QUANTITATIVE METHODOLOGY FOR ASSESSING STATE-LEVEL NUCLEAR SECURITY MEASURES

A Dissertation

by

CHRISTOPHER TYSON MYERS

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

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	William S. Charlton
Committee Members,	John W. Poston, Sr.
	David R. Boyle
	Arnold Vedlitz
Head of Department,	Yassin A. Hassan

December 2012

Major Subject: Nuclear Engineering

ABSTRACT

The international community faces a growing threat from nuclear terrorism. The complexity of the threats of nuclear terrorism, the variety of nuclear security measures that States can devote resources towards to address the threats, and the limited resources States have to invest in these nuclear security measures make it imperative that resources are applied in the most effective way possible. In this dissertation, we develop a quantitative, risk-based methodology that States can employ to gain a better understanding of the nuclear threat they face, assist them in determining what nuclear security measures they should invest in, and facilitate communication to stake-holders to request and justify investment in these measures.

The risk-based methodology has been developed employing a combination of pathways analysis, game-theory, multiple-attribute utility analysis, decision theory and risk analysis. The methodology was designed to account for the wide variety of nuclear security measures that States can invest in, the range of possible consequences from different nuclear threats, and the severity of these consequences to the State. In addition, the methodology models the adversary's strategic decision making while accounting for the capabilities, motivations, and disincentives that may influence which nuclear threat a terrorist group will attempt.

The methodology is introduced into a Visual Basic for Applications code, which we demonstrate through verification and qualitative validation tests. We then develop three State nuclear infrastructures with varying levels of complexity, meant to provide a realistic representation of real-world States. We then utilize the code to evaluate the risk of nuclear terrorism against terrorist threats that have different motivations for nuclear terrorism to demonstrate how different motivations for nuclear terrorism may affect both State-level risk and the State's optimal risk-reduction strategy. These risk analyses are then used to both evaluate various nuclear security strategies and determine which nuclear security measures will have the greatest risk-reduction value. Finally, we conduct a sensitivity analysis on capabilities of terrorist groups to understand how changes in these capabilities affect the State-level risk from nuclear terrorism.

DEDICATION

To my parents, who have made all this possible, by providing me with countless opportunities and unending support, and my wonderful fiancée Jessica.

ACKNOWLEDGEMENTS

I would like to thank my advisor and committee chair, Dr. William Charlton, for the years of support, guidance, and advice. I would also like to thank my committee members, Dr. David Boyle, Dr. John Poston, and Dr. Arnold Vedlitz, for their helpful comments and feedback on this work. Additionally, I would like to thank the IAEA Office of Nuclear Security Cooperative Research Program and the Deputy Assistant Secretary of Defense for Nuclear Matters for funding this research. Thanks also go to the entire faculty and staff of the Nuclear Engineering Department for making my time at Texas A&M University a rewarding experience.

TABLE OF CONTENTS

Page

ABSTRACT ii

DEDICATION iv

ACKNOWLEDGEMENTS v

TABLE OF CONTENTS vi

LIST OF FIGURES viii

LIST OF TABLES x

I. INTRODUCTION 1

I.A Background 1
I.B Background on the Threat of Nuclear Terrorism 3
I.C The International Nuclear Security Regime 11
I.D Research Motivations 16
I.E Research Objectives 17
I.F Overview of Chapters 18

II. SECURITY RISK ANALYSIS 20

II.A Probabilistic Risk Assessments 20
II.B Security Risk Assessments 25
II.C Current Approaches in Security Risk Analysis 36

III. METHODOLOGY 55

III.A Overview of Methodology 55
III.B Methodology Inputs 57
III.C Utility Functions 87
III.D Solution Method 100

IV. NUMERICAL TESTS 107

IV.A Verification Tests 107
IV.B Validation Tests 121

IV.C Behavioral Tests 142

V. TEST CASES 146

V.A Small State Infrastructure 148
V.B Intermediate State Infrastructure 163
V.C Complex State Infrastructure 177

VI. CONCLUSIONS AND RECOMMENDATIONS 196

VI.A Summary of Results 196
VI.B Recommendations for Future Work 200

REFERENCES 203

APPENDIX A 210

APPENDIX B 221

APPENDIX C 226

APPENDIX D 233

APPENDIX E 237

APPENDIX F 241

LIST OF FIGURES

Figure 1. Would They vs. Could They Plot for Nuclear Weapons and IND 10

Figure 2. Example Event Tree..23

Figure 3. Example Fault Tree...23

Figure 4. Example PRA Probability Density Function for Nuclear Reactor 24

Figure 5. Risk of Fatalities From Man-Made Systems 25

Figure 6. Security Risk is the Intersection of Threat, Vulnerability, and Consequences..26

Figure 7. Simple Bayesian Network Using Netica 31

Figure 8. Security Layers Diagram 38

Figure 9. Influence Diagram Representing an Overarching Model for Prioritizing Threats and Countermeasures 44

Figure 10. Single-Period, Two-Sided Global Influence Diagram...................................46

Figure 11. Threat Intensity for a Given Delivery System 50

Figure 12. Overview of Asset-Driven Risk Analysis...53

Figure 13. Methodology Flowchart..56

Figure 14. Task Event Tree 60

Figure 15. Significant Quantities of Nuclear Materials 69

Figure 16. Critical Mass of a Beryllium-Reflected Uranium Sphere As a Function of U-235 Enrichment...71

Figure 17. Probability of a Spontaneous-Fission-Free Millisecond in One Bare Critical Mass of Uranium of Varying Enrichment...72

Figure 18. Bare Critical Mass for Unreflected Metal Spheres for Various Qualities of Pu and Enrichments of U 73

Figure 19. Graph of Items per SQ Utility Function 92

Figure 20. Graph of Dose Rate Utility Function 93

Figure 21. Graph of Items per SQ Utility Function 94

Figure 22. Mass per SQ Utility Function 95

Figure 23. Utility Functions of Plutonium Quality and Uranium Enrichment....98

Figure 24. Process of Determining Upgrades to Reach Target Risk....105

Figure 25. The Risk of Nuclear Terrorism is a Subset of Terrorism Risk 145

LIST OF TABLES

Table 1. Terrorist Traits for the Four Nuclear Threats..8

Table 2. Marginal Probabilities of Attack Scenarios Without Countermeasures (Status Quo)..47

Table 3. Expected Disutilities of Attack Scenarios Without Countermeasures (Status Quo)..47

Table 4. Asset-Level Consequence Dimensions 49

Table 5. Assessed Likelihoods Adversary Capabilities and Resources Inputs 59

Table 6. Motivation and Disincentive Inputs 62

Table 7. Motivations and Disincentives for Nuclear Terrorism......................................64

Table 8. Consequence Weights for Sample Terrorist Groups...66

Table 9. Risk Attitude Exponent Values 66

Table 10. Example Physical Security Inputs..81

Table 11. Pathway Attractiveness Based on Risk Attitude 89

Table 12. Normalized Values Based on Risk Attitude..90

Table 13. Utility Values for Various Plutonium Qualities and Uranium Enrichments....97

Table 14. SNM Pathway Generation Verification Results 109

Table 15. Probability of Success for Each Task...110

Table 16. MAUA Attractiveness Results 111

Table 17. IND Pathways 112

Table 18. RDD Pathways..113

Table 19. Research Reactor Materials P_E Values...114

Table 20. Hospital Materials P_E Values 114

Table 21. Material Attractiveness Value for Each Material 115

Table 22. Probability of Success for Each Pathway Task 116

Table 23. RDD Consequences for Each Pathway 117

Table 24. Sabotage Pathways 118

Table 25. Probability of Attack Calculations 119

Table 26. Pathway Risk Values 120

Table 27. Terrorist Profiles 123

Table 28. MAUA Attractiveness Results 124

Table 29. Probabilities of Choosing Paths 125

Table 30. Group A Capability Assessments 127

Table 31. Group A Probabilities of Attack 128

Table 32. Group B Capability Assessments 129

Table 33. Group B Probabilities of Attack for Various Materials 130

Table 34. Probability of Achieving Indicated Yield Based on Neutron Source Strength 132

Table 35. IND Related Symmetric Sensitivity Results 132

Table 36. Sabotage Related Symmetric Sensitivity Results 134

Table 37. IND Related Non-Symmetric Sensitivity Results 135

Table 38. Sabotage Related Non-Symmetric Sensitivity Results 135

Table 39. IND Related Symmetric Relative Sensitivity Results 136

Table 40. IND Related Non-Symmetric Relative Sensitivity Results 136

Table 41. Sabotage Related Symmetric Relative Sensitivity Results 137

Table 42. Sabotage Related Non-Symmetric Relative Sensitivity Results 137

Table 43. Modified Sabotage Consequence Values 138

Table 44. Relative Likelihood of Choosing and Relative Risk of Each Pathway for Modified Sabotage Consequences 139

Table 45. Sabotage Related Symmetric Sensitivity Results for Modified Case 140

Table 46. Sabotage Related Non-Symmetric Sensitivity Results for Modified Case ... 140

Table 47. Sabotage Related Symmetric Relative Sensitivity Results for Modified Case 141

Table 48. Sabotage Related Non-Symmetric Relative Sensitivity Results for Modified Case 141

Table 49. Risks for Behavioral Tests Normalized to P_A=1 142

Table 50. Un-normalized Risks for Behavioral Tests 144

Table 51. Small Infrastructure Threats Risk 149

Table 52. Small State Pathway Risk 149

Table 53. Small State Risk Reduction Results 150

Table 54. Small State Most Sensitive Security Measures - Group 1 152

Table 55. Small State Most Sensitive Security Measures - Group 2 153

Table 56. Small State Most Sensitive Security Measures - Group 3 153

Table 57. Optimal Security Measures for Small State - Group 1 155

Table 58. State-Level Risk Breakdown for Group 1 After Upgrades 156

Table 59. Optimal Security Measures for Small State - Group 2 157

Table 60. Optimal Security Measures for Small State - Group 3 158

Table 61. Small State Capability Assessment Risk Sensitivity - Group 1 160

Table 62. Small State Capability Assessment Risk Sensitivity - Group 2 161

Table 63. Small State Capability Assessment Risk Sensitivity - Group 3 162

Table 64. Intermediate State Risk by Threat 164

Table 65. Intermediate State Pathways Risk 164

Table 66. Intermediate State Risk Reduction Strategy Results 166

Table 67. Intermediate State Security Measure Risk Sensitivity Results - Group 1 167

Table 68. Intermediate State Security Measure Risk Sensitivity Results - Group 2 168

Table 69. Intermediate State Security Measure Risk Sensitivity Results - Group 3 169

Table 70. Intermediate State Optimal Security Upgrades for 50% Risk Reduction - Group 1 170

Table 71. Intermediate State Optimal Security Upgrades for 50% Risk Reduction - Group 2 171

Table 72. Intermediate State Optimal Security Upgrades for 50% Risk Reduction - Group 3 172

Table 73. Intermediate State Adversary Capability Assessment Risk Sensitivity - Group 1 174

Table 74. Intermediate State Adversary Capability Assessment Risk Sensitivity - Group 2 174

Table 75. Intermediate State Adversary Capability Assessment Risk Sensitivity - Group 3 176

Table 76. Complex State Risk by Threat 178

Table 77. Complex State Pathways Risk 179

Table 78. Complex State Risk Reduction Strategy Results 181

Table 79. Complex State Security Measure Risk Sensitivity Results - Group 1 182

Table 80. Complex State Security Measure Risk Sensitivity Results - Group 2 183

Table 81. Complex State Security Measure Risk Sensitivity Results - Group 3 184

Table 82. Complex State Optimal Security Upgrades for 50% Risk Reduction - Group 1 187

Table 83. Complex State Optimal Security Upgrades for 50% Risk Reduction - Group 2 188

Table 84. Complex State Optimal Security Upgrades for 50% Risk Reduction - Group 3 189

Table 85. Complex State Capability Assessment Risk Sensitivity - Group 1 191

Table 86. Complex State Capability Assessment Risk Sensitivity - Group 2 192

Table 87. Complex State Capability Assessment Risk Sensitivity - Group 3 193

Table 88. Failed Complex State Risk Analysis 194

Table 89. Failed Complex State Relative Probability of Choosing Threats 195

CHAPTER I

INTRODUCTION

I.A. Background

The events of September 11, 2001 demonstrated a new level of dedication and organization by a terrorist group, prompting the international community to re-evaluate the threat posed by terrorism. Terrorist attempts to cause widespread death and destruction with no regard for their own lives have prompted new nuclear security awareness.[1] The acquisition and detonation of even one crude nuclear device represents a real and urgent threat to international security. Some terrorist organizations have made numerous attempts to acquire the materials and expertise to make nuclear weapons. Various studies have shown that if a sophisticated sub-state actor was able to acquire enough Special Nuclear Material (SNM), it is plausible they could fabricate a crude nuclear device. [2,3]

Nuclear weapons are not the only face of nuclear terrorism, and terrorist organizations are known to have sought radiological "dirty" bombs and considered the sabotage of nuclear facilities or materials during transport. Though they won’t cause the devastating loss of life that a nuclear weapon could, radiological weapons and the sabotage of a facility or material in transport both represent significant threats. Each has the potential to cause severe economic consequences and public unrest. Unlike the SNM needed to make nuclear weapons, radioactive materials are much more widely available and typically do not have the level of security that sources of SNM do. A simple Radiological Dispersal Device (RDD) could entail adding radioactive material to conventional explosives, well within the capabilities of any terrorist group. More sophisticated devices may utilize deadlier levels of radioactivity and cause a significantly larger number of deaths.[4] In addition to the costly decontamination, the consequences of the sabotage of a nuclear facility may considerably impact the development of nuclear technology for peaceful purposes.[5]

The responsibility of securing nuclear and radiological materials and protecting nuclear facilities from sabotage rests entirely with the State.[6] States can address the threat of nuclear terrorism in many different ways. The three main options that States have to reduce the risk posed by nuclear terrorism are[7]:

- Reducing the threat through reducing adversary capabilities or intentions;
- Improving the effectiveness of physical protection systems to reduce vulnerabilities; and
- Reducing the potential consequences of malicious acts.

To accomplish these options, States can employ various nuclear security measures, including material control systems, physical protection systems, safety systems, and second-line-of-defense measures[a]. Managing resources among the variety of measures at their disposal represents a multi-faceted problem that encompasses a variety of fields. With limited resources, the State will want to ensure that investments made in nuclear security measures are the most effective at addressing the threats posed to the State by nuclear terrorism.

In this dissertation, we introduce, analyze and numerically test a methodology that yields a State-level risk metric derived from details of the State's nuclear infrastructure, security measures that are employed, and various characteristics of the threat. This metric is a quantitative value that represents the relative severity of the threat posed by nuclear terrorism to the State. It also provides a means to analyze the impact of various nuclear security measures based on the degree that these measures reduce the risk of nuclear terrorism to the State. This tool can assist States to optimize the allocation of resources for nuclear security measures and provides a mechanism to evaluate various nuclear security activities at the State level.

I.B. Background on the Threat of Nuclear Terrorism

Nuclear terrorism is defined as the actual or potential use of nuclear or radiological materials, or attacks on nuclear facilities or transportation carrying nuclear materials, by an individual or a sub-state group to generate fear or destruction in the pursuit of

[a] Second-line-of-defense measures are security measures deployed to search, detect and identify the illicit movement of nuclear and radiological materials. Such measures include installing radiation detectors at

political objectives. The threats posed by nuclear terrorism are broken down into four categories based on the different characteristics of each threat. These four threats are defined by the IAEA as:[8]

- the theft of a nuclear weapon;
- the theft of SNM and development of an improvised nuclear device (IND);
- the theft of radiological material and development of an RDD;
- sabotage of a nuclear facility or transport resulting in the release of radioactivity.

The first threat, which is concerned with a sub-state group stealing a nuclear weapon, only affects a small number of countries, as possessing a nuclear weapon is a prerequisite to this threat. Taking possession of an intact nuclear weapon is the most appealing option for a terrorist group intent upon acquiring a nuclear capability, given the many hurdles they would have to overcome to produce their own device. However, nuclear weapons are among a State's most heavily protected assets, and a terrorist group has a very low likelihood of successfully stealing an intact nuclear weapon. Even if a terrorist organization was able to acquire a nuclear weapon, they could not simply detonate it, as States have strict control measures, like permissive action links (PALs), that render the weapon useless without the proper authorization codes. PALs are designed to not be susceptible to reverse engineering or be bypassed.[9] The other option for the adversary would be to scrap the weapon and remove the fissile material and other useful components. However, this is not an attractive pathway because States possess advanced designs and technical capabilities that allow them to produce weapons with a smaller amount of fissile material than a non-state actor would require to produce their own, crude nuclear device. In addition, there are likely other sources of SNM within the State that are less heavily protected.

The threat of an adversary developing an IND is the most complex of the four threats. An IND is similar to a nuclear weapon based on how it generates its energy, utilizing a supercritical configuration of fissile material to produce a nuclear explosion. However, an IND is a crude nuclear device, and a terrorist is more concerned with generating some level of nuclear yield and less concerned with producing a device that is safe and has a predictable yield. As a result safety, security, and reliability are not as significant of concerns in the design of an IND as they are in nuclear weapons. The type of nuclear material dictates the steps required to convert the material to be usable in a nuclear weapon. The prevailing belief among the intelligence community is that if a sub-state group gained possession of enough weapons usable material, highly enriched uranium[b] (HEU) or plutonium, they could plausibly produce an IND. Conversely, the consensus is that even if a sub-state group obtained enough non-direct use materials, such as spent fuel or uranium enriched to less than 20% U^{235}, they would not likely be able to produce an IND.[2]

[b] Highly Enriched Uranium is Uranium that is enriched in the fissile isotope U-235 from its natural abundance of approximately 0.7% to 20% or more.

The third threat of nuclear terrorism is an RDD, where radioactive sources are combined with conventional explosives to disperse radioactive contamination. Given the availability of radiological sources and terrorist familiarity with conventional explosives, the effort required to gather the materials for an RDD is far outweighed by the potential consequences a successful attack would generate.[4] While in a majority of cases an RDD would not be expected to inflict many casualties, it could create significant economic consequences. An RDD also plays into the public's nearly universal fear of radiation inspired by events like Chernobyl, Three Mile Island and the Cold War, meaning it has the ability to incite mass hysteria.

The final threat of nuclear terrorism is nuclear sabotage, where a terrorist group undertakes deliberate acts against a nuclear facility or a vehicle transporting nuclear material in an attempt to cause the release of radiation. Nuclear sabotage ranges in scenario complexity, from relatively straight-forward acts of breaking into a facility and detonating nuclear or radiological material in place with conventional explosives, to an extremely complex task of disabling safety features on a nuclear reactor by attacking vital areas of the safety systems with the intent to cause a core meltdown and radiological release. After witnessing the amount of international attention given to the Fukushima Daiichi accident in Japan, sabotage of a nuclear facility may appear an attractive option for a terrorist group. The consequences of a sabotage event would likely involve few casualties, but severe economic consequences and public and political backlash would ensue.

The four threats of nuclear terrorism not only differ based on the effects they generate, but also in the types and numbers of terrorist groups that could potentially execute each threat and have the motivation to do so. Table 1 summarizes the general traits of a terrorist group that are prerequisites to pursue each of the four threats as well as the number of groups that fit each description as of 2004.

Because nuclear weapons and INDs are high consequence scenarios, they have typically received greater attention than the other threats and therefore have been analyzed in greater detail. Historically, there have been few documented, serious attempts by terrorist groups to acquire a nuclear capability. The two best known cases are the Japanese cult Aum Shirinkyo and the militant Islamic organization al Qaeda. Both Aum and al Qaeda failed in their attempts to illicitly acquire a nuclear weapon from a State and failed to acquire the nuclear material necessary to produce their own crude nuclear device.[10] Current estimates are that the number of groups with an interest and the capability to pursue nuclear terrorism remain low, with four groups that have demonstrated an interest in acquiring nuclear weapons and five groups who have the capability to acquire nuclear weapons or produce an IND.[11]

Table 1. Terrorist Traits for the Four Nuclear Threats[12]

Traits	**Steal Nuclear Device**	**Steal Nuclear Material for IND**	**Sabotage Nuclear Facility**	**Steal Radioactive Material for RDD**
Motivation	Extreme; desire to cause mass deaths, destruction; likely limited to apocalyptic and politico-religious groups	Extreme; desire to cause mass deaths, destruction; likely limited to apocalyptic and politico-religious groups	Very high; desire to cause great property damage, disruption, some loss of life	Very high; desire to cause great property damage, disruption, some loss of life
Organizational Skills	Very high	Very high	Very high	Moderate
Financial Resources	High	High	Moderate to high	Modest
Technical Skills	High	High; moderate for some scenarios	Moderate to high	Modest
Number of groups (in 2004)	Few (possibly none currently able to meet all criteria for foreign country incident)	Few (possibly none currently able to meet all criteria for foreign country incident)	10+	10-100's

It is important to acknowledge that scholars do not agree on the level of threat that nuclear weapons and INDs present. Given the historical lack of nuclear terrorism events and the few groups who have attempted to acquire nuclear capabilities, the likelihood that terrorists successfully employ a nuclear weapon or IND depends on two key questions. These questions are 'Would terrorists be interested in nuclear terrorism?' and 'Could they succeed in an act of nuclear terrorism if they were interested?'. There has been a scholarly debate over these questions since the 1970's, with the debate being revived after certain terrorist events such as the sarin gas attack in Tokyo in 1995 and the events of September 11th. There is no consensus among experts about the intentions and capabilities of sub-state groups with respect to nuclear terrorism. This disagreement is illustrated by plotting the viewpoints expressed in various publications concerning these two questions in Figure 1[13]

The answers to these two questions provide important policy implications. If sub-state groups both want to develop a nuclear capability and have the capability to do so, then devoting resources to prevent such an act is incredibly important and urgent. However, if sub-state groups have little to no interest in nuclear terrorism, then resources devoted to stopping the perceived nuclear terrorist threat might be better applied to other counter-terrorism strategies. It is also important to understand how to balance protection against the high consequence, low likelihood threats of nuclear weapons and INDs and the other nuclear threats that have lower consequences yet higher likelihoods of occurring. A State-level risk assessment that incorporates terrorist intentions and motivations, like the one presented in this dissertation, can assist States to ensure that resources are applied effectively across the entire threat spectrum. In addition, it can quantify how important the answers to these two questions are to the risk of nuclear terrorism.

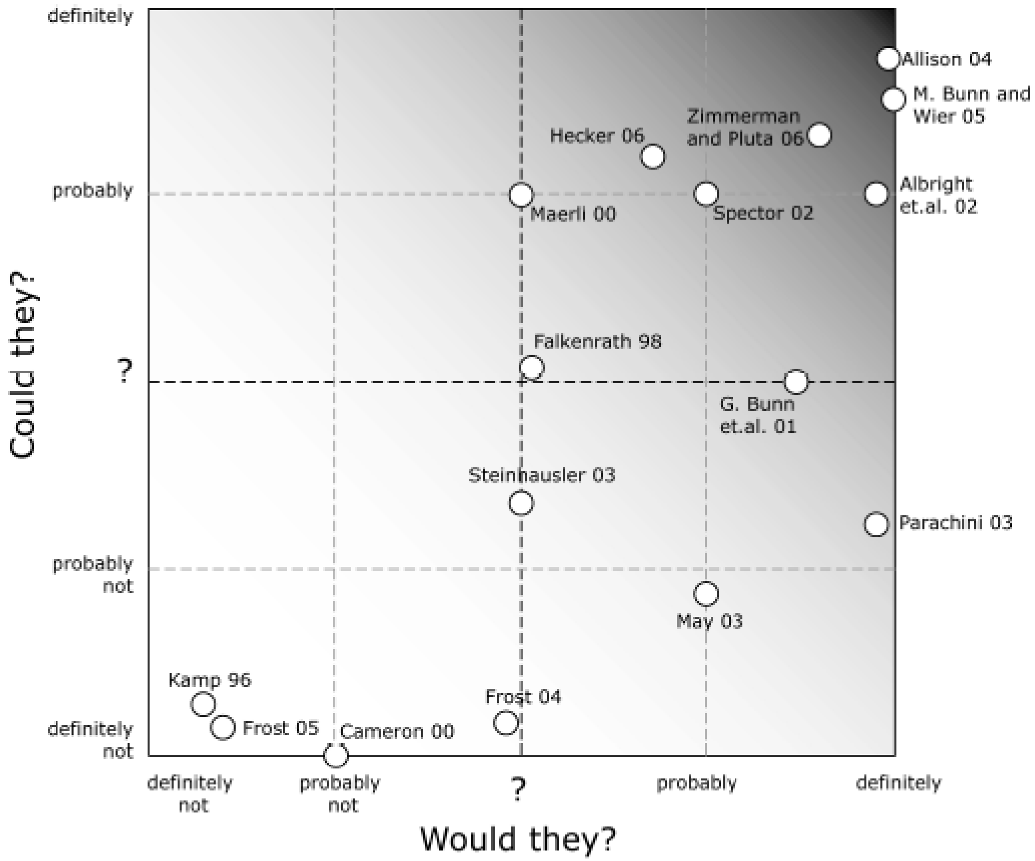


Figure 1. Would They vs. Could They Plot for Nuclear Weapons and IND[13]

While the likelihood of nuclear terrorism is disputed by some experts, it is clear that nuclear terrorism is and will remain a significant international policy concern. In 2009, President Obama publically stated, "we must ensure that terrorists never acquire a nuclear weapon. This is the most immediate and extreme threat to global security. One terrorist with one nuclear weapon could unleash massive destruction."[14] In 2010, President Obama and the United States brought nuclear security to the forefront of international awareness by hosting leaders from 47 countries at the inaugural Nuclear Security Summit. At the summit, Obama singled out nuclear terrorism as the most serious threat to international security. The Nuclear Security Summit is scheduled as a biennial event to keep nuclear security on the international agenda, most recently held in Seoul in 2012.

I.C. The International Nuclear Security Regime

Currently, the international nuclear security regime is made up of a number of various international agreements that are either binding or non-binding. Unlike the international safeguards regime, which is governed primarily by the Treaty on Non-Proliferation of Nuclear Weapons, there is no verification regime for nuclear security or even performance based standards that States must meet. As Ken Luongo, co-chair of the Fissile Materials Working Group (FMWG) describes it, "The current nuclear material security regime is a patchwork of unaccountable voluntary arrangements that are inconsistent across borders."[15] The result being that though each State is required to secure their nuclear and radiological materials, the degree to which they secure them is up to their discretion and can vary from State to State. The main instruments that make up the international nuclear security regime are summarized in this section.

I.C.1. The Convention on Physical Protection of Nuclear Materials (CPPNM) and Amendment[16,17]

CPPNM is the only international legally binding agreement focused on to the physical protection of nuclear material. It entered into force on February 8, 1987, and establishes State obligations to protect nuclear material during international transport, in addition to establishing measures related to the prevention, detection and punishment of nuclear material related offenses. It currently has 145 parties, which includes most of the nations using nuclear and radiological materials. To address perceived shortcomings in the original agreement, the CPPNM has since been amended to strengthen its provisions. On July 8, 2005, the amendment was adopted and awaits ratification by two-thirds of the State Parties to enter into force. The amendment makes it legally binding for States Parties to protect nuclear facilities and material in peaceful (e.g. non-military), domestic use, storage and transport. It also provides for cooperation between States to locate and recover stolen or smuggled nuclear material and mitigate any radiological consequences from sabotage.

1.C.2. International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT)[18,19]

ICSANT is a binding legal agreement adopted at the UN General Assembly in April 2005 and brought into effect in July 2007. The convention requires States to define acts of nuclear terrorism as criminal offenses. Acts of nuclear terrorism are defined by ICSANT as:

- The possession of radioactive material or a device containing radioactive material with the intent to cause death or serious bodily injury or with the intent to cause substantial damage to property or the environment; and
- The use of radioactive material or a device, or the use of or damage to a nuclear facility, which releases or risks the release of radioactive material with the intent to either cause death or serious bodily injury or with the intent to cause substantial damage to property or the environment or to coerce a person, organization or government to do or refrain from doing an act.

ICSANT also has some requirements for States to provide protection against these events, stating that "States Parties shall make every effort to adopt appropriate measures to ensure the protection of radioactive material."

1.C.3. UN Resolution 1540[20]

Security Council Resolution 1540 was adopted by the United Nations Security Council in April 2004. It established obligations for UN member States to take and enforce effective measures against the proliferation of Weapons of Mass Destruction (WMD), their means of delivery and related materials. The three primary responsibilities of States under UNSCR 1540 are:

- Prohibit support to non-State actors seeking such items;
- To adopt and enforce effective laws to prohibit the proliferation of such items to non-State actors;
- Prohibit assisting or financing such proliferation, and to take and enforce effective measures to control these items, in order to prevent their proliferation.

1.C.4. Non-Binding Agreements

In addition to these legal agreements, a number of voluntary agreements exist that encompass nuclear security. Included in these are a number of guidance documents released by the IAEA related to the security of nuclear and radiological materials, two of which are the most significant. The first document is "The Physical Protection of Nuclear Materials and Nuclear Facilities" (INFCIRC/225/Rev. 5)" which provides guidance for States in establishing physical protection systems. INFCIRC/225 covers the physical protection of nuclear materials in use, storage and transport. Its recommendations have been incorporated into the domestic laws of many States. While typically non-binding, the provisions in INFCIRC/225 are required for Agency-sponsored cooperation and assistance programs.[21] The second IAEA publication is the "Code of Conduct on the Safety and Security of Radioactive Sources" (IAEA/CODEOC/2004), which recommends the establishment and maintenance of regulatory controls over all radioactive sources that may pose a significant threat to individuals, society, and the environment.[22] As of June 30, 2008, 92 States had written the IAEA stating that they fully endorse the code of conduct.[23] A comprehensive list of the binding and non-binding legal instruments related to nuclear security are available at http://www-ns.iaea.org/security/legal_instruments_list.asp?s=4&l=28.

1.C.5. The IAEA's Role

Some States with nuclear and radiological material lack the necessary expertise or resources to effectively secure their nuclear infrastructure. In addition to releasing guidance documents, the IAEA assists States, upon request from that State, to evaluate and help improve the State's nuclear security regime. Through its advisory services, the IAEA assists requesting States in establishing the infrastructure required to protect against nuclear threats. The Agency also assists States in their ability to detect and respond to nuclear terrorist activities, and identify potential threats and vulnerabilities to nuclear and radiological materials.[24]

I.D. Research Motivations

The international nuclear security regime faces two major obstacles. The first is that there is no international standard or verification regime for securing nuclear materials. Second, it is up to each State to determine what level of nuclear security is adequate. The nuclear security summits are part of a larger, international awareness campaign designed to demonstrate to States that nuclear security threats are urgent and require their attention. However, even if a State acknowledges nuclear terrorism as a significant security issue, it may not take precedence over other issues that threaten their national security. Naturally, a State with issues like famine, corruption, or disease may be reluctant to devote resources to securing nuclear materials instead of addressing these other issues. Therefore, it is imperative that States have the means to fully understand the threat of nuclear terrorism as it pertains to other national security issues. Additionally, nuclear security is costly and there is no global consensus on what security measures are optimal as each situation is unique to the threats and nuclear activities specific to that State. When addressing the threat of nuclear terrorism, States need assurance that the limited resources they devote to nuclear terrorism are used in the best way to reduce their risk.

When States do not have the means to devote towards nuclear security, they can request assistance through the IAEA. The IAEA's nuclear security efforts are largely dependent on voluntary contributions to its Nuclear Security Fund, which has a somewhat detrimental effect on the IAEA's ability to most effectively allocate resources for nuclear security assistance. Between 2002 and 2004, approximately 89% of the IAEA's nuclear security activities were supported by voluntary contributions. Many of the voluntary contributions came with stipulations on how the contributions could be used. In 2002 and 2003, less than five percent of the contributions were provided without conditions. The result is that the IAEA is not always able to direct funding to areas where it is most needed. The United States, the largest single contributor to the IAEA's Nuclear Security Fund, has expressed concerns over the lack of results-oriented reporting on how contributions are used.[25] To date, the IAEA has not developed a satisfactory approach that measures the effectiveness of its nuclear security services.[26] However without a transparent, results-oriented mechanism to report back to donors, the IAEA is limited by restrictions placed on funds. In the 2006-2009 nuclear security progress report, the IAEA stated that "the need for programmatic prioritization is, to a certain degree, overtaken by the specific conditions assigned by a State providing financial contributions to the Nuclear Security Fund. Separate contributions agreements have been negotiated with donors, taking into account programmatic considerations as well as wishes and conditions by the donor State or group of States."[27]

I.E. Research Objectives

The primary objective of this research is to develop and demonstrate a methodology for assessing State-level risk that can provide recommendations for nuclear security measures based on their risk reduction value. An objective security risk metric can have a number of potential benefits. One benefit is that applying the methodology to a State's nuclear infrastructure can yield a concrete justification for why certain nuclear security measures should be employed in a State. The risk-metric can also be used to request additional funding or support for the implementation of improved nuclear security measures through objectively demonstrating the benefit of the proposed measures. Additionally, the ability to determine each State's performance through a State-level risk metric can be used as justification when directing funding to the State or States where funds would have the maximum impact. Lastly, a methodology of this sort would allow a State to better understand the impacts of risk transfer when modifications are made to security systems. For these reasons, a methodology that addresses the impact of all of the potential nuclear security measures across the entire nuclear infrastructure of a State will be a powerful tool that can assist the IAEA and member States to most effectively secure the nuclear sector.

I.F. Overview of Chapters

In this chapter, we provided background information on nuclear terrorism and the international nuclear security regime. We also described the objectives and potential implications of this research.

Chapter II explains the theory behind the solution method for determining a State-level risk metric. It includes background information on security risk analysis and a summary of recent work applicable to nuclear security.

In Chapter III, the solution method is explained. This includes an overview of the methodology, including assumptions and limitations. It also describes what information is required and how it is used to determine a State-level risk metric.

In Chapter IV, we show the results of verification and validation tests conducted on the code. Because no benchmark data exists, this methodology cannot be validated in the traditional sense. Instead, we demonstrate that the code acts as expected and that given problems where the solution is intuitively obvious, the code produces the correct result.

In Chapter V, we introduce three fictional States having varying complexities of nuclear infrastructures. We then simulate a variety of State-level nuclear security strategies and evaluate their effectiveness. Finally, we present the results of the tests conducted on these States.

We finish our discussion in Chapter VI with a summary of results as well as general conclusions and recommendations.

CHAPTER II

SECURITY RISK ANALYSIS

Security Risk Analysis (SRA) is a well-established practice that facilities and enterprises use to verify that they are sufficiently protecting assets. A variety of methods exist that are used to assess the vulnerability and risk from potential threats.[28] The application of SRA can provide a consistent and repeatable process to analyze security risks, provide useful insights into potential vulnerabilities, and assist in determining the most effective ways to mitigate these vulnerabilities. SRA results are used as part of a risk-informed decision process and play a vital role in ensuring that risk is being effectively managed.

II.A. Probabilistic Risk Analysis

Every action has risk associated with it. Risk is "the likelihood of specified undesired events occurring within a specified period arising from the realization of a specified hazard."[29] Risk assessments are performed on actions or systems to understand what adverse events could occur and the frequency with which they are expected to occur. Any risk assessment seeks to answer three basic questions:

1. What can go wrong?
2. How likely is it?
3. What are its consequences?

These three basic questions are known as the triplet definition of risk, which was introduced by Kaplan and Garrick in the first issue of *Risk Analysis*.[30] This definition of risk is the basis for Probabilistic Risk Analysis (PRA). PRA is a systematic process that integrates information about design, operational practices, historical information, human interaction, and component reliability to determine likelihood and severity ratings for potential adverse events. PRA was first applied to study the reliability of nuclear reactors in the *Reactor Safety Study* released in 1974, [31] and since has been used as a major tool to assess risks and inform risk management decisions by many government agencies and private companies. [32]

The answer to the first question of a risk assessment requires technical knowledge of possible detrimental outcomes of a given activity or action.[33] There are two methods of answering this question. The first method is deductive analysis, a top-down approach that takes a system failure and analyzes behaviors of that system that could contribute to the failure. The second method is inductive analysis, a bottom-up approach that analyzes the failure of individual components of the system to determine the likelihood of overall system failure.[34] The first question of risk assessments feeds into the second and third questions through developing and quantifying accident scenarios, which are chains of events that link an initiating event to an end-point detrimental consequence. PRA can be performed for either internal initiating events, which are events such as system failures or operator error that occur during the normal mode of operation, or external initiating events, which are events like natural disasters.[33] Accident scenarios are typically represented by event trees and fault trees. Event trees are inductive reliability analysis tools that graphically explore system responses that could occur following some initiating event. Event tree analysis shows all plausible operating paths from an initiating event to illustrate ways in which the system either succeeds or fails. As shown in Figure 2, the likelihood of system success or system failure is determined from the likelihood of success or failure at each subsequent event. The likelihood of reaching each end-state can then be found by simply tracing each branch in the event tree. Fault trees are deductive reliability analysis tools that graphically depict the sequence of events that can lead to an undesirable event. Fault tree analysis can provide a quantitative estimate of system reliability by generating a symbolic logic model of failures and faults. The probability of a fault or failure at each individual component is then combined to determine the probability of some top-level event. An example of a fault tree is displayed in Figure 3[34]. The results from event and fault trees are a set of probability density functions for the expected frequency of occurrence from various adverse events, which typically are represented per year. An example for a nuclear reactor is shown in Figure 4, where each probability density function represents the likelihood of a specific accident type.

