineering* article, "Securing Oil and Gas Infrastructure," [12]. Rather than calculate risk against a defined threat, the article provides a checklist of security features and conditions. Risk values are provided for various categories such as the number of security elements and environmental conditions (proximity to a city, local terrorist activity, etc.). The total facility risk is calculated by taking the sum of the individual risk values. While they are an interesting alternative to using a DBT, checklist methods for determining risk are incapable of identifying vulnerabilities that exist based on the site's layout. If Facility A has the same security elements as Facility B, they are given the same risk level without considering the different element layouts and site pathways.

1.3 Project Significance

This thesis analyzes the weaknesses involved with using a strictly defined graded DBT and presents potential improvements to the DBT design and definition process to mitigate those weaknesses. The conventional methods of analyzing physical security with the Design and Evaluation Process Outline (DEPO) Model are discussed in Section 2. The author selected DEPO for this analysis because of the extensive availability of information concerning its usage and his previous experience with the model, as well as DEPO's similarity to other design methodologies based on INFCIRC225/Rev5. Because the actual DBTs used by the various departments and agencies are classified, we devised an unclassified, strictly-defined graded DBT with open-source characteristics of known terrorist threats. The unclassified DBT was used to initially develop and test the security features of each facility and scenario. Quantifying physical security system sensitivity to the use of a strictly defined DBT revealed that the above mentioned concerns, both from within the national laboratory system and the public interest groups were not without reason. A strictly defined DBT can misrepresent the effectiveness of a security system, creating vulnerabilities that can be exploited by adversaries that differ from the DBT. This is especially true when the DBT is shared between different facilities (as in a graded DBT methodology). Our proposed methods to either improve the graded DBT system or implement a new point based DBT are described in Section 3, following discussion of the sensitivity analysis.

2. APPROACH

To verify that using a strictly defined graded DBT to determine physical security risk results in inherent vulnerabilities, we employed the Design and Evaluation Process Outline Model (DEPO). DEPO is a methodology capable of quantitatively gauging the effectiveness of physical security systems against adversaries with defined capabilities. DEPO provides a set of tools that determine the most efficient adversary pathway through a facility to reach a designated target. This method also quantifies the adversary's ability to avoid detection, the value of physical obstacles that serve as delay elements, and the outcome probabilities associated with an engagement between the attackers and the response force. We kept the analysis quantitative so the reader can verify the work performed, recalculate probabilities with updated parameters, or apply the same mathematical models to their own problems.

2.1 Methods Used

It is the objective of this thesis to understand how perturbations in the adversary's capabilities will affect the physical security system's performance against a strictly defined graded DBT. The term "graded" refers to a DBT system where facilities are graded based on the consequence or value of contained material, with each facility with the same grade sharing the same DBT. "Strictly defined" refers to adversary capabilities such as the number of attackers, weapon types, financial backing, etc. that have been explicitly defined rather than given as a range of possibilities. While each

facility's physical security system may be designed to be capable of defeating the defined adversary, how each facility fairs against adversaries with unexpected capabilities will vary. Knowledge of each facility's unique vulnerabilities and sensitivities to these unexpected capabilities should be well established and accounted for to help reduce the risk of system failure when an actual attack varies from what was expected. We hypothesized that variations in some adversary characteristics would have the same effect across multiple facilities whereas the sensitivity to other characteristics would be largely site dependent. To confirm that site specific sensitivities exist, and therefore that overreliance on a strictly defined DBT is dangerous, we modeled multiple facilities and tested their physical security systems against systematically perturbed, strictly defined DBTs.

Because the modeled facilities possessed high consequence targets, they required sophisticated physical security systems. We validated the initial security systems by ensuring they were capable of defeating the realistic adversary defined in the DBT, discussed fully in Section 2.2. Perturbations of the DBT's adversary characteristics across a realistic range resulted in changes to either the probability the response force would intercept the attack force (P_I) or the probability the response force would prevail over or neutralize the attackers (P_N). The level of fluctuation in P_I and P_N determined the system's sensitivity to the DBT perturbation.

2.1.1 Risk Equation

The standard risk equation calculates the overall security risk of a given facility (R) based on several factors:

- Probability of an adversary attack (P_A),
- Probability of the response team intercepting the adversary (P_I),
- Probability the response team will neutralize the adversary (P_N), and
- Consequences of a successful adversary attack (C).

The full equation commonly combines P_I and P_N into a probability that the attack will be successful (P_S). The main advantage of this risk equation is its ability to compare different facilities to determine where to allocate resources. Facilities possessing different types of material can be compared based on the differences in the value of C. Facilities with higher consequence material such as HEU require more effective physical security systems to achieve the same level of acceptable risk as low risk facilities.

The full risk equation is shown in (Eq. 1), the breakdown of P_S is given in (Eq. 2), and the substitution is shown in (Eq. 3).

$$R = P_A * P_S * C \quad \text{(Eq. 1)}$$

$$P_S = 1 - P_I * P_N \quad \text{(Eq. 2)}$$

$$R = P_A * (1 - P_I * P_N) * C \quad \text{(Eq. 3)}$$

The effects of perturbing the DBT on P_N and P_I were the primary focus for determining facility vulnerability. The consequence value did not change with DBT

variation since the target (which determines the consequences of a successful attack) is not a DBT parameter. For the first two modeled facilities (discussed in Section 2.3), it was assumed that an attack would occur and P_A was set to one. Deterrence plays a major role in whether the adversary considers an attack to be cost effective, but deterrence is not accounted for with DEPO. Because deterrence is neglected, it is common to set P_A to one. In the third modeled facility, an HEU-containing convoy and two decoy convoys, P_A represents the probability of attacking the actual transport as opposed to a decoy. The adversary's ability to simultaneously attack multiple targets, and therefore P_A, depends on their level of resources as defined in the DBT.

2.1.2 Probability of Interception

A tool commonly called an adversary sequence diagram (ASD) calculates a given facility's P_I (see Fig. 1). The ASD's purpose is to illustrate every reasonable pathway through the facility to reach the target, determine the most vulnerable pathway (MVP), and then calculate the overall P_I associated with the MVP and the total time it takes to traverse the MVP. For these calculations, we assume the adversary will take the path of minimum detection until the point where an interception is not possible (also known as the critical detection point (CDP)), whereupon they would switch to the fastest pathway.

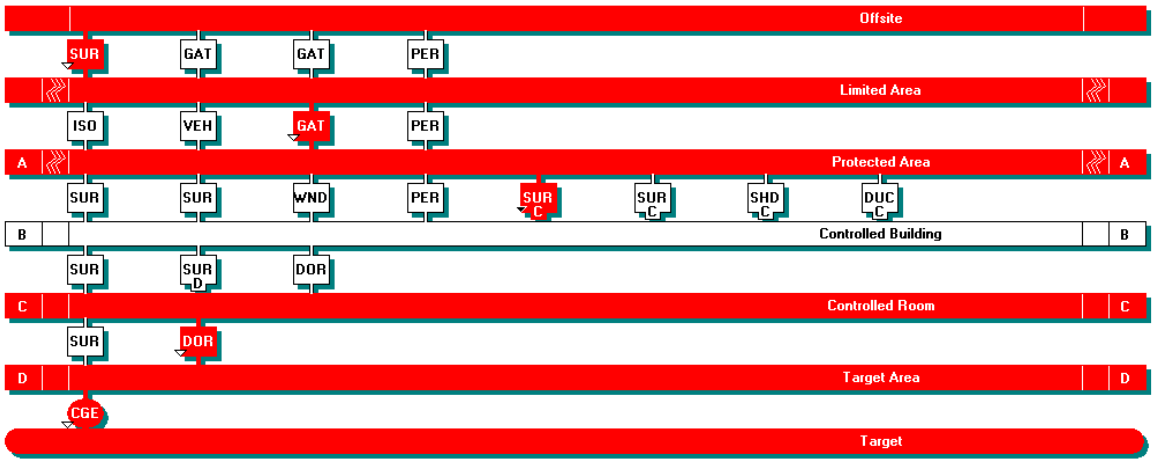

Fig. 1. Sample ASD displaying MVP of an adversary with breaching charges.

The best security design practice is to maximize delay elements close to the target and achieve detection as far from the target as possible. Placing delay elements close to the target pushes the CDP further down the ASD allowing more detection opportunities (note: detection/assessment after the CDP has no value). The ASD is arranged into rows that represent the various facility security levels, such as the limited and protected areas, with each possible path through that level listed horizontally. Each pathway element has an associated delay and detection chance. For an actual facility, these numbers would be determined through repeated testing, but for this analysis a table of average values generated by Sandia National Laboratory was used. The MVP will involve the elements with the lowest detection probability until the CDP and the minimum delay elements afterwards. Assuming all security elements and pathways have been accounted for and the detection/delay numbers are valid, this MVP gives the worst

case scenario with the defined adversary. Alternatively, this methodology will fail if a pathway has not been considered, an insider disables a security element, or the adversary has greater breaching capabilities than expected (each element has a set of delay times based on the equipment used in the breaching maneuver).

We constructed each facility's ASD using the Facility Description Module of Sandia's SAVI program [13]. A summary of each facility and the corresponding ASD's can be found in Section 2.3. More thorough descriptions are located in the Appendix, so that that the reader can recreate the thesis's facilities in SAVI. Unless otherwise noted, all elements possess the default delay and detection characteristics found in SAVI Version 4.0. SAVI contains two executable modules, the Outsider Module and the Facility Module. The Facility Module allows the user to create an ASD complete with all delay and detection elements. The Outsider Analysis Module determines the MVP and CDP of the ASD based on user defined adversary capabilities, response force deployment time, intrusion method, and response strategy.

2.1.3 Probability of Neutralization

Although DEPO provides a fairly accurate method to calculate P_I using values that have been developed with scores of tests, calculation of P_N is either much less accurate or very expensive. Force-on-force exercises are one of the more accurate methods used to test engagements at key points of a facility, but they are costly in both resources and time. While this method may be the best way to test the most important areas of a high value facility, it is much more common to use virtual simulations such as

the Joint Conflict and Tactical Simulation also known as JCATS. Though significantly less costly than force-on-force exercises, the manpower resources required for the JCATS approach exceeded the scope of this project. Since the main goal of this effort is to analyze changes in P_N rather than to determine a single accurate value, P_N was calculated using simple probabilities that convert various factors into force multipliers. The attacker and defender force multipliers were then compared in a straightforward fashion to determine the probability of neutralization (P_N). While this approach does not produce the most accurate absolute results, the relative fluctuation of P_N caused by changes in the adversary's capabilities does provide the information we seek.

The main factors used to determine the force multipliers for the response and adversary forces were:

- Availability of cover and fortifications,
- Combat related training and experience,
- Level of insider assistance, and
- Weaponry and explosives.

The response force was given a defensive force multiplier based on the advantage of using cover and fortifications. This defensive advantage was predetermined based on the scenario, but the multiplier was lowered if the adversary possessed specialized weaponry (e.g., light anti-tank weaponry (LAW)). For Facility One and Two, the use of fortified fighting positions translated into a 2x multiplier if the adversary possessed LAW capability and a 3x multiplier if they did not. The response force

possessed a 2x cover multiplier in Facility Three when the adversary lacked LAW, but the multiplier was fully removed when LAW were allowed. The cover multiplier for Facility Three was lower to account for armored vehicles rather than fixed positions.

Whereas the defensive position multiplier may vary slightly with DBT perturbations, the other multipliers were entirely dependent on the DBT's definition. The possible range of combat training and experience was split into three categories: that of an inexperienced novice with no real training (no multiplier), a combatant with military training equivalent to an Army private with limited combat experience (1.5x multiplier), and an experienced operator comparable to special forces (2x multiplier). The level of adversary training was a DBT characteristic while the response force was always given the 2x multiplier. When the adversary possessed sufficient insider knowledge to prepare for an engagement with the response force, they were provided a 1.5x force multiplier. This multiplier accounted for the adversary being able to: predict where the engagement will occur to avoid expected fields of fire or ambushes, take advantage of site features such as cover, and practice with specialized weaponry to neutralize defensive positions. Advanced weaponry and the training required to use it efficiently was portrayed as a range of multipliers from 1x to 5x for direct fire kinetic weapons and a 2x multiplier for area kill weapons such as grenades and suicide vests. The low end of the range represented combatants equipped either with minimal capabilities (such as handguns) or the inability to efficiently operate their weaponry (attempted handling of a complicated weapon without proper training). The response force received the maximum 5x multiplier due to their training with and use of high-grade military rifles, while the

adversary multiplier was a function of the weapon and training definitions in the DBT. If the adversary was defined as possessing grenades, they were given the additional 2x multiplier. For the purposes of this thesis, it was assumed the response force did not extensively use area kill weaponry.

After force multipliers were factored into each side's strength, simple probability was used to determine the odds that the response force would neutralize the attackers. The probability function can be compared to a series of coin flips, since each effective response force point was equal to an adversary force point. As an example, if the total response-force-to-adversary-force ratio was 5 to 2, the probability that the response force would win was equivalent to the odds of flipping two heads before five tails. In this case, each flip that results in heads represents neutralization of an adversary whereas tails represents a response force casualty. It is important to note that this methodology is not a comparison of the number of defenders versus attackers, but a comparison of the product of force multipliers for each side (of which the physical number of personnel is the original term). The combined product of force multipliers will hereafter be referred to as the "effective force." Figure 2 shows the resulting curve from this probability method when plotting P_N versus the ratio of the effective response force to effective adversary force.

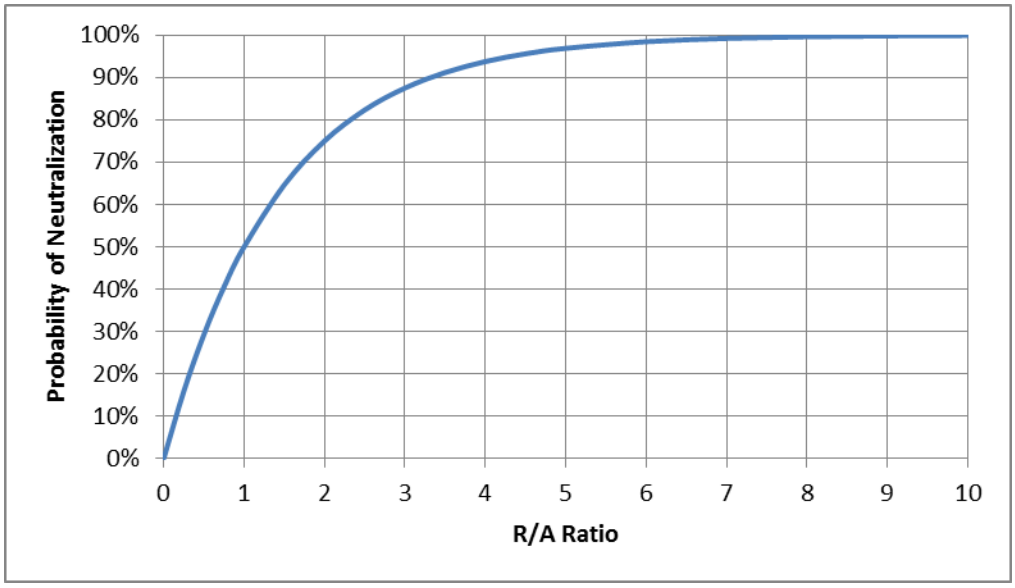

Fig. 2. Probability of neutralization as a function of the effective response force (R) divided by the effective adversary force (A).

As expected, when the two sides are of equivalent strength there is a 50% chance that the response force will succeed. The figure also displays the diminishing returns of increasing the effective response force beyond the 50% mark. Despite the diminishing returns, it is important to use some level of conservatism when equipping a response force to account for unexpected adversary capabilities. It should also be noted that even though the response force is generally small, it often possesses a higher effective force than a numerically superior adversary due to inherent force multipliers from being on the defending side.

Realistic limits were placed on how far the response-to-adversary ratio was altered throughout the thesis work. Because the adversary was considered a rational

actor, it was assumed that any attack overly reliant on force rather than stealth would not be initiated if the effective response force was more than nine times the adversary force ($P_N = 90\%$). Attacks that required only one out of multiple simultaneous attacks to succeed were still permitted in Scenarios 3 and 4, even when each individual attack crossed this threshold. A limit was also placed on the adversary force. Dealing with an adversary force of overwhelming numbers or equipment (e.g., helicopters or heavy armored vehicles) falls within the domain of the state's military rather than being the facility's responsibility. A commonly used assumption limiting the adversary force is that an overly large force would be detected before reaching the facility, either while training or during deployment. Variations on the initial DBT were therefore kept to reasonable levels, such as the addition of two or three combatants rather than doubling the number of attackers.

2.2 Facility DBT Definition

The baseline DBT used to construct the physical security systems for each test facility was designed to represent what would be used for a facility possessing Category 1 material in a large developed nation not containing hostile domestic forces. "Hostile domestic forces" refers to any adversary presence within the country that regularly carries out guerilla or terrorist attacks. Because the state assumed for this thesis is a developed nation without domestic sources of attackers, the adversary is limited to an attack force size that would not be noticed passing through and training within the country. Possession of Category 1 material, in this case significant quantities of HEU,

means the facilities are within the top grade of a graded DBT. Based on these conditions, the baseline adversary force was designed to be a cell of foreign terrorists with access to military equipment and moderate levels of combat experience or training. A breakdown of how their capabilities translate into force multipliers and the total effective force value can be found in Table I.

TABLE I

Force Multipliers and Characteristics of the Baseline DBT

Characteristic	Multiplier
Actual #	8
Cover	1
Experience	1.5
Insider	1
Weapon	3
Grenades	1
Effective Force	36
No LAW Capability	

The overall adversary force size of 8 represents two squads working together, but they possess the training to split up and attack different targets in Scenarios 3 and 4. They are given a 1.5x multiplier for experience based on previous small-arms and tactical training at a jihadi camp, which is considered equivalent to basic military training. While enough passive insider information is known by the adversary to enable them to determine the best route to the target, they are not given credit for knowing information about the response force or defensive positions, and therefore do not receive

the insider multiplier. A weapons multiplier of 3x represents standard military equipment such as assault rifles and optics, but not an expert level of proficiency. While in possession of breaching explosives and tools, the adversary does not possess area kill weapons such as grenades, suicide vests, or antitank weaponry. Light antitank weaponry would not directly increase the effective force of the adversary, but would reduce the response force's cover multiplier. Similar tables are provided for the perturbed cases in Section 3, highlighting which DBT characteristics have been altered.

While not a part of the DBT, the response force's characteristics are provided in Table II. Each scenario is based on the same response force, with minor variations in the cover multiplier for certain scenarios. In scenarios with fixed facilities the cover multiplier is 3x, with a reduction to 2x in scenarios where the target is mobile. The cover multiplier is also reduced when the adversary possesses LAW capability.

TABLE II

Force Multipliers Used for the Response Force

Characteristic	Multiplier
Actual #	4
Cover*	3
Experience	2
Insider	N/A
Weapon	5
Grenades	N/A
Effective Force	120

While the total number of response force personnel at each facility is higher than four, only a single squad will be deployed to prevent diversion attacks from compromising security (each attack faces a four-man response force squad). This assumption was made based on each facility possessing several targets that could be attacked, where full deployment to one target would result in the other targets being undefended. As mentioned above, the response force receives a significant cover multiplier of 3x when defending from fortified positions and 2x when fighting from armored vehicles. Based on typical response forces in the United States, the operators are equipped with high quality military gear and possess the weapons training necessary to achieve top performance. Combined with Special Forces equivalent experience, the response force is given the maximum multiplier for both experience and weaponry. While response force personnel are often equipped with grenades, we assumed the response force was more limited in area kill weaponry than an attacker with suicide vest capabilities; this assumption was represented by removing the response force's grenade multiplier. It was also assumed that any inside information the state possessed on the adversary would be used for counter-terrorism rather than playing a role in individual facility attacks. Any scenario deviation from the response force characteristics in Table II is defined under that scenario's characterization.

2.3 Facility and Scenario Characterization

Four scenarios, involving three modeled facilities, were used to determine the effects of DBT variations on physical security performance. The first two facilities are stationary sites that store Category 1 material, whereas the third facility is an armored transport carrying nuclear weapons components. The general layout, security levels, and delay/detection mechanics are summarized for each scenario below. A more in-depth description of each facility is located in the Appendix, should the reader desire to recreate the facility for further testing.

Rather than physically modeling the structures in each facility, as is done for more sophisticated studies with software such as JCATS, an ASD with explicitly defined detection and delay measures was constructed for each facility using Sandia's SAVI program. As noted in the Section 2.1.2, the Facility module is used to create the ASD and the Outsider module tests a defined adversary against this ASD.

2.3.1 Facility One – Scenario One

The first facility is a 2x2 mile site in which the initial construction was assumed to have not focused heavily on security against 21st century threats. Standard security features such as detectors and reinforced walls exist, but the overall building and road arrangement was designed for ease of use rather than to maximize delay or detection opportunities. There are several vulnerable points, such as an air duct large enough for human transit, which would not be present in a newly constructed facility. Each perceived vulnerable point has been reinforced with additional delay and detection

components, but the vulnerable points were not physically removed. The full facility layout is given in Fig. 3 with security level designations shown. The general layout was taken from a section of an existing nuclear facility, but security layers, actual distances, and the target building itself were fabricated for this thesis.

Fig. 3. Exterior image of Facility One with security level labels.

The ASD breaks the facility down into several security layers: Offsite, Limited Area, Protected Area, Controlled Building, Controlled Room, Target Area, and Target. Both the Limited Area and the Protected Area can be traversed by vehicle, but use of a vehicle requires special identification in inner layers. The various elements that can be defeated to cross from one layer to another are shown in the ASD given as Fig. 4.

Fig. 4. Adversary sequence diagram for Facility One.

Security elements separating the Offsite and Limited Areas are meant to designate the property boundary and control the flow of traffic rather than to detect covert adversaries. There are two vehicle entrances and a pedestrian portal into the Limited Area that possess limited contraband detection capabilities. The first real detection opportunities occur within the Limited Area when an adversary attempts to cross into the Protected Area. The Protected Area is surrounded by double fences with a

central isolation zone possessing multiple detector systems and is crossed by a site vehicle portal, shipping and receiving gate, and a personnel portal. This set of portals is equipped with the capability to detect explosives, and all personnel and cargo are subjected to searches. The target building can be entered conventionally in the Protected Area either through a personnel portal or the shipping and receiving portal, both equipped with sophisticated contraband detection systems. With the use of breaching equipment, the building can be entered through a set of office windows, a ventilation duct, several walls, or the ceiling. The interior of the target building is broken into several security layers shown in Fig. 5. The target is protected by a security glass cage within a secured vault in the Target Area behind the front offices.

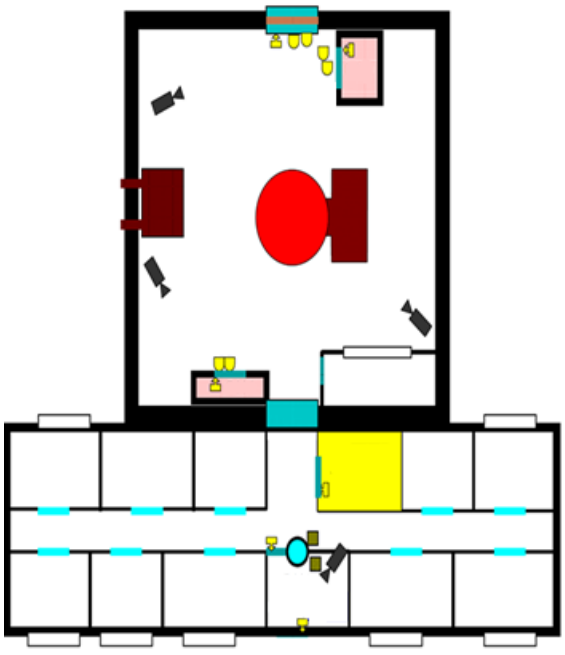

Fig. 5. Interior security levels of Facility 1's target building.

2.3.2 Facility Two – Scenario Two

The second facility is a 500x500m controlled area within a larger property protection area. The overall site represents a large government industrial complex with significant pedestrian and vehicle traffic outside the various limited areas. Security features in the property protection area are focused on controlling traffic and responding to emergencies rather than detecting a covert adversary force, so the first detection opportunities in this simulation will occur when crossing into the Limited Area. The only vehicles with access to this facility must take a shipping/receiving road which wraps around the Protected Area to increase delay. This can be seen in Fig. 6 which breaks the facility into various exterior security levels.