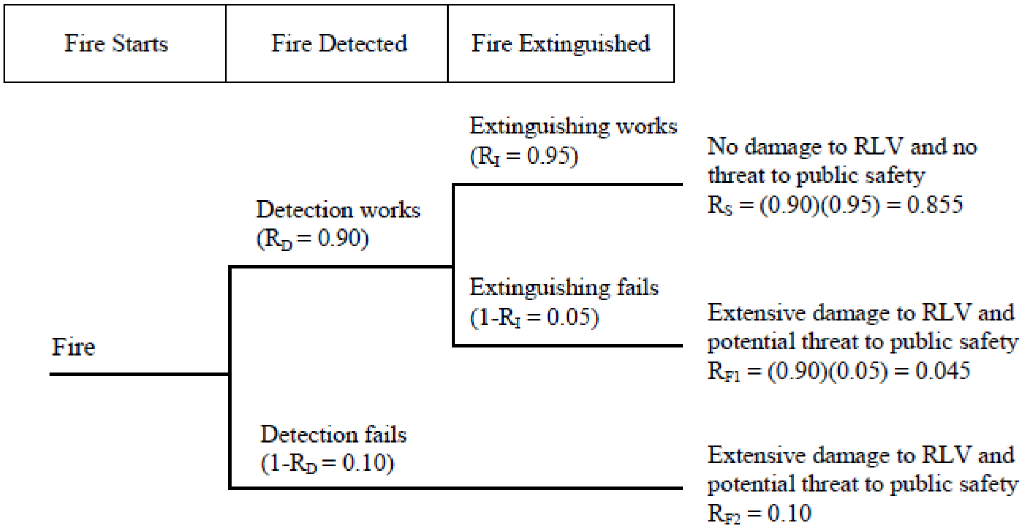


Figure 2. Example Event Tree[34]

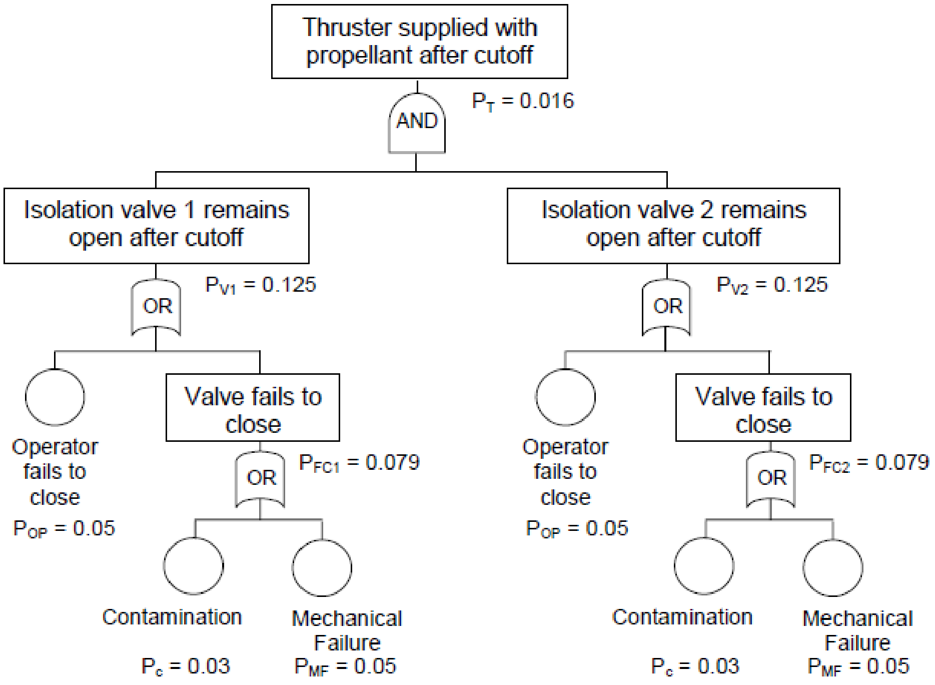


Figure 3. Example Fault Tree[34]

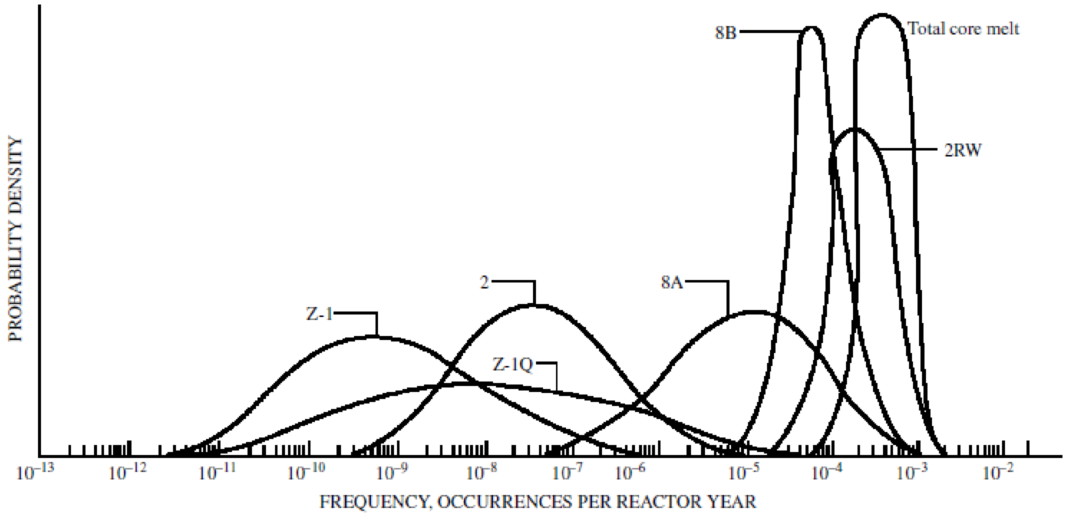


Figure 4. Example PRA Probability Density Function for Nuclear Reactor[29]

The final step of risk assessment is to determine the consequences of adverse events if they occur. These are typically expressed using an attribute that the analyst is trying to prevent, such as expected number of deaths or expected financial loss. For events that have occurred a large number of times, the consequences can be determined from historical data. For events that are rare or have not yet happened, their consequences are determined using models or subject matter experts (SME). The expected consequences of each event are then multiplied by the expected frequency of that event to yield risk. The result is a risk curve, which can be used as a means for comparison to other systems. The risk curve in Figure 5 compares the annual risk of deaths due to various man-made systems.[29]

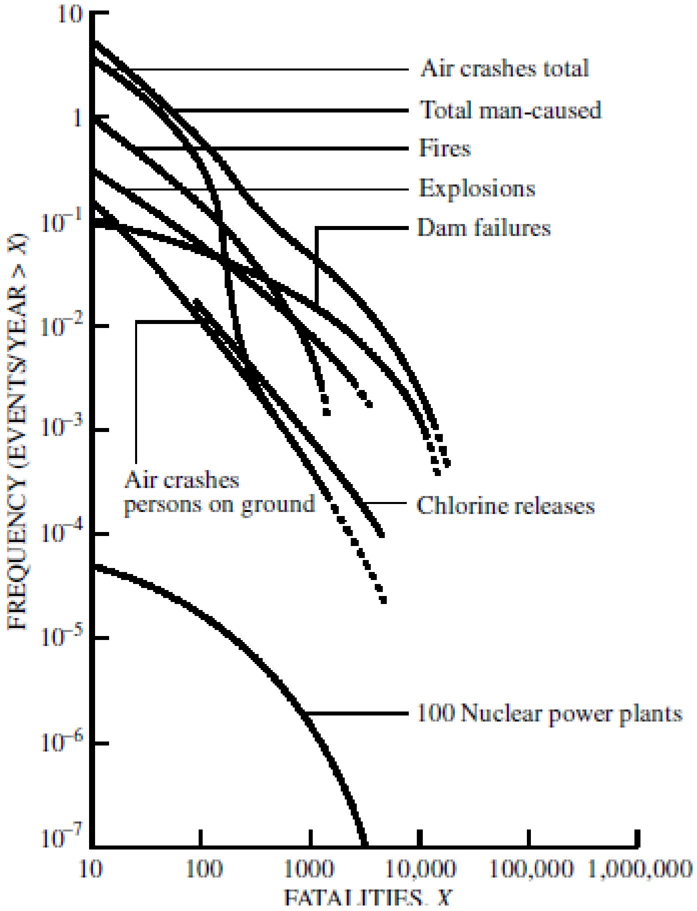


Figure 5. Risk of Fatalities From Man-Made Systems[29]

II.B. Security Risk Assessments

PRA is used to analyze safety risks. However, enterprises must also evaluate security risks. Risk in the context of security carries a slightly different meaning than safety risk, and is defined as "the anticipated consequences over a period of time to a defined set of targets, resulting from a defined set of threats, and considering the vulnerabilities of the specific targets." [35] Unlike safety risks, which include the vulnerability of the system and the consequences of an adverse event, security risks also require the intent to cause the adverse event by some threat. Therefore, security risk exists at the intersection of threat, vulnerability, and consequences.[35] This means security risk can be addressed in three different ways. Security systems can be upgraded to decrease the likelihood that a threat succeeds in creating an adverse event and consequences can be minimized through mitigation techniques. Security risks can also be addressed by minimizing the capabilities and intentions of the threat to cause an adverse event. In the context of terrorism, counterterrorism is the strategy applied to decrease the threat.

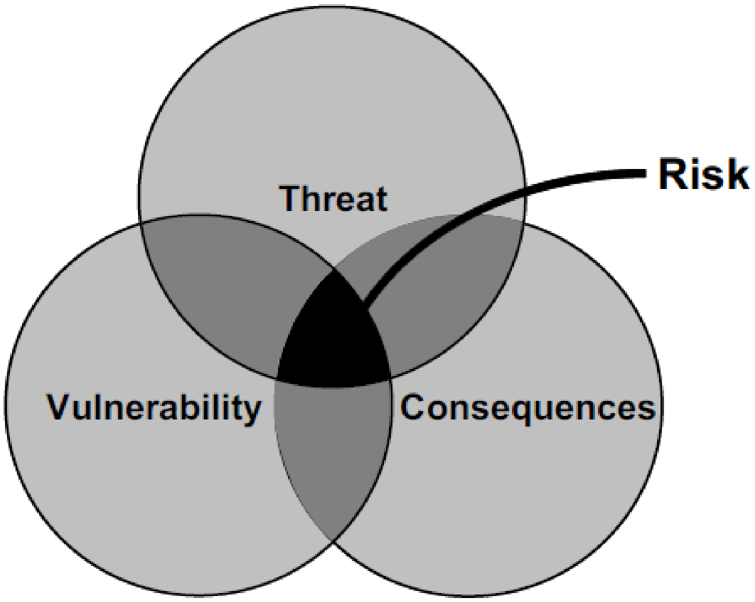


Figure 6. Security Risk is the Intersection of Threat, Vulnerability, and Consequences[35]

Much like with PRA, the triplet definition of risk is consistently used as a common framework for SRA, evidenced by its utilization in government agencies and private sector organizations such as the U.S. Nuclear Regulatory Commission (NRC), the National Aeronautics and Space Administration (NASA), the U.S. Department of Energy (DOE), and most of the nuclear electric utilities.[36]

In SRA, the first question of risk assessment, *"What can go wrong?"*, is addressed similarly to that of PRA. For nuclear terrorism, this question has already been answered by the four threats introduced in Chapter 1. However the second question *"How likely is it"*, is much more difficult to address. Typically, this question is broken down to *"How likely is it that an adversary decides to attack?"* and "*How likely is the adversary to succeed given they initiate an attack"*.[28] The likelihood an adversary decides to attack is the initiating event of SRA. Unlike PRA, where an initiating event is a random, uncontrollable event, initiating events in SRA are the result of strategic and planned decisions made by an adversary. The adversary can purposely act in deceptive or unpredictable ways and can alter their attack strategy based on countermeasures taken by the defender. Because an intelligent adversary can make strategic decisions, the likelihood they decide to attack will depend to some degree on the likelihood they will succeed. The likelihood an adversary succeeds depends on the attack scenario they plan, their resources, and their capabilities. For many high security facilities, such as nuclear facilities, the lack of data on previous attacks requires SRA to rely on the characteristics of potential adversaries, which is derived from the intelligence community. The intelligence community continuously monitors and assesses the activities and capabilities of different terrorist organizations, both domestically and internationally. This information is evaluated in an attempt to determine the capabilities, resources, and intentions of terrorist organizations and how these translate into their decision to attack various targets. However, this intelligence information can be incomplete or inaccurate. Additionally, given the same information analysts can disagree on the likelihood that an adversary will attack, which was conveyed by Figure 1 in chapter 1. Therefore, an essential aspect and an ongoing challenge in SRA is how to best incorporate relevant intelligence information into meaningful inputs.[32]

The final question in SRA, *"What are the consequences?"*, are solved similarly to PRA, employing the use of consequence models and SME. However, the adversary adds additional complexity to the problem. For example, the potential safety consequences of exposure to a strong radiological source, like a Cobalt-60 teletherapy unit, are straight forward to calculate because it is fixed and enclosed a heavily shielded container. The consequence analysis therefore only has to consider the effectiveness of well defined safety features against a bounded set of potential accident scenarios. Conversely, the security risks of that same source are much more complex to analyze. In the security context, the consequences now depend on who decides to steal the source, what capabilities they have to weaponize the source, and what targets they may decide to attack. This requires the analysis of an essentially unbounded set of attack scenarios, all of which may have very different consequences.

Though fault trees and event trees have been employed in SRA, the ability of the adversary to optimize his attack strategy and adapt to security upgrades necessitates different modeling techniques that can better capture this dynamic relationship. A combination of models are typically applied to SRA problems to determine the second question of risk analysis, "*How likely is it?"*. Three mathematical methods commonly used to determine the likelihood that an adversary will attack are Bayesian network analysis, multiple attribute utility analysis, and game theory. The probability of success given an attack is determined using pathways analysis. In many cases measured data either does not exist or would be impractical to determine, and SME are employed to provide informed data to use in these mathematical methods.

II.B.1. Bayesian Network Analysis

A Bayesian network (BN) is a graphical representation of the probabilistic relationships among variables of interest. The relationships between variables are expresses using Bayes' Theorem, which calculates the probability of one event occurring based on whether a prior event has occurred. If both A and B are events, and the probability of each event occurring respectively is known, if B occurs then the probability that A occurs is determined using Bayes' theorem in Equation 1.

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \qquad (1)$$

BNs assimilate information that can be either measured (objective information) or inferred (subjective information). Bayesian networks offer the ability to combine objective and subjective data and update results as new threat data is received. BNs also account for subjective assessments of how intelligent adversaries may modify future attack strategies and deviate from historical patterns.[37] A simple example of a Bayesian network is displayed in Figure 7, where four pieces of evidence about an adversary are assimilated to determine the likelihood that the adversary chooses a particular pathway. Each piece of evidence influences the likelihood of the adversary choosing pathway 1. The input is the degree of belief that each individual piece of evidence is either true or false. Bayes' theorem then assimilates this information into the likelihood of the event based on the evidence provided. As any piece of evidence changes, the network can be updated to reflect these changes and determine the impact of the updated evidence on the event of interest.

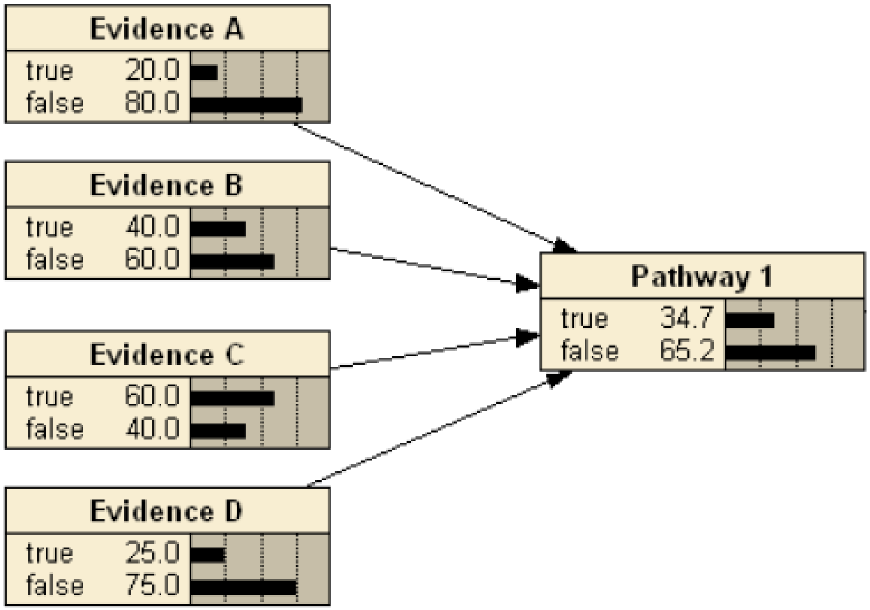


Figure 7. Simple Bayesian Network Using Netica[38]

II.B.2. Multiple Attribute Utility Analysis

Multiple Attribute Utility Analysis (MAUA) [39,40] is a mathematical modeling tool that can assign scores representing preferences among alternative choices in a decision situation. The model assumes that the relative desirability of a particular alternative depends on how its attributes are viewed. Attributes are any measurable characteristic that may influence a decision. For example, attributes for buying a car would be characteristics about cars that the decision maker thought was important, such as price, reliability, safety ratings, fuel economy, color, etc. Each attribute is weighted based on its importance to the decision maker. A utility function is also assigned to each attribute, which represents how the decision maker views that attribute. In the car example, the utility function for gas mileage may be represented by Equation 2, where the utility of a car with gas mileage of 50 mpg would be 1.0 and the utility of a car with gas mileage of 10 mpg would be 0.2.

$$u(x_1) = x_1/50 \tag{2}$$

These utility functions would then be assigned weights based on the relative importance of each attribute to decision maker in making the decision being analyzed. The utility functions and weights corresponding to each attribute can be assimilated in two ways, as the MAUA function has both an additive and multiplicative form. The additive form is given by Equation 3.

$$U(x) = \sum_{i=1}^{n} k_i u_i(x_i) \tag{3}$$

The constants k_i are the weighting factors assigned to each attribute and n is the total number of attributed being evaluated. The multiplicative form of the MAUA function is given by Equation 4.

$$1 + kU(x) = \prod_{i=1}^{n} [k k_i u_i(x_i) + 1] \tag{4}$$

where k is a scaling parameter that satisfies Equation 5.

$$1 + k = \prod_{i=1}^{n}[1 + kk_i] \tag{5}$$

The additive form of the MAUA function is a simplification of the multiplicative form where the sum of all of the $k_i$weighting factors is equal to unity.

The additive MAUA function is essentially a weighted average. This has a potential drawback where the relative impact to the final result is directly related to the value of the weighting factor k_i. If k_i is 0.01, that attribute only has a 1% impact on the final utility value. For security applications, this means that the method will not perform correctly in limiting cases. For example, if one attribute of a terrorists decision to develop a nuclear weapon is the type of nuclear material, and this attribute is weighted with 10% importance compared to other attributes, the difference between weapons usable material with a utility value of unity and uranium ore with a utility value of essentially zero will only affect the overall utility value by 10%. This is not an accurate representation of reality. Conversely, the multiplicative MAUA function behaves differently. For limiting cases where an attribute's utility value approaches unity or zero, it will drive the overall utility value in that direction. This demonstrates correct behavior for limiting cases, however the drawback is that the multiplicative method is less sensitive to changes in attribute utility functions with intermediate values.[41] The use multiplicative or additive MAUA therefore should be based on the characteristics of the decision being analyzed.

II.B.3. Game Theory

Game theory is the study of multiple player decision problems. In security problems, the two players are the terrorists who represent the attacker and the State who represents the defender. An important assumption in game-theoretic models is that the utilities of different consequences must be derivable for each player, which requires knowledge about the adversary's goals and decision process. The use of game theory in SRA is somewhat controversial. It assumes that players are rational and intelligent, which may not be accurate if players are not as sophisticated as they are given credit (e.g. they miscalculate the consequences of their actions). Typically terrorists are modeled as utility maximizers, an assumption that is intended to default to the worst case and therefore add in some conservatism to the results. This makes sense from the perspective that defending against the worst an adversary could do is not a bad thing. However, it can potentially lead to less than optimal allocation of resources. Despite these potential drawbacks, game theory has contributed to a number of studies in SRA, mainly because of its ability to capture the dynamic nature of security problems. These concerns do highlight the importance of understanding what game theory does. Given a set of opponents and their respective goals, game theory yields the optimal way for each player to play the game, not how the game will actually be played. When applying game theory, it is vital to both define the goals of the adversary and defender as accurately as possible, but also assess the impacts of the adversary behaving in less than optimal ways.[32]

II.B.4. Pathways Analysis

Pathways analysis is a systematic technique to analyze the different combinations of actions that an adversary could take to cause undesired events. It requires technical knowledge about how an adversary would accomplish a set of consequences in addition to knowledge about the system being analyzed. Each pathway can be evaluated by breaking it down into the individual tasks required to complete each path. Each individual task is then analyzed to determine the likelihood that the adversary succeeds. Analyzing how the adversary can succeed at each task requires scenario analysis, which details how an adversary will accomplish each pathway task. For example, a pathway element may be that an adversary gains entry into a facility. The subsequent scenario analysis must consider all ways that could allow the adversary to complete this task. Potential scenarios could include falsifying credentials to gain access, analyzing the facility layout to find covert ways to sneak into the facility without detection, or using force to attempt to defeat the guard force. Scenario analysis requires assessments of the adversary's ability to accomplish each of these scenarios, as the adversary will attempt the scenario that gives them the best chance for success.

For complex systems there will typically be a large number of pathways and subsequently an even larger number of scenarios. This may make it impractical to model every potential scenario. In this case, some sort of screening methodology must be introduced to eliminate **t**he pathways that are of least concern. However when not analyzing an exhaustive set of pathways, care must be taken to ensure that the subset of pathways and scenarios analyzed is representative of all potential pathways.

II.B.5. Subject Matter Experts (SME)

A SME is an individual who is an expert in particular field or topic. SME can be applied to a variety of issues in SRA. They can evaluate metrics that cannot be measured with any statistical validity, such as the utility functions of terrorists for MAUA or game theory, or can be employed when acquiring sufficient data on a value would be too costly or time consuming. SME will look at information about a system and give a subjective, qualitative assessment. This can then be translated into a quantitative value to use in SRA. When SME are used to determine likelihood or risk values, the results run the risk of reflecting "classic biases grounded in the nature of the last attack or in a professional familiarity with some terrifying scenarios."[42] Biases can be minimized by eliciting a number of experts in a variety of fields or by eliciting the most qualified experts in each particular field.[42]

II.C. Current Approaches in Security Risk Analysis

While SRA approaches share a common framework based on the triplet definition of risk, they differ based on the specific details that each approach uses to define the threat, how they evaluate the likelihood of events, and the methods used to combine these into meaningful risk calculations. The consensus among the literature is that a SRA approach must meet three key criteria. First, the approach must model the terrorist group as an intelligent adversary that makes strategic decisions to achieve their objectives. Second, the approach must dynamically model proposed security upgrades, allowing the adversary to change their decisions based on where resources are applied by the defender. Finally, the approach must provide results that can be easily communicated to stakeholders. Currently, there are no studies in the open literature that apply all of these criteria to the effectiveness of nuclear security measures at the State level.

An overview of three SRA approaches is provided. These methodologies were selected because they were the most relevant to this work. Other SRA approaches are available in references 44-53.

II.C.1. Design and Evaluation of Physical Protection Systems[28,52]

M. L. Garcia introduces a methodology to design and evaluate the Physical Protection System (PPS) of a facility. The methodology calls for the development of a Design Basis Threat (DBT), which is derived from a threat assessment and defines the details of the threat the facility must protect against. A typical DBT includes information about the threat such as the number of adversaries, their weapons, equipment, training, etc. The DBT is used as a basis to test the components of the security system. The IAEA recommends the use of a DBT as the basis of a State's physical protection system at nuclear facilities.[53] Garcia's methodology requires a very detailed characterization of the facility being tested, down to the level of the construction materials in each building, and any security equipment installed on all fences, walls, doors, etc.. Once this is done, the methodology divides the facility into layers, with the outer layer typically being offsite and the final layer being the location of a target. Layers are definable areas between a location off-site and the target on-site. For a simple facility, this will typically include at minimum the layers shown in Figure 8.

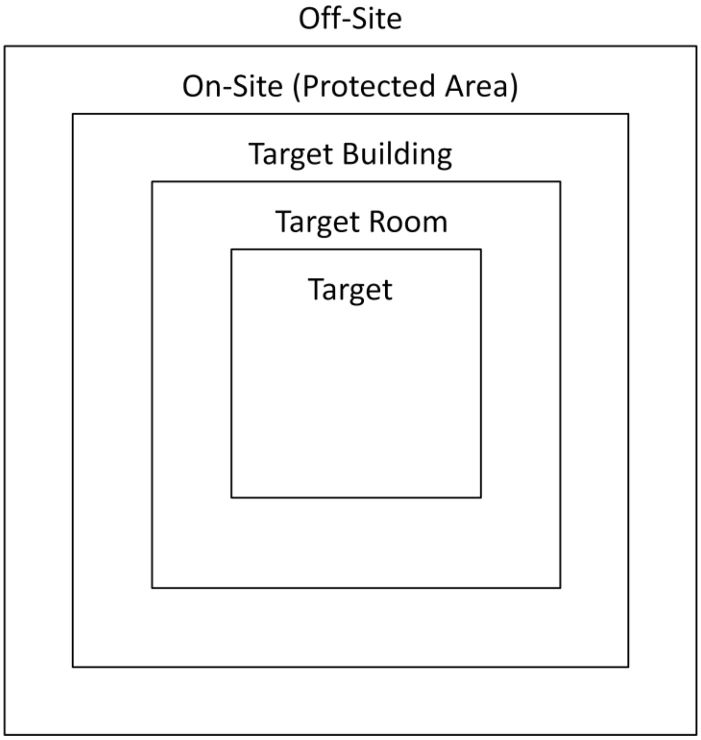


Figure 8. Security Layers Diagram

The features that make up the border between each layer are then defined. For the example in Figure 8, a fence and gate typically define the barriers that separate off-site and on-site. Additionally, the target will likely be stored in a vault or safe in the target room. The next step is to determine the time it would take to breach each layer, which is referred to as the delay time. Adding the delay times at each layer yields the time required to go from off-site to the target, which is the total adversary task time (TATT).

In addition to installed features, the security system relies on a response force, which could be on-site guards or the local police force. The response force is described by two pieces of information. The first is the response force time (RFT), which is the time it will take the response force to respond to an alarm. The second is the probability of neutralization (P_N), which is the probability that the response force can defeat the adversary defined in the DBT. The RFT is used to determine the critical detection point (CDP), which is the last security layer where TATT remaining is greater than RFT. The CDP is therefore the last point at which the adversary can be detected to allow the response force to interrupt the adversary. For example, if it will take 120 seconds for an adversary to breach a safe to get to the target and RFT is 100 seconds, as long as the adversary is detected attempting to open the safe the response force can interrupt them. However if RFT is 150 seconds, even if the adversary is detected opening the safe they will have achieved their goal before the response force arrives.

The CDP is then used to determine the probability of interruption (P_I), which is the probability the response force will interdict an adversary attempting to reach the target. This requires the security elements that detect the adversary breaching each layer to be defined. P_I is then determined by finding the joint probability of detection for each layer outside the CDP.

P_I and P_N are used to calculate the effectiveness of the security system, represented by P_E, the value of which is determined using Equation 6. P_E is a quantitative value representing the effectiveness of the security system and is equivalent to the probability that an adversary succeeds given they decide to attack.

$$P_E = P_I P_N \tag{6}$$

Risk can then be calculated using this value and incorporating the probability the adversary decided to attack (P_A) and the consequences of a successful attack (C)

$$R = P_A * (1 - P_E) * C \tag{7}$$

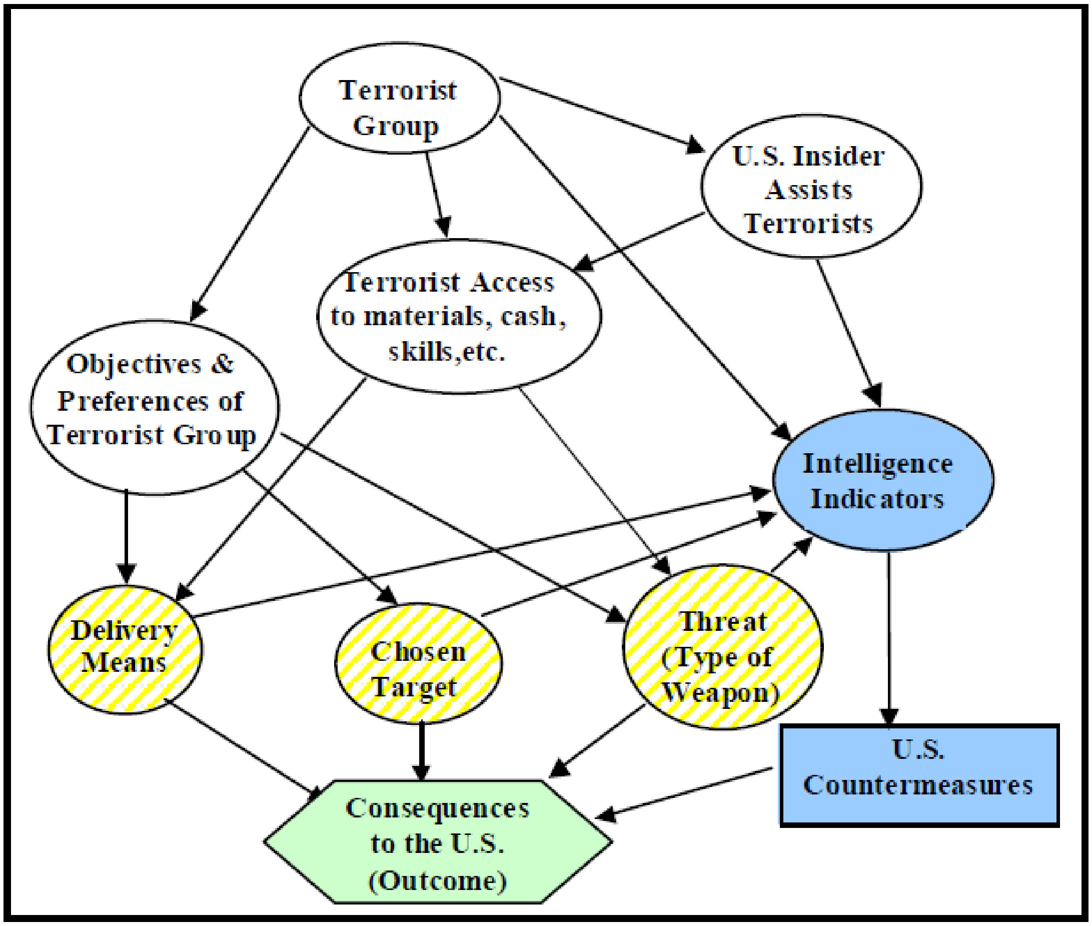
The major strength of this approach is that all of the values used to determine P_E can be based on measured data. All detectors can be tested to determine the probability of detecting an adversary passing that detector, barriers can be tested to determine how long it takes to breach each barrier, and the response force and adversary force can be modeled to simulate P_N. This aspect of the methodology is one of the main reasons it is the basis of the approach employed at US nuclear facilities to calculate the probability the adversary will succeed if they attack.[54]

While this methodology calculates a very precise value for the probability the adversary succeeds given an attack, the probability that the adversary decided to attack cannot be treated with the same precision. As a result, the application of this methodology is most useful for calculating conditional risk rather than absolute risk. In addition, everything in Garcia's methodology is based on the DBT, meaning the security system may be sensitive to changes in the DBT.[55] Also, this method is strictly a facility based approach, meaning the risk at each facility is considered in isolation. When looking at risk from the State-level, it is imperative to understand how upgrades at individual facilities affect risk to the State as a whole. Security upgrades at a particular facility will decrease the risk at that facility, but may simply cause the adversary to attack somewhere else causing the risk to other facilities in the State increase. This transfer of risk within the State could offset any risk reduction value received by upgrading the one facility, negating or minimizing the benefit of these resources on the State-level risk.

II.C.2. Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures[42]

Pate-Cornell and Guikema introduce an approach that incorporates risk analysis, systems analysis, decision analysis, and game theory that can be used to evaluate countermeasures intended to address terrorist threats from a national level. The approach used multiple levels of systems analysis in order to be detailed enough to support decisions among various countermeasures. At the highest level, Pate-Cornell and Guikema introduce an overarching model that consolidates the massive amount of information about the different threat scenarios and the objectives and capabilities of different terrorist groups. The top level model is used to determine the targets adversaries will choose and an assessment on the effects of different attacks on these targets. The second-level system analyzes the potential targets to determine the vulnerabilities of each of them. At this level, the interdependencies among various networks and systems (for example the dependency of communications systems on electric power) that could be potential targets are captured in order to identify the most effective measures to increase the robustness of these systems. The third level assesses the consequences of various attack scenarios. The main objectives of the model are to determine the priority of U.S. infrastructure components that need to be strengthened, the most effective ways to reduce the capabilities of the threat, and prioritize what types of intelligence information should be collected.

The top level model is represented by the influence diagram in Figure 9. The influence diagrams show the variables that affect the respective decisions of different terrorist groups and those of the U.S. The first step in the analysis is to probabilistically combine the actions of different terrorist groups with assessments of their objectives and the consequences to U.S. interests. This step identifies all classes of attack scenarios, essentially answering what can go wrong. It then assesses the likelihood that these classes of scenarios will occur based on the intent, chance of adversary success, and relative attractiveness to the terrorist. These attack scenarios are then prioritized based on their likelihood and expected damage to the US if they occur (based on the U.S. point of view). These three steps satisfy the three essential questions of risk analysis. The final step is to model the dynamics of the problem as a game, by periodically updating the model with new information to represent learning by both the terrorist organization and the State defender.


Terrorist Group
U.S. Insider Assists Terrorists
Terrorist Access to materials, cash, skills,etc.
Objectives & Preferences of Terrorist Group
Intelligence Indicators
Delivery Means
Chosen Target
Threat (Type of Weapon)
U.S. Countermeasures
Consequences to the U.S. (Outcome)

Legend: Oval nodes: uncertainties about events and random variables. White nodes: uncertainty about terrorist groups and their activities, including (striped) the elements of an attack scenario. Grey nodes: U.S. side. Square node: decision node. Hexagonal node: consequences to the U.S. of an attack scenario given countermeasures. Arrows: probabilistic dependencies

Figure 9. Influence Diagram Representing an Overarching Model for Prioritizing Threats and Countermeasures

The dynamic, game-theoretic stage of the model uses data that represent the beliefs of U.S. experts regarding the actions and the value systems of different adversaries. This is because the model is built to support U.S. decisions based on U.S. knowledge. The first step in the dynamic portion of the analysis is to assess the expected utility of each attack scenario for various potential adversaries. The utility to each terrorist group is assumed to be the sum of the damages (e.g. casualties inflicted or economic damage inflicted) caused by successfully completing that scenario. The expected utilities are then normalized to provide the probability of terrorist actions for each group, applying the simplifying assumption that each terrorist group only plans one type of attack for each time period analyzed. It is also assumed that the modeled terrorists behave as rational decision makers, choosing scenarios that yield a higher level of utility. At the same time, the disutility[c] of a successful attack based on the U.S. perspective is determined. This dynamic model analyzes the benefits of various countermeasures by modeling how the application of each countermeasure affects the probability of attack or the consequences of an attack.

Pate-Cornell and Guikema then expand this approach to include a two-sides influence diagram, shown in Figure 10. This allows the terrorist utility functions to be modeled independently of U.S. disutility values (equivalent to consequence values). They then apply this method to fictional scenarios and display the results. The first result is the marginal probabilities of different attack scenarios, displayed in Table 2. This is then used to determine the expected disutility to the U.S. of each attack scenario, displayed in Table 3, by combining these probabilities with the consequences associated with each attack scenario.

[c] Utility is the net benefit of some action to the decision maker. Disutility, therefore, is the negative effect (or loss) felt by the decision maker. In security problems, the adversary benefits from damages inflicted on the defender.

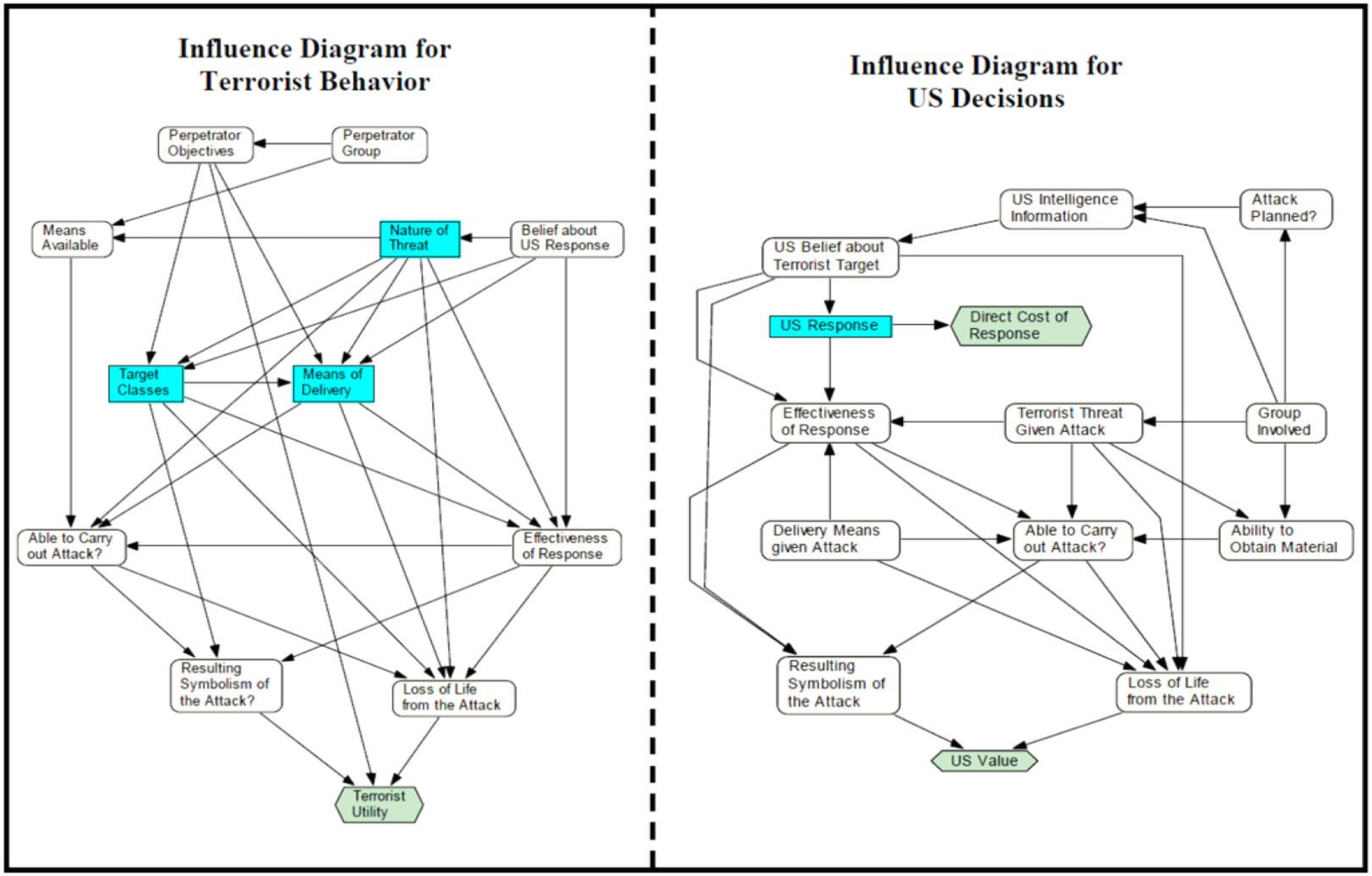
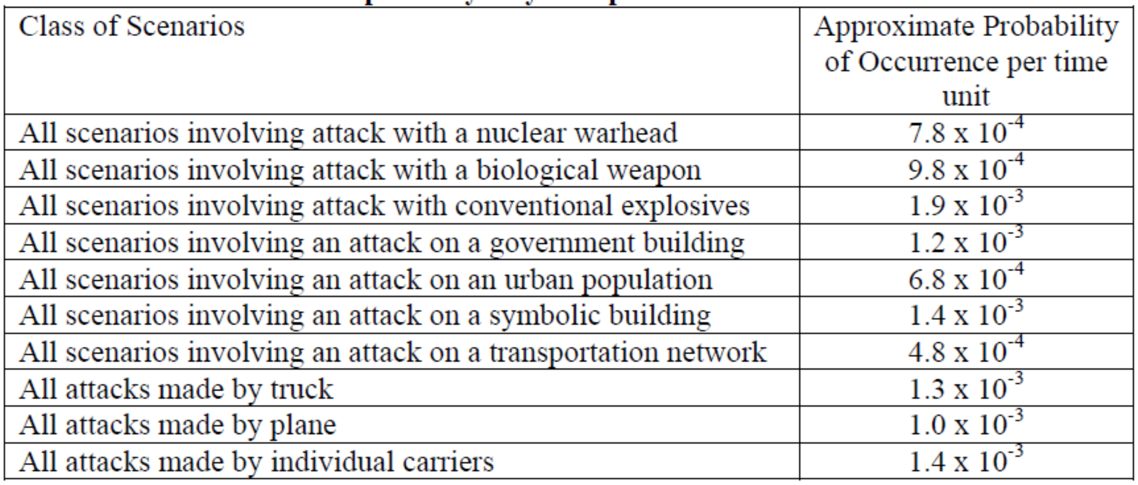

Influence Diagram for Terrorist Behavior
Perpetrator Objectives
Perpetrator Group
Means Available
Nature of Threat
Belief about US Response
Target Classes
Means of Delivery
Able to Carry out Attack?
Effectiveness of Response
Resulting Symbolism of the Attack?
Loss of Life from the Attack
Terrorist Utility
Influence Diagram for US Decisions
US Intelligence Information
Attack Planned?
US Belief about Terrorist Target
US Response
Direct Cost of Response
Effectiveness of Response
Terrorist Threat Given Attack
Group Involved
Delivery Means given Attack
Able to Carry out Attack?
Ability to Obtain Material
Resulting Symbolism of the Attack
Loss of Life from the Attack
US Value

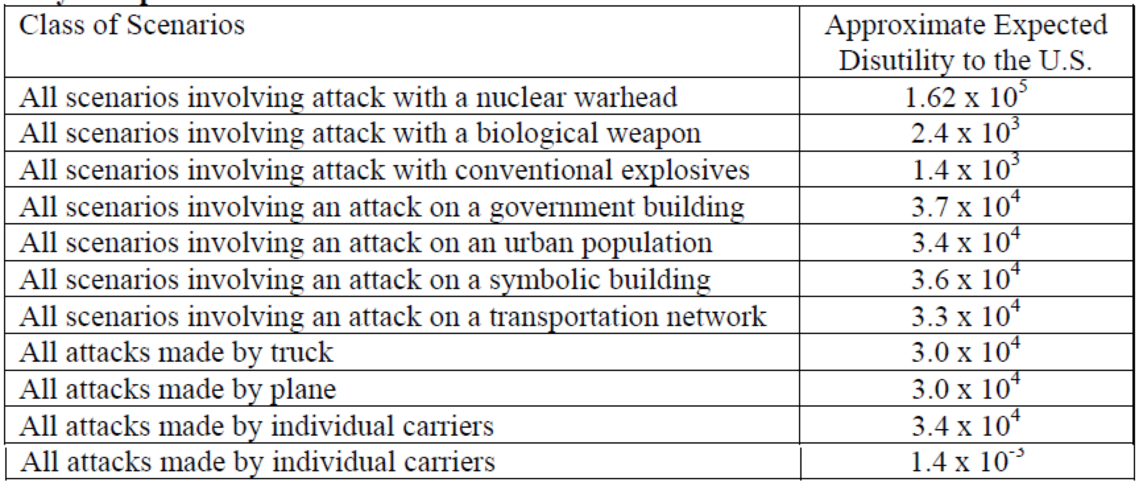
Figure 10. Single-Period, Two-Sided Global Influence Diagram

Table 2. Marginal Probabilities of Attack Scenarios Without Countermeasures (Status Quo)



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

Table 3. Expected Disutilities of Attack Scenarios Without Countermeasures (Status Quo)



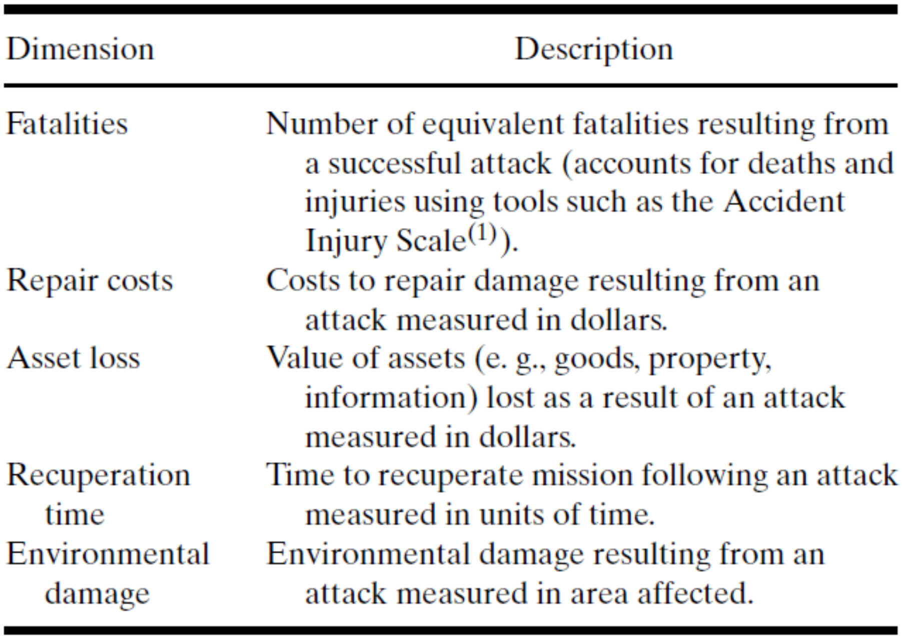
Class of Scenarios	Approximate Expected Disutility to the U.S.
All scenarios involving attack with a nuclear warhead	1.62×10^{5}
All scenarios involving attack with a biological weapon	2.4×10^{3}
All scenarios involving attack with conventional explosives	1.4×10^{3}
All scenarios involving an attack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

The values in Table 2 and Table 3 are then used as a baseline risk value, which is used to determine the cost-effectiveness of various countermeasures by modeling these countermeasures in the system and evaluating the resulting decrease in expected disutility (U.S. benefits).