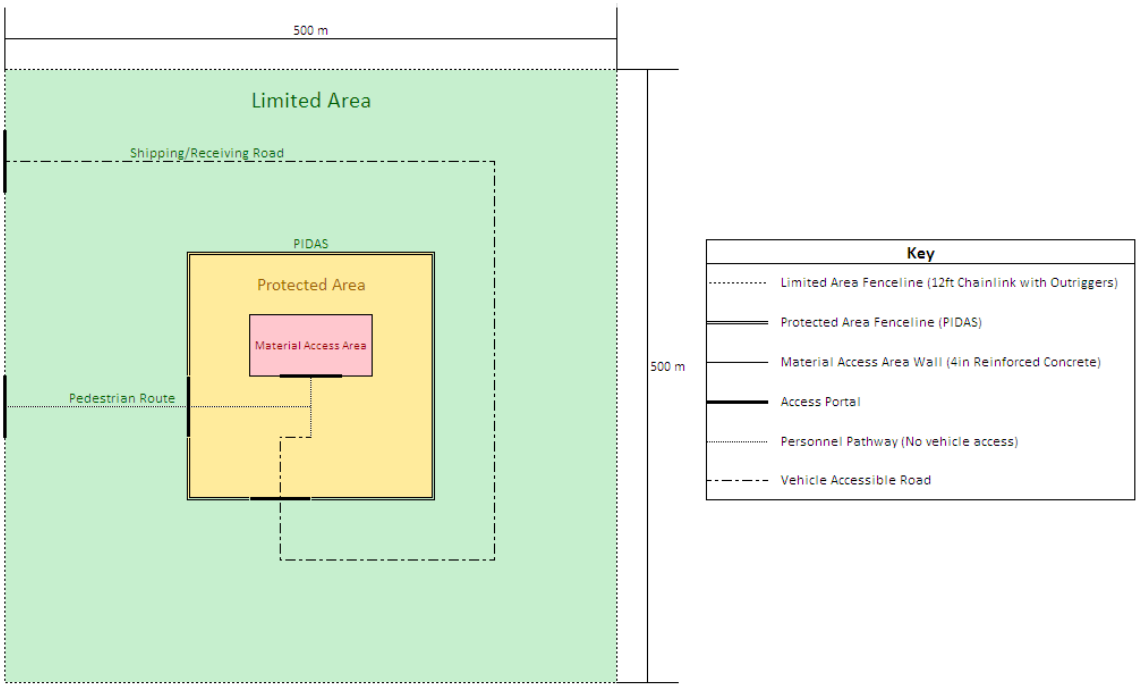

Fig. 6. Exterior security layers of the second simulated facility.

The ASD for Facility Two splits the layout into a series of security layers: the Property Protection Area, Limited Areas (one to represent use of a vehicle on the shipment route and the second representing travel along the pedestrian path by foot), Protected Area, Material Access Area, Target Building, Radiation Area, Target Area, and the Target. As with Facility One, there are several different elements that can be defeated at each phase to cross to the next layer. These elements and their corresponding layers are shown in Fig. 7.

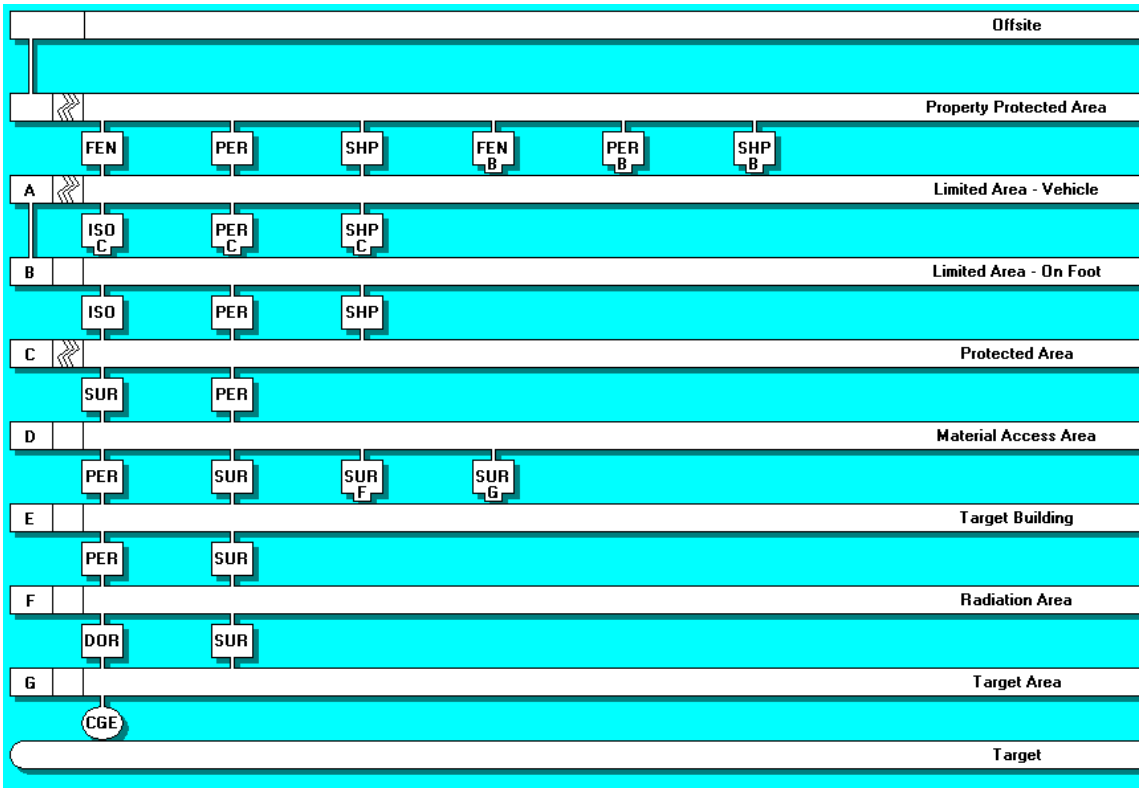

Fig. 7. ASD showing the security elements and layers of Facility Two.

Standard employee traffic into the limited area is through the main personnel portal with site and shipment vehicles passing through a vehicle portal (civilian vehicles are prohibited). All packages and cargo must be brought through the vehicle portal where they undergo a thorough search. A second set of portals allows passage through the Perimeter Intrusion Detection and Assessment System (PIDAS) that surrounds the Protected Area. These portals have more comprehensive contraband detection systems designed to prevent explosives from entering the more highly controlled sections of the facility. Passage into the Material Access Area is limited to a single personnel portal where employees are screened for material that could be used to smuggle HEU out of the facility. The target building is located within the Material Access Area, and its interior is broken into the security sections shown in Fig. 8. The entrance portal possesses the same detection measures as the Material Access Portal, but also screens for radiological material on personnel leaving the building. A security portal separates the laboratories that deal with minor sources from the vault containing fissile material and the two laboratory spaces that handle the material. Only those personnel with special clearance are allowed beyond this point. The target is located within a wire mesh cage in the vault. Access to the vault requires two trained workers who must contact the central alarm station (CAS) upon entry and exit.

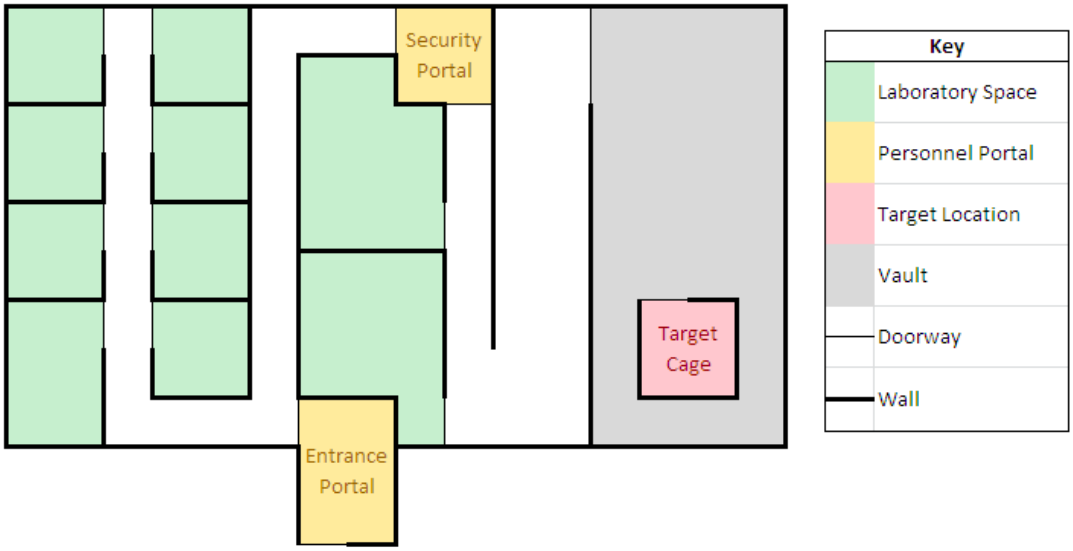

Fig. 8. Interior layout of Facility Two's target building.

2.3.3 Facility Three – Scenarios Three and Four

The third facility represents a series of armored convoys consisting of one real transport, two decoys transports, and response force personnel protecting each transport. Each convoy is geographically separated so that a single group of attackers can only strike one transport. Both scenarios begin with an adversary ambush. In Scenario Three the ambush succeeds in only stopping the convoy while in Scenario Four the response force is immediately reduced to half capability. There are three cases for each scenario based on how the adversary chooses to divide their capabilities. The first case uses the adversary's full capabilities against a single convoy, but the adversary only has a 33% chance of attacking the correct target. The second case involves attacks on two convoys at half capability (P_A = 67%), and in the third case, all convoys are attacked with a one-

third capability (P_A = 100%). Because response force personnel and the transport drivers are not told which convoy contains the actual material, any insider information the adversary receives is related to delay elements and response force tactics rather than revealing which transports are decoys.

Unlike in the previous scenarios, the response force in the transport scenarios (3 and 4) engages the adversary before the adversary attempts to reach the target. The purpose of delay elements in this case is to allow a secondary response force to arrive should the first set of defenders be defeated. In this thesis the secondary response force will not be defined. It is assumed to be overwhelming and capable of arriving within the delay time of the original DBT. For the transport facility, P_I was set to 100% with P_A and P_N changing based on the adversary capability perturbations.

Because the response force uses armored vehicles instead of fortified positions, the base cover multiplier received is reduced from 3x to 2x and is fully removed if the adversary possesses LAW capabilities. The adversary force is also allowed vehicle-based improvised explosive devices (VBIED) for the attacks on Facility Three. Both scenarios are initiated with the VBIED, the VBIED's effect being the only difference between Scenario 3 and 4. In Scenario 3 the VBIED succeeds in stopping the convoy, while in Scenario 4 it also eliminates half of the response force.

3. ANALYSIS OF RESULTS

The original strictly defined DBT, shown again in Table III, served as a test case to calibrate the physical security systems of each facility. We tweaked detection and delay elements until each facility's risk factor against this DBT was below 0.2. We decided a rational adversary would not consider an attack with a chance of success below 20% to be cost effective (considering the enormous costs of attacking a high security facility). After the initial security modifications to reach the target risk values, the physical security systems at each facility were kept constant. The P_N, P_I, response force time (RFT), and overall risk for each facility against the original DBT are given in Table IV (Scenarios 3 and 4 assume only a single attack with P_A equal to 33%). The effects of perturbing each adversary capability were tested separately (with the exception of explosives and LAW capability) to determine which are most important to correctly define when using a strictly defined DBT.

TABLE III

DBT Used to Design the Physical Security Systems

Characteristic	Multiplier
Actual #	8
Cover	1
Experience	1.5
Insider	1
Weapon	3
Grenades	1
Effective Force	36
No LAW Capability	

TABLE IV

Risk Equation Parameters Calculated with Original DBT

Scenario	P_I	P_N	P_A	RFT(s)	Risk
1	98.26%	90.08%	100.00%	150	0.115
2	97.70%	90.07%	100.00%	300	0.120
3	100.00%	64.19%	33.33%	0	0.119
4	100.00%	40.16%	33.33%	0	0.199

3.1 DBT Characteristic Sensitivities

The results of each perturbation of the original DBT will be discussed individually, followed by a summary of which adversary characteristics produce the greatest shifts in security system performance and how the perturbation effects varied from facility to facility. To ensure the perturbations would be comparable, deviations from the DBT were mostly limited to small perturbations.

3.1.1 Probability of Neutralization (P_N) Sensitivities

Many of the DBT characteristics only play a role in determining P_N since they do not change the adversary's pathway. These characteristics include the number of attackers, their levels of combat training and experience, insider information about the response force, and the type and proficiency of weaponry used.

Changes in these characteristics can also affect which tactics the adversary group uses when multiple targets exist. A larger group of adversaries has the option of splitting into several groups to strike multiple targets simultaneously or conduct an initial

diversionary attack to misdirect the response force. While Scenarios 1 and 2 were limited to an attack on a single target, the adversary's capability to defeat the response in Scenarios 3 and 4 determined whether it was more effective to strike at one target or split into groups to hit two or three targets. In the following risk tables, Scenarios 3 and 4 are assessed under three different attack plans: "a" represents a single attack at full capacity, "b" represents an attack on two targets simultaneously at half capability, and "c" represents attacks on all three targets at one-third capability.

TABLE V

Characteristics of DBT Perturbation Featuring Increased Weapons Capability

Characteristic	Multiplier
Actual #	8
Cover	1
Experience	1.5
Insider	1
Weapon	5
Grenades	1
Effective Force	60
LAW Capability	

TABLE VI

Facility Risk with DBT Perturbation Featuring Increased Weapons Capability

Scenario	Risk
1	0.263
2	0.267
3 a	0.180
3 b	0.194
3 c	0.157
4 a	0.245
4 b	0.360
4 c	0.397

The following pages display how various perturbations changed the adversary's effective force and how this revised force affected the risk level for each scenario. In each of these perturbations, the increase (or decrease) in effective force directly changed P_N. Tables V and VI present the effects of the first DBT perturbation, an increase to full weapon capability. Tables VII and VIII show the results of a small increase in the number of attackers. Tables IX and X involve a reduction in adversary capability (two fewer attackers). Tables XI and XII feature greatly heightened adversary capabilities based on maximum adversary experience, insider assistance, and weaponry.