II.C.3. Risk Analysis For Critical Asset Protection[56]

McGill *et al*. propose an asset-driven risk assessment framework that is intended to assist in deciding how to protect critical infrastructure and key resources. The framework is broken into five steps. The first is scenario identification, where an exhaustive set of plausible threat scenarios for an asset are defined. The second step is the consequence and criticality assessment, where the losses associated with a threat scenario are estimated assuming adversary success. McGill *et al*. propose five consequence dimensions, displayed in Table 4.

Table 4. Asset-Level Consequence Dimensions



Dimension	Description
Fatalities	Number of equivalent fatalities resulting from a successful attack (accounts for deaths and injuries using tools such as the Accident Injury Scale$^{(1)}$).
Repair costs	Costs to repair damage resulting from an attack measured in dollars.
Asset loss	Value of assets (e. g., goods, property, information) lost as a result of an attack measured in dollars.
Recuperation time	Time to recuperate mission following an attack measured in units of time.
Environmental damage	Environmental damage resulting from an attack measured in area affected.

The result of the consequence assessment is the loss (L) given adversary success, calculated using Equation 8.

$$L = L_{mpl} V_P (1 - E_R) \tag{8}$$

where:

L_{mpl} = the maximum credible loss (in units lost per event)

V_P = the physical vulnerability for a given threat intensity

E_R = the effectiveness of response and recovery capabilities

The values in Equation 8 are determined using systems modeling techniques such as event trees or fault trees, or can be elicited from experts knowledgeable in appropriate fields. To determine total losses, the consequence assessment then incorporates the threat intensity using a probability density function for a finite number of threat intensity levels, like the one in Figure 11.

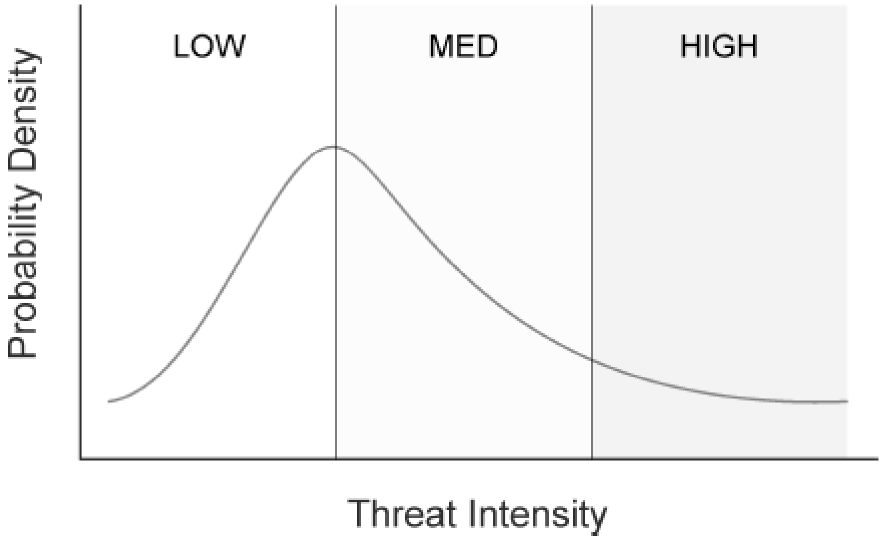


Figure 11. Threat Intensity for a Given Delivery System

The total losses, $\hat{L}$, are then determined using Equation 9.

$$\hat{L} = \sum_j p_j L_j \tag{9}$$

where:

p_j = the probability of imparting threat intensity level j

L_j = the total loss assuming adversary success (from Equation 8)

The consequence assessment is followed by a security vulnerability assessment that evaluates the probability that the adversary is detected and successfully defeated by the security system. The security vulnerability assessment is similar to that of Garcia, calculating the probability of security system effectiveness as the product of the probability of interruption (P_I) and probability of neutralization (P_N). The probability of adversary success is then calculated using Equation 10, which includes the probability the adversary is successful even if the security system fails (P_K).

$$P_s = (1 - P_I * P_N) * P_K \tag{10}$$

The product of probability of adversary success (P_s) and total expected loss for each attack profile ($\hat{L}$) yields the conditional risk (R_C).

The fourth step is the threat likelihood assessment, which assesses the annual rate of occurrence of plausible scenarios. This step is used to take available information about the adversary and translate them into quantitative values that are used to determine the relative attractiveness, the adversary's perceived expected utility, and the actual expected utility for each attack scenario. The final step is a benefit-cost analysis where proposed risk mitigation actions are evaluated based on the ratio of the expected improvement in risk level and the cost of the actions. An overview of these five steps is given in Figure 12.

McGill *et al.* recommend using an annual attack frequency in their model, but point out the inherent difficulty in deriving an accurate estimate for the frequency given the complexity and dynamic nature of security problems. However, they have built the model in a way that they can make calculations based on the relative attractiveness of targets without trying to estimate the frequency of attacks. While no longer yielding a value for total annual risk, ignoring the frequency of attacks will still provide insights into the relative contribution to total risk.

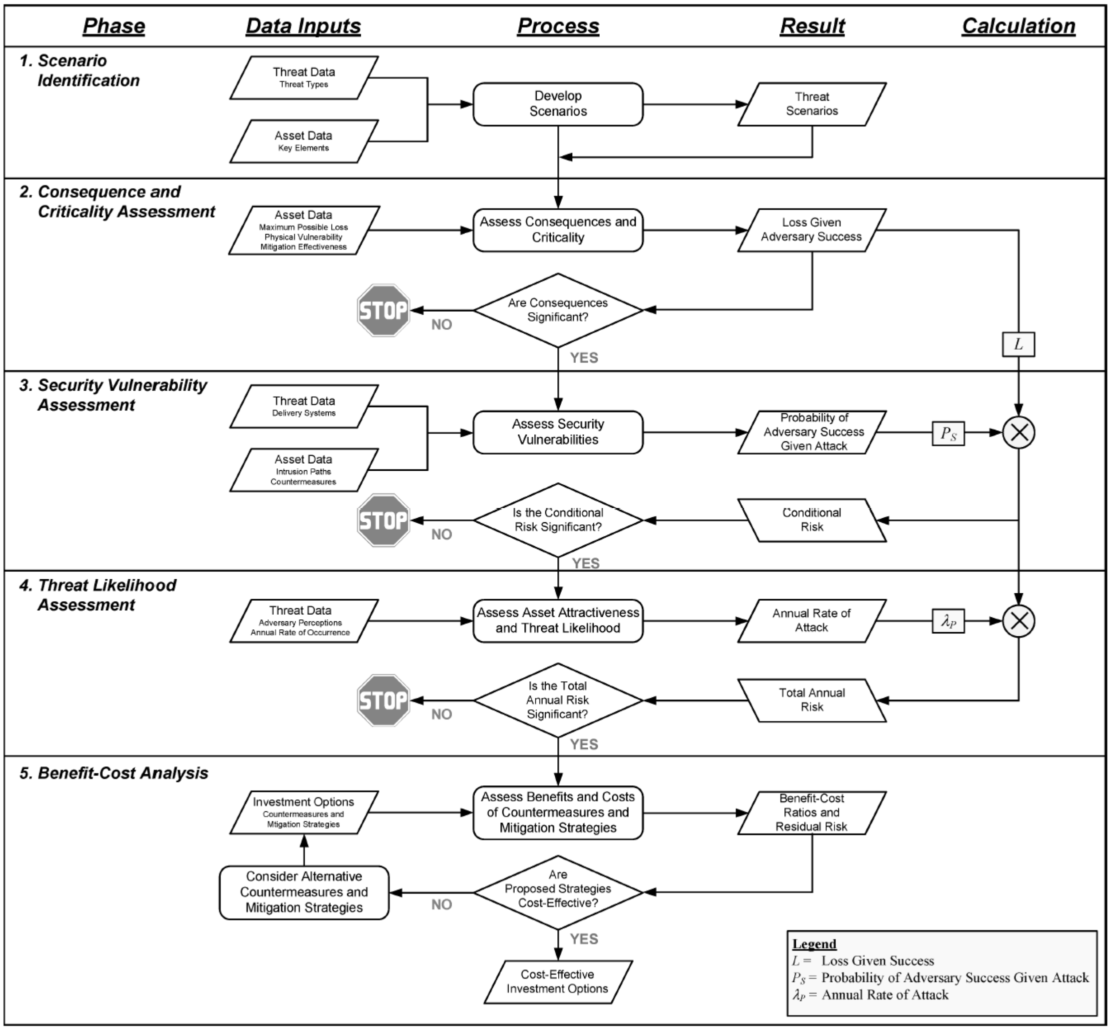

Phase
Data Inputs
Process
Result
Calculation
1. Scenario Identification
Threat Data
Threat Types
Asset Data
Key Elements
Develop Scenarios
Threat Scenarios
2. Consequence and Criticality Assessment
Asset Data
Maximum Possible Loss
Physical Vulnerability
Mitigation Effectiveness
Assess Consequences and Criticality
Loss Given Adversary Success
STOP
NO
Are Consequences Significant?
YES
L
3. Security Vulnerability Assessment
Threat Data
Delivery Systems
Asset Data
Intrusion Paths
Countermeasures
Assess Security Vulnerabilities
Probability of Adversary Success Given Attack
P_S
STOP
NO
Is the Conditional Risk Significant?
Conditional Risk
YES
4. Threat Likelihood Assessment
Threat Data
Adversary Perceptions
Annual Rate of Occurrence
Assess Asset Attractiveness and Threat Likelihood
Annual Rate of Attack
λ_P
STOP
NO
Is the Total Annual Risk Significant?
Total Annual Risk
YES
5. Benefit-Cost Analysis
Investment Options
Countermeasures and
Mtigation Strategies
Assess Benefits and Costs of Countermeasures and Mitigation Strategies
Benefit-Cost Ratios and Residual Risk
Consider Alternative Countermeasures and Mitigation Strategies
NO
Are Proposed Strategies Cost-Effective?
YES
Cost-Effective Investment Options
Legend
L = Loss Given Success
P_S = Probability of Adversary Success Given Attack
λ_P = Annual Rate of Attack

Figure 12. Overview of Asset-Driven Risk Analysis

II.C.4. Literature Summary

The consensus among the literature is that a SRA approach has three key requirements. First, the approach must model the terrorist group as an intelligent adversary that makes strategic decisions to achieve their objectives. Second, the approach must dynamically model proposed security upgrades, allowing the adversary to change their decisions based on where resources are applied by the State. Finally, the approach must provide results that can be easily communicated to stakeholders. Currently, there are no studies in the open literature that evaluate the effectiveness of all State-level nuclear security measures and meet all three of these requirements.

CHAPTER III

METHODOLOGY

III.A. Overview of Methodology

The methodology requires a large amount of information about the state infrastructure and the adversary. There are three major portions that must be defined. These are the adversary characteristics, details about the State infrastructure, and the State's utility functions. Once the necessary inputs are defined, pathways are generated and analyzed. A flowchart of this methodology is shown in Figure 13.

Each of the four threats of nuclear terrorism require an adversary to accomplish a variety of sequential tasks that are specific to that threat. For example, to create an IND the adversary must acquire SNM, a viable weapon design, and the non-nuclear components for that design. Depending on the properties of the SNM that the adversary acquires, multiple processing steps (such as fission product removal, metallurgy, machining, etc.) may be needed before the SNM is weapons usable. Therefore, the characteristics of the nuclear material will dictate what potential pathways the adversary must take to execute one of the four nuclear threats. Because each threat has unique pathways, pathways analysis is used to calculate the risk for each threat. The probability of the adversary successfully completing one of the four threats can be derived from the product of the probabilities of adversary success at each subsequent task along the pathway.

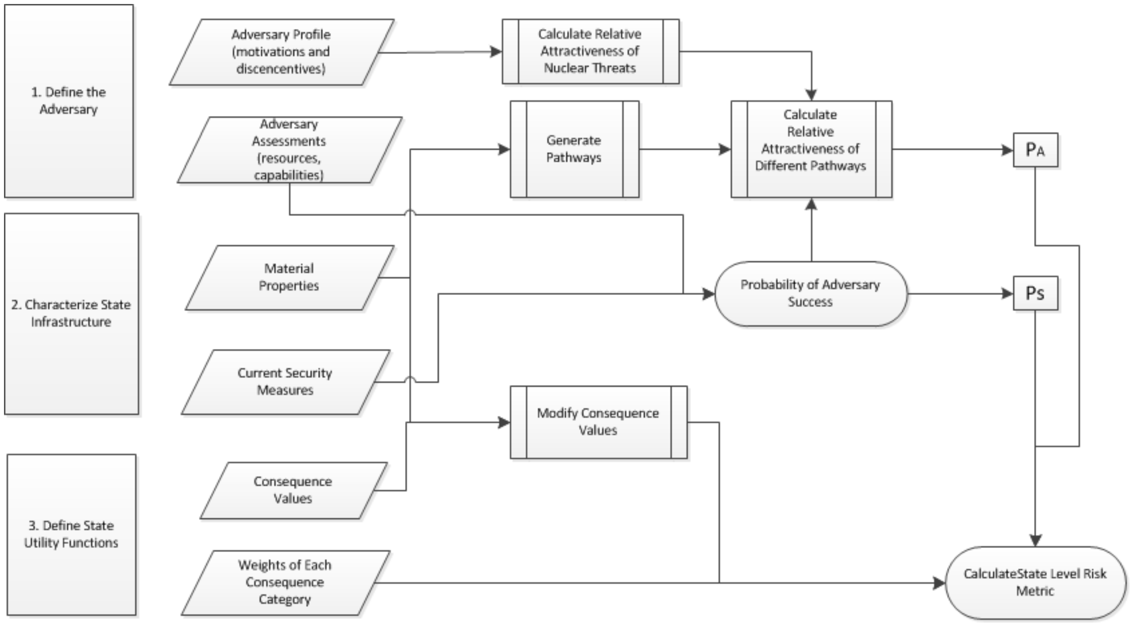

1. Define the Adversary
Adversary Profile (motivations and discencentives)
Calculate Relative Attractiveness of Nuclear Threats
Adversary Assessments (resources, capabilities)
Generate Pathways
Calculate Relative Attractiveness of Different Pathways
P_A
2. Characterize State Infrastructure
Material Properties
Probability of Adversary Success
P_S
Current Security Measures
Modify Consequence Values
3. Define State Utility Functions
Consequence Values
Weights of Each Consequence Category
CalculateState Level Risk Metric

Figure 13. Methodology Flowchart

Each nuclear threat also carries potential consequences that are unique to that threat. This methodology uses four separate consequence categories, which are:

1. Loss of life - the total number of deaths associated with an executed threat;
2. Economic Loss - The net present value of the monetary loss directly or indirectly resulting from an executed threat. (property damage, decontamination costs, business down time, etc.);
3. Loss of Infrastructure - The impact that the loss of a target would have on the ability for society to function; and

4. Secondary Consequences - Consequences that do not fit in the previous three categories but are of significant concern to the stakeholder (e.g. political consequences).

III.B. Methodology Inputs

The essential information about the State's nuclear infrastructure is summarized in this section. The adversary inputs require expert opinion to estimate capabilities and motivations of the adversary.

III.B.1. Adversary Inputs

Adversary inputs are related to their motivations, capabilities and resources. The motivations behind an organization's choices for nuclear terrorism influence the type of nuclear threat the adversary is most likely to choose to achieve their goals. Similarly, an adversary is more likely to attempt a path where the expected benefit of success is worth the potential for failure. The likelihood of completing a path depends on the capabilities and resources of the terrorist group and the perceived benefit of successfully completing the path depends on the group's goals.

III.B.1.i. Adversary Capability and Resource Inputs

The capabilities and resources of a terrorist organization related to nuclear terrorism will be best characterized by the intelligence community, as there is little to no historical data from which to draw conclusions. Capabilities are defined in the code based on the assessed likelihood of a sub-state group to complete various processing tasks associated with different nuclear threats. This assessment would be performed by State intelligence and terrorism SME[d]. For example, to machine weapons usable SNM to a usable shape for an IND, a terrorist group must be able to construct a makeshift facility and acquire the necessary equipment (e.g. a lathe capable of shaping Uranium), acquire the expertise to successfully use the equipment, and do all of this without being detected by the State. The likelihood of successfully machining a part therefore is the product of the probability of creating a facility and successfully using the facility, both without being detected by the State. The tasks defined in the methodology are theft of material, conversion, reprocessing, enrichment, machining, metallurgy, IND weaponization using gun-type or implosion assembly methods, and RDD weaponization. The four inputs associated with each of these are listed in Table 5. Theft of material is not defined in Table 5, because this task is dependent on the particular facility and therefore is captured in the facility inputs.

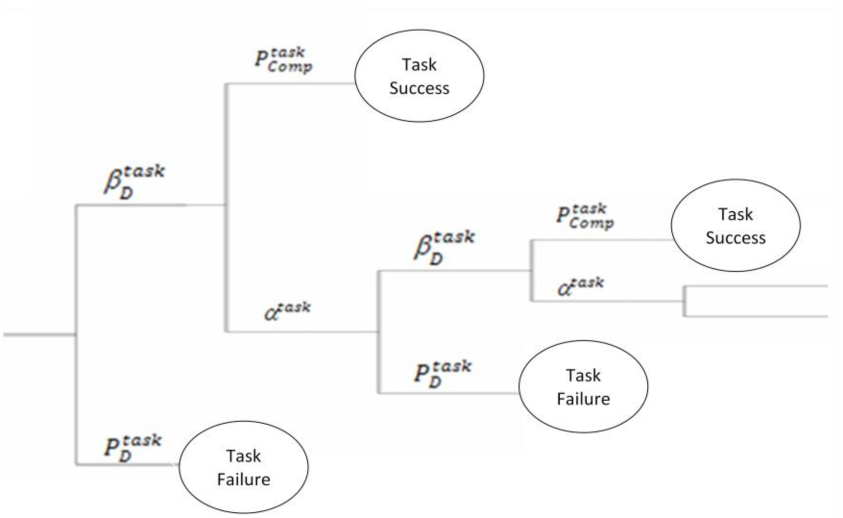
[d] These values should not be considered hard values, but rather educated guesses. The sensitivity of the final risk value to these assumptions is calculated to determine how risk changes based on capability assumptions.

Table 5. Assessed Likelihoods Adversary Capabilities and Resources Inputs

Assessed Task Likelihood	Probability Build	Probability Use	Probability Not-Detected	Processing Attempts
Conversion	P_B^{conv}	P_U^{conv}	β_D^{conv}	N^{conv}
Reprocessing	P_B^{repr}	P_U^{repr}	β_D^{repr}	N^{repr}
Enrichment	P_B^{enri}	P_U^{enri}	β_D^{enri}	N^{enri}
Machining	P_B^{mach}	P_U^{mach}	β_D^{mach}	N^{mach}
Metallurgy	P_B^{meta}	P_U^{meta}	β_D^{meta}	N^{meta}
IND Weaponization: Implosion	$P_B^{IND,I}$	$P_U^{IND,I}$	$\beta_D^{IND,I}$	$N^{IND,I}$
IND Weaponization: Gun-Type	$P_B^{IND,G}$	$P_U^{IND,G}$	$\beta_D^{IND,G}$	$N^{IND,G}$
RDD Weaponization	P_B^{RDDw}	P_U^{RDDw}	β_D^{RDDw}	N^{RDDw}

Breaking the probability of success into constituent parts allows each parameter to be treated individually which more easily reflects areas of weakness or strength of the adversary or the State. For example, a high value for P_B^{task} may indicate weaknesses in the State's ability to enforce export control and dual-use technology laws and a low value for P_U^{task} represents a lack of technical knowledge by terrorist group that is necessary to complete the task. For tasks where P_B^{task} is low, the adversary may seek dual-use facilities within the State's infrastructure if P_U^{task} is sufficiently large and such facilities exist.

These values are used to determine the overall probability of success along a path. The only way the adversary can move on to the next task is if they successfully complete the current task without detection. If the adversary is detected, the State interdicts and stops the threat scenario from progressing. If the adversary fails the task but is not detected, the task can be retried if the adversary has the resources to try again. The resources of the terrorist group are considered in the model by defining a variable, N^{task}, as the maximum number of times that an adversary would be able to attempt a task. Combining this information, the probability of completing a task is determined by the event tree in Figure 14, where the probability of failing the task is denoted by α^{task} and the probability the State detects the adversary is P_D^{task}.



$$P_{Comp}^{task} = P_B^{task} * \; P_U^{task} \qquad P_D^{task} = 1 - \beta_D^{task} \qquad \alpha^{task} = 1 - P_{Comp}^{task}$$

Figure 14. Task Event Tree

The probability of success for an individual task is a geometric series, and can be calculated using Equation 11.

$$P_S^{task} = \left(P_{Comp}^{task} * \beta_D^{task}\right) * \frac{1-(\alpha^{task} * \beta_D^{task})^{N^{task}}}{1-(\alpha^{task} * \beta_D^{task})} \tag{11}$$

Examination of Equation 11 shows that if the adversary has inadequate resources to complete a task (N^{task} = 0), the adversary does not have the capabilities to complete a task (P_{Comp}^{task}= 0), or the State is guaranteed to detect an adversary attempting the task (β_D^{task}=0), then there is no chance of adversary success (P_S^{task} = 0).

III.B.1.ii. Adversary Motivations Inputs

Terrorist motivations are incorporated into the model through Multiple Attribute Utility Analysis (MAUA). Each motivation or disincentive is described in Appendix A[e], along with the terrorist group or groups that have demonstrated each. The input required is how well each motivation or disincentive corresponds to the goals of the terrorist group being modeled. These inputs are summarized in Table 6 and correspond to a weighting value that is applied to the utility functions associated with that motivation or

[e] The information in Appendix A is based on research conducted by Kristin Childress, a Master's student at the George Bush School of Government and Public Service at Texas A&M University

disincentive. For example, if the group is highly motivated by apocalyptic beliefs then the apocalyptic belief input would be "high".

Table 6. Motivation and Disincentive Inputs

Motivation/Disincentive Alignment	**Input**	$\boldsymbol{W_U^m}$
Perfectly aligns with motivating factors of group	High	5
Moderately aligns with motivating factors of group	Medium	3
Slightly aligns with motivating factors of group	Low	1
Does not align with motivating factor of group	None	0

Each motivation and disincentive has been assigned a relative utility value based on how well they indicate the intention of the modeled terrorist group. Each motivation and disincentive has also been weighted based on its relative importance to the decision to conduct nuclear terrorism. The motivations and disincentives along with the assigned weights and utility values are summarized in Table 7.

The weights are designed so that $\sum_{(motivations)} k_m = \sum_{(disincentives)} k_m$. The utility of each nuclear threat is determined by applying Equation 12, where $u_m(t)$ is the utility function value for threat t from and motivation or disincentive m from Table 7 and W_U^m is the scaling weight from Table 6.

$$1 + k * U_t = \prod_{m=1}^{20}(1 + k * k_m[\, W_U^m * u_m(t)]) \tag{12}$$

In Equation 12, k has value 5.00006, which satisfies Equation 13.

$$1 + k = \prod_{m=1}^{20}(1 + k * k_m) \tag{13}$$

The relative likelihood that the adversary will attempt each nuclear threat based solely on how each threat meets the adversary's motivations and disincentives is then determined using Equation 14.

$$U[threat] = \frac{U_t}{U_{NW} + U_{IND} + U_{RDD} + U_{SAB}} \tag{14}$$

Table 7. Motivations and Disincentives for Nuclear Terrorism

Motivations	$\boldsymbol{k_m}$	u_m(NW)	u_m(IND)	u_m(RDD)	u_m(Sabotage)
Prestige of Successful Capabilities	0.25	0.12	0.2	0.02	0.02
Manipulate Adversaries	0.3	0.2	0.2	0.04	0.04
Apocalyptic Beliefs	1	0.2	0.2	0.08	0.1
War on Own Nation	0.25	0.2	0.2	0.1	0.1
War on Another Nation	0.3	0.2	0.2	0.06	0.06
Redress Conventional Military Asymmetry	0.5	0.2	0.2	0.06	0.06
Ensure Security	0.25	0.2	0.2	0.08	0
Mass Devastation/Chaos					
-Deaths	2	0.2	0.2	0	0.02
-Other	1	0.2	0.2	0.1	0.16
Religious Imperative	0.25	0.2	0.2	0.06	0.06
Manipulate Policy	0.2	0.2	0.2	0.06	0.12
Fascination of Nuclear Weapons	1	0.2	0.2	0	0
Fascination of Radiological Weapons	1	0	0	0.2	0
Fascination of Sabotage	1	0	0	0	0.2
Disincentives	$\boldsymbol{k_m}$	u_m(NW)	u_m(IND)	u_m(RDD)	u_m(Sabotage)
Fear of Retaliation on Base of Support	1.25	0	0	0.14	0.06
Fear of Attracting Attention	1.25	0	0	0.14	0.04
Alienation	1.25	0	0	0.06	0.04
Contradict Goals of Group					
-Mass killings	2.25	0	0	0.2	0.18
- Contamination of territory or environment	0.5	0	0	0.12	0.04
Lack of Religious Mandate	0.75	0	0	0.16	0.12
Internal Group Division	1.2	0	0	0.06	0.06

III.B.1.ii. Other Adversary Inputs

Other adversary inputs are:

1. Domestic Group: This is a Boolean input that has a value of true or false, which indicates whether the terrorist group being analyzed is a domestic or international terrorist group. If the terrorist group is domestic, then the latitude and longitude coordinates where they are known to operate are also input if they are known.

2. Consequence Preferences $\{w_a^{LL}, w_a^{EL}, w_a^{IL}, w_a^{SC}\}$: The consequence preferences of the terrorist group being analyzed are a numerical weighting value between zero and unity corresponding to how well each of the four consequence categories represent the group's goals for inflicting damage. An example of consequence weighting for three different groups is given in Table 8. The primary objective of group 1 is to cause loss of life, with secondary objectives being to destroy the State's infrastructure and inflict economic damage. Group 2 is interested in creating mass panic and fear among the State's stakeholders and population through any means necessary, and does not have a preference of how they achieve these objectives. The third group only wants to cause economic losses.

Table 8. Consequence Weights for Sample Terrorist Groups

Consequence Weights	Loss of Life	Loss of Infrastructure	Economic Loss	Secondary Consequences
Group 1	1	0.5	0.5	0
Group 2	0.5	0.5	0.5	1
Group 3	0	0	1	0

3. Risk Attitude: The risk attitude of the terrorist group being analyzed. There are seven options that can be input for risk attitude. Each option corresponds to different weightings for the probability of success and consequences that describe how the adversary evaluates strategic objectives. The seven options are displayed in Table 9.

Table 9. Risk Attitude Exponent Values

Risk Attitude	a,b
Extremely Risk Seeking	5,0
Moderately Risk Seeking	3,0
Slightly Risk Seeking	1,0
Risk Neutral	0,0
Slightly Risk Averse	0,1
Moderately Risk Averse	0,3
Extremely Risk Averse	0,5

III.B.2. State Infrastructure Inputs

The State's nuclear infrastructure is composed of a variety of facilities, including the nuclear fuel cycle and medical and industrial facilities that possess and use radiological materials. Each facility likely has unique security and MC&A characteristics applied to each material that they possess, and the nuclear threats that each material could potentially be used for are dependent upon the material's properties.

III.B.2.i. Nuclear Weapons Inputs

Intact nuclear weapons are the most attractive target for a terrorist group intent on nuclear terrorism. Two inputs are required for nuclear weapons. These are:

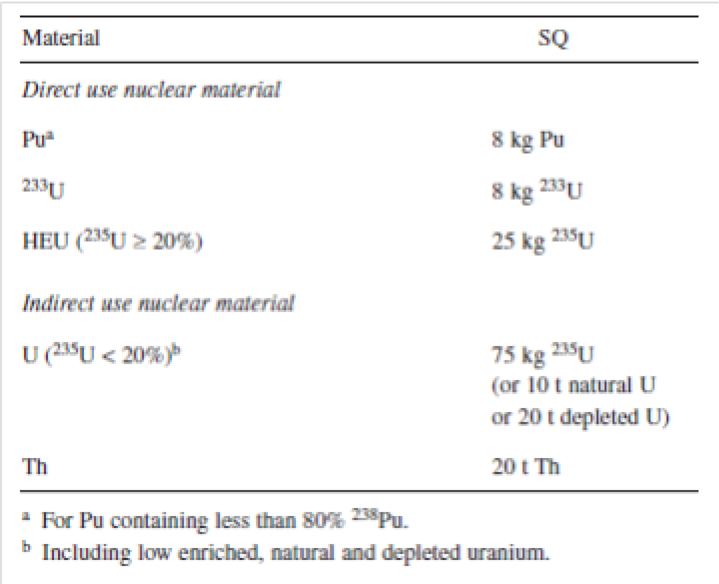
1. Expected yield: $\{Y_E\}$ the maximum designed weapon yield, in kilotons (kT); and
2. Engineered control effectiveness: $\{P_{NSU}^{NW}\}$ If the State possesses nuclear weapons, additional measures used to disable them in the event of a theft must be defined. For example, the effectiveness of PALs or similar control systems employed on nuclear weapons. This is captured by the methodology by defining a probability of non-State use of nuclear weapons.

III.B.2.ii. Special Nuclear Material Inputs

This methodology requires the following inputs to characterize SNM:

1. Number of SQ's: $\{N_{SQ}\}$ The number of significant quantities of uranium or plutonium present at the facility for each type of material. A material is of a different type if it either has significant chemical, isotopic or physical differences or is located in an area of the facility that is under unique security or accountancy systems. For example, uranium oxide and uranium metal stored in the same location are different types of materials and are listed separately. Additionally, if some uranium metal is stored in a heavily secured vault and identical material is stored in a less secure processing location, they are considered two different materials.

   A significant quantity is defined by the IAEA as "the approximate amount of nuclear material for which the possibility of manufacturing a nuclear explosive device cannot be excluded. Significant quantities take into account unavoidable losses due to conversion and manufacturing processes and should not be confused with critical masses." [57] Therefore, at least one SQ of SNM is required for the material to be usable in an IND. The IAEA defined SQ amounts are displayed in Figure 15. Though it has been argued that less nuclear material than the IAEA's definition of an SQ is required for use in a nuclear weapon[58], and that other materials besides those listed could be used in a crude nuclear weapon,[59] for the purpose of demonstrating this methodology we consider only uranium and plutonium. Any other fissile materials of interest could easily be incorporated if desired.



Material	SQ
Direct use nuclear material	
Pu[a]	8 kg Pu
^{233}U	8 kg ^{233}U
HEU (^{235}U ≥ 20%)	25 kg ^{235}U
Indirect use nuclear material	
U (^{235}U < 20%)[b]	75 kg ^{235}U (or 10 t natural U or 20 t depleted U)
Th	20 t Th

[a] For Pu containing less than 80% ^{238}Pu.

[b] Including low enriched, natural and depleted uranium.

Figure 15. Significant Quantities of Nuclear Materials

2. Number of Items: $\{N_I\}$ The total number of a particular type of item present at the facility under identical protection measures.

3. Total Mass Per Item: $\{M_I\}$ The mass of one entire SNM object in kilograms, for example one fuel assembly or one can of UO_2 powder.

4. Activity Per Item: $\{A_I\}$ The total activity of each item in units of Curies. This is used to determine the usefulness of SNM as an RDD material and not used in the IND evaluation.

5. Dose Rate: $\{D_{SNM}\}$ The dose rate from SNM is the quantity of radiation absorbed per unit time. The methodology uses the dose rate in units of Sieverts/hour measured at one meter from the surface of the source.

6. Uranium Enrichment: $\{E_U\}$ Enrichment is the weight percent of the fissile isotope U-235 in uranium. Enrichment affects the production of a crude nuclear device in a number of ways. Primarily, higher enriched uranium requires significantly less material to form a critical mass. This is shown in Figure 16. In addition, nuclear weapons require some amount of assembly time for the SNM to reach its optimal supercritical configuration. For implosion type weapons the assembly time is on the order of 1 μs and for gun-type devices it is on the order of 1 ms. If the fission chain reaction is started before the weapon has reached its final supercritical configuration, usually the result of a spontaneous fission neutron, the device may initiate prematurely leading to a fizzle. If it fizzles, a nuclear weapon fails to reach its designed yield, though it may still result in a significant explosive yield. Uranium-238 has a spontaneous fission rate that is approximately 1000 times greater than uranium-235. Therefore the more U-238 present the greater chance that the nuclear device will fizzle. Figure 17 displays

the probability of a spontaneous-fission-free millisecond in a bare critical mass of uranium based on U-235 enrichment.[60]

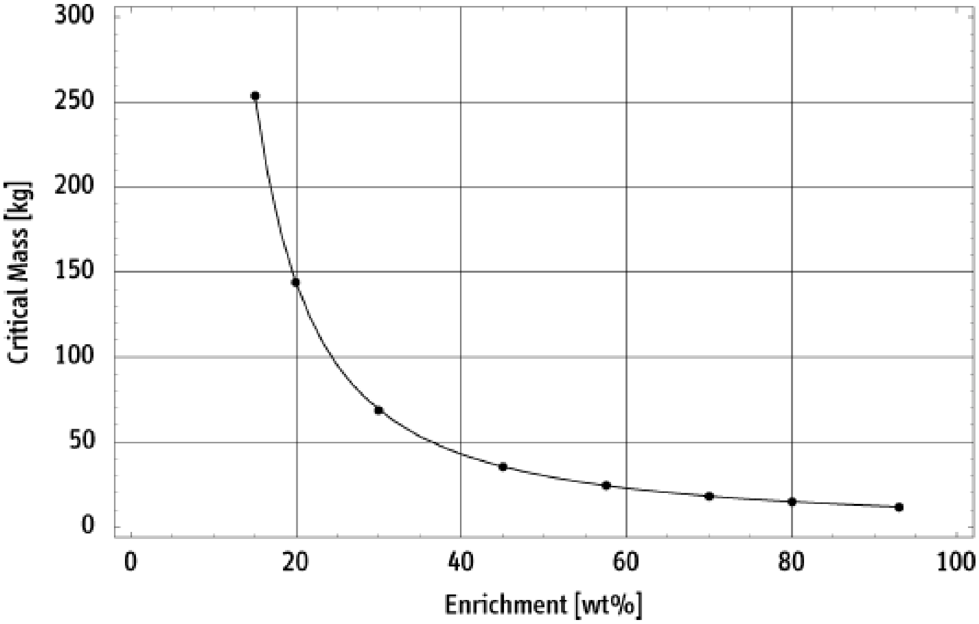


Figure 16. Critical Mass of a Beryllium-Reflected Uranium Sphere As a Function of U-235 Enrichment[60]

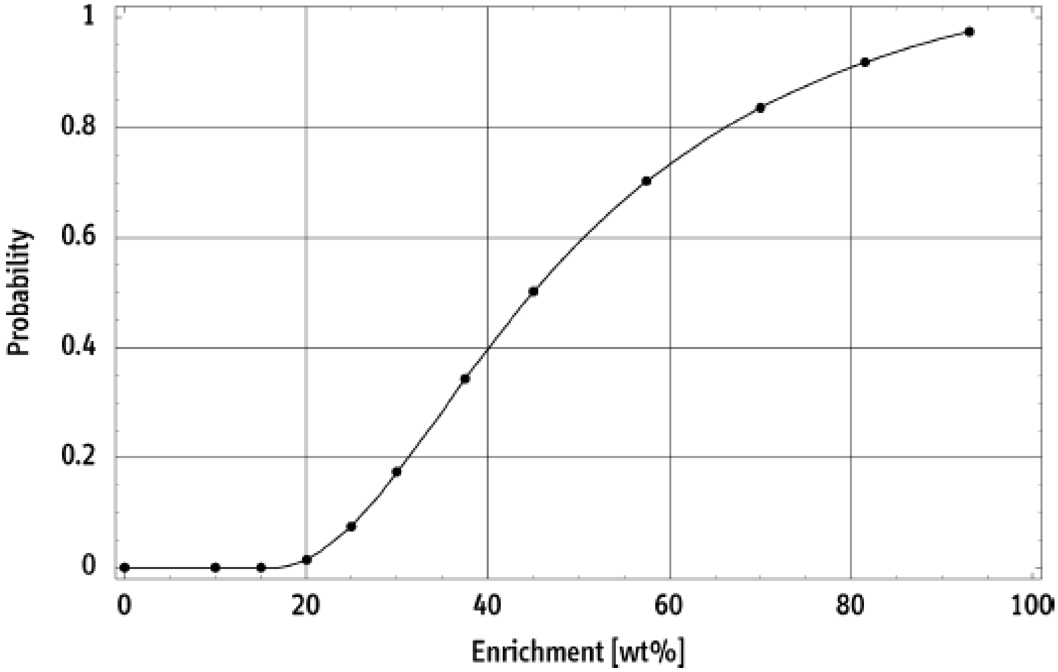


Figure 17. Probability of a Spontaneous-Fission-Free Millisecond in One Bare Critical Mass of Uranium of Varying Enrichment[60]

7. Plutonium Quality: $\{Q_{Pu}\}$ Quality is the weight percent of fissile plutonium isotopes Pu-239 and Pu-241 present in a mass of plutonium. Quality is an important measure for the attractiveness of plutonium for use in a nuclear explosive device for similar reasons as enrichment is for uranium. Like uranium enrichment, lower quality plutonium necessitates a larger critical mass. However the relationship between quality and critical mass, displayed in Figure 18, is not as simple as that for uranium enrichment. [61] With plutonium weapons, the greatest concern is predetonation (which causes the weapon to fizzle), because

the spontaneous fission rate of the fissile isotopes Pu-239 and Pu-241 are similar to that of U-238. Referencing Figure 17, this means that a gun-type device using plutonium is almost guaranteed to fizzle.[60] Implosion type assembly was developed for plutonium to overcome these predetonation issues. As the quality of plutonium gets worse, the predetonation issues become more and more significant.[62] This is because Pu-238, Pu-240 and Pu-242 have spontaneous fission rates approximately 100,000 times greater than Pu-239, Pu-241 and U-238.