TABLE VII

Characteristics of DBT Perturbation with Two Additional Attackers

Characteristic	Multiplier
Actual #	10
Cover	1
Experience	1.5
Insider	1
Weapon	3
Grenades	1
Effective Force	45
LAW Capability	

TABLE VIII

Facility Risk with DBT Perturbation of Two Additional Attackers

Scenario	Risk
1	0.172
2	0.177
3 a	0.147
3 b	0.129
3 c	0.085
4 a	0.221
4 b	0.293
4 c	0.292

TABLE IX

Characteristics of DBT Perturbation with Two Fewer Attackers

Characteristic	Multiplier
Actual #	6
Cover	1
Experience	1.5
Insider	1
Weapon	3
Grenades	1
Effective Force	27
LAW Capability	

TABLE X

Facility Risk with DBT Perturbation of Two Fewer Attackers

Scenario	Risk
1	0.063
2	0.068
3 a	0.085
3 b	0.043
3 c	0.016
4 a	0.168
4 b	0.170
4 c	0.128

TABLE XI

Characteristics of DBT Perturbation Featuring Greatly Heightened Combat Capabilities

Characteristic	Multiplier
Actual #	8
Cover	1
Experience	2
Insider	1.5
Weapon	5
Grenades	1
Effective Force	120
LAW Capability	

TABLE XII

Facility Risk with DBT Perturbation Featuring Greatly Heightened Combat Capabilities

Scenario	Risk
1	0.509
2	0.512
3 a	0.245
3 b	0.360
3 c	0.397
4 a	0.286
4 b	0.490
4 c	0.630

These tables show how perturbations in adversary numbers and weaponry produce proportional changes to facility risk. An interesting observation in Scenarios 3 and 4 is the effectiveness of the adversary splitting into groups to strike at multiple targets. Since each target is protected by an equal number of response force operators, this tactic results in the adversary effectively fighting three times as many combatants. Despite the response force now having a better chance to win each engagement, the increased odds of attacking the correct convoy outweigh the disadvantages from the increased P_N. The exception to this trend occurs when the adversary will win an engagement less than 18% of the time ($P_N > 82\%$), as was the case in Scenario 3c in Table VI. The adversary's best tactic for hijacking nuclear material in transit (when decoys are present) is to attack as many targets as possible until the point where the response force possesses an overwhelming advantage. In the case where the adversary

possesses the highest capabilities, shown in Table XII, the facility risk value is more than doubled in Scenario 4 when the adversary splits into three groups.

3.1.2 Probability of Interception Sensitivities

The only tested force multiplier that affected both P_I and P_N was the inclusion of non-breaching explosives such as grenades, suicide vests, and anti-tank weaponry. The direct advantage gained over the response force is represented in the "Grenades" force multiplier while the ability to quickly puncture fortified positions both lowers the response force's cover multiplier and reduces the delay values of guard towers. The perturbed force multipliers are shown in Table XIII, with the results of adding LAW and explosives shown in Table XIV.

TABLE XIII

Characteristics of DBT Perturbation with Increased Explosives Capability

Characteristic	Multiplier
Actual #	8
Cover	1
Experience	1.5
Insider	1
Weapon	3
Grenades	2
Effective Force	72
LAW Capability	

TABLE XIV

Facility Risk with DBT Perturbation of Increased Explosives Capability

Scenario	Risk
1	0.935
2	0.609
3 a	0.258
3 b	0.399
3 c	0.463
4 a	0.293
4 b	0.516
4 c	0.680

Despite the adversary possessing a lower effective force than is seen in Table XI and 12, LAW capability opened new pathways in Scenarios 1 and 2 which greatly increased risk. Accounting for the reduction in the response force's cover multiplier (due to the added LAW capability), the effective force ratio between the case in Table XII and Table XIV are similar, as can be seen with Scenarios 3 and 4. Facility 1 proved particularly sensitive to the adversary acquiring LAW capability due to its reliance on small arms resistant guard posts (risk increased by a factor of 8), whereas Facility 2 was slightly more resistant (risk increased by a factor of 4).

It is possible for some adversary capabilities to affect the response force deployment time (RFT), which alters P_I instead of P_N. There are several factors that can increase the RFT, but these factors were modeled together as a series of three 15-sec increases in RFT. Capabilities that would modify the response time include having an active insider who misdirects the response force (such as an alarm station operator or a

ranking member of the response force), utilizing a tactic such as a form of diversion or subterfuge to limit the response force's ability to correctly deploy, or using radio jamming equipment to interfere with the response force's ability to communicate and receive updates. We modeled these conditions by changing the RFT parameter in the Outsider module of SAVI. The results of RFT perturbations on Scenarios 1 and 2 are given in Tables XV and XVI. The sensitivity to adversary capabilities that interfere with RFT proved highly dependent on the facility and its corresponding ASD. The critical detection point (CDP) will not change when a facility is designed with a conservative buffer (a large time remaining after the predicted interception point (TRI)). However when the TRI is small, a slight delay in RFT will push back the CDP. The rapid loss in system performance when the CDP changes is evident in Scenario 1; the first CDP shift lowers P_I from 98.26% to 9.50%. A change in the CDP does not always result in such a large performance penalty. There are four CDP shifts in Scenario 2 as the RFT is varied from 285s to 330s, but it is not until the last shift that P_I drops to an unacceptable level.

TABLE XV

Scenario 1's P_I and TRI as a Function of RFT

RFT (s)	TRI (s)	P_I
120	92	98.26%
135	77	98.26%
150	62	98.26%
165	12	98.26%
180	4	9.50%
195	N/A	0.00%

TABLE XVI

Scenario 2's P_I and TRI as a Function of RFT

RFT (s)	TRI (s)	P_I
270	27	97.75%
285	12	97.75%
300	4	97.70%
315	5	95.62%
330	33	14.40%
345	18	14.40%

The final case for testing DBT perturbations allowed the adversary to possess false credentials, facility uniforms, and key cards. All previous cases were performed under the assumption that the adversary would attempt stealth oriented tactics until the CDP, then proceed along the pathway of minimum delay. Modern identification cards are very difficult to falsify or replicate when equipped with ID microchips and standard policy is to deactivate any cards the moment they are reported stolen or lost. The repercussions can be severe if the adversary is capable of acquiring fake identification that unlocks doors. A comparison of facility risk with and without the adversary efficiently using deceit based tactics can be found in Table XVII.

TABLE XVII

Risk Values against Adversary Successfully Utilizing Deceitful Tactics

Adversary and Tactic Definiton	Scenario 1			Scenario 2		
	P_I	P_N	R	P_I	P_N	R
Terrorist w/o Deceit	98.26%	90.08%	0.115	97.70%	90.08%	0.120
Terrorist w/ Deceit	19.00%	90.08%	0.829	81.92%	90.08%	0.262
Criminal w/ Deceit	19.00%	98.36%	0.813	81.92%	98.36%	0.194

To simulate an adversary possessing false credentials and identification badges, we changed the adversary strategy in the Outsider module of SAVI from "Force/Stealth Only" to "Force/Stealth/Deceit". Three values of risk for the first two scenarios are given in Table XVII. The first adversary definition was the previously defined original DBT without false credentials, the second was the adversary with deceit capabilities, and the third was the adversary using deceit and reduced numbers. The reduced force multipliers of the third set reflect a small criminal group rather than a small force of terrorists (multipliers are listed in Table XVIII). We assumed the criminal threat to possess three outsiders supported by at least one insider. In this case the insider provided the information necessary for the outsiders to efficiently practice deceit. The second definition is fairly unrealistic; a large group of commandos would not be able to pose as facility employees while staying together. The main focus of the table is between the terrorist definition without deceit and the criminal definition with deceit. Because Facility 1 is a civilian oriented site (originally built with ease of transit in mind rather than security) with security features added later in its life, it is highly sensitive to capabilities that could bypass security locks. Facility 2's intrinsic delay features

(winding roads and corridors to maximize delay and detection) provide a relatively high resistance to the deceit capabilities that easily defeated Facility 1.

TABLE XVIII

Criminal Adversary's Force Multipliers

Characteristic	Multiplier
Actual #	3
Cover	1
Experience	1.5
Insider	1.5
Weapon	3
Grenades	1
Effective Force	20.25
No LAW Capability	

3.1.3 DBT Characteristic Sensitivity Summary

It is easy to predict how a facility's risk will change with perturbations of combat related capabilities (those that affect only P_N) in cases where the adversary focuses all their capabilities against a single target. The sensitivity to adversary combat capabilities is dependent on the effective response force value. Small shifts in adversary capability have the largest effect when the effective response-force-to-adversary-ratio (R/A) is close to one. When security is designed so that R/A is further along the P_N curve (Fig. 9), there is reduced security system sensitivity to small shifts in adversary capability. While each facility possesses unique characteristics that altered the effective response force value, the sensitivity to adversary combat capability is facility independent when looking

at R/A. The exception is when multiple targets are present. As long as the response force does not possesses an overwhelming force advantage ($P_N > 82\%$), it is in the adversary's best interest to strike multiple targets. The slight disadvantage the adversary takes by increasing the R/A ratio is offset by the linear increase in P_A when only one target is real. The same is true when considering multiple real targets that would increase consequence linearly rather than P_A.

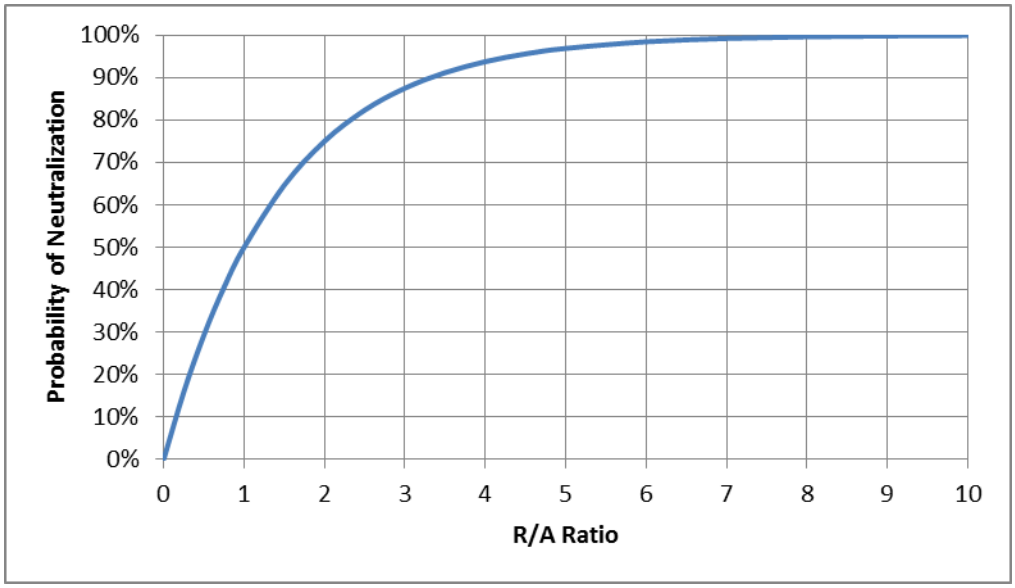

Fig. 9. Probability of neutralization as a function of the effective response force (R) divided by the effective adversary force (A).

Sensitivity to any capability that affects P_I is highly dependent on facility characteristics. These capabilities normally change the delay values of various security elements which can significantly impact the overall facility risk if the CDP changes. The

same is true for any capability that increases the RFT in that there is minimal effect until the CDP shifts, but risk can increase rapidly afterwards.

Based on the results of Scenarios 1 and 2, facility physical security systems are highly sensitive to perturbations of adversary capabilities that affect P_I compared to capabilities that only affect P_N. To further illustrate this point, Table XIX compares the change in risk associated with the greatest increase in combat exclusive capabilities (maxed adversary experience, insider support, and weaponry quality/proficiency) to an adversary possessing explosive capabilities. While effective adversary force is much higher when combat capabilities are increased, the R/A ratio for both cases are similar (explosives capability reduced the response forces cover multiplier). Even with similar R/A ratios, the risk value for the adversary with explosives was significantly higher due to a shift in the CDP. Because interception is guaranteed in Scenarios 3 and 4, risk is similar for both capabilities because of their R/A ratios.

TABLE XIX

Comparison between Explosives and Advanced Weaponry/Training

Scenario	Weapon Risk	Explosive Risk
1	0.509	0.935
2	0.512	0.609
3 a	0.245	0.258
3 b	0.360	0.399
3 c	0.397	0.463
4 a	0.286	0.293
4 b	0.490	0.516
4 c	0.630	0.680

The sensitivity to capabilities that enable the adversary to successfully execute tactics that utilize deceit, normally a combination of insider support and false credentials, also varies based on each facility's features. Facility 1's P_I dropped to 19% when the adversary used deceit as a tactic compared to Facility 2's P_I of 81.92%.