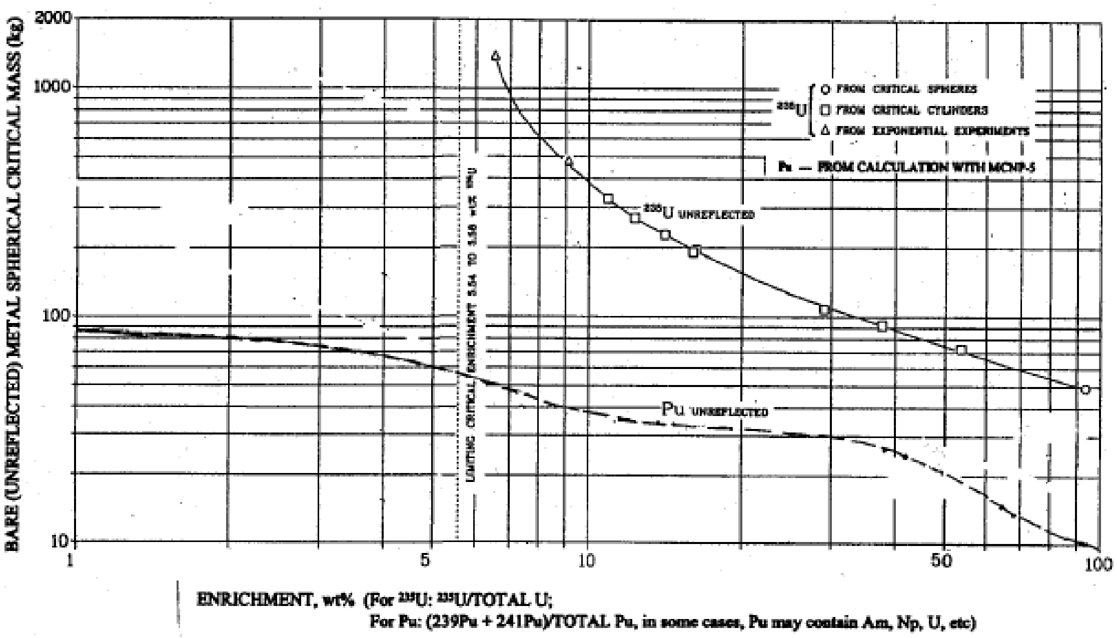


Figure 18. Bare Critical Mass for Unreflected Metal Spheres for Various Qualities of Pu and Enrichments of U

8. Chemical Reactivity With Air: {Fast, Slow, None} Some chemical forms of SNM are chemically reactive with air. If the material has rapid reactions with air it must be kept in an inert atmosphere. If the material slowly reacts (i.e. corrosion or oxidation) it will increase the difficulty in handling and processing that material.[41] The inputs used in this methodology to describe chemical reactivity rates are fast, slow, and none.

9. Requires Active Cooling: {True, False} This input is a Boolean input and can have a value of true or false. Some nuclear materials generate heat and require active cooling to prevent damage and material release. Materials that require active cooling require complex portable cooling systems in order to transport them.[41]

10. Processing Steps Required: Of the many types of nuclear materials present throughout the State's nuclear infrastructure, few if any will be in a form directly usable in an IND. The processing steps required details the types of processing needed to take the material from its current state to a weapons usable metal. The processing steps that could be required are fission product removal, chemical conversion, enrichment, metallurgy and machining. In addition, IND weaponization is always required for any SNM to produce an IND.

    a. Fission product removal, similar to reprocessing in the nuclear fuel cycle, is the removal of fission products from nuclear material, typically spent fuel. In 1978, the United States conducted a feasibility study on the clandestine production of a crude reprocessing plant by a non-nuclear weapons State and concludes that a "quick and simple" reprocessing plant could be built in a matter of months and used to produce enough plutonium for a nuclear device in a matter of weeks.[63] A similar type of facility would be expected to be used by a terrorist group attempting to remove fission products from stolen spent fuel. While the likelihood of a sub-state group secretly constructing and using a crude reprocessing facility is incredibly low, it is non-zero and is considered in this risk assessment.

b. Chemical conversion is the process of converting uranium into UF_6 gas , which is capable of being used in enrichment operations.

c. Enrichment is the process of increasing the weight percentage of U-235 in uranium to make it more attractive for use in a weapon. Currently, few States have the capability to enrich Uranium, which requires large and expensive facilities and some of the world's most sensitive technology. As a result, the feasibility of a sub-state group successfully building an enrichment facility is essentially zero. Enriching uranium is also a very lengthy process and if a sub-state group somehow acquired possession of enrichment capabilities, it would be difficult to complete the enrichment undetected. This processing step is included in this methodology for completeness, as future technology developments may make this process more plausible. In addition, it is useful to know how sensitive risk is to this processing step.

d. Metallurgy is the process of taking various forms of uranium and plutonium and converting them to a metallic form.

e. Machining is the process of taking metallic uranium or plutonium and shaping them for use in a weapon. This process would require advanced equipment, such as precision calibrated, computer-guided machine tools with the ability to produce complex shapes within a very small tolerance.[64]

f. IND Weaponization involves assimilating the weapons usable SNM into a crude nuclear weapons design with the other non-nuclear components. This step can be completed using the simpler gun-type design or the much more technically sophisticated implosion design.

III.B.2.iii. Radiological Material Inputs

This methodology requires the following inputs to characterize radiological materials:

1. Number of items: $\{N_I^{Rad}\}$ The number of individual items of each type of radiological material present at a facility under equivalent security and safeguards.

2. Total Mass Per Item: $\{m_I^{Rad}\}$ The mass of one item measured in kilograms. Typically, radiological sources are stored in shielding containers.

3. Dose Rate Per Item: $\{D_{Rad}\}$ The dose rate from radiological material is the quantity of radiation absorbed per unit time. The methodology uses the dose rate at 1 meter from the source in units of Sieverts/hour from each individual item of radiological material.

4. Activity Per Item: $\{A_I^{rad}\}$ The total activity of each item in Curies. This input is used to determine the relative consequences of various radiological sources.

5. D-value: $\{D_{val}^{Rad}\}$ The D-value, or danger value, is a numerical value used to categorize the relative severity of health effects per unit activity from different radiological sources. The danger value may be applied to accident situations or malevolent acts and is based on the amount of activity required from a given radiological isotope to deliver an amount of radiation dose that causes serious health effects.[65]

III.B.3.iv. Sabotage Inputs

Sabotage is a different fundamental threat than the other threats of nuclear terrorism and is therefore modeled independently. Sabotage requires a single act by the adversary rather than set of sequential tasks. Also, in other threats the adversary has a fabricated weapon that can then be delivered to a choice of targets. Conversely, sabotage scenarios are fixed scenarios, meaning the target is the location of the material itself. Therefore, systems and procedures that mitigate consequences can be installed at facilities and employed with the transportation of nuclear materials that minimize potential consequences. For each sabotage scenario, the following inputs are required:

1. Number of Vital Areas: $\{N_{VA}^{Sab}\}$ Facilities protect against sabotage by identifying vital areas, which are defined as areas "inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences."[66] Each sabotage scenario may have one vital area or multiple vital areas, and therefore the methodology treats each sabotage scenario separately. The vital areas for each sabotage event are input individually and treated as sabotage targets when characterizing the physical security of the facility.

2. Probability of Consequences Given Vital Area Compromise: $\{P_{Cons}^{Sab}\}$ Depending on the scenario there is a possibility that destruction of vital areas may not lead to a radiological consequence. Therefore, the probability that destruction of vital areas leads to the specified consequences must also be defined.

3. Insider Sabotage Mitigation:$\{\varepsilon_{Sab}^{Ins}\}$ This variable corresponds to the ability of installed security systems to prevent employees from executing sabotage threats. This may include human reliability programs, but also includes security systems that prevent access to vital areas or checks employees for tools that could be used in a sabotage event, such as explosives or metallic tools

III.B.3.v. Facility Inputs

Each facility that stores or has the capability to processes nuclear or radiological material has security and safeguards functions that are unique to that facility. Additionally, the geographic location of the facility within the State may be a significant risk factor based on proximity to regions where sub-state groups are known to exist, potentially outside the State's control. The inputs required to characterize the State infrastructure are:

1. Geographic Location: The methodology incorporates the location of a facility through latitude and longitude coordinates. Distances between two locations are calculated using Equation 15.

$D_{1\to 2} = \text{arccos}\,(\sin\left(\frac{\pi*lat_1}{180}\right)) * \sin\left(\frac{\pi*lat_2}{180}\right) + \cos\left(\frac{\pi*lat_1}{180}\right) * \cos\left(\frac{\pi*lat_2}{180}\right) *$

cos$(\pi*(long2-long1)180)*Rearth$

(15)

where:

$D_{1\to 2}$ =the distance between two locations in kilometers

lat_n = the latitude for location n in degrees where north is positive

$long_n$ = the longitude for location n in degrees where east is positive

R_{earth} =6371 km

The distance calculation requires the location inputs to be in degrees, so the longitude of Texas A&M University which is W 96º19'56.71" is -96.3261º. Similarly, the longitude of the IAEA, which is E 16º25'01.25", would be 16.4169º. A State would have the resources to employ graphical information systems (GIS) and develop more accurate transportation routes. For the purpose of demonstrating this methodology, transportation routes are simplified to include straight line distance.

2. Mean Distance Within State: $\{\overline{D}_{fac}\}$ In addition to geographic location, the methodology uses the average distance from the State border to the facility. This is used to determine the relative distance an adversary must travel within the State when targeting this facility relative to other facilities.

3. Physical Security: The methodology requires the number of security layers at the facility, the P_N and P_I values for each layer, and the targets under each layer. The physical security system at a facility defends against an adversary attack attempting theft or sabotage. If the State is using IAEA recommendations, the facility's physical security system should be designed using a layered approach, similar to the facility based methodology presented in Chapter 2 by Garcia. To account for multiple targets being under the same layer, the methodology assigns a unique number to each material at the facility and then takes the P_I and P_N values of each layer and assigns them to each applicable target. An example of the physical security inputs for a facility that has two targets and three unique security layers is given in Table 10.

Table 10. Example Physical Security Inputs

Layer Number	P_I	P_N	Targets Under Layer
1	0.7	0.8	1,2
2	0.8	0.8	1,2
3	0.9	0.8	2

The corresponding effectiveness values (P_E) for each target would then be 0.752 for target type 1 and 0.795 for target type 2. A target can be either be a theft target or a vital area for sabotage. 1-P_E is the probability of the adversary successfully defeating the physical protection system and steals each target.

4. Material Accountancy and Containment and Surveillance: The methodology requires the effectiveness of material accountancy and containment and surveillance (C&S) systems to be defined. These systems defend material against covert theft by an insider, a person with access to the facility who may be able to bypass physical security functions. If in compliance with IAEA safeguards, the State is required to have accountancy measures that can be verified by the IAEA to ensure the State is not diverting material. Material accountancy systems periodically quantify the amount of material present to ensure none has been removed. C&S systems monitor material to ensure it has not been tampered with since it was last assayed using cameras, seals and tags. An example of containment that a facility could employ is to have an active tamper seal on the container where material is stored, which alerts the facility operator whenever someone has access to the material. A common surveillance technique is to employ a two-person rule, where no facility employee ever has unobserved access to material. The probability the adversary successfully diverts material is calculated using Equation 16, where β^{MA} and β^{CS} are the non-detection probabilities for 1 SQ of SNM or 1 item of radiological material of the material accountancy and containment and surveillance systems respectively.

$$P_E^{Divert} = (1 - \beta^{MA} * \beta^{CS}) \tag{16}$$

5. Human Reliability Effectiveness:$\{\varepsilon_{HR}\}$ This value relates to the effectiveness of employee vetting employed by the facility and describes the likelihood that an employee will attempt to divert material, as a result of financial gain or having ideological agreement or association with terrorist groups intent on nuclear terrorism. Though the thoroughness of background checks that the State can conduct may be limited by national law, the lack of background checks on employees is seen as a lapse in security.[67] This value is used to calculate the probability of diversion of material using Equation 17.

$$P_S^{Divert} = (1 - \varepsilon_{HR}) * (1 - P_E^{Divert}) \tag{17}$$

III.B.3.vi. State-Level Inputs

Additional State-level inputs are required to completely characterize the State's nuclear infrastructure. These are:

1. Border Crossing Security Effectiveness: $\{B_{eff}^{ent}, B_{eff}^{ext}\}$ The first input considers the likelihood that a non-domestic terrorist group can infiltrate the State's border.

The second input is based on the likelihood of detecting an adversary leaving the State with nuclear or radiological material.

2. <u>Background Probability of Interdiction</u>: $\{\bar{D}^{BKG}_{Capt}\}$ The mean capture distance by a random encounter measured in km. This input considers the State's ability to interdict an adversary during transportation of material to complete one of the threats. If the adversary acquires material covertly, either through diversion or black market purchase, the State may have passive systems in place that could potentially detect the illicit material. In addition, there is a non-zero probability of the State interdicting the adversary for legal offenses not related to nuclear terrorism that may lead to discovery of the illicit material. These probabilities make up the background probability of interdiction per unit distance. The probability of being interdicted when traveling between two locations is then calculated using $D_{1\to2}$ from Equation 15 and the background probability of interdiction per unit distance in Equation 18.[68]

$$P^{interdict} = e^{\left(\frac{-\bar{D}^{BKG}_{Capt} * D_{1\to2}}{\ln(2)}\right)} \tag{18}$$

3. <u>Active Search Probability of Interdiction</u>: $\{\bar{D}^{AS}_{Capt}\}$ The mean capture distance by a deliberate search by the State. If an adversary overtly steals material or once a covert theft has been discovered, the State can employ additional resources to actively search for the adversary. This variable is independent of the background

interdiction probability and used in Equation 19 calculate the probability of interdiction.[68]

$$P^{interdict} = e^{\left(\frac{-(\bar{D}_{Capt}^{BKG}+\bar{D}_{Capt}^{AS})*D_{1\to 2}}{\ln(2)}\right)} \tag{19}$$

For the purpose of this methodology, these probabilities are assumed uniform for the entire State. However, realistically these values vary in different locations and the State will have the resources and information to more accurately define these probabilities.

4. <u>Processing (Dual-Use) Facilities</u>: Some facilities not within the nuclear fuel cycle may have the capabilities or only require slight modifications to be used to process nuclear or radiological materials. The most obvious examples would be industrial metalworking or chemical processing facilities. For each facility of this type, the type of processing and likelihood of the State detecting illicit activities at that facility should be indicated. The input for the State's probability for detecting illicit activity is independent of the probability of detecting the adversary as defined in the adversary inputs.

5. <u>Target Locations</u>: Target locations require three inputs, which are consequence values, geographic location, and target security effectiveness.

a. The first input is the consequence values for Nuclear Weapon, IND and RDD threats for each of the four consequence categories. Consequence values are numerical values between 0 and 1 that represent the relative severity of threats in each consequence category. The consequences are defined based on the specific scenarios and are scaled according to scenario variations.

    i. For nuclear weapons, consequences are defined for 100 kT weapon detonated at the target and scaled based on variations in weapon yield.

    ii. For IND's, the consequences are defined based on a the detonation of a 10 kT crude nuclear device.

    iii. For RDD's, the consequences are defined for a dispersion using a source with an A/D value of 850 (e.g. 2295 Ci Cs-137, 687 Ci Co-60, 1150 Ci Cm-244, etc.) and scaled using the A/D_{value} and equations in Appendix B.

    iv. Sabotage consequences have already been defined at the facility.

b. The second input is the geographic location of the target. This input is the longitude and latitude of the target and is in the same format as the geographic location of the facility. It is used to determine the minimum distance required to transport the weapon to the specified target.

c. The final input is the effectiveness of security systems employed at the target. This input represents the capability to harden certain high-value targets to provide a last line of defense against potential attacks. { P_{targ} }

III.C. Utility Functions

Utility functions associated with adversary inputs correspond to how well particular threats match with the characteristics of the terrorist group. For material characteristics, each utility function corresponds to challenges that a terrorist group would encounter when trying to develop one of the nuclear threats based on each input or group of inputs. Utility functions are used to rank the relative attractiveness of various pathways to the terrorist group being analyzed. The functions introduced in this section are designed so that the overall utility of each material is equal to the product of each utility function.

III.C.1. Adversary Utility Functions

The MAUA analysis on motivations and disincentives introduced in the previous section is used to determine the relative likelihood of the adversary choosing one of each of the four nuclear threats independent of pathway information. The adversary utility functions introduced in this section are used to determine the relative likelihood that an adversary will choose each pathway. The utility functions incorporate the material attractiveness developed from material inputs, the likelihood of successfully completing the pathway which is based on the adversary's capabilities as well as security measures present in the State, and the adversary's consequence preferences. The risk attitude of the adversary is used to determine how the adversary strategically evaluates the likelihood of success vs. consequences.

The probability of success for J tasks on a pathway is calculated by multiplying the results from Equation 11 for each jth task, shown in Equation 20. For theft or diversion, the value for P_S^j is derived from the effectiveness of security systems employed at the facility.

$$P_S^{Path} = \prod_{j=1}^{J} P_S^j \tag{20}$$

The net consequence for the path based on the adversary's consequence preferences is determined using Equation 21. Because the adversary is attempting to damage the State, we assume the consequences suffered by the State are equivalent to the adversary's perceived payoff from completing the pathway.

$$C_{net,a}^{Path} = \frac{w_a^{LL} * C_a^{LL} + w_a^{EL} * C_a^{EL} + w_a^{IL} * C_a^{IL} + w_a^{SC} * C_a^{SC}}{w_a^{LL} + w_a^{EL} + w_a^{IL} + w_a^{SC}} \tag{21}$$

The risk attitude of the adversary is used to weight the relative attractiveness of various scenarios to the adversary. Given three scenario options with the same expected value, an adversary is expected to choose the option based on their perception of risk. An example is shown in Table 11, where the relative value of each scenario is shown based on risk attitude. The table is populated using Equation 22. The values for a and b are derived from Table 9.

$$U[Scenario] = \left(P_S^{Scenario}\right)^{\left(\frac{1}{a+1}\right)}\left(C_{net,a}^{Scenario}\right)^{\left(\frac{1}{b+1}\right)}\ ;\ P_S^{Path}, C_{net,a}^{Scenario} \leq 1 \quad (22)$$

where:

P_S^{Path} is the probability of completing the path, and

$C_{net,a}^{Scenario}$ is the benefit the adversary receives upon completing the path

Table 11. Pathway Attractiveness Based on Risk Attitude

Value vs. Risk Attitude	**Scenario**	**Scenario 2**	**Scenario 3**
$P_S^{Scenario}$	0.100	0.300	0.900
$C_{net,a}^{Scenario}$	0.900	0.300	0.100
Extremely Risk Seeking	0.613	0.245	0.098
Moderately Risk Seeking	0.506	0.222	0.097
Slightly Risk Seeking	0.285	0.164	0.095
Risk Neutral	0.090	0.090	0.090
Slightly Risk Averse	0.095	0.164	0.285
Moderately Risk Averse	0.097	0.222	0.506
Extremely Risk Averse	0.098	0.245	0.613

Table 11 shows that the risk neutral adversary had no preference between the scenarios, which is expected because each scenario has the same expected value. The more risk seeking the adversary, the more they prefer the scenario with the highest consequence. Conversely the more risk averse the adversary, the more the adversary prefers the scenario with the greatest chance of success. To get the relative likelihood each adversary will choose each path, the values in Table 11 are normalized across each row, shown in Table 12.

Table 12. Normalized Values Based on Risk Attitude

Value vs. Risk Attitude	**Scenario**	**Scenario 2**	**Scenario 3**
$P_S^{Scenario}$	0.100	0.300	0.900
$C_{net,a}^{Scenario}$	0.900	0.300	0.100
Extremely Risk Seeking	0.641	0.257	0.102
Moderately Risk Seeking	0.613	0.269	0.118
Slightly Risk Seeking	0.523	0.302	0.174
Risk Neutral	0.333	0.333	0.333
Slightly Risk Averse	0.174	0.302	0.523
Moderately Risk Averse	0.118	0.269	0.613
Extremely Risk Averse	0.102	0.257	0.641

The attractiveness of individual pathways is determined by refining Equation 7 to include the attractiveness of various materials to the adversary in completing that scenario. The material attractiveness is derived from utility functions based on how nuclear material inputs affect the difficulty in completing a given scenario. The adversary's utility value for each scenario is then combined with the utility value for each material in Equation 23, to yield the utility of each pathway to the adversary. The variable $P_{A,i}^{V}$ is used to distinguish that it is not a probability, but rather a value that influences the probability that the adversary will choose pathway i.

$$P_{A,i}^{V} \propto U[Pathway\ i] \quad = \quad U\ [threat] * U\ [scenario] * U[material] \qquad (23)$$

III.C.2. Material Utility Functions

Each material utility function represents the relative difficulty with which each material input will complicate the ability of the adversary to complete each threat. These utility functions do not indicate the probability of success at various tasks, which is determined through adversary capabilities and not material attractiveness.

III.C.2.i. Nuclear Weapons Utility Functions

For nuclear weapons, the attractiveness of weapons are assumed unity. The yield of the weapon is incorporated into relative attractiveness through weighting of the consequences based on yield, and the effectiveness of engineered controls on the weapons are used in the probability of success of completing the pathway.

III.C.2.ii. Nuclear Materials Utility Functions

1. Items per SQ: The items per SQ utility function indicates that the more items that an adversary must steal, the more difficult the task. The utility function is given in Equation 24 and displayed in Figure 19

.

$$u(x_{Items/SQ}) \quad = \quad e^{(-0.1*(x_{Items/SQ})^{0.25}+0.1)} \tag{24}$$

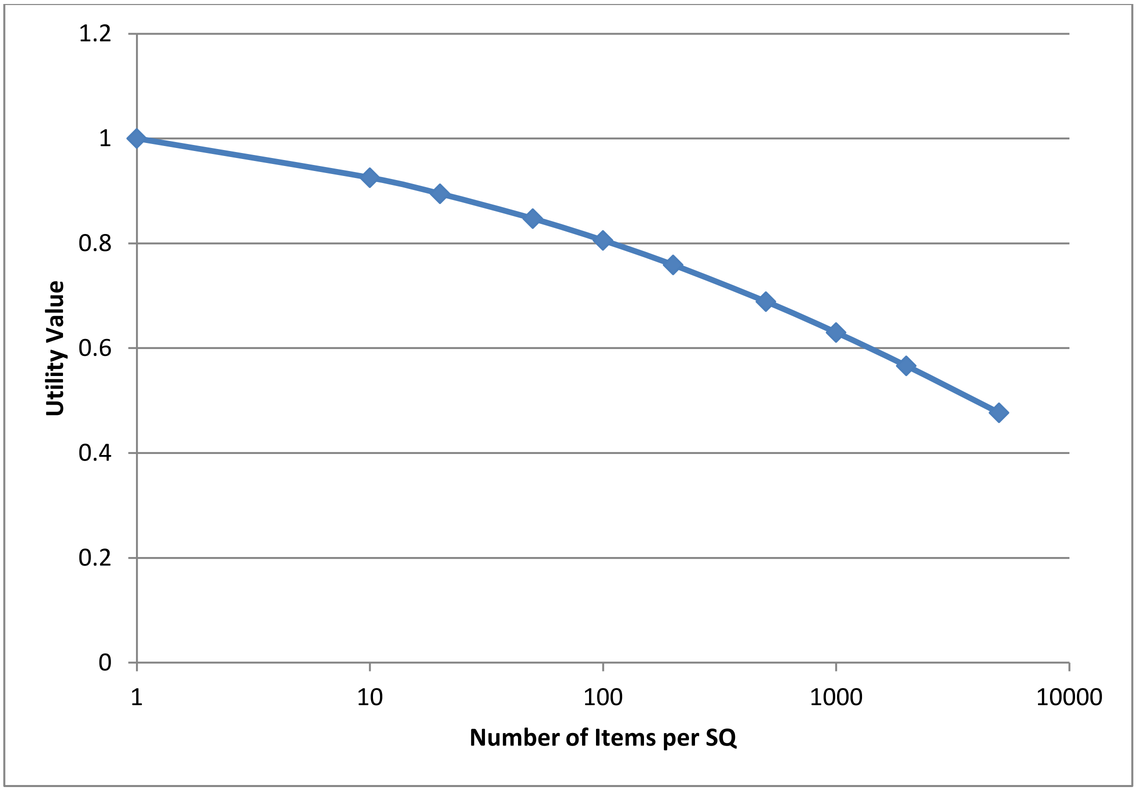


Figure 19. Graph of Items per SQ Utility Function

2. Dose Rate: The dose rate is the dose rate in Sv/Hr measured at 1 meter from one item of material. At low dose rates, there is no impact to the adversary. As the dose rate increases, the time that the adversary can handle and work with the material before experienced adverse health effects decreases. The utility function is given in Equation 25 and displayed in Figure 20.

$$U(D) = \begin{cases} 1, \quad for\ D \leq 0.002 \\ 1.0104 - 5.20833 * D, \quad for\ 0.002 < D \leq 0.05 \\ 0.7679 - 0.35714 * D, \quad for\ 0.05\ <\ D\ \leq\ 0.75 \\ 0.5715 - 0.09524 * D, \quad for\ 0.75\ <\ D\ \leq\ 5 \\ e^{\left(\frac{-2.3507*D^{1.5}}{11.18}\right)}, \ for\ D > 5 \end{cases} \tag{25}$$

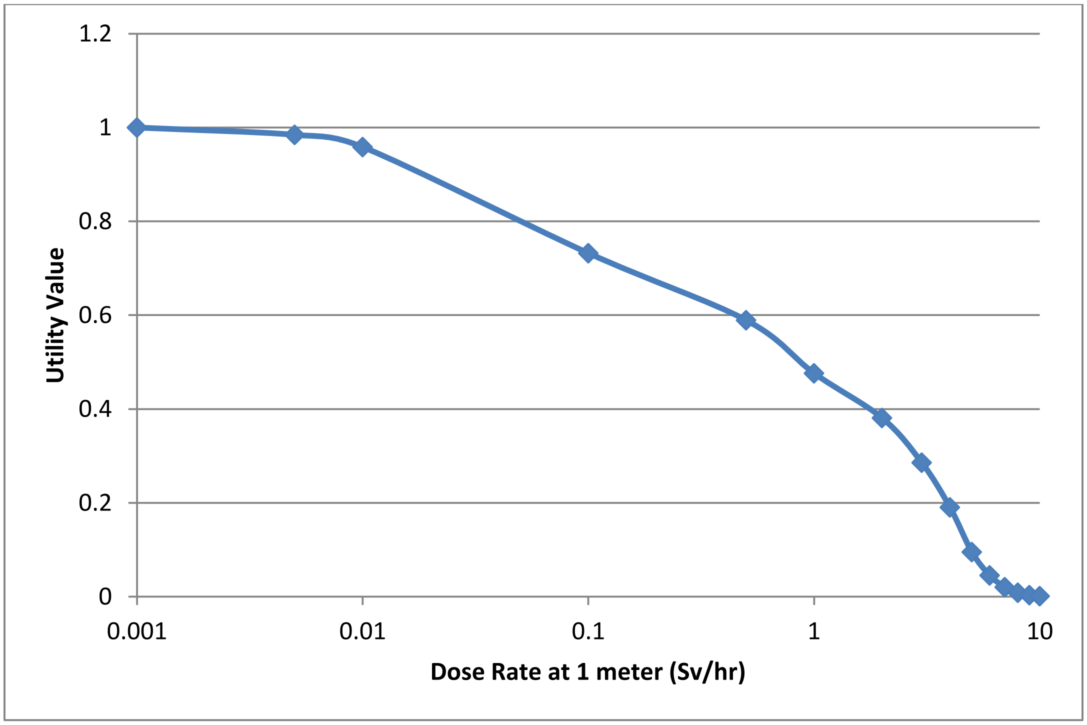


Figure 20. Graph of Dose Rate Utility Function

3. Mass Per SQ: Mass per SQ of material is the amount of material that an adversary must acquire to obtain 1 SQ of fissile material. The utility function is derived from Giangelli[41] and is given in Equation 26, where m_{SQ}^{min} is the minimum weight for an SQ of material (e.g. 8 kg for plutonium and 25 kg for uranium). The equation is plotted in Figure 21.

$$u_t(m_{SQ}) = 1 - e^{\left(-25*\left[\frac{m_{SQ}^{min}}{m_{SQ}}\right]^{1.5}\right)} \qquad (26)$$

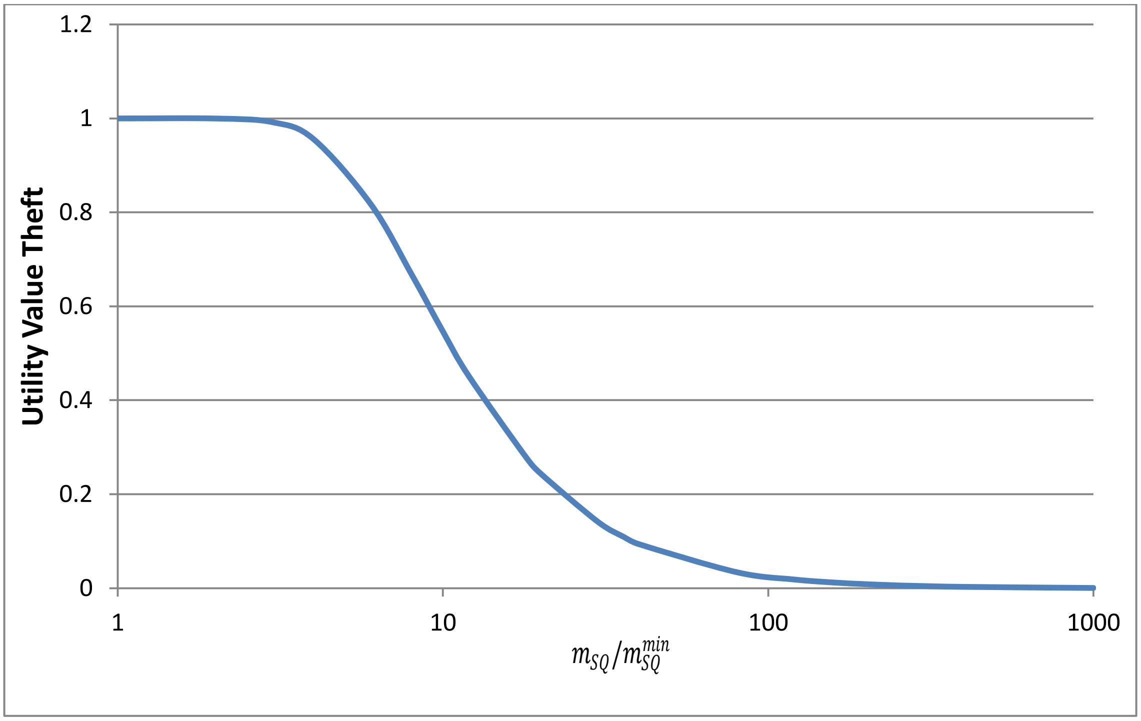


Figure 21. Graph of Items per SQ Utility Function

For diversion scenarios, a large item mass is a much more significant factor than in a theft scenario. A larger quantity will be much more difficult to divert either because it's size makes it difficult to conceal or the number of concealable items the adversary must divert provides more detection opportunities for the State. As a result, the utility factor for mass per SQ is modified for diversion scenarios and is given in Equation 27 and displayed in Figure 22.

$$u_d\left(m_{SQ}\right) = 1 - e^{\left(-25*\left[\frac{m_{SQ}^{min}}{m_{SQ}}\right]^{2.5}\right)} \tag{27}$$

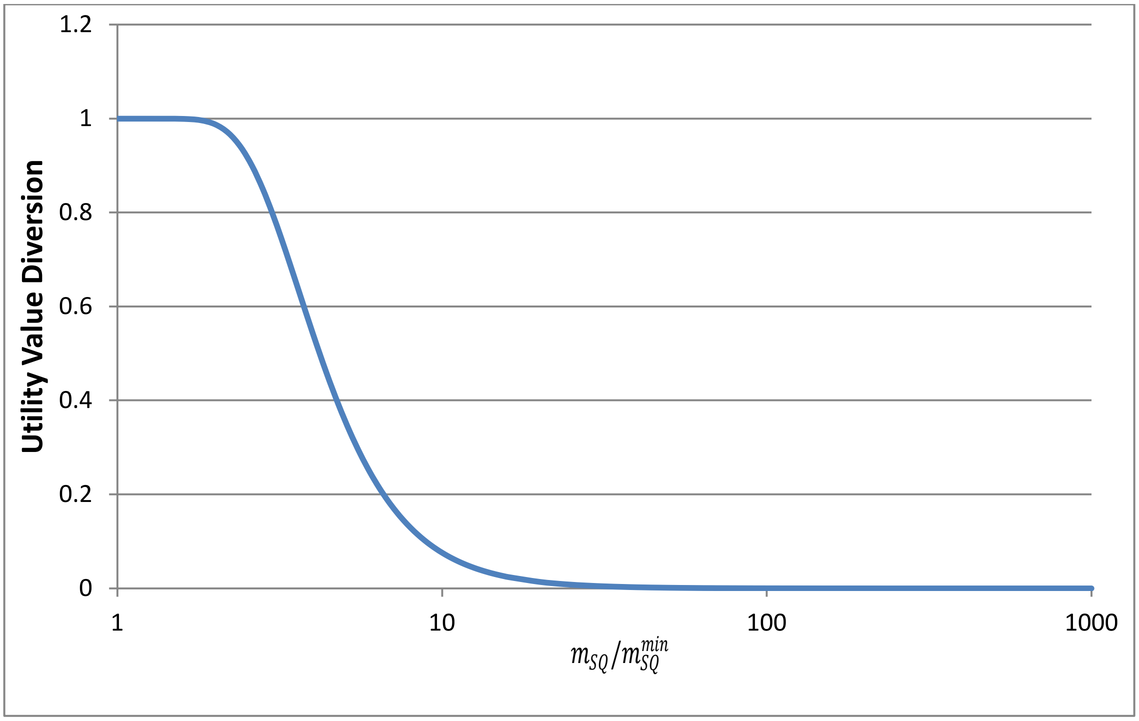


Figure 22. Mass per SQ Utility Function

7. Uranium Enrichment and Plutonium Quality : The utility function for enrichment and quality is derived from the material attractiveness figure of merit (FOM) developed by Bathke *et al*. in Equation 28.[69] In the equation the four factors that are added together are a size factor, stability factor, yield factor and acquisition factor respectively.

$$FOM = 1 - \log_{10}\left(\frac{M}{800} + \frac{Mh}{4500} + \frac{MS}{6.8e6} + \frac{M}{50}\left[\frac{D}{500}\right]^{\frac{1}{0.30103}}\right) \tag{28}$$

where:

$M =$ the bare critical mass in unpurified metal form (kg)

$h = the\ heat\ content\ in\ unpurified\ metal\ form$ (W/kg)

$S = spontaneous - fission\ neutron\ production\ rate$ (n/s/kg)

$D = dose\ rate\ of\ 0.2 * M\ at\ 1\ meter$ (rad/hr)

As a function of U enrichment and Pu quality, Equation 29 yields the approximate mass of a bare critical mass in kilograms, Equation 30 yields the approximate spontaneous fission rate in neutrons per second per gram, and Equation 31 yields the approximate heating rate in Watts per kilogram.

$$M(x) = \begin{cases} 786 * e^{-2.952*x},\ x = U\ enrichment \\ 51.821 * e^{-1.778*x},\ x = Pu\ quality \end{cases} \tag{29}$$

$$S(x) = \begin{cases} 0.6x + 2.5 * 10^4 * (1 - x),\ x = U\ enrichment \\ 22x + 9.1 * 10^5 * (1 - x),\ x = Pu\ quality \end{cases} \tag{30}$$

$$h(x) = \begin{cases} 6 * 10^{-5}x + 8.5 * 10^{-6} * (1 - x),\ \ x = U\ enrichment \\ 1.93 * x + 0.95 * (1 - x) * 7.06 + 0.05 * (1 - x) * 5.6 * 10^2, x = Pu\ quality \end{cases} \tag{31}$$

These are used in Equation 32, which is the utility function for uranium enrichment and plutonium quality. They are calculated together so that they are on the same scale. The resulting utility values for various enrichments of Uranium and qualities of Plutonium calculated using Equation 32 are displayed in Figure 23. These values are used for both theft and diversion scenarios.

$$u(x) = \frac{\left[2 - \log_{10}\left(\frac{M(x)}{800} + \frac{M(x)h(x)}{4500} + \frac{M(x)S(x)}{6.8e6}\right)\right]}{3.832} \tag{32}$$

Table 13. Utility Values for Various Plutonium Qualities and Uranium Enrichments

X_{Pu}	$U(x_{Pu})$	X_U	$U(x_U)$
1	1.000	1	0.858
0.99	0.862	0.9	0.796
0.9	0.619	0.8	0.739
0.8	0.522	0.7	0.686
0.7	0.457	0.6	0.637
0.6	0.405	0.5	0.589
0.5	0.360	0.4	0.542
0.4	0.319	0.3	0.498
0.3	0.281	0.2	0.454
0.2	0.246		
0.1	0.213		
0.05	0.197		

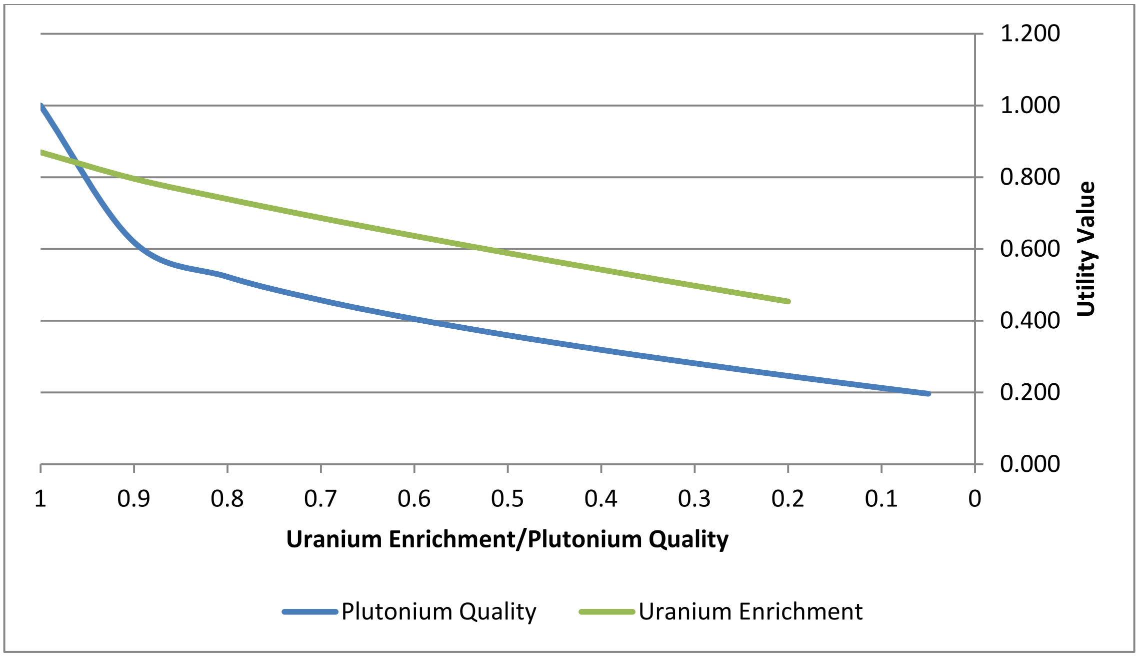


Figure 23. Utility Functions of Plutonium Quality and Uranium Enrichment

8. Chemical Reactivity With Air: The values for chemical reactivity with air are either "none", "slow", or "fast". The corresponding utility values for material theft determined using Equation 33 and utility values for diversion are determined using Equation 34.

$$u_t(c) = \begin{cases} 1, & none \\ 0.5, & slow \\ 0.2, & fast \end{cases} \tag{33}$$

$$u_d(c) = \begin{cases} 1, & none \\ 0.4, & slow \\ 0.05, & fast \end{cases} \tag{34}$$

9. Requires Active Cooling: This input for this attribute is a Boolean input, having value of either true or false. The utility value for this attribute for theft scenarios is given by Equation 35, and the utility value for diversion scenarios is given in Equation 36.

$$u_t(V) = \begin{cases} 1, & false \\ 0.2, & true \end{cases} \tag{35}$$

$$u_d(V) = \begin{cases} 1, & false \\ 0.05, & true \end{cases} \tag{36}$$

III.C.2.iii. Radiological Materials Utility Functions

There are two utility functions for radiological materials. The first is the dose rate in Sv/hr at 1 meter from the source, which is identical to the utility function for nuclear material in Equation 26. The second utility function is given for theft scenarios in Equation 37 and diversion scenarios in Equation 38, where m_{rad} is the mass per item in kg, A_{rad} is the activity in curies per item, and D_{rad} is the danger value for the radiological isotope. For diversion scenarios, the additional term represents the difficulty in diverting extremely strong radiological sources, which require extremely heavy shielding.

$$u_t(m_{rad}) = 1 - e^{\left(-\left[\frac{A/D}{m_{rad}}\right]^3\right)} \tag{37}$$

$$u_d(m_{rad}) = \left(1 - e^{\left(-\left[\frac{A/D}{m_{rad}}\right]^3\right)}\right) * e^{\left(\frac{-m_{rad}{}^{0.75}}{100}\right)} \tag{38}$$

III.C.2.iv. State Utility Functions

The utility functions for the State involve the consequence values. This involves normalizing the consequence values to a value between zero and unity that represents the degree of the negative effect that the consequence has on the State. An example calculation is provided in Appendix B. Each consequence category is determined independently of the other categories, and each consequence category is weighted based on its relative attractiveness to the State.