3.2 Methods to Limit Perturbation Sensitivity

The high sensitivity to changes in adversary capabilities that affect P_I resulted from how these changes affected the critical detection point (CDP). Extra conservatism can be placed into the security system's design to provide a buffer against CDP shifts. As mentioned above, each completed ASD (after attackers and CDP have been defined) contains an associated time remaining after interception (TRI). If a perturbation in the DBT's adversary capabilities reduces delay or increases RFT by less than TRI, the CDP and the facility's calculated security risk do not change. It is important to note that a conservatively large TRI does not protect against adversary capability changes that reduce the probability of detecting the adversary (such as deceit). If the chance to detect the adversary is reduced, risk will increase whether or not the CDP changes.

The best way to protect against adversary capabilities that can spoof or fool detection measures is to enhance the implementation of detection systems. Mixing different types of complementary detectors (one detector accounts for the other's weak points) forces the adversary to perform more difficult maneuvers and invest significant amounts of time. Examples of this practice include combining volumetric microwave detectors with infrared motion detectors in an isolation zone or adding biometric locks to

complement badge readers in high security areas. The complementary detection systems should be geographically focused prior to the CDP to ensure the response force has time to respond after detection and assessment.

When financial or resource constraints limit the amount of conservatism that can be built into the security system, it can be desirable to shift resources away from system components that deal with low-sensitivity threat capabilities. This step is more practical when the facility is still at the design stages rather than having facility operators physically remove existing system elements. There is still some value to removing unnecessary security features after facility construction is complete if it lowers upkeep costs, but it would still be better to catch unnecessary elements during the design phase. For example, the resources associated with construction of a reinforced fighting position or hiring additional response force personnel would be better allocated to improving delay and detection measures if the system is already resistant to adversary capabilities that affect P_N (on the upper end of the P_N curve in Fig. 9).

Instead of strictly defining a balanced set of threat capabilities for each DBT grade, defining adversary capabilities as a range can reduce the sensitivity of a facility security system to DBT changes. With a flexible range of capabilities, several different types of adversaries would be tested against each facility's security system. However, simultaneously increasing all adversary capabilities to conservative levels would result in an unrealistic amalgamation. Protecting against this unrealistic threat would be unreasonably expensive and a waste of resources. A flexible DBT means the physical

security system must be capable of defeating adversaries with military explosives or high quality spoofing measures, but not an adversary with both capabilities.

3.3 Point Based DBT

Rather than implement upgrades or additional flexibility to a strictly defined DBT system, a more efficient approach to addressing security system sensitivity to DBT perturbations could be to use a point-based DBT. A point-based DBT is similar to having a unique DBT for each facility, even though facilities are still divided into different categories or grades. To reduce the strain of using a more sophisticated DBT, the competent authority (the main government agency responsible for nuclear security) is assisted by an in-house vulnerability assessment team at each facility. Under this point-based system, the different adversary characteristics are given weighted factors or point costs that reflect the difficulties the adversary would face in developing that capability. The point cost would reflect the difficulty in avoiding government attention, at both local and federal levels, as well as the financial burden. In a fully developed model, capability point costs would vary across the state based on local conditions. As the facilities used in this thesis are hypothetical, local environmental conditions have been ignored. Development of the point costs for each capability would require input from the state's intelligence community and local law enforcement to establish the difficulty in covertly developing each capability within the state.

The proposed point-based DBT is similar to a graded DBT in that facilities are split into groups based on the consequence of a successful adversary action. Rather than

sharing DBT characteristics however, each group would share a total point-cap. Points would then be allocated into different sets of threat capabilities to develop several sets of possible adversaries. The facility grouping, total point-cap, and capability point costs would be determined by the state's competent authority while scenario development and tweaking of point costs based on local factors would be handled by the facility's vulnerability assessment team. The intent of analyzing a range of threat capabilities in this fashion is to discover unexpected security system vulnerabilities that could be missed when using a strictly defined DBT. Tested scenarios should cover a large range of possibilities based on the perceived capabilities of existing adversaries, predicted future capabilities, and historical events (not limited to attacks on nuclear assets). After successfully developing, testing, and defeating a range of scenarios, the vulnerability assessment staff would report findings and recommendations back to the competent authority.

To demonstrate how this process would be performed, we generated a set of capability point costs and used them to develop scenarios for the first two facilities employed earlier in this study. While investigations into the merits of a point-based system are already being performed at several facilities in the United States, we decided on the exact breakdown of capabilities and assignment of point values for this thesis's point system without input from any federal agency to ensure the work remains open-source. The point based DBT will be discussed in the following order: how the point cost assignments were devised, development of several adversary groups, analysis of the point based DBT on the first two facilities, historical events that could be used to

validate point costs, and a summary discussion of the author's initial conclusion of the costs versus benefits of implementing a point-based system.

3.3.1 Capability Cost Development

The different types of threat capabilities considered in the point-based DBT were carried over from the breakdown of capabilities used in the previous strictly defined DBT. Point costs for each capability were assigned based on the assumed ability of the adversary to procure, develop, and train covertly. In order to estimate the difficulty associated with these covert activities, it is necessary to further define the host state. The state's size, political stability, presence of hostile domestic actors, black market activities, freedom of citizens to acquire munitions, and a host of other characteristics all affect the difficulty an adversary would face in developing each capability.

In this thesis the state is defined as a developed democracy of considerable size that possesses efficient intelligence and law enforcement abilities. Small anti-government elements exist along the fringe of the state's society, but they lack the motivation required to act and are under government scrutiny. The lack of hostile domestic forces means it is difficult for the adversary to recruit and train large numbers of fighters covertly. Gun laws are slightly stricter than those found in the United States; civilians are allowed to possess hunting rifles, but not military type weaponry or handguns. Because the state has a free economy, black market and organized crime activities are minimal. Explosives and military equipment are both expensive and difficult to obtain. These factors went into the capability point costs seen in Table XX.

TABLE XX

Sample Capability Point Costs

Capability	Allowed Range	Point Cost	Force Multiplier
Number of Attackers (n)	1-12	n x 10 (n ≤ 6)	n
		n x 12 (n > 6)	
Tactical Training and Experience	None	0	1
	Basic	n x 2	1.5
	Spec Ops	n x 5	2
Insider	Passive	50	1.5
Weaponry Quality and Profiency Training	1	0	1
	2	n x 1	2
	3	n x 3	3
	4	n x 8	4
	5	n x 10	5
Explosive Weapons	Grenades	n x 5	2
	LAW	50	*
Counter Measures	Fake ID	n x 20 + 50	**
	Jamming	20	***

* Reduces RF Cover and SI Post Delay Times
** Allows Deceit as a Tactic
*** Increases RFT by 30s

Training a larger group of attackers comes with a slight increase in cost due to their increased training footprint. The more attackers involved, the more likely the state will become aware of their activities. Training equivalent to a military's boot camp was set to a low cost since it can easily be disguised as survival or hunting training whereas Special Operations equivalent training would require a trainer who already possessed this level of military skill. While the financial cost of obtaining an insider has not historically been high, it is difficult to attempt recruitment covertly. Weaponry

multipliers have again been broken into five categories. The first three represent varying degrees of expertise with legal weapons (hunting rifles in the thesis's state) while the last two categories are illegal military equipment. Explosive weaponry is split into two categories since the number of grenades (a placeholder for any antipersonnel explosive) equipped varies with the number of attackers whereas only a single antitank (AT) launcher is needed to eliminate an armored position. The fake identification capability includes false credentials that can open locked doors and facility uniforms. In addition to the cost per attacker, there is also the added cost of obtaining an insider who can provide site material to counterfeit. Jamming equipment represents any device that disrupts radio or signal communications to the response force. All of these costs can vary based on local conditions, and their initial definition is likely to be a time consuming process for the responsible authorities.

3.3.2 Scenario Development and Analysis

The total point cap that limits the possible adversary definitions was set to the original strictly defined graded DBT's point cost. Based on the capability costs in Table XX, the total point cap was computed as 136 and set to 140. With the total point cap in place, a set of adversary definitions was developed that would ensure each sensitive adversary capability (as determined in Section 3.1.3) was tested at least once.

In addition to the original DBT, adversary definitions added with the point-based system include:

- Two attackers with basic training, weapon multiplier of 3, fake identification, and jamming equipment (140 pts),
- Four attackers with SF training, weapon multiplier of 5, grenades, and jamming equipment (140 pts), and
- Four attackers with basic training, weapon multiplier of 3, grenades, and AT capability (130 pts).

This adversary set included the base definition and the three capabilities that altered P_I (jamming equipment, false identification, and AT weapons). The resulting security risk value of each attack can be found below in the order they were presented (with the original DBT coming first).

TABLE XXI

Scenario Risk against Original DBT

Scenario	Risk
1	0.115
2	0.120
3 a	0.119
3 b	0.086
3 c	0.046
4 a	0.199
4 b	0.239
4 c	0.214

TABLE XXII

Scenario Risk against Criminal Adversary Practicing Deceit

Scenario	Risk
1	0.540
2	0.121
3 a	0.001
3 b	0.000
3 c	N/A
4 a	0.015
4 b	0.001
4 c	N/A

TABLE XXIII

Scenario Risk against Adversary with Maximum Combat Multipliers

Scenario	Risk
1	0.365
2	0.382
3 a	0.210
3 b	0.265
3 c	0.250
4 a	0.265
4 b	0.420
4 c	0.500

TABLE XXIV

Scenario Risk against Adversary with AT Capability

Scenario	Risk
1	0.914
2	0.485
3 a	0.199
3 b	0.239
3 c	0.214
4 a	0.258
4 b	0.399
4 c	0.463

The various adversaries designed with the point-based system produced similar results to those shown in Section 3.1. These results show that while the original DBT appears to be a realistic threat with a balance of capabilities, it results in a false sense of security. A specialized adversary that focuses on one particular strategy proved more effective against each facility.

The criminal adversary attempting to avoid confrontation proved highly effective against the first facility (Table XXII). This would be important for security designers to learn before the facility's security system was established since the insider threat has historically been the most common attacker. There have been numerous cases of insiders stealing material in Eastern Europe after the fall of the Soviet Union that were uncovered only after forensics was performed on stolen material. Facility Two proved highly resistant to the insider threat based on the previously mentioned passive delay elements and general site layout. In this case, vulnerability assessment team members could shift resources whose original purpose was insider resistance to address other vulnerabilities. This benefit is more practical when the facility's physical security system is still in the design phase; however, savings could still be found by, say, reducing the scope of a human reliability program (HRP). Enrollment in an HRP is meant to reduce the risk of insiders and can involve time consuming tests such as polygraphs. By mitigating the consequences of an insider with other security measures, the need for HRP clearance can be reduced.

An adversary with reduced numbers and maximum combat multipliers proved more effective against each facility than the original DBT (Table XXIII). Facility Three was particularly vulnerable to this threat. By maximizing effective force, the adversary was able to efficiently attack multiple convoys in both Scenarios 3 and 4. While it is still beneficial to use decoy convoys in Scenario 3, the decoys made a much smaller difference in this case than when used against the original DBT (Table XXI).

Despite having a slightly lower point cost, an adversary equipped with AT weaponry produced the highest risk level in the first two facilities. Vulnerability assessment personnel could reduce this risk by strengthening some of the guard posts, pushing explosives detection from the inner security levels to the outer security levels, or reducing the reliance on guard posts as a form of delay.

Examining this set of scenarios revealed vulnerabilities in the physical security systems that were missed when using only the original DBT. Additional measures to mitigate the insider threat in Facility 1 (Table XXII) and a reduced reliance on small-arms resistant portals for Facilities 1 and 2 (Table XXIV) would help balance risk across the range of possible threats. A vulnerability assessment team would recognize this fact when using the point-based system, and they could report the results and improvements back to the state's competent authority.

3.3.3 Verifying Point Costs with Historic Events

An effective method to verify point costs and caps, or even initially determine their values, is to apply the point-based system to historic events that still have

relevance. Since most countries have not experienced physical assaults on their nuclear assets, it is necessary to expand the scope of historic events to include terrorist attacks on any large or high value target. Historical precedents exist for the full range of adversary capabilities considered in most DBTs. A selection of events that could be used for this purpose is discussed below based on the capabilities used by the attacking groups. At the time we wrote this thesis, fairly accurate summaries of each of the following events could be found at Wikipedia. Though encyclopedias are not the best place for authoritative facts, the exact numbers related to most of these events are not available in open literature and estimates tabulated from new stories and press reports served our purpose.