III.D. Solution Method

The methodology introduced in this section has been modeled using Microsoft Visual Basic for Applications (VBA), using Microsoft Visio as the user interface coupled with Microsoft Excel which serves as both the information database and computational tool. The first solution step is to calculate the base-line risk, which is the risk of nuclear terrorism calculated based on current State and adversary information. This baseline risk is then used as the benchmark to assess the effectiveness of various security measures and the impact of changes in adversary characteristics. The second step is modeling upgrades to various nuclear security measures or changes in adversary characteristics to determine the sensitivity of the State-level risk to various variables. The variables of highest sensitivity represent the security measures that the State should focus resources on to most effectively decrease risk. The final step is to determine what nuclear security measure upgrades can provide a desired degree of risk reduction.

III.D.1. Calculating the Baseline Risk

All of the inputs introduced in this chapter are combined to calculate the baseline State-level risk. This is a three step process. The first step is determining the pathways for each threat, based on the material inputs. The probability of overtly stealing and covertly diverting material from each facility is determined using the security parameters associated with each material at that facility. The probability of completing all of the processing steps in the pathway is then determined by coupling the capability values from Table 5 with the associated tasks, using Equation 11 to calculate the probability of success along each path. The total distance traveled to complete a pathway is then calculated based on longitude and latitude values associated with each location along the pathway, which is then incorporated into Equation 18 or Equation 19 to determine the probability of successfully transporting the material throughout the entire pathway to the target. Finally, the consequences of completing each path at each target is calculated.

Once these are compiled, the second step is to calculate the relative attractiveness of each material for each pathway. The probability of success along each path and the resulting consequences are then combined with the adversary risk attitude and consequence preferences to determine the relative probability the adversary attempts each path.

Once the pathways and the probability of attack for each pathway are generated, the risk for each pathway is calculated for each threat using Equation 39,

$$\mathrm{R_i} = \sum_{m=1}^{4} P_{A,i} * W_m * C_m * \prod_{j=1}^{J} \mathrm{P_{S,i,j}} \tag{39}$$

where: $\mathrm{R_i}$= the risk for pathway i

$\mathrm{P_{A,i}}$ = the probability that the adversary attempts pathway i

$\mathrm{W_m}$ = the State's weighted value of consequence m

$\mathrm{C_{m,i}}$ = the value of consequence m for pathway i

$\mathrm{P_{S,i,j}}$ = the probability of adversary success along pathway i

The value of *J* is specific to each pathway, and represents the total number of tasks required to complete that pathway. The final step involves aggregating the risk for each pathway and normalizing by the sum of the State's consequence weights, which will yield the State-level risk (ℝ), calculated using Equation 40.

$$\mathbb{R} = {\sum_{i=1}^{I} R_i}\Big/{\sum_{m=4} W_m} \tag{40}$$

III.D.2. Sensitivity Analysis of State-Level Risk

All pathways within the State are represented by a dynamic network, where the inter-dependencies of each variable are modeled. Changes to nuclear security measures can then be simulated to study the corresponding outcome in risk. The long form of the risk equation is given in Equation 41, where the probability the adversary attacks is given in the curly brackets and the risk of each type of nuclear threat is in the standard brackets..

$$\mathbb{R} = \sum_{t=1}^{4}\left(\sum_{m=1}^{4}\frac{\left[\sum_{i=1}^{I_t}\left\{(P_S^i)^{(\frac{1}{a+1})}(C_{net,a}^i)^{(\frac{1}{b+1})}\, U_a^{mat}(m_i)\right\} * C_{i,s}^m * \prod_{j=1}^{J} \mathrm{P}_{\mathrm{S,i,j}}\right]}{W_m}\right) \tag{41}$$

where: t represents the four nuclear threats

m represents the four consequence categories

i represents an individual pathway within each threat

I_t = the total number of pathways for each threat

P_S^i = the total adversary probability of success for the pathway i

$C_{net,a}^i$ = the net benefit to the adversary for completing pathway i

U_a^{mat} = the relative attractiveness of the material on pathway i

$C_{i,s}^m$ = is the consequence to the State of the adversary completing pathway i.

Upgrades to various security measures throughout the State are simulated by perturbing the value of the corresponding variable by a standard amount and observing the change this has on the value of $\mathbb{R}$. Most perturbations will directly change the probability of success $P_{S,i,j}$, which will subsequently affect the likelihood the adversary chooses each path. In addition to simulating individual variables, sets of variables are also simulated so that the effects of risk transfer can be captured. For example, if a State has two sites that store HEU, upgrading either one site independently may simply transfer the risk to the other site, minimizing the impact on $\Delta\mathbb{R}$. However, upgrading both sites may have a significant impact on $\Delta\mathbb{R}$. Finally, changes such as replacing HEU with LEU will negate all pathways associated with those HEU sources and replace them with more complex LEU pathways.

The upgrades with the greatest sensitivity (max$\{\Delta\mathbb{R}/\Delta V\}$), will be the upgrades that are the most effective at reducing State-level risk. These can then be multiplied by the corresponding cost functions for each upgrade, $(\frac{\Delta V}{\Delta \$})$, to yield the most cost-effective security measures.

III.D.3. Determining Optimal Risk Reduction Strategies

The final step is to determine the optimal strategy to reach a desired risk-reduction goal. This is accomplished by using the perturbation results from the sensitivity analysis. The $\Delta\mathbb{R}/\Delta V$ values are sorted and upgrades to the variable with the maximum sensitivity to risk is simulated. Once upgrades to that variable are simulated, the sensitivity analysis is repeated to determine if the risk is now most sensitive to a new variable. This process is repeated until the desired risk level is met.

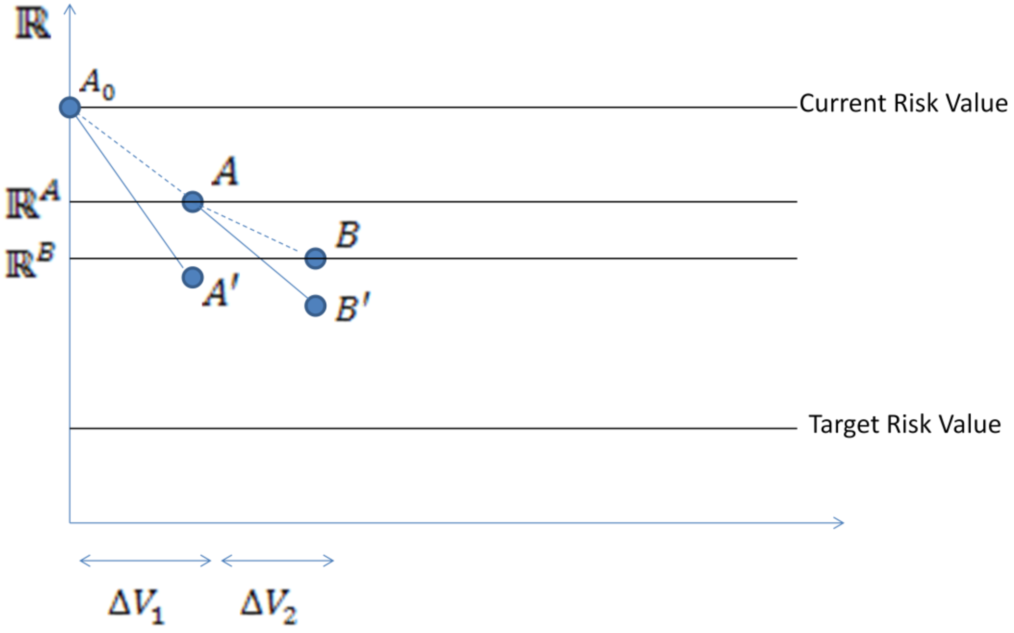


Figure 24. Process of Determining Upgrades to Reach Target Risk

The general process is displayed in Figure 24. The first step is determining the variable where $\frac{\Delta\mathbb{R}}{\Delta V}|_{A_0}$ has the maximum value. Upgrades to this variable are then simulated by changing that variable by ΔV_1. The figure shows that based on extrapolating $\frac{\Delta\mathbb{R}}{\Delta V}|_{A_0}$, the change ΔV_1 is expected to change the risk value to point A'. However, because the adversary can change their tactics based on this upgrade, the decrease in risk value will likely be less than expected, resulting in a new value for risk $\mathbb{R}^A$ at point A. Sensitivity values are then calculated for all variables at this point, where upgrades for the variable with maximum value for $\frac{\Delta\mathbb{R}^A}{\Delta V}|_A$ are simulated yielding $\mathbb{R}^B$at point B. This process is repeated until the new risk value is equal to or less than the target risk value. The process can be run by implementing different step sizes for each ΔV. The value of the change to ΔV is determined using Equation 42, where δ represents the step size.

$$\Delta V = \frac{\left(\frac{\mathbb{R}^{current} - \mathbb{R}^{target}}{\delta}\right)}{\left(\frac{\Delta\mathbb{R}}{\Delta V}\right)} \tag{42}$$

In Figure 24, upgrades are simulated based on the projected change that reduces the risk halfway to the target value, meaning δ=2. This process can also be accomplished using $\frac{\Delta\mathbb{R}}{\Delta\$}$ values to maximize the cost effectiveness of risk reduction. When applying resources, the searching algorithm can search using some number of variables with the highest values for $\frac{\Delta\mathbb{R}}{\Delta\$}$, rather than just using the single highest value as displayed in Figure 24.

CHAPTER IV

NUMERICAL TESTS

Numerical tests are performed on the computational model developed based on the methodology introduced in Chapter III to provide confidence in model results. First, verification tests are performed on the VBA code to ensure the code produces results that are consistent with the methodology and confirm the absence of programming errors. Next, validation tests are performed to confirm that the results are true representations of reality. Finally, we conduct a set of behavioral tests to further characterize the performance of the code.

IV.A. Verification Tests

Verification tests ensure the conceptual description given in Chapter III and the solution of the model are implemented correctly and that the code is free of programming errors. The first verification test ensures that the pathways generation function is performing adequately. Next, a sample problem is both manually solved and simulated by the code, verifying that the results from the code are accurate for each step.

IV.A.1 Pathways Generation Verification

The pathways generation function develops all potential pathways based on the properties of the material, which dictate the processing steps required to develop weapons usable metal. The network of pathways is then populated with all of the other data to determine the risk of each pathway and subsequently, the State-level risk. The pathway generation function is verified by simulating a sufficient variety of materials to ensure every potential pathway combination is employed. The results are displayed in Table 14 and verify that pathways are generated as expected based on material properties. In the table, metallurgy includes any processes, including chemical processing, that converts any uranium material into a metal while conversion involves converting one chemical form of uranium to another chemical form, such as U_3O_8 or UO_2 to UF_6.

Table 14. SNM Pathway Generation Verification Results

Material	Reprocessing	Conversion	Enrichment	Metallurgy	Machining	IND Weaponization
Irradiated LEU Fuel (U Path)	X	X	X	X	X	Gun-Type
Irradiated HEU Fuel (U Path)	X			X	X	Gun-Type
Natural Uranium		X	X	X	X	Gun-Type
Natural UF_6			X	X	X	Gun-Type
HEU UF_6				X	X	Gun-Type
HEU UO_2				X	X	Gun-Type
HEU Metal					X	Gun-Type
Spent Fuel (Pu Path)	X			X	X	Implosion
PuO_2				X	X	Implosion
Pu Metal					X	Implosion

IV.A.2 Risk Calculation Results Verification

A simple problem is introduced to verify the VBA model's results and confirm the absence of programming errors. All inputs used in this calculation are provided in Appendix C. The problem involves two facilities; a research reactor with HEU and a hospital with two types of radiological sources of concern. The risk calculation analyzes a set of two potential targets.

The first step is calculating the probability of adversary success for each task. Table 15 shows the results for each task using Equation 11 and adversary capability inputs from Table C.3.

Using Equation 12 and Equation 14 with the motivation and disincentive data in Table C.2, and accounting for the lack of nuclear weapons in the State, Table 16 gives the relative attractiveness of the four nuclear threats.

Table 15. Probability of Success for Each Task

Assessed Likelihoods	$\boldsymbol{P_S^{task}}$
Conversion	0.125
Reprocessing	1E-08
Enrichment	5E-13
Machining	0.25
Metallurgy	0.25
IND Weaponization: Gun-Type	0.225
RDD Weaponization	0.67687
IND Weaponization: Implosion	0.00025

Table 16. MAUA Attractiveness Results

Nuclear Threat	Relative Attractiveness
Nuclear Weapon	0
IND	10.81 %
RDD	46.07 %
Sabotage	43.12%

In this example, there are eight unique IND pathways and 16 unique RDD pathways. The IND and RDD pathways are displayed in Table 17 and Table 18 respectively. The additional RDD pathways come from the irradiated fuel, which makes an attractive RDD material. Additionally, the presence of multiple items of radiological material at two of the three facilities represent scenarios where the source material can be divided into multiple RDD devices and delivered to both targets. One assumption in this analysis is that the Cs-137 Blood Irradiator source cannot be split into two RDDs due to the incredibly high dose rate of the material when unshielded. This assumption could be changed in the model by changing the number of Cs-137 items to two and halving all of its material property values.

Table 17. IND Pathways

Material	Pathway	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6	Task 7
Fresh HEU Fuel	IND1	Steal Material	Transport to Conversion Facility	Convert to Metal	Machine Metal	Develop Weapon	Transport to Target 1	x
Fresh HEU Fuel	IND2	Steal Material	Transport to Conversion Facility	Convert to Metal	Machine Metal	Develop Weapon	Transport to Target 2	x
Fresh HEU Fuel	IND3	Divert Material	Transport to Conversion Facility	Convert to Metal	Machine Metal	Develop Weapon	Transport to Target 1	x
Fresh HEU Fuel	IND4	Divert Material	Transport to Conversion Facility	Convert to Metal	Machine Metal	Develop Weapon	Transport to Target 2	x
Irradiated HEU Fuel	IND5	Steal Material	Transport to Reprocessing Facility	Remove Fission Products	Convert to Metal	Machine Metal	Develop Weapon	Transport to Target 1
Irradiated HEU Fuel	IND6	Steal Material	Transport to Reprocessing Facility	Remove Fission Products	Convert to Metal	Machine Metal	Develop Weapon	Transport to Target 2
Irradiated HEU Fuel	IND7	Divert Material	Transport to Reprocessing Facility	Remove Fission Products	Convert to Metal	Machine Metal	Develop Weapon	Transport to Target 1
Irradiated HEU Fuel	IND8	Divert Material	Transport to Reprocessing Facility	Remove Fission Products	Convert to Metal	Machine Metal	Develop Weapon	Transport to Target 2

Table 18. RDD Pathways

Material	Pathway	Task 1	Task 2	Task 3	Task 3	Task 4
HDR Brachytherapy Sources Co-60	RDD1	Steal Material	Transport to Covert Facility	Develop Weapon	Transport to Target 1	x
HDR Brachytherapy Sources Co-60	RDD2	Steal Material	Transport to Covert Facility	Develop Weapon	Transport to Target 2	x
HDR Brachytherapy Sources Co-60	RDD3	Divert Material	Transport to Covert Facility	Develop Weapon	Transport to Target 1	x
HDR Brachytherapy Sources Co-60	RDD4	Divert Material	Transport to Covert Facility	Develop Weapon	Transport to Target 2	x
Blood Irradiator Cs-137	RDD5	Steal Material	Transport to Covert Facility	Develop Weapon	Transport to Target 1	x
Blood Irradiator Cs-137	RDD6	Steal Material	Transport to Covert Facility	Develop Weapon	Transport to Target 2	x
Blood Irradiator Cs-137	RDD7	Divert Material	Transport to Covert Facility	Develop Weapon	Transport to Target 1	x
Blood Irradiator Cs-137	RDD8	Divert Material	Transport to Covert Facility	Develop Weapon	Transport to Target 2	x
HDR Brachytherapy Sources Co-60	RDD9	Steal Material	Transport to Covert Facility	Develop 2 Weapons	Transport Weapon 1 to Target 1	Transport Weapon 2 to Target 2
HDR Brachytherapy Sources Co-60	RDD10	Divert Material	Transport to Covert Facility	Develop 2 Weapons	Transport Weapon 1 to Target 1	Transport Weapon 2 to Target 2
Irradiated HEU Fuel	RDD11	Steal Material	Transport to Covert Facility	Develop Weapon	Transport to Target 1	x
Irradiated HEU Fuel	RDD12	Steal Material	Transport to Covert Facility	Develop Weapon	Transport to Target 2	x
Irradiated HEU Fuel	RDD13	Divert Material	Transport to Covert Facility	Develop Weapon	Transport to Target 1	x
Irradiated HEU Fuel	RDD14	Divert Material	Transport to Covert Facility	Develop Weapon	Transport to Target 2	x
Irradiated HEU Fuel	RDD15	Steal Material	Transport to Covert Facility	Develop 2 Weapons	Transport Weapon 1 to Target 1	Transport Weapon 2 to Target 2
Irradiated HEU Fuel	RDD16	Divert Material	Transport to Covert Facility	Develop 2 Weapons	Transport Weapon 1 to Target 1	Transport Weapon 2 to Target 2

Each facility's physical protection system data given in Table C.7 and Table C.8 are used to determine the likelihood of stealing each material. In addition, the effectiveness of security systems designed to prevent diversion of each material is determined using Equation 16. Table 19 and Table 20 give these results for each material.

Table 19. Research Reactor Materials P_E Values

Research Reactor	Layer #	P_I-Layer	P_N-Layer	P_E-Layer	P_E Material	$P_E^{Diversion}$
Fresh Fuel HEU	1	0.5	0.7	0.35	0.665	0.964
	2	0.9	0.7	0.63		
Spent Fuel HEU	1	0.5	0.7	0.35	0.525	0.9955
	2	0.7	0.5	0.35		

Table 20. Hospital Materials P_E Values

Hospital	Layer #	P_I-Layer	P_N-Layer	P_E-Layer	P_E Material	$P_E^{Diversion}$
Brachytherapy Sources	1	0.5	0.1	0.05	0.05	0.703
Blood Irradiator	1	0.7	0.1	0.07	0.07	0.9505

The material attractiveness values for each material are presented in Table 21 and determined using the material inputs from Table C.4 and Table C.5 and Equation 24 - Equation 37. The spent fuel has different attractiveness values for both IND and RDD pathways.

Table 21. Material Attractiveness Value for Each Material

Material	MA-Value
Fresh Fuel theft	0.24679
Fresh Fuel diversion	0.04253
Spent Fuel theft (IND)	0.04530
Spent Fuel diversion (IND)	0.00758
Spent HEU theft (RDD)	0.19054
Spent Fuel diversion (RDD)	0.07396
Brachytherapy Sources theft	0.99579
Brachytherapy Sources diversion	0.44334
Blood Irradiator theft	0.80440
Blood Irradiator diversion	0.03239

The probability of success for each pathway in Table 18 is determined using the results from Table 15, Table 19, and Table 20. The probability of successfully producing two RDD's is determined by dividing the resources evenly between both weapons. The probability of successfully transporting material is determined by calculating transportation distances using Equation 15 and inserting this value into Equation 18 for diversion scenarios and Equation 19 for theft scenarios. Table 22 shows the resulting probability of success for each task.

Table 22. Probability of Success for Each Pathway Task

Pathway	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6	Task 7
IND1	3.35E-01	7.87E-01	4.13E-01	1.13E-01	2.45E-01	4.66E-01	x
IND2	3.35E-01	7.87E-01	4.13E-01	1.13E-01	2.45E-01	3.26E-01	x
IND3	3.600-02	9.61E-01	4.13E-01	1.13E-01	2.45E-01	6.54E-01	x
IND4	3.600-02	9.61E-01	4.13E-01	1.13E-01	2.45E-01	4.66E-01	x
IND5	4.75E-01	7.87E-01	1.00E-08	4.13E-01	1.13E-01	2.45E-01	4.66E-01
IND6	4.75E-01	7.87E-01	1.00E-08	4.13E-01	1.13E-01	2.45E-01	3.26E-01
IND7	4.500E-3	9.61E-01	1.00E-08	4.13E-01	1.13E-01	2.45E-01	6.54E-01
IND8	4.500E-3	9.61E-01	1.00E-08	4.13E-01	1.13E-01	2.45E-01	4.66E-01
RDD1	9.50E-01	6.02E-01	8.36E-01	4.66E-01	x	x	x
RDD2	9.50E-01	6.02E-01	8.36E-01	3.26E-01	x	x	x
RDD3	2.97E-01	9.19E-01	8.36E-01	6.54E-01	x	x	x
RDD4	2.97E-01	9.19E-01	8.36E-01	4.66E-01	x	x	x
RDD5	9.30E-01	6.02E-01	8.36E-01	4.66E-01	x	x	x
RDD6	9.30E-01	6.02E-01	8.36E-01	3.26E-01	x	x	x
RDD7	4.95E-02	9.19E-01	8.36E-01	6.54E-01	x	x	x
RDD8	4.95E-02	9.19E-01	8.36E-01	4.66E-01	x	x	x
RDD9	9.50E-01	6.02E-01	6.90E-01	4.66E-01	3.26E-01	x	x
RDD10	2.97E-01	9.19E-01	6.90E-01	6.54E-01	4.66E-01	x	x
RDD11	4.75E-01	7.87E-01	8.36E-01	4.66E-01	x	x	x
RDD12	4.75E-01	7.87E-01	8.36E-01	3.26E-01	x	x	x
RDD13	4.500E-3	9.61E-01	8.36E-01	6.54E-01	x	x	x
RDD14	4.500E-3	9.61E-01	8.36E-01	4.66E-01	x	x	x
RDD15	4.75E-01	7.87E-01	6.90E-01	4.66E-01	3.26E-01	x	x
RDD16	4.500E-3	9.61E-01	6.90E-01	6.54E-01	4.66E-01	x	x

Table 23 gives the consequences for each RDD pathway, calculated using the consequence inputs for each target in Table C.10 and scaling these values with Equations B3-B6.

Table 23. RDD Consequences for Each Pathway

Pathway	C_{RDD}^{LL}	C_{RDD}^{IL}	C_{RDD}^{EL}	C_{RD}^{SC}
RDD1	5.08E-11	3.64E-06	2.18E-04	4.49E-04
RDD2	7.26E-11	2.91E-06	3.63E-04	4.49E-04
RDD3	5.08E-11	3.64E-06	2.18E-04	4.49E-04
RDD4	7.26E-11	2.91E-06	3.63E-04	4.49E-04
RDD5	2.13E-10	9.46E-06	3.13E-04	7.25E-04
RDD6	3.05E-10	7.57E-06	5.22E-04	7.25E-04
RDD7	2.13E-10	9.46E-06	3.13E-04	7.25E-04
RDD8	3.05E-10	7.57E-06	5.22E-04	7.25E-04
RDD9	6.17E-11	4.12E-06	2.90E-04	7.13E-04
RDD10	6.17E-11	4.12E-06	2.90E-04	7.13E-04
RDD11	5.27E-09	8.12E-05	7.79E-04	2.12E-03
RDD12	7.53E-09	6.49E-05	1.30E-03	2.12E-03
RDD13	5.27E-09	8.12E-05	7.79E-04	2.12E-03
RDD14	7.53E-09	6.49E-05	1.30E-03	2.12E-03
RDD15	6.46E-09	9.20E-05	1.43E-03	3.37E-03
RDD16	6.46E-09	9.20E-05	1.43E-03	3.37E-03

In addition to these RDD and IND pathways, there are 8 sabotage pathways. Table 24 lists each sabotage event and the adversary's corresponding probability of success.

Table 24. Sabotage Pathways

Pathway	Target	P_s^{Path}
SAB1	Spent Fuel Pool	0.35625
SAB2	Spent Fuel Pool - Insider	0.675
SAB3	Reactor	0.26
SAB4	Reactor - Insider	0.28
SAB5	HRD Storage Vault	0.95
SAB6	HRD Storage Vault - Insider	0.999
SAB7	Irradiator Room	0.93
SAB8	Irradiator Room - Insider	0.999

The probability of success for each IND and RDD pathway is determined by multiplying the probability of each successive task in Table 22. These results are presented in Table 25. In addition, Table 25 shows the adversary's net consequences for each pathway calculated using data from Table C.1, Table C.10, and Equation 21. The probability of success and net consequences for each path are then combined considering the adversary's risk attitude using Equation 22. These values are then multiplied by the material attractiveness values in Table 21 to yield the adversary utility value for each path ($P_{A,i}^{V}$). These values are then biased to match the adversary's intentions using the motivation and disincentive MAUA results from Table 16 to give the net utility of each pathway (U_{path}^{adv}). The relative probability that the adversary chooses each pathway is then determined by dividing the utility of each pathway by the sum of all utilities.

Table 25. Probability of Attack Calculations

Pathway	$\boldsymbol{P_s^{path}}$	$C_{net,a}^{Path}$	$\boldsymbol{P_{A,i}^{V}}$	$\boldsymbol{U_{path}^{adv}}$	$\boldsymbol{P_a^{path}} = \frac{\boldsymbol{U_{path}^{adv}}}{\sum \boldsymbol{U_{path}^{adv}}}$
IND1	1.40E-03	8.67E-01	3.21E-04	3.47E-05	2.49E-03
IND2	9.79E-04	9.33E-01	2.33E-04	2.52E-05	1.81E-03
IND3	2.58E-04	8.67E-01	1.02E-05	1.10E-06	7.92E-05
IND4	1.83E-04	9.33E-01	7.54E-06	8.15E-07	5.85E-05
IND5	1.98E-11	8.67E-01	8.35E-13	9.03E-14	6.48E-12
IND6	1.39E-11	9.33E-01	6.08E-13	6.57E-14	4.72E-12
IND7	3.22E-13	8.67E-01	2.27E-15	2.46E-16	1.76E-14
IND8	2.29E-13	9.33E-01	1.68E-15	1.81E-16	1.30E-14
RDD1	2.23E-01	2.24E-04	3.32E-03	1.53E-03	1.10E-01
RDD2	1.56E-01	2.72E-04	2.57E-03	1.18E-03	8.49E-02
RDD3	1.49E-01	2.24E-04	9.90E-04	4.56E-04	3.27E-02
RDD4	1.06E-01	2.72E-04	7.77E-04	3.58E-04	2.57E-02
RDD5	2.18E-01	3.49E-04	3.28E-03	1.51E-03	1.09E-01
RDD6	1.53E-01	4.18E-04	2.52E-03	1.16E-03	8.33E-02
RDD7	2.49E-02	3.49E-04	1.51E-05	6.95E-06	4.99E-04
RDD8	1.77E-02	4.18E-04	1.18E-05	5.41E-06	3.89E-04
RDD9	6.00E-02	3.36E-04	1.10E-03	5.05E-04	3.62E-02
RDD10	5.74E-02	3.36E-04	4.66E-04	2.15E-04	1.54E-02
RDD11	1.46E-01	9.95E-04	8.74E-04	4.03E-04	2.89E-02
RDD12	1.02E-01	1.16E-03	6.63E-04	3.05E-04	2.19E-02
RDD13	2.37E-03	9.95E-04	5.52E-06	2.54E-06	1.82E-04
RDD14	1.68E-03	1.16E-03	4.25E-06	1.96E-06	1.40E-04
RDD15	3.92E-02	1.63E-03	3.01E-04	1.39E-04	9.97E-03
RDD16	9.09E-04	1.63E-03	2.71E-06	1.25E-06	8.97E-05
SAB1	3.56E-01	3.33E-05	2.06E-03	8.87E-04	6.37E-02
SAB2	6.75E-01	3.33E-05	3.90E-03	1.68E-03	1.21E-01
SAB3	2.60E-01	3.33E-05	1.50E-03	6.47E-04	4.65E-02
SAB4	2.80E-01	3.33E-05	1.62E-03	6.97E-04	5.01E-02
SAB5	9.50E-01	1.67E-06	1.23E-03	5.29E-04	3.80E-02
SAB6	9.99E-01	1.67E-06	1.29E-03	5.56E-04	3.99E-02
SAB7	9.30E-01	1.70E-06	1.21E-03	5.23E-04	3.76E-02
SAB8	9.99E-01	1.70E-06	1.30E-03	5.62E-04	4.04E-02

Table 26. Pathway Risk Values

Pathway	$R_{pathway}$	$\%\mathbb{R}$
IND1	7.31E-06	18.27%
IND2	4.26E-06	10.65%
IND3	4.28E-08	0.11%
IND4	2.57E-08	0.06%
IND5	2.70E-22	0.00%
IND6	1.38E-22	0.00%
IND7	1.36E-26	0.00%
IND8	7.17E-27	0.00%
RDD1	3.85E-06	9.64%
RDD2	3.04E-06	7.60%
RDD3	7.70E-07	1.93%
RDD4	6.27E-07	1.57%
RDD5	5.65E-06	14.14%
RDD6	4.35E-06	10.87%
RDD7	2.96E-09	0.01%
RDD8	2.35E-09	0.01%
RDD9	4.80E-07	1.20%
RDD10	1.95E-07	0.49%
RDD11	2.87E-06	7.19%
RDD12	2.07E-06	5.18%
RDD13	2.95E-10	0.00%
RDD14	2.19E-10	0.00%
RDD15	4.46E-07	1.12%
RDD16	9.32E-11	0.00%
SAB1	6.81E-07	1.70%
SAB2	2.45E-06	6.12%
SAB3	3.63E-07	0.91%
SAB4	4.21E-07	1.05%
SAB5	1.80E-08	0.05%
SAB6	1.99E-08	0.05%
SAB7	1.96E-08	0.05%
SAB8	2.26E-08	0.06%

Applying Equation 39, the P_A values in Table 25 are multiplied by the adversary's probability of success and the State's weighted consequence values for each pathway. Table 26 shows the resulting risk values for each pathway and their relative contribution to the overall risk. Applying Equation 40 yields a State-level risk value of 1.538×10^{-5}. Examining the pathway risk values, pathway IND1 is the largest contributor to risk, making up 18.27% of the total State-level risk and four of the 32 total pathways (IND1, IND2, RDD5 and RDD6) make up over half (53.93%) of the total State-level risk. The pathways IND1 and IND2 correspond to theft of the HEU fuel and RDD5 and RDD6 correspond to theft of the large Cs-137 irradiator source. Overall, IND pathways make up 29.1% of the State risk, RDD pathways make up 60.9% of the risk, and sabotage pathways make up the remaining 10%.

IV.B. Validation Tests

Validation tests verify that the results are true representations of reality. Typical validation involves comparing real-world data against simulation results. In this case, there is no experimental data and therefore the code cannot be traditionally validated. For the validation tests in this section, we introduce problems where the solution is intuitively obvious to qualitatively validate the results.

IV.B.1. MAUA Validation

The MAUA results are used to bias terrorist pathway selection based on their motivations and disincentives for the four nuclear threats. The purpose of this validation test is to ensure that the methodology assimilates motivations and disincentives properly and that the results add value to the solution.

We introduce two groups with different motivation profiles into the verification test problem from the previous section. The first group has a motivational profile that is expected to prefer INDs and nuclear weapons, while the second group should prefer RDD's and sabotage. Using Equation 12 and Equation 14 with the motivation and disincentive data in Table 27, and accounting for the lack of nuclear weapons in the State, Table 28 gives the relative attractiveness of the four nuclear threats.

Table 27. Terrorist Profiles

Motivations	W_U^m **Group 1**	W_U^m **Group 2**
Prestige of Successful Capabilities	3	0
Manipulate Adversaries	5	0
Apocalyptic Beliefs	5	0
War on Own Nation	0	3
War on Another Nation	0	0
Redress Conventional Military Asymmetry	5	0
Ensure Security	0	0
Mass Devastation/Chaos		
-Deaths	5	0
-Other	5	5
Religious Imperative	0	0
Manipulate Policy	0	0
Fascination of Nuclear Weapons	5	0
Fascination of Radiological	0	0
Fascination of Sabotage	0	0
Disincentives		
Fear of Retaliation on Base of Support	0	5
Fear of Attracting Attention	0	3
Alienation	0	0
Contradict Goals of Group		
-Mass killings	0	5
-Contamination of territory or environment	0	0
Lack of Religious Mandate	0	5
Internal Group Division	0	0

Table 28. MAUA Attractiveness Results

Nuclear Threat	**Group 1**	**Group 2**
Nuclear Weapon	0	0
IND	99.7 %	0.16%
RDD	0.07 %	78.49%
Sabotage	0.23%	21.35%

The results from Table 25 are recalculated using the results from Table 28. In addition, we introduce a third calculation where no MAUA data is used. Table 29 gives the results for the probability of choosing each pathway for both groups and for the case where no MAUA data is used. The results in Table 29 show what is expected; group 1 is significantly more likely to choose IND pathways and group 2 is significantly more likely to choose RDD pathways.

Table 29. Probabilities of Choosing Paths

Pathway	P_a^{path} Group 1	P_a^{path} No MAUA	P_a^{path} Group 2
IND1	3.12E-01	8.47E-03	2.45E-05
IND2	2.27E-01	6.16E-03	1.78E-05
IND3	2.38E-01	6.46E-03	1.87E-05
IND4	1.76E-01	4.77E-03	1.38E-05
IND5	8.12E-10	2.20E-11	6.39E-14
IND6	5.91E-10	1.60E-11	4.65E-14
IND7	4.39E-10	1.19E-11	3.46E-14
IND8	3.25E-10	8.81E-12	2.55E-14
RDD1	2.27E-03	8.76E-02	1.24E-01
RDD2	1.75E-03	6.77E-02	9.62E-02
RDD3	1.58E-03	6.09E-02	8.66E-02
RDD4	1.24E-03	4.78E-02	6.80E-02
RDD5	2.24E-03	8.66E-02	1.23E-01
RDD6	1.72E-03	6.64E-02	9.45E-02
RDD7	1.96E-04	7.56E-03	1.07E-02
RDD8	1.52E-04	5.89E-03	8.37E-03
RDD9	7.48E-04	2.89E-02	4.11E-02
RDD10	7.43E-04	2.87E-02	4.08E-02
RDD11	5.97E-04	2.31E-02	3.28E-02
RDD12	4.52E-04	1.75E-02	2.48E-02
RDD13	7.49E-04	2.90E-02	4.12E-02
RDD14	5.77E-04	2.23E-02	3.17E-02
RDD15	2.06E-04	7.95E-03	1.13E-02
RDD16	3.69E-04	1.42E-02	2.02E-02
SAB1	4.61E-03	5.43E-02	2.10E-02
SAB2	8.74E-03	1.03E-01	3.98E-02
SAB3	3.37E-03	3.96E-02	1.53E-02
SAB4	3.63E-03	4.26E-02	1.65E-02
SAB5	2.75E-03	3.24E-02	1.25E-02
SAB6	2.89E-03	3.40E-02	1.32E-02
SAB7	2.72E-03	3.20E-02	1.24E-02
SAB8	2.92E-03	3.44E-02	1.33E-02

IV.B.2. Probability of Attack Validation

To validate the probability of attack calculations, we simulate various nuclear materials that could be found in the nuclear fuel cycle and materials that could be part of nuclear weapons programs. The data used for each material was developed to realistically represent real world materials and is available in Appendix D. To ensure the probability of attack numbers are solely based on nuclear material properties and terrorist capabilities, any variables not related to these two groups (e.g. physical security systems, safeguards systems, material interdiction, etc.) were eliminated from the calculation. Two tests were conducted. The first used a terrorist group (Group A) with a much higher probability of producing a gun-type IND than an implosion IND. The second group (Group B) is equally likely to produce either a gun-type or implosion based IND weapon. Table 30 lists the assessed capabilities of Group A, and Table 31 has the material attractiveness calculations and normalized probabilities of attack for each material tested. The complete results are available in Table D.1.