When it comes to setting the overall point cap, several different terrorist events in Russia display some of the highest numbers of well-equipped adversaries outside of military engagements. The 2002 Nord-Ost siege[14] and the Beslan massacre[15] stand out in particular due the same terrorist organization using a large number of attackers equipped with military weaponry.[14,15] Consisting of more than 30 combatants with military experience in the Second Chechen War and military grade weapons and explosives, Riyadus-Salikhin (the Chechen terrorist group) more than tripled what is commonly used as a DBT. These events would serve as good upper limits to a point cap for a state that does not possess the intelligence capability to uncover large operations beforehand. In the point-based system outlined in Table XX, both of these events would have a point cost that would more than double the point cap used in Section 3.3.2. This large point difference can be largely attributed to how the country used in our analysis was defined.

The country was defined as being under effective government control at federal and local levels, which results in the covert acquisition and training of threat capabilities being much more difficult than in Russia during the early 2000s.

The Pakistani Naval Station (PNS) Mehran attack[16] in 2011 is a good example of highly trained attackers utilizing insider intelligence. During this event at least 15 attackers assaulted a Pakistani Naval Airforce base just outside Karachi. The attackers operated in several coordinated squads and exploited physical security system flaws to enter the facility undetected. Pakistan's Naval Intelligence believes that insiders supplied information about which sections of the perimeter were not under active surveillance. The high level of preparation that went into the attack went undetected largely due to the lack of Pakistani influence in the Federally Administered Tribal Areas where the TTP operates. The large point cost of this attack using the values defined in Table XX further illustrates the need to adjust the capability costs of the point based system when hostile domestic forces exist, especially if corrupt members of the state's government or military are believed to support these domestic forces.

In addition to raw combat capabilities, training, and insider support, the other major threat capability to accurately define is the type of specialized weapons the adversary possesses and is willing to use. While rare, chemical attacks have been performed by terrorist groups (though with only limited success). The most famous incident of a terrorist chemical attack is Aum Shinrikyo's 1995 sarin gas attack[17] in the Tokyo subway. Despite the fear the public holds for exotic weaponry such as chemical

weapons, their effect tends to be less efficient than more conventional explosives. Al Qaeda's ability to convert airliners into human-guided missiles demonstrated how devastating unexpected vehicle based improvised explosive device (VBIED) capabilities can be. After the many cases of terrorists using VBIEDs against federal targets (the most famous being the bombing of the marine barracks in Lebanon), at least one scenario with the point-based DBT should include this capability.

3.3.4 Point Based DBT Conclusions

Though the point-based DBT results in increased security, the point-based DBT has a slightly higher initial cost than conventional strictly defined DBTs based on the need for vulnerability assessment personnel. It is necessary to weigh the benefits against these increased costs. In the thesis test case, the point-based system revealed several large vulnerabilities that were missed when using the initial DBT. This benefit could justify the increased initial costs. It is unlikely (hopefully) that most real facilities would possess such large vulnerabilities. But when it comes to high consequence facilities, addressing even small vulnerabilities is important. A large portion of the costs associated with the proposed point-based DBT come from requiring vulnerability assessment teams whose members are familiar with the various facilities.

Several measures can be taken to address the increased costs incurred from requiring dedicated vulnerability assessment staff. One option would be to continue to use conventional strict DBT definitions for lower grade facilities and implement the point-based system for high grade facilities, many of which are likely to already possess

vulnerability assessment staff in some form. Alternatively, several low grade facilities could have their point-based system managed by a single vulnerability assessment group, since development of a low point-cap DBT is comparatively easier than a high point-cap DBT.

Based on the test case, we believe the benefits should outweigh the additional costs associated with the point-based DBT system for high consequence facilities. For lower risk facilities, the point-based DBT could still prove efficient if vulnerability assessment capabilities already exist or can be effectively shared between multiple sites. Over the long-run, the point based system could even be cheaper than using a strictly defined DBT. Each time a strictly defined DBT is changed by the competent authority, there is a chance it will reveal facility weaknesses that require costly upgrades that would have been caught during the security system's development with the point-based system. If the point-based system is utilized during the initial development of a new security system, ideally any overly sensitive adversary capabilities will be caught and accounted for before physical security elements have been implemented (it is far cheaper to change a design than to upgrade systems that already exist).

4. FUTURE WORK

The thesis work can be expanded in several different directions. The extent of additional work that can be performed while maintaining an open source status, however, is likely to be a limiting factor. There are two main directions that can be pursued with additional unclassified work, (1) further development of the proposed solutions and (2) a reexamination of the assumptions used in the analysis.

The point-based DBT system could be further validated with a cost-benefit analysis. This assessment could focus on the financial requirements of maintaining a vulnerability assessment team versus the costs associated with physical protection system upgrades required after a sudden escalation of the national threat spectrum. If updating a conventional DBT includes added or shifted adversary capabilities that exploit a previously unknown PPS vulnerability, sudden costly upgrades to the facility's security system would be required. If the point-based DBT system had been used in the initial development of the PPS, shifts in the national threat spectrum would be less likely to result in large changes in PPS effectiveness, as the vulnerabilities would have already been found and mitigated.

The capability point costs could be further developed with comparisons to historic DBTs and actual incidents. If it is found that terrorist events in the same region demonstrate similar capabilities, the point costs could be more accurately defined to predict the capabilities of future attacks. Many of the specifics of recent terrorist attacks are classified, but estimates and press releases should be available. A consistently

accurate point cost is unlikely to be possible to define when looking at incidents conducted by different groups, in different locations, at different periods of time. It is also important to consider the adversary's goal and target for each event. If their objective was simply to gain public attention, they are unlikely to have devoted a significant amount of resources. Attacking a nuclear depot or convoy would require a substantial resource investment, so only historic events that possessed similarly lofty goals should be analyzed.

If security classification is not an issue, older DBTs could be used as a point cap, and terrorist events in the same time period could be compared. This approach could reveal whether DBTs have been historically over or under designed compared to the existing demonstrated threats. An unrealistically capable DBT results in excessive PPS investment while an under equipped DBT might result in the PPS systems not being properly configured to defeat an actual attack. The best situation would be a DBT that is more capable than what has been historically demonstrated, but not equipped to excessive levels. This approach allows slight perturbations from demonstrated capabilities to be defeatable while still resulting in efficient resource allocation.

Future work could also focus on the assumptions that were used in this thesis. A major assumption used in the implementation of the risk equation resulted in the removal of the consequence factor. This simplification assumed that when all of the facilities possessed the same target, the consequence values would be equal. It was also assumed that consequence would not change with DBT capability perturbations because the

adversary's objective would remain the same. This assumption could be invalid if certain capability shifts result in different adversary objectives. An adversary with advanced nuclear capabilities might have construction or detonation of an RDD or IND rather than theft of material as their goal. This adversary objective would result in a completely different consequence value.

The set of tested scenarios could also be expanded upon. Multiple targets in a fixed facility could be tested in a fashion similar to how the convoy scenarios were implemented. The main difference is that each target would be valid rather than possibly being a decoy. Each target could also have different P_I and P_N values, which makes the calculations slightly more complicated. An additional consideration is that attacking two identical targets successfully might not double the consequence value. For example, two RDD detonations in close proximity would not inflict twice the damage of a single RDD because the contamination fields would overlap (even accounting for the overlap area being more dangerous). In any case where consequence is not removed from the risk equation, consequence values must be developed for the various possible outcomes. This consequence valuation step was not performed in this thesis, and the actual values, as defined by the United States government, are likely to be classified.

5. CONCLUSIONS

After testing perturbations of various DBT adversary capabilities against multiple facility security systems, we found that use of a strictly defined DBT fails to assure security measures are up to standards. Because a conventional DBT is designed to represent a realistic threat, each individual attack team capability cannot be raised to the degree a specialized adversary could attain. Our analysis showed the modeled facilities possessed vulnerabilities to several adversary capabilities that went undetected when the scenarios were analyzed with the original strictly defined graded DBT. By maximizing one capability at the expense of others, a specialized adversary force was able to efficiently defeat each facility's security system.

Each adversary capability perturbation affected the probability of neutralization (P_N) and/or the probability of interception (P_I). The combat related capabilities (those that affect P_N) predictably change P_N based on where the balance of power rests when comparing the response force and the adversary force (shown in Fig. 10). When the response force is decidedly more effective than the adversary force, P_N is resistant to adversary capability perturbations. It is common practice for the response force to have the advantage in engagements, not because they necessarily outnumber the adversary, but because they have better fighting positions, knowledge of the environment, and coordination through the central alarm station.

The perturbation's effects are slightly more complicated when multiple targets exist. Attacking multiple targets creates linear increases in either the probability of attack

(P_A) or consequence value of the risk equation. When only one target is real and the rest are decoys, as was the case in the convoy scenarios, P_A is changed. If all of the targets are real, the consequence value is changed. With sufficient combat capabilities, it can be advantageous to the adversary to split their capabilities and attack multiple targets simultaneously. When operating on the upper end of Fig. 10, the slight disadvantage to the adversary of increasing P_N by splitting into an additional squad is outweighed by doubling P_A (or consequence). If an increase in adversary capability crosses the point where it is efficient to attack an additional target, P_N will actually increase due to there being fewer adversaries attacking each target. The overall security risk still increases because of the change in P_A or consequence.

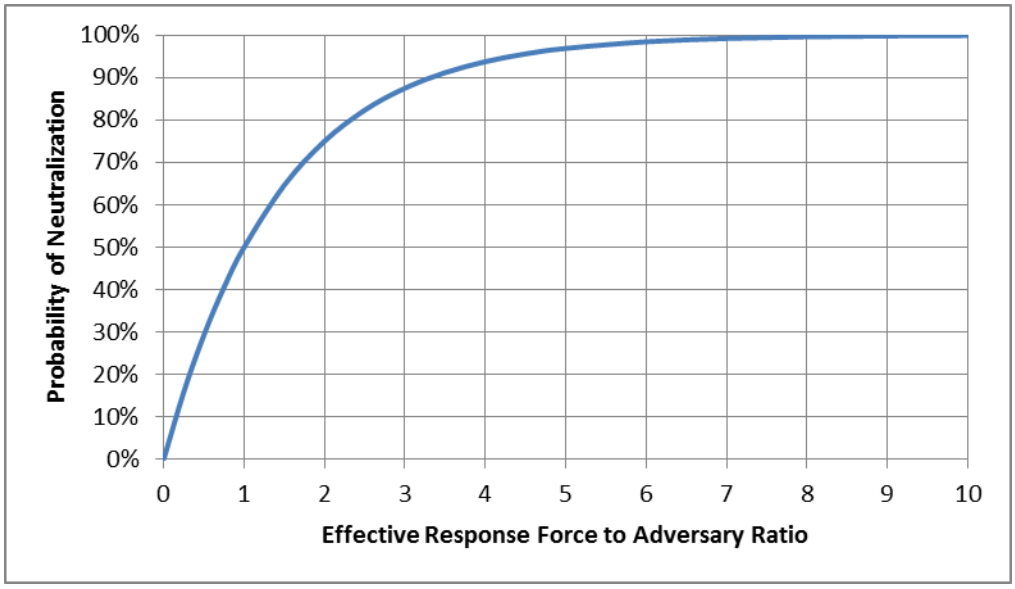

Fig. 10. Probability of neutralization as a function of the effective response force (R) divided by the effective adversary force (A).

Adversary capability perturbations that affected P_I tended to produce greater increases in security risk than the combat related capabilities, but it is also possible to reduce the security system's sensitivity to these perturbations with the careful use of conservative buffers. For most of the tested perturbations, the adversary's most advantageous option is to take the path of minimum detection (stealth) until a critical detection point (CDP), at which point they shift to the fastest path (force). The CDP is defined as the point where detection and assessment must occur for the response force to have time to intercept the adversary. Large increases in risk occurred when the adversary capability perturbation changed the CDP. In this thesis, the CDP changed when the adversary overcame delay elements faster than expected (antitank weaponry), evaded detection elements (false identification and credentials), or increased the response force time (radio jamming equipment). For each CDP there is a corresponding time remaining after interception (TRI). If the perturbed capability does not hasten the adversary by more than the TRI, the CDP, and therefore the security risk, does not change. Implementing an amount of conservatism into the security system to ensure a substantial TRI mitigates the impact of the perturbations in most capabilities that affect P_I. Increasing TRI is not an effective way to counter adversary capabilities that change detection values such as insider assistance and forged key cards (referred to as deceit rather than stealth or force). The best way to counter deceit is to use complementary overlapping detection elements (such as placing a biometric scanner alongside a badge reader).