Table 30. Group A Capability Assessments

Assessed Likelihoods	Build	Use	Undetected	Attempts	P_S^{task}
Conversion	0.5	0.5	0.5	1	0.125
Reprocessing	1.00E-03	1.00E-03	1.00E-02	1	1E-08
Enrichment	1.00E-08	1.00E-03	0.05	1	5E-13
Machining	0.5	0.5	1	1	0.25
Metallurgy	0.5	0.5	1	1	0.25
IND Weaponization Gun-Type	0.9	0.5	0.5	1	0.225
RDD Weaponization	0.95	0.95	0.75	1	0.67687
IND Weaponization Implosion	0.075	0.01	0.5	1	3.75E-04

The Group A adversary should prefer all HEU over plutonium because of the greater likelihood of successfully weaponizing it. The results in Table 31 that correspond to diversion are indicated with (d) next to the material. The results for each material are as expected, with the adversary heavily favoring the HEU metals, a direct-use material. HEU metal is chosen 81.25% of the time. The remainder of the HEU materials make up the next 18.62%, and the likelihood of choosing plutonium pathways requiring implosion IND weaponization is essentially zero. The difference between probability of attack values for theft and diversion are based on the material attractiveness values, which are lower for diversion indicating the increased difficulty in covertly removing material verses overt removal. Because all other security parameters that favor covert diversion over overt theft were eliminated for this particular test, the diversion likelihoods are lower for each material when compared to theft likelihoods.

Table 31. Group A Probabilities of Attack

Material	U_a^{mat}	P_S	Normalized P_A
Uranium Weapons Grade Metal	3.94E-01	4.33E-03	3.31E-01
HEU (21.5%) metal	3.15E-01	4.33E-03	2.65E-01
Uranium Weapons Grade Metal (d)	1.92E-01	4.33E-03	1.61E-01
HEU (21.5%) metal (d)	6.60E-02	4.33E-03	5.54E-02
Weapons Grade UO_2 Cans	7.64E-01	3.61E-04	5.35E-02
Weapons Grade UO2 Cans (d)	7.57E-01	3.61E-04	5.30E-02
HEU (36%) Research Reactor Fresh Fuel Assembly	4.24E-01	3.61E-04	2.97E-02
HEU (36%) Research Reactor Fresh Fuel Assembly(d)	3.26E-01	3.61E-04	2.28E-02
HEU (21.5%) UO_2 Cans	3.11E-01	3.61E-04	2.17E-02
HEU (21.5%) UO_2 cans (d)	7.84E-02	3.61E-04	5.49E-03
Pu Metal Super Grade	4.18E-01	2.14E-06	1.74E-04
Pu Metal Weapons Grade	3.77E-01	2.14E-06	1.56E-04
Pu Metal Fuel Grade	3.34E-01	2.14E-06	1.39E-04
Pu Metal Reactor Grade	3.31E-01	2.14E-06	1.37E-04
Super Grade Pu Metal (d)	3.11E-01	2.14E-06	1.29E-04
Weapons Grade Pu Metal (d)	3.01E-01	2.14E-06	1.25E-04
Fuel Grade Pu Metal (d)	2.65E-01	2.14E-06	1.10E-04
Reactor Grade Pu Metal (d)	2.49E-01	2.14E-06	1.03E-04
PuO_2 Cans Super Grade	8.35E-01	1.78E-07	2.89E-05
PuO_2 Cans Super Grade (d)	8.35E-01	1.78E-07	2.89E-05
PuO_2 Cans Weapons Grade	7.53E-01	1.78E-07	2.61E-05
PuO_2 Cans Weapons Grade (d)	7.53E-01	1.78E-07	2.61E-05
PuO_2 Cans Fuel Grade	6.61E-01	1.78E-07	2.29E-05
PuO_2 Cans Fuel Grade(d)	6.61E-01	1.78E-07	2.29E-05
PuO_2 Cans Reactor Grade	6.22E-01	1.78E-07	2.15E-05
PuO_2 Cans Reactor Grade (d)	6.22E-01	1.78E-07	2.15E-05

Group B's assessed capabilities are presented in Table 32, and match Group A's capabilities except the likelihood of completing an implosion based IND is equivalent to the likelihood of producing a gun-type IND.

Table 32. Group B Capability Assessments

Assessed Likelihoods	Build	Use	Undetected	Attempts	P_S^{task}
Conversion	0.5	0.5	0.5	1	0.125
Reprocessing	1.00E-03	1.00E-03	1.00E-02	1	1E-08
Enrichment	1.00E-08	1.00E-03	0.05	1	5E-13
Machining	0.5	0.5	1	1	0.25
Metallurgy	0.5	0.5	1	1	0.25
IND Weaponization Gun-Type	0.9	0.5	0.5	1	0.225
RDD Weaponization	0.95	0.95	0.75	1	0.67687
IND Weaponization Implosion	0.9	0.5	0.5	1	0.225

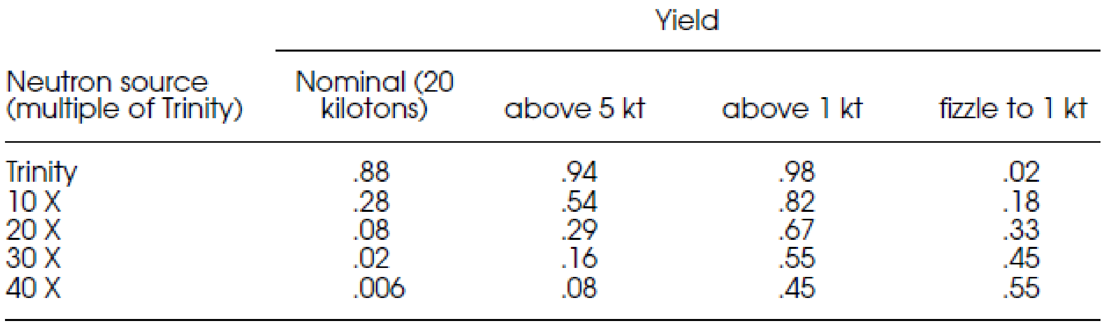
Table 33. Group B Probabilities of Attack for Various Materials

Material	$\boldsymbol{U_a^{mat}}$	$\mathbf{P_S}$	**Normalized** $\mathbf{P_A}$
Super Grade Pu Metal	4.18E-01	4.33E-03	9.82E-02
Weapons Grade U Metal	3.94E-01	4.33E-03	9.27E-02
Weapons Grade Pu Metal	3.77E-01	4.33E-03	8.86E-02
Super Grade Pu Metal (d)	3.34E-01	4.33E-03	7.86E-02
Fuel Grade Pu Metal	3.31E-01	4.33E-03	7.78E-02
Weapons Grade U metal (d)	3.15E-01	4.33E-03	7.42E-02
Reactor Grade Pu Metal	3.11E-01	4.33E-03	7.31E-02
Weapons Grade Pu Metal (d)	3.01E-01	4.33E-03	7.08E-02
Fuel Grade Pu Metal (d)	2.65E-01	4.33E-03	6.22E-02
Reactor Grade Pu Metal (d)	2.49E-01	4.33E-03	5.85E-02
HEU (21.5%) Metal	1.92E-01	4.33E-03	4.50E-02
Super Grade PuO_2	8.35E-01	3.61E-04	1.64E-02
Super Grade PuO_2 (d)	8.35E-01	3.61E-04	1.64E-02
HEU (21.5%) Metal (d)	6.60E-02	4.33E-03	1.55E-02
Weapons Grade UO_2 cans	7.64E-01	3.61E-04	1.50E-02
Weapons Grade UO_2 cans (d)	7.57E-01	3.61E-04	1.48E-02
Weapons Grade PuO_2	7.53E-01	3.61E-04	1.48E-02
Weapons Grade PuO_2 (d)	7.53E-01	3.61E-04	1.48E-02
Fuel Grade PuO_2	6.61E-01	3.61E-04	1.30E-02
Fuel Grade PuO_2 (d)	6.61E-01	3.61E-04	1.30E-02
Reactor Grade PuO_2	6.22E-01	3.61E-04	1.22E-02
Reactor Grade PuO_2 (d)	6.22E-01	3.61E-04	1.22E-02
HEU Research Reactor Fresh Fuel Assembly	4.24E-01	3.61E-04	8.31E-03
HEU Research Reactor Fresh Fuel Assembly (d)	3.26E-01	3.61E-04	6.39E-03
HEU (21.5%) UO_2 cans	3.11E-01	3.61E-04	6.09E-03
HEU (21.5%) UO_2 cans (d)	7.84E-02	3.61E-04	1.54E-03

Table 33 gives Group B's probabilities of choosing each material. The top tier of materials is made up of all direct-use weapons materials, with super grade plutonium metal being slightly preferred to weapons grade uranium metal. One observation from Table 33 is that there is not much difference between the likelihood of choosing super grade plutonium and reactor grade plutonium. A State would certainly prefer super grade plutonium over reactor grade plutonium, because a State is much more concerned with weapons reliability and maintenance. The degree to which a terrorist group would be deterred from lower quality plutonium is likely much less. The reason using higher quality plutonium in a weapon is preferred is that lower qualities of plutonium have a higher spontaneous fission rate which increases the chance of fizzling due to pre-initiation.[70] For most terrorist groups, the fact that the material produced any yield at all is likely more important than the actual size of the yield. There is also not a significant degradation in expected yield from lower quality plutonium.[f] Based on a letter from Oppenheimer, the neutron source strength effects on the expected yield of a weapon assuming an assembly rate twice as fast as the Trinity tests are presented in Table 34. Reactor grade plutonium has a neutron emission rate of approximately 6X greater than weapons grade plutonium, and based on the data in Table 34, the expected yields from weapons grade plutonium and reactor grade plutonium are approximately 17.94 kT and 13.54 kT respectively.

[f] This statement only considers the spontaneous fission neutron rate of the material. If the adversary doesn't have the explosives capability to achieve the necessary assembly rate or cannot devise provisions that account for the greater heating rate of reactor grade plutonium, the expected yield from an IND made with reactor grade material will be significantly less than that of a weapon that uses weapons grade plutonium. These considerations can be captured by using a more sophisticated IND consequence model than we were able to apply in this work.

Table 34. Probability of Achieving Indicated Yield Based on Neutron Source Strength[70]



	Yield			
Neutron source (multiple of Trinity)	Nominal (20 kilotons)	above 5 kt	above 1 kt	fizzle to 1 kt
Trinity	.88	.94	.98	.02
10 X	.28	.54	.82	.18
20 X	.08	.29	.67	.33
30 X	.02	.16	.55	.45
40 X	.006	.08	.45	.55

IV.B.3. Sensitivity Analysis Validation

To validate the sensitivity analysis calculations, we introduce a symmetric problem that has identical facilities by taking the verification test and replicating each facility so that there are three identical hospitals and three identical research reactors. We then conduct a sensitivity analysis on each of the security parameters at all facilities to confirm that they are identical to each other. The five facility related variables that caused the greatest change in risk based on a 10% perturbation in the original value are given in Table 35.

Table 35. IND Related Symmetric Sensitivity Results

	Research Reactor 1		Research Reactor 2		Research Reactor 3	
	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$
HEU → LEU	1	1.47E-06	1	1.47E-06	1	1.47E-06
PPS Layer 1 P_N	0.07	3.48E-07	0.07	3.48E-07	0.07	3.48E-07
PPS Layer 3 P_N	0.07	2.64E-07	0.07	2.64E-07	0.07	2.64E-07
PPS Layer 3 P_I	0.075	2.09E-07	0.075	2.09E-07	0.075	2.09E-07
PPS Layer 1 P_I	0.05	5.55E-08	0.05	5.55E-08	0.05	5.55E-08

The results from Table 35 validate that the sensitivity values for each variable are identical. In addition, the five highest sensitivity values correspond to security measures associated with HEU fuel, which makes sense considering the results from Table 26 show this material is the single largest contributor to risk. The first variable represents replacing the HEU with LEU fuel and the next four variables are physical protection parameters.

The sensitivity for variables related to sabotage at each research reactor are displayed in Table 36, and while each variable has the same sensitivity value, the risk sensitivities for three variables are negative. This means upgrades to these parameters actually increase risk. This occurs because these risk values represent conditional risk, meaning the likelihood the adversary chooses to attack is unity. This assumption causes the adversary to react to security upgrades on these paths by increasing the relative likelihood of other paths. The negative conditional risk change is a result of the differences between the relative likelihood of choosing the sabotage pathways associated with the research reactor and the relative risk these pathways represent. From the verification test, the likelihood of choosing these pathways (pathways SAB1-SAB4) is 28.13%, while these pathways only contribute to 9.78% of the total risk. The result is that sabotage upgrades cause some of the relative likelihood of choosing the less-risky sabotage paths to be redistributed to higher-risk pathways. An increase in conditional risk does not necessarily mean the absolute value of risk has increase, because upgrades that cause a conditional risk increase may simultaneously decrease the probability the adversary decides to attack.

Table 36. Sabotage Related Symmetric Sensitivity Results

	Research Reactor 1		Research Reactor 2		Research Reactor 3	
	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$
P_{Cons}^{Sab} Reactor	0.036	-2.8E-08	0.036	-2.8E-08	0.036	-2.8E-08
P_{Cons}^{Sab} Spent Fuel Pool	0.068	-1.6E-08	0.068	-1.6E-08	0.068	-1.6E-08
ε_{Sab}^{Ins} Reactor	0.030	-6.47E-09	0.030	-6.47E-09	0.030	-6.47E-09
ε_{Sab}^{Ins} Spent Fuel	0.100	-2.9E-09	0.100	-2.9E-09	0.100	-2.9E-09

The next validation test checks the behavior of sensitivity values in an non-symmetric system. The security parameters (PPS at all layers, $\varepsilon_{Sab}^{Ins}, P_{Cons}^{Sab}$) at the first research reactor are all degraded, keeping those parameters at the other two facilities the same as the symmetric case. This increases the risk along pathways associated with research reactor 1 relative to the other two research reactors, and as a result the sensitivity to changes should also increase relative to the other two research reactors. The results from the sensitivity tests for this non-symmetric test are presented in Table 37 and Table 38.

Table 37. IND Related Non-Symmetric Sensitivity Results

	Research Reactor 1*		Research Reactor 2		Research Reactor 3	
	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$
HEU → LEU	1	4.22E-06	1	1.39E-06	1	1.39E-06
PPS Layer 1 P_N	0.0525	3.34E-07	0.07	3.18E-07	0.07	3.18E-07
PPS Layer 3 P_N	0.0525	3.16E-07	0.07	2.50E-07	0.07	2.50E-07
PPS Layer 3 P_I	0.0675	3.16E-07	0.075	1.98E-07	0.075	1.98E-07
PPS Layer 1 P_I	0.0375	1.23E-07	0.05	4.55E-08	0.05	4.55E-08

Table 38. Sabotage Related Non-Symmetric Sensitivity Results

	Research Reactor 1		Research Reactor 2		Research Reactor 3	
	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$
P_{Cons}^{Sab} Reactor	0.048	-4.05E-08	0.036	-3.52E-08	0.036	-3.52E-08
P_{Cons}^{Sab} Spent Fuel Pool	0.082	-1.72E-08	0.068	-3.27E-08	0.068	-3.27E-08
ε_{Sab}^{Ins} Reactor	0.0225	-6.24E-09	0.030	-8.33E-09	0.030	-8.33E-09
ε_{Sab}^{Ins} Spent Fuel	0.075	-5.46E-10	0.100	-1.65E-08	0.100	-1.65E-08

Degrading security features changes the value of $\mathbb{R}$ for the non-symmetric case, and because most sensitivity values were calculated by perturbing the variable by 10%, the value for ΔVar also changes in the non-symmetric case. To compare the sensitivity values between the symmetric and non-symmetric cases, Table 39 shows the IND related normalized change in risk $\left(\frac{\Delta\mathbb{R}}{\mathbb{R}}\right)$ for the symmetric case. For the non-symmetric IND related case, Table 40 shows the normalized change in risk, compensating for different ΔVar values for research reactor 1 using $\left(\frac{\Delta\mathbb{R}}{\mathbb{R}}\right)*\left(\frac{\Delta Var_{Symmetric}}{\Delta Var_{Non-Symmetric}}\right)$.

Table 39. IND Related Symmetric Relative Sensitivity Results

Variable	Research Reactor 1	Research Reactor 2	Research Reactor 3
Replace HEU with LEU	9.56%	9.56%	9.56%
PPS Layer 1 P_N	2.26%	2.26%	2.26%
PPS Layer 3 P_N	1.71%	1.71%	1.71%
PPS Layer 3 P_I	1.36%	1.36%	1.36%
PPS Layer 1 P_I	0.36%	0.36%	0.36%

Table 40. IND Related Non-Symmetric Relative Sensitivity Results

Variable	Research Reactor 1*	Research Reactor 2	Research Reactor 3
Replace HEU with LEU	22.70%	7.49%	7.49%
PPS Layer 1 P_N	2.39%	1.71%	1.71%
PPS Layer 3 P_N	2.26%	1.35%	1.35%
PPS Layer 3 P_I	1.89%	1.06%	1.06%
PPS Layer 1 P_I	0.89%	0.24%	0.24%

Comparing Table 39 and Table 40, the relative sensitivity at research reactor 1 increased for every IND related security measure in the non-symmetric case, while decreasing at the other two research reactors. The relative sensitivity results from the sabotage related security measures are displayed in Table 41 and Table 42, and show the same relationship.

Table 41. Sabotage Related Symmetric Relative Sensitivity Results

Variable	Research Reactor 1	Research Reactor 2	Research Reactor 3
P_{Cons}^{Sab} Reactor	-0.18%	-0.18%	-0.18%
P_{Cons}^{Sab} Spent Fuel Pool	-0.11%	-0.11%	-0.11%
ε_{Sab}^{Ins} Reactor	-0.042%	-0.042%	-0.042%
ε_{Sab}^{Ins} Spent Fuel	-0.02%	-0.02%	-0.02%

Table 42. Sabotage Related Non-Symmetric Relative Sensitivity Results

Variable	Research Reactor 1*	Research Reactor 2	Research Reactor 3
P_{Cons}^{Sab} Reactor	-0.16%	-0.19%	-0.19%
P_{Cons}^{Sab} Spent Fuel Pool	-0.08%	-0.18%	-0.18%
ε_{Sab}^{Ins} Reactor	-0.034%	-0.045%	-0.045%
ε_{Sab}^{Ins} Spent Fuel	0.00%	-0.09%	-0.09%

To test the assumption that the negative sensitivity values are a result of the sabotage pathways being low risk, the same problem is repeated, but the consequence values from the verification test are increased at each reactor to the values in Table 43, which correspond to a 20-times increase in loss of life, infrastructure loss and economic loss. The original set of consequence values assumed the research reactor was in a remote location, while the new values may represent the consequences associated with the same reactor being near a more populated area.

Table 43. Modified Sabotage Consequence Values

Sabotage Event	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	1.00E-10	9.00E-05	6.00E-05	5.00E-04
Reactor	2.00E-07	7.20E-05	2.00E-05	5.00E-04

Changing these consequence values increases the State-level risk value to $2.42 \text{x} 10^{-5}$ from $1.538 \text{x} 10^{-5}$. The likelihood of choosing each pathway and relative risk of each pathway are given in Table 44, which shows a shift from the IND paths being the highest risk pathways to the sabotage pathways associated with the research reactors accounting for 59.73% of the total risk.

Table 44. Relative Likelihood of Choosing and Relative Risk of Each Pathway for Modified Sabotage Consequences

Pathway	$\boldsymbol{P_a^{path}}$	$\%\mathbb{R}$
IND1	1.75E-03	8.16%
IND2	1.27E-03	4.75%
IND3	5.56E-05	0.05%
IND4	4.11E-05	0.03%
IND5	4.55E-12	0.00%
IND6	3.31E-12	0.00%
IND7	1.24E-14	0.00%
IND8	9.15E-15	0.00%
RDD1	7.71E-02	4.30%
RDD2	5.96E-02	3.39%
RDD3	2.30E-02	0.86%
RDD4	1.81E-02	0.70%
RDD5	7.63E-02	6.31%
RDD6	5.85E-02	4.85%
RDD7	3.50E-04	0.00%
RDD8	2.73E-04	0.00%
RDD9	2.55E-02	0.54%
RDD10	1.08E-02	0.22%
RDD11	2.03E-02	3.21%
RDD12	1.54E-02	2.31%
RDD13	1.28E-04	0.00%
RDD14	9.86E-05	0.00%
RDD15	7.00E-03	0.50%
RDD16	6.30E-05	0.00%
SAB1	1.14E-01	10.97%
SAB2	2.16E-01	39.39%
SAB3	7.94E-02	4.34%
SAB4	8.55E-02	5.03%
SAB5	2.67E-02	0.02%
SAB6	2.80E-02	0.02%
SAB7	2.64E-02	0.02%
SAB8	2.83E-02	0.03%

The sensitivity analysis is re-run and the results for the sabotage variables that had negative sensitivities in the first problem are presented in Table 45 for the symmetric case and Table 46 for the non-symmetric case. These values are converted to relative sensitivity values in Table 47 and Table 48 to allow for a direct comparison.

Table 45. Sabotage Related Symmetric Sensitivity Results for Modified Case

	Research Reactor 1		Research Reactor 2		Research Reactor 3	
	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$
P_{Cons}^{Sab} Reactor	0.036	1.03E-08	0.036	1.03E-08	0.036	1.03E-08
P_{Cons}^{Sab} Spent Fuel Pool	0.068	4.68E-07	0.068	4.68E-07	0.068	4.68E-07
ε_{Sab}^{Ins} Reactor	0.200	1.7E-09	0.200	1.7E-09	0.200	1.7E-09
ε_{Sab}^{Ins} Spent Fuel	0.200	8.82E-07	0.200	8.82E-07	0.200	8.82E-07

Table 46. Sabotage Related Non-Symmetric Sensitivity Results for Modified Case

	Research Reactor 1		Research Reactor 2		Research Reactor 3	
	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$	ΔVar	$\Delta\mathbb{R}$
P_{Cons}^{Sab} Reactor	0.048	8.67E-08	0.036	-1.2E-08	0.036	-1.2E-08
P_{Cons}^{Sab} Spent Fuel Pool	0.082	8.31E-07	0.068	3.88E-07	0.068	3.88E-07
ε_{Sab}^{Ins} Reactor	0.200	7.81E-08	0.200	-3.4E-08	0.200	-3.4E-08
ε_{Sab}^{Ins} Spent Fuel	0.200	1.23E-06	0.200	7.44E-07	0.200	7.44E-07

Table 47. Sabotage Related Symmetric Relative Sensitivity Results for Modified Case

Variable	Research Reactor 1	Research Reactor 2	Research Reactor 3
P_{Cons}^{Sab} Reactor	0.04%	0.04%	0.04%
P_{Cons}^{Sab} Spent Fuel Pool	1.93%	1.93%	1.93%
ε_{Sab}^{Ins} Reactor	0.01%	0.01%	0.01%
ε_{Sab}^{Ins} Spent Fuel	3.65%	3.65%	3.65%

Table 48. Sabotage Related Non-Symmetric Relative Sensitivity Results for Modified Case

Variable	Research Reactor 1*	Research Reactor 2	Research Reactor 3
P_{Cons}^{Sab} Reactor	0.22%	-0.04%	-0.04%
P_{Cons}^{Sab} Spent Fuel Pool	2.40%	1.34%	1.34%
ε_{Sab}^{Ins} Reactor	0.27%	-0.12%	-0.12%
ε_{Sab}^{Ins} Spent Fuel	4.26%	2.57%	2.57%

From Table 44, pathways SAB1 and SAB2 correspond to the spent fuel pool sabotage scenario, which made up over 50% of the total state level risk. As expected, the sensitivity for variables associated with these pathways increased significantly from the previous case where IND and RDD routes made up a much larger portion of the State-level risk. Table 47 shows that the sensitivity values are all positive for the modified symmetric case, with variables associated with sabotage of the spent fuel pool being much more sensitive than the reactor sabotage variables. Table 48 shows the same trend as the un-modified case for a non-symmetric system, where variables associated with the degraded research reactor increase relative to their symmetric values, while the associated variables at the other two research reactors decrease.

IV.C. Behavioral Tests

Behavioral tests introduce different scenarios into the code to look for unexpected trends or behaviors. For these tests we take one facility and replicate it multiple times, observing the change in risk value. We then run each case again adding a target that has consequence values for each nuclear threat with one one-half those of the first target. The data for these tests is available in Appendix E. The results are displayed in Table 49.

Table 49. Risks for Behavioral Tests Normalized to P_A=1

	1 Target	2 Targets
1 Facility	2.018E-05	1.694E-05
2 Facilities	2.018E-05	1.694E-05
3 Facilities	2.018E-05	1.694E-05
4 Facilities	2.018E-05	1.694E-05
5 Facilities	2.018E-05	1.694E-05

There are two observations from the results in Table 49. The first is that adding more facilities and more materials had no effect on risk. This is due to the normalization of P_A values to unity, meaning the risk values in Table 49 represent the conditional risk of a single nuclear terrorist attack. Based on this assumption, the probability of adversary success and consequences along each pathway stays the same because each facility is identical, and the relative likelihood of choosing each path simply decreases proportionally to the number of facilities that are added. The second observation is that adding a second target decreased the risk value, with all other things the same. This is counter-intuitive because the security infrastructure within the State did not change. The decrease in risk value is attributed to the fact that in the scenario with a single target, the adversary must choose to attack that target. By adding a second target, some of the probability of the adversary choosing the higher consequence target is diverted to the lower consequence target. Thus, lower consequence pathways are averaged with the higher risk pathways. If a representative set consisting of multiple targets is analyzed, then this effect should be minimized. However, to ensure that additional variables aren't introduced into the analysis when analyzing security measure upgrades, if the number of targets a State is analyzing changes, the base-line risk should be recalculated.

The assumption used in this model is the value of $P_{A,i}^{V}$ from Equation 23 is proportional to the actual probability the adversary chooses each pathway. These $P_{A,i}^{V}$ values are then normalized to unity. Normalizing $P_{A,i}^{V}$ values is required to capture the dynamic relationship between security upgrades and terrorist decision making when evaluating upgrades within the State. Without normalizing these values, characteristics such as risk transfer are not captured by the model. Relating the conditional risk of nuclear terrorism calculated by the model to the absolute risk of nuclear terrorism requires information on the frequency the adversary chooses nuclear terrorism. This frequency is related to factors outside of nuclear terrorism, such as the attractiveness and likelihood of success of other types of terrorism. For this dissertation, we use conditional risk because it is independent of other these other factors. A simplified diagram that shows the risk of nuclear terrorism as a subset of terrorism risk is provided in Figure 25. It shows all of the various factors that contribute to the likelihood an adversary chooses nuclear terrorism.

The model can also be used to calculate the absolute risk of nuclear terrorism. If we take the assumption that the likelihood of choosing nuclear terrorism is proportional to the value of $P_{A,i}^{V}$, the same calculation displayed in Table 49 is repeated without normalizing P_A values. These results are displayed in Table 50. The values in the first column represent the risk to the one target, and the difference in the values in column 1 and 2 represent the risk to the second, lower consequence target. These un-normalized risk values still must be multiplied by the frequency of attack.

Table 50. Un-normalized Risks for Behavioral Tests

	1 Target	2 Targets
1 Facility	2.242E-10	2.803E-10
2 Facilities	4.485E-10	5.606E-10
3 Facilities	6.727E-10	8.409E-10
4 Facilities	8.970E-10	1.121E-09
5 Facilities	1.121E-09	1.402E-09

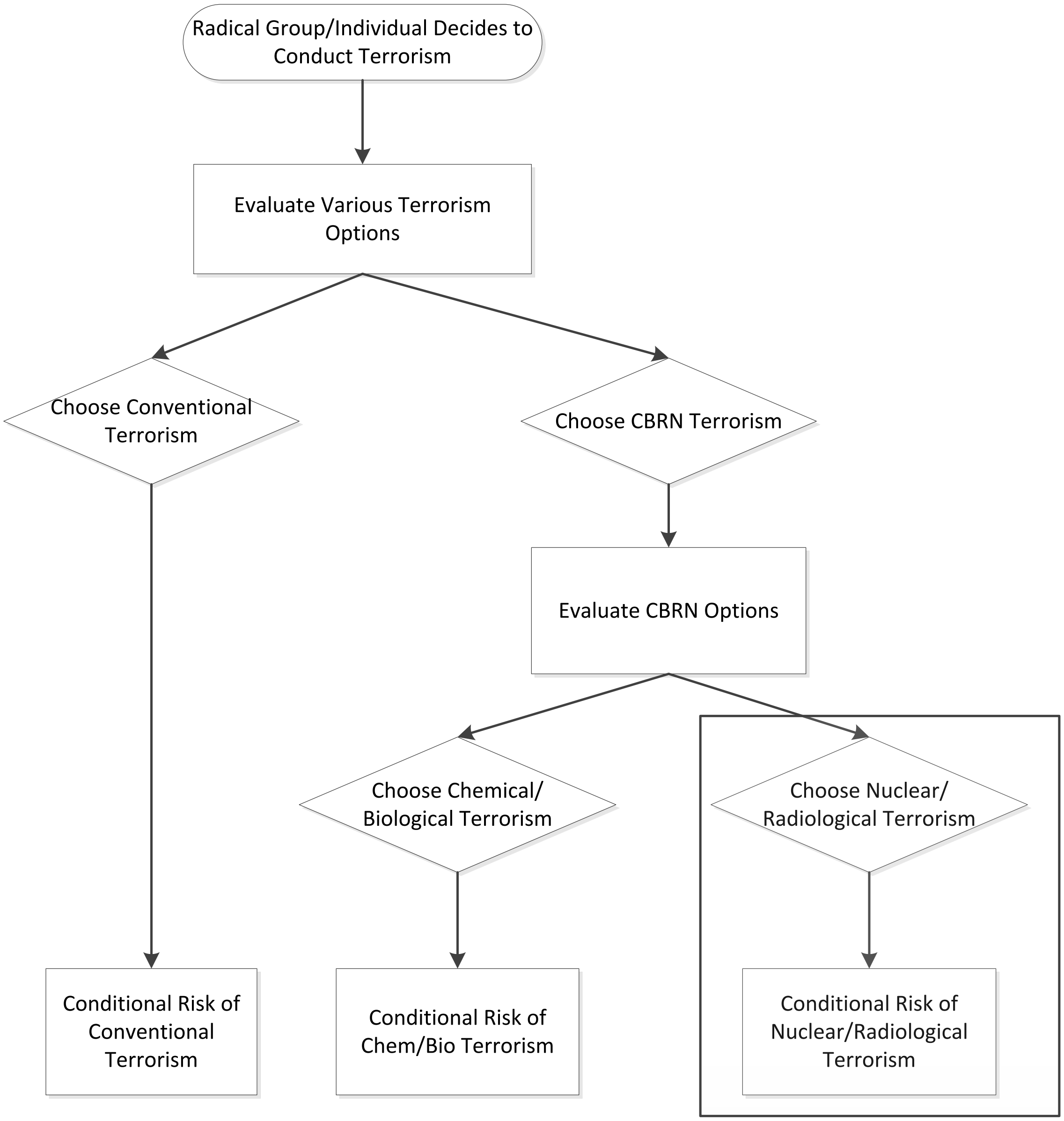

Radical Group/Individual Decides to Conduct Terrorism
Evaluate Various Terrorism Options
Choose Conventional Terrorism
Choose CBRN Terrorism
Evaluate CBRN Options
Choose Chemical/ Biological Terrorism
Choose Nuclear/ Radiological Terrorism
Conditional Risk of Conventional Terrorism
Conditional Risk of Chem/Bio Terrorism
Conditional Risk of Nuclear/Radiological Terrorism

Figure 25. The Risk of Nuclear Terrorism is a Subset of Terrorism Risk

CHAPTER V

TEST CASES

A number of strategies can be employed to manage State-level risk, and the effectiveness of each strategy likely varies based on the complexity of the State's infrastructure and threat characteristics faced by that State. In this chapter, we develop three fictional States with nuclear infrastructures of varying complexities. Each infrastructure was developed to provide a representative sample of nuclear and radiological materials that could be present in a real-world State. We then apply the methodology in Chapter III to assess different risk reductions strategies and how the effectiveness of these strategies may change based on the complexity of the State's infrastructure and the characteristics of the adversary. The strategies investigated are:

- Material Consolidation - consolidating materials from multiple facilities into a smaller number of hardened facilities;
- Material Conversion - converting materials to less attractive categories (e.g. replacement of HEU with LEU); and
- Material Removal - removing material from a State.

In addition, we conduct a sensitivity analysis on all nuclear security measures to determine which security measures the State can upgrade to have the maximum risk reduction. We then simulate the set of nuclear security measure upgrades that will decrease the risk by 50%.

Finally, we conduct sensitivity analysis on the assessed terrorist capabilities to determine how changes in terrorist capabilities affect the State-level risk. These tests serve a couple purposes. First, this methodology uses terrorist capabilities as inputs, and it is likely that there is a good amount of uncertainty in the assessed likelihoods of the adversary completing each task. Observing how the State-level risk of nuclear terrorism changes based on changes in terrorist capabilities gives insight into which capabilities the State should be concerned with. These concerns can be addressed by applying resources to gain confidence in the value or using more conservative values to evaluate the State-level risk. The second purpose these tests serve to add quantitative data to the discussion in Chapter I, where we introduced the lack of consensus between terrorism experts on the likelihood that a terrorist could and would produce a nuclear weapon. Because we use conditional risk, we assume the terrorist group will conduct nuclear terrorism, however these tests show how sensitive the State-level risk is to the answer to *"Could terrorists produce a nuclear weapon?"*.

Three adversaries are modeled against each State infrastructure. Each of the three adversaries has identical capabilities, but different motivations and disincentives. The first group's motivations for nuclear terrorism favor lower consequence threats such as RDD and sabotage threats. The second group has no preference between the nuclear threats. The third group's motivations for nuclear terrorism heavily favor higher consequence threats, like nuclear weapon theft and IND threats. Details on the adversaries modeled in these test cases are available in Appendix F.

V.A. Small State Infrastructure

The small State analyzed in this section does not have commercial nuclear power reactors. Their nuclear materials consist of fresh LEU fuel and spent HEU fuel at research reactors that are used for research and isotope production. The small State also has various industrial and medical isotopes. Compared to the States with more complex nuclear infrastructures, the State has less stringent nuclear security measures employed at each facility. The details the State infrastructure are available in Appendix F.

V.A.1. Small State Infrastructure Risk Analysis

Table 51 gives the risk from each nuclear threat for the small State infrastructure. The lack of risk from IND is due to the lack of direct-use nuclear material in the State which leads to a very low likelihood that either adversary group could acquire weapons usable material. The pathways that contribute the most to the State-level risk and their relative contribution to risk are presented in Table 52.

Table 51. Small Infrastructure Threats Risk

Threat	$\mathbb{R}_{Group\ 1}$	$\mathbb{R}_{Group\ 2}$	$\mathbb{R}_{Group\ 3}$
IND	0.00%	0.00%	0.00%
RDD	37.93%	28.99%	20.53%
Sabotage	51.87%	63.22%	73.95%

Table 52. Small State Pathway Risk

Radiological Dispersion Device				
Facility	**Material**	$\%\mathbb{R}_{Group\ 1}$	$\%\mathbb{R}_{Group\ 2}$	$\%\mathbb{R}_{Group\ 3}$
Hospital	Gamma-Knife Co-60 Source	14.37%	11.93%	7.63%
Industrial Source Location 1	Co-60 Industrial Radiography Sources	8.30%	6.36%	4.41%
Industrial Source Location 2	Co-60 Industrial Radiography Sources	5.17%	3.97%	2.75%
Industrial Source Location 1	Ir-192 Industrial Radiography Sources	4.94%	3.83%	2.62%
Hospital	HDR Brachytherapy Seeds	4.87%	3.71%	2.59%
30 MWth Reactor	Irradiated LEU Fuel	3.36%	2.96%	1.78%
2 MWth Reactor	Irradiated LEU Fuel	3.44%	2.8%	1.83%
Sabotage				
Facility	**Sabotage Target**	$\%\mathbb{R}_{Group\ 1}$	$\%\mathbb{R}_{Group\ 2}$	$\%\mathbb{R}_{Group\ 3}$
30 MWth Reactor	Spent Fuel Pool	27.76%	32.53%	38.84%
30 MWth Reactor	Reactor	19.96%	23.26%	27.92%
100Wth Reactor	Spent Fuel Pool	3.56%	4.14%	4.98%
100Wth Reactor	Reactor	2.34%	2.81%	3.27%

Based on the results in Table 52, the largest single contributor to risk is the sabotage of the 30 MWth reactor, followed by the high activity Co-60 source. The change in motivations for group 3 towards higher consequence pathways leads to a higher likelihood of choosing the higher consequence sabotage pathways instead of the RDD pathways, which is represented by the greater risk to sabotage targets and lower risk to RDD targets.

V.A.2. Small State Infrastructure Risk Reduction Analysis

Applying the methodology from Chapter III, we evaluate three risk reduction strategies that this State could employ to address the State-level risk of nuclear terrorism. The first option is to remove the spent fuel from on-site storage at each reactor to a location that is away from population centers and has better physical security measures in place. The details of the facility are given in Appendix F. The second option is to decommission the 30 MWth reactor and remove the material. The third option is to remove the Co-60 Gamma Knife source from the hospital. The results for each option are given in Table 53.

Table 53. Small State Risk Reduction Results

Security Measure	$\%\mathbb{R}_{Group\ 1}$	$\%\mathbb{R}_{Group\ 2}$	$\%\mathbb{R}_{Group\ 3}$
Consolidate Spent Fuel	28.79%	31.58%	33.23%
Remove 30 MWth Reactor	53.79%	60.36%	66.35%
Remove Gamma Knife Source	4.70%	1.86%	-0.28%

The results from Table 53 must be analyzed in context. Based on the results, removing the 30 MWth reactor would be the preferred option. However, the State will lose both the research capabilities provided by the reactor and will lose their domestic ability to produce radioisotopes for medical applications. Consolidating the spent fuel is an attractive option, as it removes spent fuel from all research reactors, some located in proximity to cities, to a lower consequence location. Removing the gamma knife source has a small risk-reduction benefit compared to its contribution to risk in Table 52. This is because there are a number of other potential RDD sources available within the State, and removing the gamma knife source transfers a good portion of risk to the other sources. For the third group, removing the gamma knife source eliminates that option and increases the likelihood they will attempt higher consequence sabotage pathways, which increases the State's conditional risk value. Removing the gamma knife source may also not be in the State's interest, as it is used to treat cancer patients. If the State lacks dependable power, replacing the gamma knife source with a linear accelerator may be impractical.

Rather than employ any of these strategies, the State can upgrade various nuclear security measures at their existing facilities. Using sensitivity analysis, the security measures which have greatest impact on State-level risk are determined for each group. The results are displayed in Table 54, Table 55, and Table 56 show the most sensitive security measures in the State for each group, the threats addressed by upgrading these security measures, and the change in risk based on a 10% improvement to that security measure. The variables that represent the upgraded nuclear security measures are defined in Chapter III.

Table 54. Small State Most Sensitive Security Measures - Group 1

Nuclear Security Measure	Threat Addressed	$\Delta\mathbb{R}$
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Spent Fuel Storage Sabotage	5.98%
30 MWth Reactor P_{Cons}^{Sab}	30MWth Reactor - Spent Fuel Storage Sabotage	3.76%
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Reactor Sabotage	3.23%
30 MWth Reactor - Layer 1 P_N	30MWth spent fuel sabotage, 30MWth spent fuel sabotage, RDD using Spent Fuel	3.11%
30 MWth P_{Cons}^{Sab}	30MWth reactor sabotage	2.59%
30 MWth Research Reactor - Layer 1 P_I	30MWth spent fuel sabotage, 30MWth spent fuel sabotage, RDD using Spent Fuel	2.40%
30 MWth Research Reactor - Layer 2 P_I	30MWth spent fuel sabotage, RDD using Spent Fuel	0.49%
30 MWth Research Reactor - Layer 2 P_N	30MWth spent fuel sabotage, RDD using Spent Fuel	0.49%
Hospital Cancer Center - Layer 3 P_N	Gamma Knife Co-60 Theft	0.42%
Hospital Cancer Center - Layer 3 P_I	Gamma Knife Co-60 Theft	0.42%
100W Reactor ε_{Sab}^{Ins}	100 W Spent Fuel Sabotage	0.35%
100W Reactor P_{Cons}^{Sab}	100 W Spent Fuel Sabotage	0.30%

Table 55. Small State Most Sensitive Security Measures - Group 2

Nuclear Security Measure	Threat Addressed	$\Delta\mathbb{R}$
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Spent Fuel Storage Sabotage	7.08%
30 MWth Reactor P_{Cons}^{Sab}	30MWth Reactor - Spent Fuel Storage Sabotage	4.47%
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Reactor Sabotage	3.77%
30 MWth Reactor - Layer 1 P_N	30MWth spent fuel sabotage, 30MWth spent fuel sabotage, RDD using Spent Fuel	3.53%
30 MWth P_{Cons}^{Sab}	30MWth reactor sabotage	3.06%
30 MWth Research Reactor - Layer 1 P_I	30MWth spent fuel sabotage, 30MWth spent fuel sabotage, RDD using Spent Fuel	2.69%
30 MWth Research Reactor - Layer 2 P_I	30MWth spent fuel sabotage, RDD using Spent Fuel	0.57%
30 MWth Research Reactor - Layer 2 P_N	30MWth spent fuel sabotage, RDD using Spent Fuel	0.57%
100W Reactor ε_{Sab}^{Ins}	100 W Spent Fuel Sabotage	0.36%
100W Reactor P_{Cons}^{Sab}	100 W Spent Fuel Sabotage	0.32%
Hospital Cancer Center - Layer 3 P_N	Gamma Knife Co-60 Theft	0.29%
Hospital Cancer Center - Layer 3 P_I	Gamma Knife Co-60 Theft	0.29%

Table 56. Small State Most Sensitive Security Measures - Group 3

Nuclear Security Measure	Threat Addressed	$\Delta\mathbb{R}$
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Spent Fuel Storage Sabotage	8.01%
30 MWth Reactor P_{Cons}^{Sab}	30MWth Reactor - Spent Fuel Storage Sabotage	5.09%
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Reactor Sabotage	4.16%
30 MWth Reactor - Layer 1 P_N	30MWth spent fuel sabotage, 30MWth spent fuel sabotage, RDD using Spent Fuel	3.89%
30 MWth P_{Cons}^{Sab}	30MWth reactor sabotage	3.44%
30 MWth Research Reactor - Layer 1 P_I	30MWth spent fuel sabotage, 30MWth spent fuel sabotage, RDD using Spent Fuel	2.94%
30 MWth Research Reactor - Layer 2 P_I	30MWth spent fuel sabotage, RDD using Spent Fuel	0.64%
30 MWth Research Reactor - Layer 2 P_N	30MWth spent fuel sabotage, RDD using Spent Fuel	0.64%
100W Reactor ε_{Sab}^{Ins}	100 W Spent Fuel Sabotage	0.33%
100W Reactor P_{Cons}^{Sab}	100 W Spent Fuel Sabotage	0.29%
Hospital Cancer Center - Layer 3 P_N	Gamma Knife Co-60 Theft	0.17%
Hospital Cancer Center - Layer 3 P_I	Gamma Knife Co-60 Theft	0.17%

The sensitivity results show that the differences in adversary motivations and disincentives between each group do not change which security measures should be employed, as the same twelve security measures are the most sensitive for each group. The changes correspond to the motivational preferences of each group. Upgrades that address the threat of group 1 are more sensitive for RDD pathways and upgrades that address the threats posed by group 3 are more sensitive to Sabotage pathways.

Employing these sensitivity results, we simulate the optimal set of upgrades that will decrease the State-level risk posed by each group by 50%. The results for group 1 are given in Table 57. The upgrades in Table 57 represent a 49.3% decrease in State-level risk. Each upgrade is associated with one of the five riskiest pathways. The upgrade analysis did not quite reach 50% because the State reached a stable condition, where any upgrades or groups of upgrades were off-set by the transfer of risk to other pathways. The risk from each material after introducing the proposed security measures in Table 57 are given in Table 58, and show that many of the pathways have equivalent risk contributions.

Table 57. Optimal Security Measures for Small State - Group 1

Security Measure	Threat Addressed	Original Value	Upgraded Value
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Spent Fuel Storage Sabotage	0.55	0.9
30 MWth Reactor P_{Cons}^{Sab}	30MWth Reactor - Spent Fuel Storage Sabotage	0.75	0.3
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Reactor Sabotage	0.55	0.8
30 MWth Reactor P_{Cons}^{Sab}	30MWth Reactor - Reactor Sabotage	0.85	0.4
Hospital Cancer Center - Layer 3 P_N	Gamma Knife Co-60 Theft and RDD	0.25	0.9
Hospital Cancer Center - Layer 3 PI	Gamma Knife Co-60 Theft and RDD	0.75	0.8
Industrial Source Location 1 Layer 1P_N	Industrial Radiography Co-60 Theft and RDD	0.1	0.9
Industrial Source Location 1 Layer 1 P_I	Industrial Radiography Co-60 Theft and RDD	0.2	0.9
Hospital Cancer Center - Layer 2 P_N	HDR Brachytherapy Seeds Theft and RDD	0.1	0.5
Industrial Source Location 1 Layer 2P_N	Industrial Radiography Co-60 Theft and RDD	0.25	0.75
Industrial Source Location 1 Layer 2 P_I	Industrial Radiography Co-60 Theft and RDD	0.5	0.6
Industrial Source Location 2 Layer 1P_N	Industrial Radiography Co-60 Theft and RDD	0.1	0.5
Industrial Source Location 2 Layer 1 P_I	Industrial Radiography Co-60 Theft and RDD	0.2	0.7

Table 58. State-Level Risk Breakdown for Group 1 After Upgrades

Facility	Material	% ℝ
Radiological Dispersion Device		
Hospital	Gamma-Knife Co-60 Source	5.09%
Industrial	Co-60 Industrial Radiography	10.72%
Industrial	Co-60 Industrial Radiography	7.41%
Industrial	Ir-192 Industrial Radiography Source	6.24%
Hospital	HDR Brachytherapy Seeds	9.27%
30 MWth Reactor	Irradiated LEU Fuel	10.00%
2 MWth Reactor	Irradiated LEU Fuel	10.24%
Sabotage		
30 MWth Reactor	Spent Fuel Pool	8.08%
30 MWth Reactor	Reactor	9.64%
100Wth Reactor	Spent Fuel Pool	10.60%
100Wth Reactor	Reactor	6.97%

The optimal risk upgrades for group 2 are given in Table 59, and represent a 50.01% decrease in State-level risk. The upgrades for group 2 required much fewer upgrades than group 1, because the risk of the 30 MWth sabotage pathways dominated the State-level risk. The risk-reduction goal was met by applying security measure upgrades to the four riskiest pathways from Table 52.

Table 59. Optimal Security Measures for Small State - Group 2

Security Measure	Threat Addressed	Original Value	Upgraded Value
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Spent Fuel Storage Sabotage	0.55	0.8
30 MWth Reactor P_{Cons}^{Sab}	30MWth Reactor - Spent Fuel Storage Sabotage	0.75	0.35
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Reactor Sabotage	0.55	0.8
30 MWth Reactor P_{Cons}^{Sab}	30MWth Reactor - Reactor Sabotage	0.85	0.4
Hospital Cancer Center - Layer 3 P_N	Gamma Knife Co-60 Theft and RDD	0.25	0.6
Hospital Cancer Center - Layer 3 PI	Gamma Knife Co-60 Theft and RDD	0.75	0.8
Industrial Source Location 1 Layer 1P_N	Industrial Radiography Co-60 Theft and RDD	0.1	0.25
Industrial Source Location 1 Layer 1 P_I	Industrial Radiography Co-60 Theft and RDD	0.2	0.25

Table 60 shows the optimal security measures for group 3 that represent a 51.45% decrease in State-level risk. For this case, the sabotage pathways dominated the risk relative to group 1 and group 2, so the relative decrease in risk for applying upgrades to these pathways for group 3 was greater resulting in fewer total upgrades being applied to reach the same risk-reduction.

Table 60. Optimal Security Measures for Small State - Group 3

Security Measure	Threat Addressed	Original Value	Upgraded Value
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Spent Fuel Storage Sabotage	0.55	0.8
30 MWth Reactor P_{Cons}^{Sab}	30MWth Reactor - Spent Fuel Storage Sabotage	0.75	0.4
30 MWth Reactor ε_{Sab}^{Ins}	30MWth Reactor - Reactor Sabotage	0.55	0.8
30 MWth Reactor P_{Cons}^{Sab}	30MWth Reactor - Reactor Sabotage	0.85	0.45
Hospital Cancer Center - Layer 3 PN	Gamma Knife Co-60 Theft and RDD	0.25	0.5
Hospital Cancer Center - Layer 3 PI	Gamma Knife Co-60 Theft and RDD	0.75	0.8

Based on the pathway risks in Table 52, these upgrade results make sense as security upgrades are applied to address the most-risky pathways for each case. The differences in motivations between the three adversary groups modeled does result in some changes in the State level-risk. However, this is expected as the conditional risk of group 3 should be higher because they are inclined to attempt higher consequence pathways relative to groups 1 and 2.

V.A.3. Small State Infrastructure Adversary Sensitivity Analysis

The sensitivity of risk values to the capability assessment made for each group is given in Table 61, Table 62, and Table 63 for group 1, group 2 and group 3 respectively. The first row gives each task and the second row gives the assessed likelihood of success at each path for the adversary. Group1, group 2 and group 3 were all modeled with the same capabilities, so the original likelihood of success for each task is the same for each group. The table then shows the percent change in risk for the adversary's actual likelihood of success at each task. For example, if the State-level risk is based on the assessment that the adversary has an 18% chance of successfully machining SNM for use in an IND, the machining task column shows the change in State-level risk based on changes in this adversary capability. For group 1, the risk is slightly sensitive to the adversary's ability to enrich uranium, which we assessed as implausible. For groups 2 and 3 who have greater motivations for higher consequence nuclear threats, the risk values become sensitive to the adversary's capability to enrich or reprocess nuclear materials. However, changes in other capabilities represent negligible changes in risk. These results make sense because the small State has no direct-use materials, meaning the State-level risk will only increase if the adversary's capability to convert non direct-use materials into weapons usable materials.

Table 61. Small State Capability Assessment Risk Sensitivity - Group 1

	Task	Conversion	Reprocessing	Enrichment	Machining	Metallurgy	IND Weaponization Gun-Type	IND Weaponization Implosion
Original P_S^{Task}		0.479391	1E-08	0	0.18	0.226318	0.13125	0.00125
Actual Task Success Probability	0	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
	0.05	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
	0.1	0.00%	0.01%	0.02%	0.00%	0.00%	0.00%	0.00%
	0.15	0.00%	0.01%	0.05%	0.00%	0.00%	0.00%	0.00%
	0.2	0.00%	0.02%	0.08%	0.00%	0.00%	0.00%	0.00%
	0.25	0.00%	0.04%	0.13%	0.00%	0.00%	0.00%	0.00%
	0.3	0.00%	0.05%	0.18%	0.00%	0.00%	0.00%	0.00%
	0.35	0.00%	0.07%	0.25%	0.00%	0.00%	0.00%	0.00%
	0.4	0.00%	0.10%	0.33%	0.00%	0.00%	0.00%	0.00%
	0.45	0.00%	0.12%	0.41%	0.00%	0.00%	0.00%	0.00%
	0.5	0.00%	0.15%	0.51%	0.00%	0.00%	0.00%	0.00%
	0.55	0.00%	0.18%	0.61%	0.00%	0.00%	0.00%	0.00%
	0.6	0.00%	0.22%	0.73%	0.00%	0.00%	0.00%	0.00%
	0.65	0.00%	0.25%	0.86%	0.00%	0.00%	0.00%	0.00%
	0.7	0.00%	0.29%	0.99%	0.00%	0.00%	0.00%	0.00%
	0.75	0.00%	0.34%	1.14%	0.00%	0.00%	0.00%	0.00%
	0.8	0.00%	0.38%	1.29%	0.00%	0.00%	0.00%	0.00%
	0.85	0.00%	0.43%	1.46%	0.00%	0.00%	0.00%	0.00%
	0.9	0.00%	0.48%	1.63%	0.00%	0.00%	0.00%	0.00%
	0.95	0.00%	0.54%	1.81%	0.00%	0.00%	0.00%	0.00%
	1	0.00%	0.60%	2.01%	0.00%	0.00%	0.00%	0.00%

Table 62. Small State Capability Assessment Risk Sensitivity - Group 2

	Task	Conversion	Reprocessing	Enrichment	Machining	Metallurgy	IND Weaponization Gun-Type	IND Weaponization Implosion
	Original Ps	0.479391	1E-08	0	0.18	0.226318	0.13125	0.00125
Actual Task Success Probability	0	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
	0.05	0.00%	0.02%	0.05%	0.00%	0.00%	0.00%	0.00%
	0.1	0.00%	0.06%	0.21%	0.00%	0.00%	0.00%	0.00%
	0.15	0.00%	0.14%	0.48%	0.00%	0.00%	0.00%	0.00%
	0.2	0.00%	0.26%	0.86%	0.00%	0.00%	0.00%	0.00%
	0.25	0.00%	0.40%	1.34%	0.00%	0.00%	0.00%	0.00%
	0.3	0.00%	0.57%	1.92%	0.00%	0.00%	0.00%	0.00%
	0.35	0.00%	0.78%	2.60%	0.00%	0.00%	0.00%	0.00%
	0.4	0.00%	1.02%	3.37%	0.00%	0.00%	0.00%	0.00%
	0.45	0.00%	1.28%	4.23%	0.00%	0.00%	0.00%	0.00%
	0.5	0.00%	1.58%	5.17%	0.00%	0.00%	0.00%	0.00%
	0.55	0.00%	1.90%	6.19%	0.00%	0.00%	0.00%	0.00%
	0.6	0.00%	2.26%	7.29%	0.00%	0.00%	0.00%	0.00%
	0.65	0.00%	2.64%	8.45%	0.00%	0.00%	0.00%	0.00%
	0.7	0.00%	3.05%	9.67%	0.00%	0.00%	0.00%	0.00%
	0.75	0.00%	3.49%	10.94%	0.00%	0.00%	0.00%	0.00%
	0.8	0.00%	3.95%	12.27%	0.00%	0.00%	0.00%	0.00%
	0.85	0.00%	4.43%	13.63%	0.00%	0.00%	0.00%	0.00%
	0.9	0.00%	4.95%	15.04%	0.00%	0.00%	0.00%	0.00%
	0.95	0.00%	5.48%	16.47%	0.00%	0.00%	0.00%	0.00%
	1	0.00%	6.04%	17.94%	0.00%	0.00%	0.00%	0.00%

Table 63. Small State Capability Assessment Risk Sensitivity - Group 3

	Task	Conversion	Reprocessing	Enrichment	Machining	Metallurgy	IND Weaponization Gun-Type	IND Weaponization Implosion
	Original Ps	0.479391	1E-08	0	0.18	0.226318	0.13125	0.00125
Actual Task Success Probability	0	0.00%	0.12%	0.00%	0.00%	0.00%	0.00%	0.00%
	0.05	0.00%	0.50%	0.41%	0.00%	0.00%	0.00%	0.00%
	0.1	0.00%	1.12%	1.67%	0.00%	0.00%	0.00%	0.00%
	0.15	0.00%	1.98%	3.71%	0.00%	0.00%	0.00%	0.00%
	0.2	0.00%	3.07%	6.42%	0.00%	0.00%	0.00%	0.00%
	0.25	0.00%	4.36%	9.70%	0.00%	0.00%	0.00%	0.00%
	0.3	0.00%	5.85%	13.42%	0.00%	0.00%	0.00%	0.00%
	0.35	0.00%	7.51%	17.43%	0.00%	0.00%	0.00%	0.00%
	0.4	0.00%	9.32%	21.62%	0.00%	0.00%	0.00%	0.00%
	0.45	0.00%	11.27%	25.88%	0.00%	0.00%	0.00%	0.00%
	0.5	0.00%	13.32%	30.13%	0.00%	0.00%	0.00%	0.00%
	0.55	0.00%	15.46%	34.29%	0.00%	0.00%	0.00%	0.00%
	0.6	0.00%	17.67%	38.32%	0.00%	0.00%	0.00%	0.00%
	0.65	0.00%	19.94%	42.17%	0.00%	0.00%	0.00%	0.00%
	0.7	0.00%	22.23%	45.82%	0.00%	0.00%	0.00%	0.00%
	0.75	0.00%	24.55%	49.26%	0.00%	0.00%	0.00%	0.00%
	0.8	0.00%	26.86%	52.48%	0.00%	0.00%	0.00%	0.00%
	0.85	0.00%	29.17%	55.49%	0.00%	0.00%	0.00%	0.00%
	0.9	0.00%	31.45%	58.29%	0.00%	0.00%	0.00%	0.00%
	0.95	0.00%	33.71%	60.90%	0.00%	0.00%	0.00%	0.00%
	1	0.00%	35.92%	63.31%	0.00%	0.00%	0.00%	0.00%

V.B. Intermediate State Infrastructure

The intermediate State has three commercial LWR reactors that supply 35% of their domestic power and two research reactors, one with HEU and one with LEU. The LEU research reactor is located at a University in their capital city, so sabotage of this reactor represents a significant concern. Their fuel cycle facilities consist of uranium mining and milling, uranium conversion and fuel fabrication. They also have a number of medical and industrial radiological sources. The majority of the population and economic productivity comes from the capital city. Details on the intermediate State nuclear infrastructure are available in Appendix F.

V.B.1. Intermediate State Risk Analysis Results

Table 64 gives the risk breakdown from each nuclear threat for the intermediate State infrastructure. In this case, the adversary motivations make a significant difference in the risk breakdown, with the RDD threat dominating the risk from group 1 and IND threats making a large contribution to the risk from group 3. The pathways that contribute the most to the State-level risk and their relative contribution to risk are presented in Table 65.

Table 64. Intermediate State Risk by Threat

Threat	$\mathbb{R}_{Group\ 1}$	$\mathbb{R}_{Group\ 2}$	$\mathbb{R}_{Group\ 3}$
IND	0.23%	2.57%	18.63%
RDD	64.72%	52.34%	33.59%
Sabotage	35.05%	45.09%	47.79%

Table 65. Intermediate State Pathways Risk

Improvised Nuclear Device				
Facility	**Material**	$\%\mathbb{R}_{Group\ 1}$	$\%\mathbb{R}_{Group\ 2}$	$\%\mathbb{R}_{Group\ 3}$
University HEU Research Reactor	Fresh HEU Fuel	0.23%	2.57%	18.63%
Radiological Dispersion Device				
Facility	**Material**	$\%\mathbb{R}_{Group\ 1}$	$\%\mathbb{R}_{Group\ 2}$	$\%\mathbb{R}_{Group\ 3}$
Food Irradiator Facility	Co-60 Source	62.88%	50.65%	32.50%
Hospital Cancer Center	Co-60 Gamma Knife Source	0.80%	0.63%	0.41%
Blood Irradiator Facility	Cs-137 Source	0.38%	0.36%	0.23%
University HEU Research Reactor	Irradiated HEU Fuel	0.23%	0.26%	0.17%
University LEU Research Reactor	Irradiated LEU Fuel	0.14%	0.19%	0.12%
Industrial Facility 2	Am-Be well logging sources	0.13%	0.10%	0.06%
Sabotage				
Facility	**Sabotage Event**	$\%\mathbb{R}_{Group\ 1}$	$\%\mathbb{R}_{Group\ 2}$	$\%\mathbb{R}_{Group\ 3}$
University LEU Research Reactor	Spent Fuel Pool	26.91%	34.61%	36.68%
University LEU Research Reactor	Reactor	7.63%	9.82%	10.41%
University HEU Research Reactor	Spent Fuel Pool	0.29%	0.38%	0.40%
University HEU Research Reactor	Reactor	0.11%	0.14%	0.14%
BWR Reactor Site	Spent Fuel Pool	0.10%	0.13%	0.14%
BWR Reactor Site	Reactor	0.01%	0.01%	0.01%

Based on the results, four pathways are contributing to essentially all of the State-level risk. The first is the 400,000 Curie Co-60 Blood Irradiator source, which has the highest risk value based on IAEA radionuclide categorization. The second is the fresh HEU research reactor fuel, which contributes to essentially all of the IND risk. Finally, the third high risk event is the sabotage of the LEU research reactor or spent fuel pool, which has severe consequences because it is located in the capital city. For the intermediate State, the differences in group motivations make a significant difference in the risk posed by the IND, but in all cases the Co-60 food irradiation source and the reactor sabotage are contributing to a significant amount to the State-level risk.

V.B.2. Intermediate State Risk-Reduction Analysis

Based on the State-infrastructure, the material removal strategies that should be investigated are replacing the food irradiator source with a linear accelerator, decommissioning the LEU research reactor and removing the material, or decommissioning the HEU research reactor and removing the fresh HEU fuel. Material replacement could include replacing the HEU research reactor fuel with LEU. These risk reduction strategies are simulated and the results displayed in Table 66.

Table 66. Intermediate State Risk Reduction Strategy Results

Risk-Reduction Strategy	$\%\mathbb{R}_{Group\ 1}$ Reduction	$\%\mathbb{R}_{Group\ 2}$ Reduction	$\%\mathbb{R}_{Group\ 3}$ Reduction
Replace Co-60 Food Irradiator Source	58.90%	46.07%	27.29%
Remove LEU Research Reactor	27.09%	34.39%	32.86%
Remove Spent Fuel From LEU Research Reactor	22.57%	28.31%	27.91%
Remove HEU Research Reactor	0.22%	2.45%	17.69%
Replace HEU Research Reactor Fuel with LEU	0.22%	2.45%	17.69%

The risk reduction strategies show that replacing the Co-60 Food Irradiator significantly reduces risk for each group and would be a worthwhile strategy to investigate. Removing the LEU research reactor also creates a significant risk reduction for all groups, however removing this reactor will result in the loss of significant research at the university. The risk analysis shows that removing the spent fuel from the reactor to another storage has a lower risk reduction, but allows the reactor to remain operational. The risk analysis results are also based on a snapshot in time of the State, so the regular transportation of spent fuel from the research reactor is not captured and should be investigated as it could decrease, to some degree, the risk reduction benefits of shipping the spent fuel off-site. Strategies at the HEU reactor show that there is no risk-based difference between decommissioning the reactor and removing the fuel or simply replacing the HEU fuel with LEU. The risk reduction benefits are also highly dependent on the motivations of the terrorist group.

Rather than employ any of these strategies, the State can upgrade various nuclear security measures at their existing facilities. Using sensitivity analysis, the security measures which have greatest impact on State-level risk are determined for each group. The results are displayed in Table 67, Table 68, and Table 69 show the most sensitive security measures in the State for each group, the threats addressed by upgrading these security measures, and the change in risk based on a 10% improvement to that security measure.

Table 67. Intermediate State Security Measure Risk Sensitivity Results - Group 1

Nuclear Security Measure	Threat Addressed	$\Delta\mathbb{R}$
Food Irradiator Source Layer 1 P_N	Food Irradiator Theft and RDD	16.14%
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Spent Fuel Sabotage	5.64%
Target Security Capital City P_{targ}	Delivering IND and RDD to Capital City	4.50%
LEU Research Reactor P_{Cons}^{Sab}	LEU Research Reactor - Spent Fuel Sabotage	4.10%
Detecting Adversary RDD Weaponization β_D^{RDDw}	All RDD Pathways	3.90%
Food Irradiator Source Layer 2 P_I	Food Irradiator Theft and RDD	2.07%
Food Irradiator Source Layer 2 P_N	Food Irradiator Theft and RDD	2.07%
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Reactor Sabotage	1.15%
LEU Research Reactor P_{Cons}^{Sab}	LEU Research Reactor - Reactor Sabotage	0.91%
Transportation Interdiction $\overline{D}_{Capt}^{AS}$	All IND and RDD	0.90%
LEU Research Reactor - Layer 1 P_N	LEU Research Reactor - Spent Fuel and Reactor Sabotage, Spent Fuel Theft and RDD	0.88%
LEU Research Reactor - Layer 1 P_I	LEU Research Reactor - Spent Fuel and Reactor Sabotage, Spent Fuel Theft and RDD	0.79%

Table 68. Intermediate State Security Measure Risk Sensitivity Results - Group 2

Nuclear Security Measure	Threat Addressed	$\Delta\mathbb{R}$
Food Irradiator Source Layer 1 P_N	Food Irradiator Theft and RDD	12.97%
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Spent Fuel Sabotage	7.23%
LEU Research Reactor P_{Cons}^{Sab}	LEU Research Reactor - Spent Fuel Sabotage	5.25%
Target Security Capital City P_{targ}	Delivering IND and RDD to Capital City	3.72%
Detecting Adversary RDD Weaponization β_D^{RDDw}	All RDD Pathways	2.33%
Food Irradiator Source Layer 2 P_I	Food Irradiator Theft and RDD	1.67%
Food Irradiator Source Layer 2 P_N	Food Irradiator Theft and RDD	1.67%
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Reactor Sabotage	1.41%
LEU Research Reactor - Layer 1 P_N	LEU Research Reactor - Spent Fuel and Reactor Sabotage, Spent Fuel Theft and RDD	1.14%
LEU Research Reactor P_{Cons}^{Sab}	LEU Research Reactor - Reactor Sabotage	1.12%
LEU Research Reactor - Layer 1 P_I	LEU Research Reactor - Spent Fuel and Reactor Sabotage, Spent Fuel Theft and RDD	1.03%
Transportation Interdiction $\bar{D}_{Capt}^{AS}$	All IND and RDD	0.70%

Table 69. Intermediate State Security Measure Risk Sensitivity Results - Group 3

Nuclear Security Measure	Threat Addressed	$\Delta\mathbb{R}$
Food Irradiator Source Layer 1 P_N	Food Irradiator Theft and RDD	8.05%
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Spent Fuel Sabotage	7.30%
LEU Research Reactor P_{Cons}^{Sab}	LEU Research Reactor - Spent Fuel Sabotage	5.32%
Detecting Adversary IND Metallurgy β_D^{meta}	All IND Pathways	4.14%
Target Security Capital City P_{targ}	Delivering IND and RDD to Capital City	3.25%
Detecting Adversary IND Gun-Type Weaponization $\beta_D^{ING,G}$	All IND Pathways	3.13%
Adversary Capability - IND Weaponization Gun Type	All IND Pathways	3.13%
Adversary Capability - Machining	All IND Pathways	3.13%
Detecting Adversary IND Gun-Type Weaponization $\beta_D^{ING,G}$	All IND Pathways	3.13%
Adversary Capability - Metallurgy	All IND Pathways	2.89%
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Reactor Sabotage	1.22%
LEU Research Reactor - Layer 1 P_N	LEU Research Reactor - Spent Fuel and Reactor Sabotage, Spent Fuel Theft and RDD	1.14%
Food Irradiator Source Layer 2 P_I	Food Irradiator Theft and RDD	1.04%
Food Irradiator Source Layer 2 P_N	Food Irradiator Theft and RDD	1.04%
LEU Research Reactor - Layer 1 P_N	LEU Research Reactor - Spent Fuel and Reactor Sabotage, Spent Fuel Theft and RDD	1.02%
LEU Research Reactor P_{Cons}^{Sab}	LEU Research Reactor - Reactor Sabotage	0.99%
Transportation Interdiction $\bar{D}_{Capt}^{AS}$	All IND and RDD	0.74%

The sensitivity results show that security upgrades to the Co-60 Food Irradiator source and upgrades to research reactor sabotage security are preferred for each case. For group 1, the State-level risk is sensitive to the ability of security at the capital city to detect and prevent an adversary attempting to deliver an IND or RDD to the city. In addition, the State-level risk is sensitive to the State's ability to the likelihood they can recapture stolen material once it is discovered and their ability to detect adversary activity in producing an RDD. For group 2, the State-level risk is most sensitive to the same security measures, but the sensitivity to RDD related security measures is less than that of group 1, while the sensitivity to sabotage related security measures increase. For group 3, the State level-risk is also sensitive to the State's ability to detect an adversary attempting to produce an IND and the adversary's assessed capabilities to machine, cast and weaponize HEU used in the risk analysis.

Employing these sensitivity results, the optimal set of security measure upgrades to reach a 50% reduction in State-level risk are simulated for each group. The results for group 1 are displayed in Table 70.

Table 70. Intermediate State Optimal Security Upgrades for 50% Risk Reduction - Group 1

Nuclear Security Measure	Threat Addressed	Original Value	New Value
Food Irradiator Source Layer 1 P_N	Food Irradiator Theft and RDD	0.8	0.92
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Spent Fuel Sabotage	0.25	0.6
LEU Research Reactor P_{Cons}^{Sab}	LEU Research Reactor - Spent Fuel Sabotage	0.5	0.25
Detecting Adversary RDD Weaponization β_D^{RDDw}	All RDD Pathways	0.85	0.75
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Reactor Sabotage	0.25	0.38

Table 70 shows that only a few security measure upgrades were required to reduce the risk by 50.18%. For this analysis, P_I and P_N values were capped at 0.92 which limited the upgrades on the Food Irradiator source. A decrease in non-detection probability is equivalent to an increase in the State's detection capability. The results from group 2 are presented in Table 71 and are similar to group 1, except hardening the target security at the capital city is upgraded instead of upgrading the State's RDD weaponization detection capabilities. The proposed set of upgrades reduces the State-level risk by 50.24%.

Table 71. Intermediate State Optimal Security Upgrades for 50% Risk Reduction - Group 2

Nuclear Security Measure	Threat Addressed	Original Value	New Value
Food Irradiator Source Layer 1 P_N	Food Irradiator Theft and RDD	0.8	0.92
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Spent Fuel Sabotage	0.25	0.55
LEU Research Reactor P_{Cons}^{Sab}	LEU Research Reactor - Spent Fuel Sabotage	0.5	0.3
Target Security Capital City P_{targ}	Delivering IND and RDD to Capital City	0.3	0.39
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Reactor Sabotage	0.25	0.38

The recommended upgrades to address the risk from group 3 are given in Table 72 and the set of upgrades represent a 51.32% decrease in State-level risk. The upgrades are similar to group 2, but the State's ability to detect the adversary attempting to acquire the equipment for casting SNM for an IND is also upgraded.

Table 72. Intermediate State Optimal Security Upgrades for 50% Risk Reduction - Group 3

Nuclear Security Measure	Threat Addressed	Original Value	New Value
Food Irradiator Source Layer 1 P_N	Food Irradiator Theft and RDD	0.8	0.92
LEU Research Reactor ε_{Sab}^{Ins}	LEU Research Reactor - Spent Fuel Sabotage	0.25	0.55
LEU Research Reactor P_{Cons}^{Sab}	LEU Research Reactor - Spent Fuel Sabotage	0.5	0.3
Target Security Capital City P_{targ}	Delivering IND and RDD to Capital City	0.3	0.42
Detecting Adversary IND Metallurgy β_D^{meta}	All IND Pathways	0.75	0.64

V.B.3. Intermediate State Infrastructure Adversary Sensitivity Analysis

The sensitivity of risk values to the capability assessment made for each group is given in Table 73, Table 74, and Table 75 for group 1, group 2, and group 3 respectively. The first row gives each task and the second row gives the assessed likelihood of success at each path for the adversary. The table then shows the percent change in risk if the for the adversary's actual likelihood of success at each task. Unlike the small State, the intermediate State has direct-use SNM, so the State-level risk is sensitive to the capabilities of the adversary to produce an IND using this material. For group 1, the risk is only slightly sensitive to changes in the group's ability to cast, machine, and weaponize HEU. For groups 2 and 3, the risk values become very sensitive to these capabilities. Especially for group 3, errors in the group's capabilities can have a significant impact on risk and the State should both investigate how changes in these capabilities effect proposed upgrades and could apply additional intelligence resources towards gaining confidence in the State's assessment of these capabilities.

Table 73. Intermediate State Adversary Capability Assessment Risk Sensitivity - Group 1

	Task	Conversion	Reprocessing	Enrichment	Machining	Metallurgy	IND Weaponization Gun-Type	IND Weaponization Implosion
	Original Ps	0.479391	1E-08	0	0.18	0.226318	0.13125	0.00125
Actual Task Success Probability	0	0.00%	0.00%	0.00%	-0.22%	-0.22%	-0.22%	0.00%
	0.05	0.00%	0.00%	0.00%	-0.20%	-0.21%	-0.19%	0.00%
	0.1	0.00%	0.00%	0.00%	-0.15%	-0.18%	-0.09%	0.00%
	0.15	0.00%	0.00%	0.00%	-0.07%	-0.12%	0.07%	0.00%
	0.2	0.00%	0.00%	0.00%	0.05%	-0.05%	0.29%	0.00%
	0.25	0.00%	0.00%	0.00%	0.21%	0.05%	0.58%	0.00%
	0.3	0.00%	0.00%	0.00%	0.39%	0.17%	0.94%	0.00%
	0.35	0.00%	0.00%	0.00%	0.62%	0.31%	1.36%	0.00%
	0.4	0.00%	0.00%	0.00%	0.88%	0.47%	1.85%	0.00%
	0.45	0.00%	0.00%	0.00%	1.17%	0.66%	2.40%	0.00%
	0.5	0.00%	0.00%	0.00%	1.50%	0.86%	3.02%	0.00%
	0.55	0.00%	0.01%	0.00%	1.86%	1.09%	3.70%	0.00%
	0.6	0.00%	0.01%	0.00%	2.26%	1.34%	4.45%	0.00%
	0.65	0.00%	0.01%	0.00%	2.69%	1.62%	5.27%	0.00%
	0.7	0.00%	0.01%	0.00%	3.16%	1.91%	6.14%	0.00%
	0.75	0.00%	0.01%	0.00%	3.66%	2.23%	7.09%	0.00%
	0.8	0.00%	0.01%	0.00%	4.19%	2.57%	8.10%	0.00%
	0.85	0.00%	0.01%	0.00%	4.77%	2.93%	9.17%	0.00%
	0.9	0.00%	0.02%	0.00%	5.37%	3.31%	10.32%	0.00%
	0.95	0.00%	0.02%	0.00%	6.01%	3.72%	11.52%	0.00%
	1	0.00%	0.02%	0.00%	6.69%	4.14%	12.79%	0.00%

Table 74. Intermediate State Adversary Capability Assessment Risk Sensitivity - Group 2

Task		Conversion	Reprocessing	Enrichment	Machining	Metallurgy	IND Weaponization Gun-Type	IND Weaponization Implosion
Original Ps		0.479391	1E-08	0	0.18	0.226318	0.13125	0.00125
Actual Task Success Probability	0	0.00%	0.00%	0.00%	-2.45%	-2.45%	-2.45%	0.00%
	0.05	0.00%	0.00%	0.00%	-2.29%	-2.35%	-2.13%	0.00%
	0.1	0.00%	0.00%	0.00%	-1.73%	-2.00%	-1.05%	0.00%
	0.15	0.00%	0.00%	0.00%	-0.77%	-1.40%	0.77%	0.00%
	0.2	0.00%	0.01%	0.00%	0.59%	-0.55%	3.33%	0.00%
	0.25	0.00%	0.01%	0.00%	2.34%	0.55%	6.64%	0.00%
	0.3	0.00%	0.02%	0.00%	4.49%	1.91%	10.69%	0.00%
	0.35	0.00%	0.03%	0.00%	7.03%	3.51%	15.48%	0.00%
	0.4	0.00%	0.03%	0.00%	9.97%	5.36%	21.02%	0.00%
	0.45	0.00%	0.04%	0.01%	13.30%	7.47%	27.29%	0.00%
	0.5	0.00%	0.05%	0.01%	17.02%	9.82%	34.30%	0.00%
	0.55	0.00%	0.07%	0.01%	21.14%	12.42%	42.04%	0.00%
	0.6	0.00%	0.08%	0.01%	25.65%	15.27%	50.53%	0.00%
	0.65	0.00%	0.09%	0.01%	30.55%	18.38%	59.74%	0.00%
	0.7	0.00%	0.11%	0.02%	35.85%	21.72%	69.70%	0.00%
	0.75	0.00%	0.12%	0.02%	41.54%	25.32%	80.38%	0.00%
	0.8	0.00%	0.14%	0.02%	47.62%	29.17%	91.80%	0.00%
	0.85	0.00%	0.16%	0.03%	54.09%	33.26%	103.95%	0.00%
	0.9	0.00%	0.18%	0.03%	60.95%	37.61%	116.82%	0.00%
	0.95	0.00%	0.20%	0.03%	68.20%	42.20%	130.43%	0.00%
	1	0.00%	0.22%	0.04%	75.84%	47.03%	144.77%	0.00%

Table 75. Intermediate State Adversary Capability Assessment Risk Sensitivity - Group 3

Task		Conversion	Reprocessing	Enrichment	Machining	Metallurgy	IND Weaponization Gun-Type	IND Weaponization Implosion
Original Ps		0.479391	1E-08	0	0.18	0.226318	0.13125	0.00125
Actual Task Success Probability	0	0.00%	0.00%	0.00%	-17.69%	-17.69%	-17.69%	0.00%
	0.05	0.00%	0.00%	0.00%	-16.50%	-16.98%	-15.33%	0.00%
	0.1	0.00%	0.01%	0.00%	-12.43%	-14.45%	-7.56%	0.00%
	0.15	0.00%	0.02%	0.00%	-5.51%	-10.10%	5.53%	0.00%
	0.2	0.00%	0.05%	0.01%	4.24%	-3.95%	23.89%	0.00%
	0.25	0.00%	0.08%	0.01%	16.79%	3.98%	47.44%	0.00%
	0.3	0.00%	0.13%	0.02%	32.11%	13.68%	76.11%	0.00%
	0.35	0.00%	0.18%	0.03%	50.18%	25.14%	109.85%	0.00%
	0.4	0.00%	0.23%	0.04%	70.98%	38.35%	148.58%	0.00%
	0.45	0.00%	0.30%	0.05%	94.47%	53.29%	192.25%	0.00%
	0.5	0.00%	0.38%	0.07%	120.63%	69.95%	240.79%	0.00%
	0.55	0.00%	0.46%	0.08%	149.44%	88.32%	294.13%	0.00%
	0.6	0.00%	0.56%	0.10%	180.87%	108.38%	352.23%	0.00%
	0.65	0.00%	0.66%	0.12%	214.90%	130.12%	415.01%	0.00%
	0.7	0.00%	0.77%	0.14%	251.51%	153.53%	482.43%	0.00%
	0.75	0.00%	0.89%	0.16%	290.66%	178.59%	554.42%	0.00%
	0.8	0.00%	1.01%	0.18%	332.34%	205.30%	630.93%	0.00%
	0.85	0.00%	1.15%	0.21%	376.52%	233.65%	711.90%	0.00%
	0.9	0.00%	1.29%	0.24%	423.19%	263.61%	797.27%	0.00%
	0.95	0.00%	1.44%	0.26%	472.31%	295.18%	887.00%	0.00%
	1	0.00%	1.60%	0.29%	523.87%	328.35%	981.03%	0.00%

V.C. Complex State Infrastructure

The complex State has five commercial LWR nuclear reactors which supply 20% of the State's power requirements. The State has a gas centrifuge enrichment facility which supplies civilian LEU, co-located conversion and fuel fabrication facility facilities, and a reprocessing and waste storage facility. The complex State also has a nuclear weapons program. The nuclear weapons complex includes:

- a super prompt critical reactor with HEU fuel to test materials under neutron burst environments;
- a nuclear weapon assembly, disassembly and servicing facility;
- A MAGNOX plutonium production reactor and reprocessing facility;
- Nuclear weapon component production facility; and
- nuclear weapons are designed at 2 mega-tons and are deployed at military and naval bases.