The proposed-point based DBT system serves as a replacement to the existing strictly defined DBT system (the point-based system can still be graded or shared amongst facilities). In a point based DBT, the various adversary capabilities are given point costs related to the difficulty and expense of covertly acquiring, training, and deploying that capability. A total point cap is assigned to each facility based on the attractiveness of its material or consequences of a successful adversary attack. Vulnerability assessment personnel create several scenarios by spending points on different capabilities until the point cap is reached. Each scenario tests a different set of adversary capabilities to better explore any security system vulnerabilities that may exist. The example point-based DBT set up in Section 3 was able to identify the vulnerabilities that were missed when using the conventional strictly defined DBT. The initial startup costs for a point-based DBT is higher because of the need for vulnerability assessment teams. We believe the benefit of using the point-based DBT to identify site vulnerabilities outweighs the additional startup costs, especially if the vulnerabilities are identified during the initial design of the security system. If the vulnerabilities are identified at an early stage, the money saved by not having to later revise the security system should outweigh the expenses associated with maintaining a vulnerability assessment team.

REFERENCES

1. International Atomic Energy Agency, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities," (INFCIRC/225/Revision 5), Vienna, January 2011.

2. International Atomic Energy Agency. "The Convention on the Physical Protection of Nuclear Material," (INFCIRC/274/Revision 1), Vienna, 1980.

3. International Atomic Energy Agency, "Development, Use, and Maintenance of the Design Basis Threat," Vienna, 2009.

4. T. FROSCHER, "Indispensable Intelligence and Inevitable Failures." *Nonproliferation Review*, **17**, *2*, July 2010.

5. M. L. GARCIA, *The Design and Evaluation of Physical Protection Systems*, Boston: Elsevier/Butterworth-Heinemann, 2008.

6. G. WYSS, J. CLEM, J. DARBY, K. DUNPHY-GUZMAN, J. HINTON, and K. MITCHINER, "Risk-Based Cost-Benefit Analysis for Security Assessment Problems," San Jose, CA, IEEE Conference on Security Technology (ICCST), October 5-8, 2010.

7. G. ALOISE, "GAO-07-1197R Nuclear Security," U.S. Government Accountability Office, September 2007.

8. A. ANDREWS and M. HOLT, "Nuclear Power Plant Security and Vulnerabilities," CRS Report for Congress, August 2010.

9. Department of Defense. *DoD Security Engineering Facilities Planning Manual. Unified Facilities Criteria* (UFC), September 2008.

10. K. CRAGIN and S. DALY, *The Dynamic Terrorist Threat*, Arlington: RAND Corporation, 2004.

11. B. C. EZELL, "Infrastructure Vulnerability Assessment Model (I-VAM)," *Risk Analysis*, **27**, *3*, 2007.

12. S. BAJPAI and J.P. GUPTA, "Securing oil and gas infrastructure," *Journal of Petroleum Science and Engineering*, **55**, 2007.

13. SAVI 4, Computer Software, Sandia National Laboratories, 1997.

14. "Moscow Theater Hostage Crisis," *Wikipedia, The Free Encyclopedia*, Wikimedia Foundation, Inc., June 2012.

15. "Beslan School Hostage Crisis," *Wikipedia, The Free Encyclopedia*, Wikimedia Foundation, Inc., June 2012.

16. "PNS Mehran Attack," *Wikipedia, The Free Encyclopedia*, Wikimedia Foundation, Inc., June 2012.

17. "Aum Shinrikyo," *Wikipedia, The Free Encyclopedia*, Wikimedia Foundation, Inc., June 2012.

APPENDIX A

The facility descriptions below are in the detail and wording required to model the facilities used in this thesis with SAVI 4. If the reader is not interested in using SAVI 4, the facility descriptions in Section 2.3 are recommended instead of the following descriptions. Security characteristics are presented one element at a time for each layer, in the terminology used by the program. Parameter wording matches the program's selectable inputs and may not make sense to those unfamiliar with the program. Each security element description includes some combination of the overall element size, detection sensors, delay elements, presence and protection of posted security inspectors (SI), contraband detection, and alarm assessment. Each paragraph corresponds to an element found in the adversary sequence diagrams shown in Section 2.3.

1 Facility One Layers

1.1 Offsite

There are four points of access leading from offsite to the Limited Area including a perimeter fence, two vehicle gates, and a personnel portal. The perimeter fence is standard chainlink mesh without any intrusion detection measures or security inspectors regularly within visible range. Its main purpose is to designate the property line and display basic trespassing signs rather than to act as a point of detection or significant delay.

Both vehicle portals have the same characteristics with one being on the north side of the facility and the other on the south. Access is not limited to site vehicles as this is the main point of entry for employees with civilian vehicles. A photo ID check for the driver and all passengers is required for entry to limit vehicular access to just employees. The gate itself is equivalent to 8 foot chainlink with outriggers and is monitored by a posted security inspector (SI) with small arms protection and a duress alarm.

The personnel portal is the primary access point for visitors and does not serve the role of contraband detection. It is approximately 10m across with an interior small arms resistant SI post equipped with a duress alarm. Both the outer and inner doors are hollow core metal with no lock or hinge protection. The structure itself is equivalent to 8 inch filled block.

1.2 Limited Area

The Limited Area completely surrounds the higher security levels of the facility and provides the first real opportunities for detection of an adversary force. The shortest route through the Limited Area is 917m and is traversable by vehicle. Surrounding the Limited Area is a Perimeter Intrusion Detection and Assessment System (PIDAS) consisting of two 8 foot chainlink fences with outriggings distanced 5 m apart with concrete blocks in between. Both fences are outfit with vibration detectors and the central region features multiple complementary systems on either side of the concrete blocks. Alarm assessment is facilitated with overlapping CCTV coverage with instant replay capability.

Passage through the PIDAS occurs at a personnel portal, a shipping and receiving portal, or a site vehicle gate. The personnel portal is the main route into and out of the Protected Area for site employees. While personal possessions, small packages, and tools/equipment are allowed through, shipments and cargo must be moved through the shipping and receiving portal instead. The entrance to the personnel portal is controlled with an electronically coded lock that is opened with a cleared employee badge swipe. The central section of the portal requires a fingerprint scan and PIN code while under surveillance of a SI. The SI post is small arms protected and equipped with a duress alarm. After proper authorization at the central section, the guard remotely unlocks the inner electronically coded lock. A cursory search is conducted on any possessions or equipment brought into the portal in the central region. All outgoing traffic also passes through a plastic scintillator portal SNM monitor. Detection at the outer and inner exterior sections of the portal is facilitated with exterior video motion sensors, a balanced magnetic switch on the door, and direct observation by security personnel at the outer section (but not the inner side). The central section also possesses video motion sensors and constant security surveillance. The inner and outer doors are hollow core metal with hinge protection and the walls and ceiling are equivalent to 8 inch filled block. In addition to the security inspectors located directly at the portal, randomized patrols pass by both the outer and inner sides. The overall distance across the portal is approximately 10m.

The cargo entrance to the Protected Area is a shipping and receiving vehicle portal. This entrance is limited to shipment vehicles and the authorized driver. Outer

access requires an authorization form and picture badge check before the electronically coded lock will be opened. A cursory search of entering and exiting vehicles is conducted and the central region, with ingoing vehicles being subjected to bomb search dogs and outgoing vehicles driving through a sodium iodide scintillator for SNM detection. After the central guard is satisfied that the vehicle does not possess contraband, the inner electronically coded lock is remotely opened. The outer and inner door and gates are monitored with balanced magnetic switches. Exterior video motion sensors are located on both inner and outer sides of the portal and interior video motion sensors are located in the central region as the primary means of detection in addition to near continuous security personnel presence at the outer and central regions. The outer SI is within a small arms protected post while the central SI is exposed. Both are equipped with duress alarms. The flow of traffic on the outer side is controlled with concrete blocks to require entry at the gate. The gates are sliding 8 foot chainlink with outriggers while the guard doors are hollow core metal with hinge protection. The portal walls and ceiling are equivalent in delay to 8 inch filled blocks.

The third entrance through the PIDAS is a gate limited to site vehicles without shipments or large cargo. Picture ID checks, explosives search with bomb sniffing dogs, and a cursory search of possessions are conducted outside the gate. When the searches are complete the electronically coded gate is opened remotely. Outgoing traffic passes through a sodium iodide scintillator, but does not undergo an explosives search. Detection is provided with exterior video motion sensors located on either side of the gate in addition the continuous presence of security personnel on either side. The gate

position is monitored with a balanced magnetic switch. Concrete blocks on the exterior side limit the angle of approach to the 8 foot chainlink gate supported with outriggings. The exterior SI is positioned in a small arms resistant post while the inner SI is unprotected, both are equipped with duress alarms.

1.3 Protected Area

The Protected Area is contained within the Limited Area's PIDAS and contains the most vital buildings within the facility, including the designated target building for this scenario. Of the routes that lead into the Controlled Building, several pass directly from the Protected Area to a section designated the Controlled Room. The target building is split into the Target Area, Controlled Room, and Controlled Building. Pathways into the Controlled Building section include the front pedestrian portal, office windows, and the Controlled Building's walls or ceiling. To pass directly into the Controlled Room the adversary can use a ventilation duct, the rear shipping and receiving doorway, or breach either the Controlled Room's exterior walls or ceiling. The shortest route across the Protected Area is 402m.

The target building pedestrian portal is the main entrance for employees without shipments or cargo. Access into the portal requires a badge swipe to open the electronically coded outer lock. In the central section an exchange picture badge is provided after confirmation of an employee's identification with a PIN check. Personnel passing through the central section pass through a portal metal detector capable of detecting ferrous materials and all forms of lead, a rigorous item search, explosives

vapor collection on entry, and a plastic scintillator SNM portal on exit. Video motion detectors are located on the exterior of the portal and within the central region along with security personnel generally on either side of the portal and always in the central region. Door positions are monitored with balanced magnetic switches and weight pads within the central region ensure that security personnel are capable of verifying the use of contraband portals. The entrance door to the portal is a steel turnstile to limit the flow of traffic while the inner door is hollow core metal with hinge and lock protection. The walls and ceiling are equivalent to 4 inch reinforced concrete. Random security patrols pass by the portal's exterior and within the Controlled Building. The outer SI post is unprotected while the central post is small arms resistant; both are equipped with duress alarms. The portals length is approximately 10m.

The other three pathways into the Controlled Building include breaching the office windows, the walls, or the ceiling. The windows consist of a single layer of security glass with an inaccessible lock to effectively make the window unopenable. The maximum diameter passage of the window is 100cm. Multiple sensors are in place to detect window penetration and security patrols pass by both sides on a randomized schedule. Both the walls and the ceiling are equivalent to 8 inch reinforced concrete with an interior grid mesh to detect penetration. Security patrols pass by both sides of walls, but do not have a line of sight of the ceiling. The interior of the Controlled Building is monitored by complementary interior detectors. Assessment of a penetration alarm for any of these features is conducted through timely deployment of security personnel (regular SI personnel as opposed to the response force).

The rear shipping and receiving doorway is limited to large shipments and cargo from designated delivery vehicles or packages and equipment from site vehicles. Entrance searches and ID checks are conducted on the outer side of the gate while exit searches are conducted within the building's cargo bay. Entry requires an authorization form and picture badge check followed by inspection for explosives with bomb dogs, passage through a portal metal detector capable of detecting all forms of lead, and a rigorous search of the driver, packages, and cargo shipments. After the searches are successfully completed by the posted SI, the electronically coded central lock is remotely opened. Exiting vehicles undergo the same rigorous item search and portal metal detector, but also pass through a plastic scintillator SNM monitor. Intrusion detectors include exterior motion sensors on the outside of the doorway, conducting tape and a balanced magnetic switch on the door, and multiple complementary interior sensors inside the building as well as personnel always present on both sides. The outer SI is in a small arms protected post while the inner SI post is unprotected; both are equipped with duress alarms. Random SI patrols pass by both sides of the doorway. The door itself is a vehicle rollup door and leads directly to the Controlled Room.

To represent the vulnerabilities that exist in older facilities designed without a focus on security, a large ventilation duct crosses from the Protected Area to the Controlled Room. The duct is 20m across and has a maximum diameter passage of 1m. Two fixed barriers are in place, each secured with a high security padlock. The barriers are defined as heavy grid and have multiple penetration sensors in place. The region between the barriers is monitored with an interior microwave intrusion sensor and the

area beyond the inner barrier contains multiple complementary interior sensors. Alarm assessment is conducted using CCTV with instant replay capability. Random SI patrols pass by both sides of the ductwork.

The Controlled Room's walls or ceiling can also be reached from the Protected Area. They are equivalent to 8 inch reinforced concrete with grid mesh surface penetration sensors. Multiple complementary interior sensors are on the interior side of the walls and ceiling, but there is no direct line-of-sight to the ceiling from the SI patrols that randomly pass through the area both outside and inside the target building. Activation of the penetration sensors results in automatic deployment of the response force.

1.4 Controlled Building

From the Controlled Building, there are two pathways into the Controlled Room and one into the Target Area. The door into the Controlled Room requires a fingerprint scan and PIN to unlock an electronically coded lock. Multiple complementary interior sensors are present on both sides of the doorway to ensure security is aware of all personnel. The door's condition is confirmed with a balanced magnetic switch and conducting tape to detect penetration. Alarm assessment is conducted with CCTV coverage with instant replay capability. The door is half inch steel plate and SI patrols pass by both sides on a randomized schedule.

Breaching the walls leads to either the Controlled Room or Target Area, depending on which section is destroyed. Both sections of wall have multiple surface

penetration sensors and complementary interior sensors on either side. In both cases, the wall is equivalent to 8 inch reinforced concrete and an alarm results in automatic deployment of the response force. Random SI patrols pass by the exterior and interior of the Controlled Room wall and the exterior of the Target Area wall. In all cases, it is approximately 20m across the Controlled Building.

1.5 Controlled Room

Within the Controlled Room is a vault defined as the Target Area. The vault can be entered through either the vault door or breaching the surrounding walls. No matter the entrance point into the Controlled Room, it is assumed 10m must be traversed to get to the next security element.

Entrance through the vault door requires a fingerprint scan and PIN before the central alarm station (CAS) unlocks the electronically coded lock. The door is a Class V vault door. An unprotected SI is posted next to the door with a duress alarm. Alarm assessment is performed by the posted SI or with CCTV coverage with instant replay.

The vault wall is equivalent to 8 inch reinforced concrete and possesses multiple surface penetration sensors which trigger an automatic deployment of the response force. Multiple complementary interior sensors are located on both sides of the wall to ensure the CAS can track individuals within the facility.

1.6 Target Area

The target is located 2m within the Target Area inside a security cage. The outside of the enclosure is made of security glass with the target tied down within. An authorization check with the CAS is required each time the location is accessed before two separate high security padlocks are allowed to be opened. Each cleared material custodian is issued a key that only unlocks a single padlock to ensure that the two person direct observation rule is enforced. Sensor coverage throughout the target area and cage is ensured with multiple complementary interior sensors. The security glass enclosure possesses multiple penetration sensors and a balanced magnetic switch on the doorway. The target itself is tied down with wire and secured with a lock. Alarm assessment is conducted with CCTV cameras with instant replay that are monitored whenever personnel are within the vault.

2 Facility Two Layers

2.1 Property Protection Area

The Property Protection Area can be entered easily by a small adversary force without detection so it plays the same role as the Offsite layer of Facility One. The three options for entering the Limited Area include breaching the outer fence, the personnel portal, or the shipping/receiving portal. A vehicle can be used for any of these elements and its continued use in the Limited Area is represented in Layer A of the ASD (which requires the adversary to take the longer vehicle accessible road). If the vehicle is abandoned to pursue to shorter on-foot path the adversary crosses into Layer B of the ASD instead of Layer A.

The outer perimeter is surrounded by a chainlink fence over 12 foot with outriggings with concrete blocks on either side to slow or stop vehicles. The fence is outfit with vibration sensors that are assessed by light anti-tank resistant (LAW) resistant SI towers just within the fenceline. Because the fenceline is large compared to the number of SI personnel in the towers the fenceline is not considered to be under general observation. The primary purpose of the guard towers is assessment and response compared to initial detection.

Access into and out of the Limited Area through the personnel portal requires a picture ID badge and PIN to open electronically coded locks. Personal possessions are allowed through the portal, but packages, tools/equipment, and shipments or cargo are not. Security inspectors are posted in a LAW resistant tower that oversees incoming

traffic, a central small arms protected duress alarm equipped post that ensures only personal possessions are brought in or out, and an unprotected duress alarm equipped inner post that handles outgoing traffic. Intrusion detection features include exterior video motion sensors at the entrance and exit, conducting tape door penetration sensors, balanced magnetic switches to monitor door position, multiple complementary interior sensors in the central section, and near continuous general observation at all points. Both doors are steel turnstiles and the portal's walls are equivalent to 8 inch filled block. Employees must use the shipping and receiving portal to bring larger packages into the Limited Area.

Access through the shipping and handling portal is prohibited to civilian or personal vehicles. Additionally, passengers are not allowed even when in site or delivery vehicles. Authorization forms and picture badges are required at the outer section for entering traffic and at the inner level for exiting traffic. The outer lock is inaccessible and unlocked from a distance by the alarm station. Bombing sniffing dogs are used on entering traffic. Both entering and exiting vehicles are subjected to a rigorous cargo search. Intrusion detection at the inner and outer levels is performed by video motion detectors, conducting tape and balanced magnetic switches on the doors, and by personnel generally in the vicinity. The central section possesses multiple complementary sensors with personnel always in the vicinity. The walls are made of 8 inch filled block with vehicle liftups at the entrance and exit. LAW resistant towers are located on outer and inner sections, a small arms resistant post with a duress alarm is in the central section, and an additional unprotected SI is posted on the inner level with a

duress alarm. The portal is 10 meters across and assessment is performed by the Posted SI's.

2.2 Limited Area

The Limited Area is 950 meters across when using a vehicle and 150 meters when using the pedestrian route. Surrounding the Limited Area is a PIDAS consisting of two 12 foot chainlink fences with outriggings distanced 5 m apart with concrete blocks and concertina wire in between. Both fences are outfit with multiple detectors and the central region features multiple complementary systems on either side of the concrete blocks. Alarm assessment is facilitated with overlapping CCTV coverage with instant replay capability.

Passage through the PIDAS occurs at a personnel portal and a shipping and receiving portal. The personnel portal is the main route into and out of the Protected Area for site employees. Only personal possessions are allowed through the portal in normal circumstances. The entrance to the personnel portal is controlled with a mechanically coded lock that is opened by an SI after showing credentials and entering a PIN. The central section of the portal provides an exchange picture badge. The outer side of the portal features a LAW resistant tower, the central SI post is small arms protected and equipped with a duress alarm, and the inner SI post possesses a duress alarm but is unprotected. All traffic is subjected to bomb sniffing dogs in the central section. Detection at the outer and inner exterior sections of the portal is provided by video motion sensors, a balanced magnetic switch and conducting tape on the door, conducting

tape in the walls, and direct observation by security. The central section possesses multiple complimentary sensors and constant security surveillance. The inner and outer doors are steel turnstiles and the walls and ceiling are equivalent to 4 inch reinforced block. The overall distance across the portal is approximately 5m.

The cargo entrance to the Protected Area is a shipping and receiving vehicle portal. This entrance is limited to shipment vehicles, site vehicles, and the authorized driver. Outer access requires an authorization form and an exchange picture badge before the inaccessible lock will be opened. A rigorous search of entering and exiting vehicles is conducted in the central region, with ingoing vehicles being subjected to bomb search dogs and outgoing vehicles driving through a sodium iodide scintillator for SNM detection. After the central guard is satisfied that the vehicle does not possess contraband, the inner mechanically coded lock is remotely opened. The outer and inner door and gates are monitored with balanced magnetic switches. Exterior video motion sensors are located on both inner and outer sides of the portal and interior multiple complementary sensors are located in the central region in addition to continuous security personnel presence at all sections of the portal. The outer SI is within a LAW resistant tower, the central SI is within a duress equipped small arms resistant post, and the inner SI is within a duress equipped unprotected post. The gates are vehicle liftups while the portal walls and ceiling are 4 inch reinforced concrete.

2.3 Protected Area

The Protected Area is 125 m across. There are two elements separating the Protected Area from the Material Access Area (MAA), a personnel portal and a concrete wall. The concrete wall is equivalent to 4 inch reinforced concrete with multiple surface penetration monitors. These sensors result in an automatic deployment of the response force should they be tripped. In addition to the penetrations sensors, there are random SI patrols on either side of the wall.

The personnel portal is the main access point into the MAA. It is 10 meters across and all forms of possessions, packages, tools, and cargo are allowed through. The outer section requires an exchange picture badge and PIN before the inaccessible lock is remotely opened. The central station requires a fingerprint scan along with re-entering the PIN. When exiting the MAA, the exchange badge is returned in the inner section of the portal. Explosives detection is facilitated with vapor collection and a portal metal detector is in place to identify all ferrous materials and forms of lead. Items are rigorously searched and personnel are subjected to a patdown. Detection at the inner and outer sections is performed with video motion sensors, multiple penetration sensors and balanced magnetic switches for the doors, multiple penetration sensors in the walls, and personnel always in the vicinity. The central section possesses multiple complementary intrusion sensors and is always manned by personnel. The walls are equivalent to 4 inch reinforced concrete and the doors are steel turnstiles. The outer SI is in a LAW resistant tower, the central SI is in a duress equipped small arms resistant post, and the inner SI is

in an unprotected duress alarm equipped post. Alarm triggers result in deployment of the response force.

2.4 Material Access Area

The main entrance from the MAA into the target building is a personnel portal. It is 125 m across the MAA and 6 m across the portal. Personnel possessions are not allowed through. The outer section requires an exchange picture badge and PIN before the mechanically and electronically coded locks are opened (there are two separate locks). The inner section requires a fingerprint scan along with re-entering the PIN to open an electronically coded lock. There is also a manually activated evacuation alarm in the inner section. When exiting the MAA, the exchange badge is returned in the inner section of the portal. Explosives detection is facilitated with vapor collection and a portal metal detector is in place to identify all ferrous materials and forms of lead. Items are rigorously searched and personnel are subjected to a patdown. Detection at the outer section is performed with multiple complementary intrusion sensors, multiple penetration sensors and balanced magnetic switches for the doors, multiple penetration sensors in the walls, and personnel always in the vicinity. The inner section features the same detection measures, but without personnel in the vicinity. The central section possesses multiple complementary intrusion sensors and is always manned by personnel. The walls are equivalent to 8 inch filled block and the doors are hollow core metal. The outer SI is in a LAW resistant tower and the central SI is in a duress equipped small

arms resistant post. Alarm triggers, including the evacuation alarm, are assessed posted SI with duress alarms.

The next security level can also be reached by breaching through the building's wall. Based on which section is breached, the attacker can either enter the target building, the radiation area, or the vault. All three sections of wall possess multiple complementary sensors on both sides and multiple surface penetration sensors within. An alarm trip automatically deploys the response force. The section of wall that allows entrance into the building is 8 inch filled block, the wall that allows entrance into the radiation area is 4 inch reinforced concrete, and the wall that allows entrance into the vault is 8 inch reinforced concrete.

2.5 Target Building

Inside the Target Building is another security portal (25 m from the entrance) that limits access into the Radiation Area. It is 6 meters across and personal possessions are not allowed through. The outer section requires an exchange picture badge and PIN before the mechanically and electronically coded locks are opened (there are two separate locks). The inner section requires a fingerprint scan along with re-entering the PIN to open an electronically coded lock. There is also a manually activated evacuation alarm in the inner section. When exiting the MAA, the exchange badge is returned in the inner section of the portal. A portal metal detector is in place to identify all ferrous materials and forms of lead and a plastic scintillator portal detects SNM. Items are rigorously searched and personnel are subjected to a patdown. Detection at the inner and

outer sections is performed with video motion sensors, multiple penetration sensors and balanced magnetic switches for the doors, multiple penetration sensors in the walls, and personnel always in the vicinity. The central section possesses multiple complementary intrusion sensors and is always manned by personnel. The walls are equivalent to 4 inch reinforced concrete and the doors are steel turnstiles. A central SI is in a duress equipped small arms resistant post. Alarm triggers are assessed by the duress alarm equipped SI.

The walls inside the Target Building can also be breached to enter the Radiation Area. Multiple complementary intrusion sensors are on either side of the wall along with multiple penetration sensors. An alarm trip results in automatic response force deployment. The wall's delay is equivalent to 4 inch reinforced concrete.

2.6 Radiation Area

The main path from the Radiation Area into the Target Area (the vault) is a Class V vault door that is 25 m from the entrance. Multiple complementary intrusion sensors are on either side of the door along with multiple penetration sensors and a balanced magnetic switch. Entrance into the vault requires a fingerprint scan, PIN, and the combination to a high security padlock. The various alarms result in automatic deployment of the response force.

The walls surrounding the vault have multiple complementary intrusion detection sensors on either side and multiple surface penetration sensors. An alarm trip results in automatic response force deployment. The wall is equivalent to 8 inch reinforced concrete.

2.7 Target Area – Vault

The target is held down in a cage 10 m within the vault. The central alarm station surveys activity within the vault through CCTV whenever workers are present and they verify the authorization of each worker before the work is performed. A strict two person rule requiring dedicated observation is in place. There are two high security padlocks on the cage, with each worker only knowing the combination to one. Multiple signals are required before the criticality alarm will trip, to reduce the chance of a false positive. Multiple complementary intrusion sensors are located throughout the vault and the cage is equipped with multiple penetration sensors and a balanced magnetic switch. The targets presence within the cage is monitored with another balanced magnetic switch and a remotely viewable tamper monitor. The cage door and surface are made of 9 gauge wire mesh and the target is tied down with wire secured with a bolt.

VITA

Name:	Curtis Alan Conchewski
Address:	16111 Wales Court, Spring, TX, 77379
Email Address:	cconchewski@gmail.com
Education:	M.S., Nuclear Engineering, Texas A&M University, 2012 B.S., Nuclear Engineering, Texas A&M University, 2010