In addition, the complex State has more industrial and medical radiological materials than the small or intermediate States. The complex State employs much more stringent security measures on nuclear facilities compared to the small and intermediate States, and even higher levels of security to protect nuclear weapons. The security employed on radiological materials is not as stringent as those employed on nuclear materials. Full details of the State infrastructure are available in Appendix F. Facilities that are part of the nuclear weapons program are designated with NWC for nuclear weapons complex.

V.C.1. Complex State Infrastructure Risk Analysis

Table 76 gives the risk breakdown from each nuclear threat for the complex State. The analysis shows that the State-level risk is dominated by the risk from RDD and sabotage. Due to the strict security measures on nuclear weapons, the State-level risk from the analyzed threats is non-existent, as the groups are much more likely to choose paths with greater chances of success. The pathways that contribute the most to the State-level risk and their relative contributions to risk are presented in Table 77.

Table 76. Complex State Risk by Threat

Threat	$\mathbb{R}_{Group\ 1}$	$\mathbb{R}_{Group\ 2}$	$\mathbb{R}_{Group\ 3}$
Nuclear Weapons	0.00%	0.00%	0.00%
IND	0.10%	1.10%	8.30%
RDD	52.27%	40.30%	26.94%
Sabotage	47.63%	58.60%	64.76%

Table 77. Complex State Pathways Risk

Improvised Nuclear Device				
Facility	**Material**	$\%\mathbb{R}_{Group\ 1}$	$\%\mathbb{R}_{Group\ 2}$	$\%\mathbb{R}_{Group\ 3}$
(NWC) Super Prompt Critical Reactor	Fresh HEU Fuel	0.06%	0.65%	4.84%
(NWC) HEU Research Reactor	Fresh HEU Fuel	0.04%	0.44%	3.26%
(NWC) Nuclear Weapon Assembly Facility	Pu Machined Metal	0.00%	0.01%	0.06%
(NWC) Weapon Component Production	Pu Metal Product	0.00%	0.00%	0.02%
Radiological Dispersion Device				
Facility	**Material**	$\%\mathbb{R}_{Group\ 1}$	$\%\mathbb{R}_{Group\ 2}$	$\%\mathbb{R}_{Group\ 3}$
Industrial Source Location 6	Food Irradiator 6	21.11%	16.25%	10.75%
Industrial Source Location 2	Food Irradiator	20.31%	15.63%	10.34%
Industrial Source Location 1	Blood/Tissue Irradiator	5.91%	4.55%	3.01%
Industrial Source Location 3	Co Radiography	1.56%	1.20%	0.79%
Industrial Source Location 3	Industrial Rad Ir 3	1.07%	0.82%	0.54%
Industrial Source Location 4	Well Logging Am-Be 4	0.81%	0.63%	0.41%
Industrial Source Location 5	Well Logging Am-Be 5	0.77%	0.59%	0.39%
Hospital 4	Gamma Knife Multi-Beam	0.24%	0.19%	0.12%
Hospital 3	Gamma Knife Multi-Beam	0.22%	0.17%	0.11%
Hospital 1	Gamma Knife Multi-Beam	0.19%	0.14%	0.09%
Sabotage				
Facility	**Sabotage Event**	$\%\mathbb{R}_{Group\ 1}$	$\%\mathbb{R}_{Group\ 2}$	$\%\mathbb{R}_{Group\ 3}$
PWR Site 2	Spent Fuel Pool PWR2	7.64%	9.38%	10.25%
PWR Site 1	Spent Fuel Pool PWR1	5.90%	7.24%	7.91%
BWR Site 1	Spent Fuel Pool BWR 1	5.78%	7.10%	7.76%
BWR Site 2	Spent Fuel Pool BWR 2	5.78%	7.10%	7.76%
PWR Site 3	Spent Fuel Pool PWR3	5.78%	7.10%	7.76%
(NWC) MAGNOX Pu Production Complex	Reactor	4.01%	4.92%	5.38%
(NWC) Military Reprocessing	Spent Fuel Pin Storage	3.51%	4.31%	4.71%
(NWC) HEU Research Reactor	Spent Fuel Sabotage	3.45%	4.24%	4.63%
(NWC) Super Prompt Critical Reactor	Spent Fuel Storage	1.92%	2.36%	2.58%
Commercial Reprocessing and Waste Storage	Spent Fuel Storage	2.02%	2.48%	2.71%
(NWC) HEU Research Reactor	Reactor	0.98%	1.21%	1.32%
(NWC) Super Prompt Critical Reactor	Reactor	0.79%	0.97%	1.06%

The results in Table 77 show that the two four-million Curie Co-60 food irradiator sources present the majority of the RDD risk, followed by the twelve-thousand Curie Cs-137 blood and tissue irradiator source. The two Co-60 sources are the largest contributor to risk for each group. The sabotage risk is dominated by the commercial reactor, with PWR site 1 representing the highest risk because of its proximity to the capital city. IND risks are relatively low, based on the strict security measures and the low assessed likelihood of the adversary producing an implosion based IND using plutonium.

V.C.2. Complex State Infrastructure Risk Reduction Results

Two risk reduction strategies were investigated for the complex State. The first was to consolidate the spent fuel from the commercial reactors to a highly secured location away from population areas. The second strategy involves replacing the high activity Co-60 and Cs-137 sources with linear accelerators. The results are given in Table 78.

The results from Table 78 show that removing the spent fuel from all commercial reactors and consolidating it at a central location provides a significant risk reduction, as it simultaneously addresses the five highest consequence sabotage pathways. Replacing either Co-60 also provides significant risk reduction by eliminating a majority of the risk posed by that source. Replacing both Co-60 sources with accelerators yield slightly greater risk reduction than the sum of the risk reduction from replacing either one independently. This is due to the fact that upgrading one source transfers some of the risk to the other Co-60 source, which is eliminated when eliminating both. The results for replacing the Cs-137 blood and tissue irradiator source are much lower, which indicates only upgrading this source transfers risk to the higher risk Co-60 pathways. For group 3, the risk transfer to the higher consequence sources is greater than the risk reduction received from removing the Cs-137 source.

Rather than employ any of these strategies, the State can upgrade various nuclear security measures at their existing facilities. Using sensitivity analysis, the security measures which have greatest impact on State-level risk are determined for each group. The results are displayed in Table 79, Table 80, and Table 81 show the most sensitive security measures in the State for each group, the threats addressed by upgrading these security measures, and the change in risk based on a 10% improvement to that security measure.

Table 78. Complex State Risk Reduction Strategy Results

Risk Reduction Strategy	$\mathbb{R}_{Group\ 1}$ Reduction	$\mathbb{R}_{Group\ 2}$ Reduction	$\mathbb{R}_{Group\ 3}$ Reduction
Consolidate Spent Fuel	29.46%	35.92%	38.43%
Replace Co-60 Food Irradiator at Location 6 With Accelerator	18.78%	13.85%	8.34%
Replace Co-60 Food Irradiator at Location 1 With Accelerator	18.00%	13.26%	7.97%
Replace Both Co-60 Food Irradiators With Accelerators	37.89%	27.90%	16.75%
Replace Cs-137 Blood/Tissue Irradiator with Accelerator	1.87%	0.56%	-0.81%

Table 79. Complex State Security Measure Risk Sensitivity Results - Group 1

Nuclear Security Measure	Threat Addressed	$\Delta\mathbb{R}$
Transportation Interdiction $\bar{D}_{Capt}^{AS}$	All IND, RDD, and Nuclear Weapon Theft	11.68%
Food Irradiator Co-60 Source 6 Layer 1 P_N	Food Irradiator Theft and RDD	5.45%
Food Irradiator Co-60 Source 2 Layer 1 P_N	Food Irradiator Theft and RDD	5.23%
Food Irradiator Co-60 Source 6 Layer 1 P_I	Food Irradiator Theft and RDD	4.01%
Food Irradiator Co-60 Source 2 Layer 1 P_I	Food Irradiator Theft and RDD	3.85%
Target Security Capital City P_{targ}	Delivering Nuclear Weapon, IND or RDD to Capital City	3.70%
PWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	3.33%
PWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	2.55%
PWR Site 3 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	2.50%
BWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	2.50%
BWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	2.50%
Transportation Interdiction $\bar{D}_{Capt}^{BKGD}$	All IND, RDD, and Nuclear Weapon Theft and Diversion	1.41%
PWR Site 2 P_{Cons}^{Sab}	PWR Site 2 Spent Fuel Sabotage	1.29%
PWR Site 1 P_{Cons}^{Sab}	PWR Site 1 Spent Fuel Sabotage	0.99%
PWR Site 3 P_{Cons}^{Sab}	PWR Site 3 Spent Fuel Sabotage	0.97%
BWR Site 2 P_{Cons}^{Sab}	BWR Site 2 Spent Fuel Sabotage	0.97%
BWR Site 1 P_{Cons}^{Sab}	BWR Site 1 Spent Fuel Sabotage	0.97%

Table 80. Complex State Security Measure Risk Sensitivity Results - Group 2

Nuclear Security Measure	Threat Addressed	$\Delta\mathbb{R}$
Transportation Interdiction $\overline{D}_{Capt}^{AS}$	All IND, RDD, and Nuclear Weapon Theft	8.06%
Food Irradiator Co-60 Source 6 Layer 1 P_N	Food Irradiator Theft and RDD	4.11%
PWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	4.05%
Food Irradiator Co-60 Source 2 Layer 1 P_N	Food Irradiator Theft and RDD	3.94%
PWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	3.09%
PWR Site 3 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	3.03%
BWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	3.03%
BWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	3.03%
Target Security Capital City P_{targ}	Delivering Nuclear Weapon, IND or RDD to Capital City	3.02%
(NWC) Super-Prompt Critical Reactor - Layer 1 P_N	Reactor and Spent Fuel Storage Sabotage, HEU Theft for IND, Irradiated Fuel theft for RDD	2.90%
Commercial Reprocessing and Waste Storage - Layer 1 P_N	Spent Fuel Storage Sabotage, Irradiated Fuel theft for RDD, PuO_2 Theft for RDD or IND	2.73%
PWR Site 2 ε_{Sab}^{Ins}	Reactor Sabotage	2.53%
(NWC) Military Reprocessing - Layer 1 P_N	Spent Fuel Sabotage, Spent Fuel Pins theft for RDD, Weapons Grade PuO_2 for IND or RDD	1.85%
PWR Site 2 P_{Cons}^{Sab}	Spent Fuel Sabotage	1.63%
PWR Site 1 P_{Cons}^{Sab}	Spent Fuel Sabotage	1.62%
PWR Site 3 P_{Cons}^{Sab}	Spent Fuel Sabotage	1.62%
BWR Site 2 P_{Cons}^{Sab}	Spent Fuel Sabotage	1.57%
BWR Site 1 P_{Cons}^{Sab}	Spent Fuel Sabotage	1.20%

Table 81. Complex State Security Measure Risk Sensitivity Results - Group 3

Nuclear Security Measure	Threat Addressed	$\Delta\mathbb{R}$
Transportation Interdiction $\bar{D}_{Capt}^{AS}$	All IND, RDD, and Nuclear Weapon Theft	5.89%
(NWC) Super-Prompt Critical Reactor - Layer 1 P_N	Reactor and Spent Fuel Storage Sabotage, HEU Theft for IND, Irradiated Fuel theft for RDD	5.32%
PWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD	4.33%
(NWC) HEU Research Reactor - Layer 1 P_N	Reactor and Spent Fuel Storage Sabotage, HEU Theft for IND, Irradiated Fuel theft for RDD	3.93%
PWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	3.29%
PWR Site 3 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	3.22%
BWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	3.22%
BWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	3.22%
Food Irradiator Source 6 Layer 1 P_N	Food Irradiator Theft and RDD	2.60%
Food Irradiator Source 2 Layer 1 P_N	Food Irradiator Theft and RDD	2.49%
Commercial Reprocessing and Waste Storage - Layer 1 P_N	Spent Fuel Storage Sabotage, Irradiated Fuel theft for RDD, PuO_2 Theft for RDD or IND	1.98%
Food Irradiator Co-60 Source 6 Layer 1 P_I	Food Irradiator Theft and RDD	1.91%
Food Irradiator Co60 Source 2 Layer 1 P_I	Food Irradiator Theft and RDD	1.84%
Detecting Adversary IND Metallurgy β_D^{meta}	All IND Pathways	1.83%
Target Security Capital City P_{targ}	Delivering Nuclear Weapon, IND or RDD to Capital City	1.78%
(NWC) Military Reprocessing - Layer 1 P_N	Spent Fuel Sabotage, Spent Fuel Pins theft for RDD, Weapons Grade PuO_2 for IND or RDD	1.72%
PWR Site 2 P_{Cons}^{Sab}	Spent Fuel Sabotage	1.69%
PWR Site 2 ε_{Sab}^{Ins}	Reactor Sabotage	1.65%

As in the other cases, the State-level risk is sensitive to security measures along the high-risk pathways, such as the two Co-60 food irradiator sources. In addition, many of the most sensitive security measures address numerous pathways. For each group, the State's ability to successfully recapture stolen material is the most sensitive security measure and addresses all RDD and IND theft scenarios. This is likely because the State-level risk is distributed among a larger number of pathways than the small and intermediate cases.

Employing these sensitivity values, the optimal set of upgrades to reduce the State-level risk by 50% are determined for each group. For each facility, P_I and P_N values were capped at 0.92. The recommended security upgrades to address the threat from group 1 are given in Table 82 and represent a 50.28% reduction in State-level risk. There are a significantly larger number of upgrades to reach a 50% risk for the complex State compared to the small and intermediate States, due to many physical security measures being maxed out at 0.92, and the larger number of pathways. For group 1, the upgrades consist of improving physical security at both Co-60 food irradiation source locations and all commercial nuclear reactors. In addition, the State should improve their ability to recapture stolen materials, harden the security at the capital city, and add additional features to prevent sabotage of the spent fuel at each commercial reactor.

The recommended security upgrades to address the threat from group 2 are given in Table 83 and represent a 50.2% reduction in State-level risk. Many of the security upgrades for group 2 are similar as for group 1 with slight differences in the degree of upgrades. In addition, upgrades are recommended at both reprocessing facilities and the Super-Prompt Critical Reactor.

The recommended security upgrades to address the threat from group 3 are given in Table 84 and represent a 50.01% reduction in State-level risk. In addition to the upgrades recommended for group 2, sabotage mitigation at both reprocessing and the Super-Prompt Critical Reactor are recommended. In addition, the upgrade options also recommend the State improve their ability to detect adversary attempts to cast SNM into a shape suitable for a crude nuclear device.

Table 82. Complex State Optimal Security Upgrades for 50% Risk Reduction - Group 1

Nuclear Security Measure	Threat Addressed	Original Value	Upgraded Value
Transportation Interdiction $\overline{D}_{Capt}^{AS}$	All IND, RDD, and Nuclear Weapon Theft	0.001	0.0012
Food Irradiator Source 6 Layer 1 P_N	Food Irradiator Theft and RDD	0.8	0.92
Food Irradiator Source 2 Layer 1 P_N	Food Irradiator Theft and RDD	0.8	0.92
Food Irradiator Source 6 Layer 1 P_I	Food Irradiator Theft and RDD	0.7	0.84
Food Irradiator Source 2 Layer 1 P_I	Food Irradiator Theft and RDD	0.7	0.82
Target Security Capital City P_{targ}	Delivering Nuclear Weapon, IND or RDD to Capital City	0.3	0.43
PWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
PWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
PWR Site 3 Layer 1 P_I	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
BWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
BWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
PWR Site 2 P_{Cons}^{Sab}	PWR Site 2 Spent Fuel Sabotage	0.2	0.14
PWR Site 1 P_{Cons}^{Sab}	PWR Site 1 Spent Fuel Sabotage	0.2	0.17
PWR Site 3 P_{Cons}^{Sab}	PWR Site 3 Spent Fuel Sabotage	0.2	0.17
BWR Site 2 P_{Cons}^{Sab}	BWR Site 2 Spent Fuel Sabotage	0.2	0.17
BWR Site 1 P_{Cons}^{Sab}	BWR Site 1 Spent Fuel Sabotage	0.2	0.17

Table 83. Complex State Optimal Security Upgrades for 50% Risk Reduction - Group 2

Nuclear Security Measure	Threat Addressed	Original Value	Upgraded Value
Transportation Interdiction $\bar{D}_{Capt}^{AS}$	All IND, RDD, and Nuclear Weapon Theft	0.001	0.00136
Food Irradiator Source 6 Layer 1 P_N	Food Irradiator Theft and RDD	0.8	0.92
PWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
Food Irradiator Source 2 Layer 1 P_N	Food Irradiator Theft and RDD	0.8	0.92
PWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
PWR Site 3 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
BWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
BWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
Target Security Capital City P_{targ}	Delivering Nuclear Weapon, IND or RDD to Capital City	0.3	0.42
(NWC) Super-Prompt Critical Reactor - Layer 1 P_N	Reactor and Spent Fuel Storage Sabotage, HEU Theft for IND, Irradiated Fuel theft for RDD	0.9	.92
Commercial Reprocessing and Waste Storage - Layer 1 P_N	Spent Fuel Storage Sabotage, Irradiated Fuel theft for RDD, PuO_2 Theft for RDD or IND	0.9	.92
(NWC) Military Reprocessing - P_{Cons}^{Sab}	Spent Fuel Sabotage	0.2	0.15
PWR Site 2 P_{Cons}^{Sab}	Spent Fuel Sabotage	0.2	0.11
PWR Site 1 P_{Cons}^{Sab}	Spent Fuel Sabotage	0.2	0.14
PWR Site 3 P_{Cons}^{Sab}	Spent Fuel Sabotage	0.2	0.14
BWR Site 2 P_{Cons}^{Sab}	Spent Fuel Sabotage	0.2	0.14
BWR Site 1 P_{Cons}^{Sab}	Spent Fuel Sabotage	0.2	0.14

Table 84. Complex State Optimal Security Upgrades for 50% Risk Reduction - Group 3

Nuclear Security Measure	Threat Addressed	Original Value	Upgraded Value
Transportation Interdiction $\bar{D}^{AS}_{Capt}$	All IND, RDD, and Nuclear Weapon Theft	0.001	0.00126
(NWC) Super-Prompt Critical Reactor - Layer 1 P_N	Reactor and Spent Fuel Storage Sabotage, HEU Theft for IND, Irradiated Fuel theft for RDD	0.9	0.92
PWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD	0.9	0.92
(NWC) HEU Research Reactor - Layer 1 P_N	Reactor and Spent Fuel Storage Sabotage, HEU Theft for IND, Irradiated Fuel theft for RDD	0.9	0.92
PWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
PWR Site 3 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
BWR Site 2 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
BWR Site 1 Layer 1 P_N	Reactor and Spent Fuel Sabotage, Irradiated Fuel for RDD, Fresh Fuel for IND	0.9	0.92
Food Irradiator Source 6 Layer 1 P_N	Food Irradiator Theft and RDD	0.8	0.92
Food Irradiator Source 2 Layer 1 P_N	Food Irradiator Theft and RDD	0.8	0.92
Commercial Reprocessing and Waste Storage - Layer 1 P_N	Spent Fuel Storage Sabotage, Irradiated Fuel theft for RDD, PuO_2 Theft for RDD or IND	0.9	0.92
Food Irradiator Source 6 Layer 1 P_I	Food Irradiator Theft and RDD	0.7	0.81
Food Irradiator Source 2 Layer 1 P_I	Food Irradiator Theft and RDD	0.7	0.79
PWR Site 2 P^{Sab}_{Cons}	Spent Fuel Sabotage	0.2	0.12
PWR Site 1 P^{Sab}_{Cons}	Spent Fuel Sabotage	0.2	0.14
PWR Site 3 P^{Sab}_{Cons}	Spent Fuel Sabotage	0.2	0.14
BWR Site 2 P^{Sab}_{Cons}	Spent Fuel Sabotage	0.2	0.14
BWR Site 1 P^{Sab}_{Cons}	Spent Fuel Sabotage	0.2	0.14
(NWC) Military Reprocessing - P^{Sab}_{Cons}	Spent Fuel Sabotage	0.2	0.15
Commercial Reprocessing and Storage - P^{Sab}_{Cons}	Spent Fuel Sabotage	0.2	0.16
Detecting Adversary IND Metallurgy β^{meta}_{D}	All IND Pathways	0.75	0.7
(NWC) Super Prompt Critical Reactor P^{Sab}_{Cons}	Spent Fuel Sabotage	0.2	0.16

V.C.3. Complex State Infrastructure Adversary Sensitivity Analysis

The sensitivity of risk values to the capability assessment made for each group is given in Table 85, Table 86, Table 87. The first row gives each task and the second row gives the assessed likelihood of success at each path for the adversary. The results show that even for terrorist groups with low motivations to conduct IND attacks, the State-level risk is highly sensitive to the group's capability to produce an implosion based weapon. This is due to the large amount of separated plutonium in the State. As the terrorist groups motivations shift towards favoring IND threats, the sensitivity to all weaponization capabilities become large. This is especially true for group 2's ability to produce an implosion based weapon and even more so for group 3's ability to fabricate either a gun-type or implosion based IND. To address these sensitivities, the State should deploy more resources to gain confidence in their assessment of the adversary's capability. In addition, eliminating separated plutonium and HEU will significantly reduce the State's sensitivity to these capabilities.

Table 85. Complex State Capability Assessment Risk Sensitivity - Group 1

	Task	Conversion	Reprocessing	Enrichment	Machining	Metallurgy	IND Weaponization Gun-Type	IND Weaponization Implosion
	Original Ps	0.479391	1E-08	0	0.18	0.226318	0.13125	0.00125
Actual Task Success Probability	0	0.00%	0.00%	0.00%	-0.10%	-0.10%	-0.10%	0.00%
	0.05	0.00%	0.00%	0.00%	-0.09%	-0.09%	-0.08%	5.83%
	0.1	0.00%	0.00%	0.00%	-0.07%	-0.08%	-0.04%	23.34%
	0.15	0.00%	0.00%	0.00%	-0.03%	-0.06%	0.03%	52.53%
	0.2	0.00%	0.00%	0.00%	0.02%	-0.02%	0.13%	93.39%
	0.25	0.00%	0.00%	0.00%	0.09%	0.02%	0.26%	145.92%
	0.3	0.00%	0.00%	0.00%	0.18%	0.07%	0.42%	210.11%
	0.35	0.00%	0.00%	0.00%	0.28%	0.14%	0.61%	285.97%
	0.4	0.00%	0.00%	0.00%	0.39%	0.21%	0.82%	373.47%
	0.45	0.00%	0.00%	0.00%	0.52%	0.29%	1.07%	472.62%
	0.5	0.00%	0.00%	0.00%	0.67%	0.39%	1.34%	583.42%
	0.55	0.00%	0.00%	0.00%	0.83%	0.49%	1.65%	705.85%
	0.6	0.00%	0.00%	0.00%	1.01%	0.60%	1.98%	839.92%
	0.65	0.00%	0.00%	0.01%	1.20%	0.72%	2.34%	985.61%
	0.7	0.00%	0.00%	0.01%	1.41%	0.85%	2.73%	1142.93%
	0.75	0.00%	0.01%	0.01%	1.63%	0.99%	3.15%	1311.86%
	0.8	0.00%	0.01%	0.01%	1.87%	1.14%	3.60%	1492.41%
	0.85	0.00%	0.01%	0.01%	2.12%	1.30%	4.08%	1684.57%
	0.9	0.00%	0.01%	0.01%	2.39%	1.47%	4.58%	1888.32%
	0.95	0.00%	0.01%	0.01%	2.68%	1.65%	5.12%	2103.68%
	1	0.00%	0.01%	0.01%	2.98%	1.84%	5.68%	2330.63%

Table 86. Complex State Capability Assessment Risk Sensitivity - Group 2

	Task	Conversion	Reprocessing	Enrichment	Machining	Metallurgy	IND Weaponization Gun-Type	IND Weaponization Implosion
	Original Ps	0.479391	1E-08	0	0.18	0.226318	0.13125	0.00125
Actual Task Success Probability	0	0.00%	0.00%	0.00%	-1.06%	-1.06%	-1.06%	-0.03%
	0.05	0.00%	0.00%	0.00%	-0.98%	-1.01%	-0.91%	63.17%
	0.1	0.00%	0.00%	0.00%	-0.74%	-0.86%	-0.45%	252.66%
	0.15	0.00%	0.00%	0.00%	-0.33%	-0.60%	0.33%	567.71%
	0.2	0.00%	0.00%	0.00%	0.25%	-0.23%	1.42%	1007.58%
	0.25	0.00%	0.01%	0.01%	1.00%	0.24%	2.83%	1571.53%
	0.3	0.00%	0.01%	0.01%	1.91%	0.81%	4.55%	2258.83%
	0.35	0.00%	0.01%	0.02%	3.00%	1.50%	6.58%	3068.77%
	0.4	0.00%	0.02%	0.02%	4.25%	2.28%	8.93%	4000.63%
	0.45	0.00%	0.02%	0.03%	5.67%	3.18%	11.60%	5053.71%
	0.5	0.00%	0.03%	0.03%	7.25%	4.18%	14.58%	6227.28%
	0.55	0.00%	0.03%	0.04%	9.00%	5.28%	17.87%	7520.67%
	0.6	0.00%	0.04%	0.05%	10.92%	6.49%	21.47%	8933.17%
	0.65	0.00%	0.05%	0.06%	13.01%	7.81%	25.39%	10464.10%
	0.7	0.00%	0.05%	0.06%	15.27%	9.23%	29.63%	12112.77%
	0.75	0.00%	0.06%	0.07%	17.69%	10.76%	34.18%	13878.51%
	0.8	0.00%	0.07%	0.08%	20.28%	12.40%	39.04%	15760.65%
	0.85	0.00%	0.08%	0.09%	23.03%	14.14%	44.21%	17758.51%
	0.9	0.00%	0.09%	0.11%	25.96%	15.98%	49.70%	19871.44%
	0.95	0.00%	0.10%	0.12%	29.05%	17.93%	55.50%	22098.77%
	1	0.00%	0.11%	0.13%	32.31%	19.99%	61.61%	24439.86%

Table 87. Complex State Capability Assessment Risk Sensitivity - Group 3

	Task	Conversion	Reprocessing	Enrichment	Machining	Metallurgy	IND Weaponization Gun-Type	IND Weaponization Implosion
Original Ps		0.479391	1E-08	0	0.18	0.226318	0.13125	0.00125
Actual Task Success Probability	0	0.00%	0.00%	0.00%	-7.85%	-7.84%	-7.85%	-0.24%
	0.05	0.00%	0.00%	0.00%	-7.30%	-7.51%	-6.77%	462.49%
	0.1	0.00%	0.01%	0.01%	-5.49%	-6.37%	-3.33%	1817.34%
	0.15	0.00%	0.02%	0.02%	-2.43%	-4.45%	2.44%	4011.38%
	0.2	0.00%	0.03%	0.04%	1.87%	-1.74%	10.55%	6995.76%
	0.25	0.00%	0.05%	0.06%	7.42%	1.75%	20.99%	10725.36%
	0.3	0.00%	0.07%	0.08%	14.21%	6.04%	33.75%	15158.42%
	0.35	0.00%	0.09%	0.11%	22.24%	11.11%	48.82%	20256.27%
	0.4	0.00%	0.12%	0.15%	31.51%	16.96%	66.20%	25982.99%
	0.45	0.00%	0.16%	0.19%	42.01%	23.59%	85.88%	32305.22%
	0.5	0.00%	0.20%	0.24%	53.74%	31.00%	107.85%	39191.91%
	0.55	0.00%	0.24%	0.29%	66.69%	39.19%	132.11%	46614.15%
	0.6	0.00%	0.29%	0.35%	80.87%	48.16%	158.65%	54544.95%
	0.65	0.00%	0.34%	0.41%	96.28%	57.90%	187.45%	62959.11%
	0.7	0.00%	0.40%	0.47%	112.89%	68.42%	218.52%	71833.08%
	0.75	0.00%	0.46%	0.54%	130.73%	79.71%	251.85%	81144.80%
	0.8	0.00%	0.52%	0.62%	149.77%	91.77%	287.43%	90873.59%
	0.85	0.00%	0.59%	0.70%	170.03%	104.61%	325.24%	101000.09%
	0.9	0.00%	0.66%	0.79%	191.49%	118.21%	365.30%	111506.08%
	0.95	0.00%	0.74%	0.88%	214.16%	132.58%	407.58%	122374.46%
	1	0.00%	0.82%	0.97%	238.03%	147.71%	452.09%	133589.14%

V.C.4. Complex State Failure Risk Analysis

The complex State results showed that the contribution to State-level risk from nuclear weapons was essentially negligible because of the extremely robust security employed on these weapons. Table 88 shows the risk breakdown from the four threats of nuclear terrorism in the event that the complex State fails. These results assume that in the event of a State failure, the security measures employed on nuclear weapons are negated.

Table 88. Failed Complex State Risk Analysis

Threat	$\mathbb{R}_{Group\ 1}$	$\mathbb{R}_{Group\ 2}$	$\mathbb{R}_{Group\ 3}$
Nuclear Weapons	98.59%	99.88%	99.98%
IND	0.00%	0.00%	0.00%
RDD	0.74%	0.05%	0.00%
Sabotage	0.67%	0.07%	0.01%

The results from Table 88 show that if the State's control of nuclear weapons is lost, the State's risk profile shifts entirely to the nuclear weapon threat. Table 89 shows the relative likelihood that each adversary group chooses each nuclear threat.

Table 89. Failed Complex State Relative Probability of Choosing Threats

Threat	$P_{A,Group\ 1}^{V}$	$P_{A,Group\ 2}^{V}$	$P_{A,Group\ 3}^{V}$
Nuclear Weapons	6.00%	48.90%	90.47%
IND	0.00%	0.02%	0.03%
RDD	89.98%	47.69%	8.50%
Sabotage	4.01%	3.39%	1.00%

The combined results from Table 88 and Table 89 show that adversary motivations have a very slight impact on the risk from nuclear weapons in the event of State failure. The consequences from the loss of control of one nuclear weapon far outweigh those of the other threats, so even if the adversary has a small relative likelihood of choosing to exploit this opportunity, the risk from the nuclear weapon threat far outweighs the other nuclear terrorism threats.

CHAPTER VI

CONCLUSIONS AND RECOMMENDATIONS

VI.A. Summary of Results

In this work, we have demonstrated a risk-based methodology to evaluate State-level risk that can be used to recommend security upgrades. The methodology accounts for adversary motivations and disincentives, adversary capabilities, all of the materials and security measures currently present in the State, and the relative consequences of each threat to that State. The methodology employs MAUA to bias adversary decision making based on their motivations and disincentives for nuclear terrorism. Utility functions that relate to the physical, material and radiological properties of materials are employed to represent the decisions of a strategic adversary. Pathways analysis is used to develop the pathways an adversary can take to execute each nuclear threat based on the material properties of each nuclear and radiological material being analyzed. Game-theory is used to replicate the strategic decision making of the adversary intent on executing threats that maximize their benefit, including the ability to change tactics in response to security upgrades by the State. Finally, decision theory is employed to determine the nuclear security measure upgrades the State should employ.

To test the methodology, a VBA code was developed in Microsoft Visio utilizing Microsoft Excel as a database. To verify the code's pathways generation function we tested a variety of materials to ensure that every possible pathway was populated properly. We then developed a verification problem and worked it out manually and ran the same problem in the Visio code. We then compared the result from every step to ensure the code performs as expected and to verify the absence of any programming errors.

Due to the lack of data on real-world security problems from the State level, the code was validated qualitatively rather than quantitatively. We validated the MAUA portion of the code, which takes the adversary's motivations and disincentives and biases their decisions to align with their intentions. We then validated the material utility functions for IND materials by simulating a variety of real world materials and assessing the results. We then validated the sensitivity analysis function by presenting the code with symmetric and non-symmetric cases where the results were intuitively obvious.

We then developed three test cases involving States with varying levels of nuclear infrastructure complexity. We tested the code against three different adversaries to observe how adversary motivations affect the State strategy to address the risk from nuclear terrorism. For the State that did not have direct-use material, the risk from IND's was negligible compared to the RDD and sabotage risk. For the States that possessed direct-use material, the threat of IND was highly dependent on adversary motivations. In cases where there were a small number of pathways contributing to the State-level risk, the analysis prioritized the State's security upgrades to address these pathways. When a large number of pathways existed, the analysis recommended upgrading those security measures that address multiple threats. For each State, the analysis of risk reduction strategies provides information that could be utilized by decision makers to understand how upgrades improve the security risk of the State. For situations where reducing State-level risk by removing material causes the loss of benefits provided by that material, such as cancer treatment or research capabilities, the code can provide security measure upgrades that provide equivalent levels of risk-reduction while keeping that material in the State.

Sensitivity analysis on the assessed capabilities of terrorist groups showed varying results. For States without nuclear materials, the risk results are insensitive to terrorist capabilities to produce IND. For States with direct-use material, the State-level risk is highly sensitive to the adversary's capability to produce an IND. To address this sensitivity, States can eliminate direct-use nuclear materials or gain confidence in their assessments of terrorist capabilities by spending resources on intelligence information. This sensitivity also shows that if the State chooses to use conservative values in risk assessments, these assumptions can have a significant impact on the perceived risk level, and subsequently the resources the State must devote to nuclear security.

While States should apply a risk methodology to determine the optimum set of upgrades, the results from the State-level risk analyses produce a some general conclusions:

1. States that have a small number of nuclear and radiological materials or have a small number of targets contributing to the majority of the State-level risk, improving security measures associated with these security measures is an effective way to address risk. These security measures will be effective regardless of adversary motivation.
2. States with a large inventory of nuclear and radiological materials or that have a risk profile that is spread among several targets should consider second-line of defense measures, such as trafficking interdiction, in addition to securing the materials at their source.
3. As a State's ability to recover and recapture material improves, sabotage becomes the nuclear terrorism risk of greatest concern.
4. For States with high-consequence targets, security measures that serve as a last line of defense at these targets are viable security investments.
5. The risk to States that don't possess direct-use materials is insensitive to adversary capabilities to produce an IND.
6. The risk to States that have substantial quantities of direct-use materials is incredibly sensitive to the ability of adversaries to produce an IND. These States should devote resources to improve their confidence in adversary capabilities to produce IND to ensure optimal investments in security. Alternatively, reducing the amount of direct-use material will decrease the State sensitivity to adversary capability.

7. Even if adversaries are highly motivated to pursue nuclear weapon or IND threats, the State's risk from RDD and sabotage threats may be greater.
8. In instances where risk reduction approaches such as material removal also results in the loss of benefit from that material, alternative approaches exist that can provide equivalent levels of risk reduction.

VI.B. Recommendations for Future Work

Within the defined scope of this dissertation, the methodology performed very well. However, a number of assumptions were made that may be further investigated in future work. In addition, this work introduces the capability to perform a State-level risk analysis which could be further applied to other areas besides nuclear terrorism. The recommendations for future work are:

1. Consequence estimation were based on crude models developed from open-source literature. States or the IAEA likely have much better information on the possible consequences of an RDD and IND attack which could be employed when conducting this analysis on a real-world State.
2. For IND cases, the adversary only stole 1 SQ of material to produce 1 IND. Further work may want to characterize the likelihood that the adversary will steal multiple SQ's and produce multiple IND's. This assumption was based on the combination of our crude consequence models and the very low likelihood of this scenario.

3. For RDD cases, the adversary stole all material and delivered it to the maximum number of cities possible, based on the number of targets analyzed and the adversary's resources. Future work may want to add optimization to the amount of material the adversary steals based on the trade-offs between the increased probability of detection and difficulty in handling the material versus the increase in RDD consequences. Based on our RDD consequence models, employing an optimization strategy had negligible effects on the results.
4. We employed a simple longitude and latitude based transportation model. States and the IAEA likely have more advanced transportation models which can be employed and the results incorporated into this model.
5. The methodology developed in this dissertation could be compared to Safeguards and Safety risk analyses to better address the risk from nuclear and radiological materials and facilities.
6. While the model was developed to incorporate cost into the analysis, because of the lack of real world cost vs. benefit information for nuclear security measures, the results focused on risk reduction. Adding real-world security measure costs to the analysis may produce some different results than a pure risk-reduction analysis.
7. This model focuses specifically on the risk of nuclear terrorism. The general framework introduced in this methodology should be applied to biological and chemical terrorism to develop a comprehensive understanding of WMD risk.

8. This model focuses on the risk at the State level. The next step would be to develop a multi-State risk model that could be used to best allocate resources internationally rather than at the State-level.

REFERENCES

[1] Taniguchi, Tomihiro, and Anita Nilsson. "Hot Spots, Weak Links: Strengthening Nuclear Security in a Changing World." International Atomic Energy Agency (IAEA),

[2] Bunn, Matthew, and Col-Gen E.P. Maslin. "All Stocks of Weapons Usable Nuclear Materials Worldwide Must Be Protected Against Global Terrorist Threats". Harvard University. (2010)

[3] Lewis, Jeffrey G. "The Economics of Nuclear Terrorism." The Fund for Peace. Washington, D.C. (2006)

[4] Van Tuyle, Gregory J. "Assessing the Radiological Dispersal Devices Threat and Addressing the Vulnerabilities." Los Alamos Nation Laboratory. LA-UR-O2-5567, (2002).

[5] Bunn, Matthew. "Securing the Bomb 2010: Securing All Nuclear Materials in Four Years." Nuclear Threat Initiative, Accessed January 16, 2011. http://www.nti.org/media/pdfs/Securing_The_Bomb_2010.pdf?_=1317159794.

[6] International Atomic Energy Agency (IAEA). "Handbook on the Physical Protection of Nuclear Materials and Facilities". TECDOC-1276 (2002).

[7] International Atomic Energy Agency (IAEA). "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities". IAEA Nuclear Security Series No. 13. INFCIRC/225/Rev. 5 (2011).

[8] The International Atomic Energy Agency. "Nuclear Security - Measures to Protect Against Nuclear Terrorism". GOV/2006/46-GC(50)/13. (2006).

[9] Elliott, Grant. "US Nuclear Weapon Safety and Control". MIT Program in Science, Technology and Society (2005)

[10] Daly, Sara, Parachini, John, Rosenau, William. "Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism." The RAND Corporation. (2005).

[11] "Nuclear Terrorism Fact Sheet". Belfer Center for Science and International Affairs, Harvard University. (2010).

[12] Ferguson, Charles D. and William C. Potter. (2004). *The Four Faces of Nuclear Terrorism*. Monterey : Center for Nonproliferation Studies, Monterey Institute of International Studies.

[13] Ellingsen, Simen A. "Nuclear Terrorism as Rational Choice". King's College, University of London, Department of War Studies. Dissertation. (2009).

[14] The White House. "Remarks by President Barack Obama". Office of the Press Secretary. (2009).

[15] The Fissile Materials Working Group . "Seoul Nuclear Security Summit Delivers Modest Results". (2012) . http://www.fmwg.org/press.cfm?action=article&page=0&id=44112099-5712-4681-946a-d298d9aeb20b

[16] The International Atomic Energy Agency. "The Convention on the Physical Protection of Nuclear Material". INFCIRC/274/Rev. 1. (1980).

[17] The International Atomic Energy Agency. "International Conventions and Legal Agreements: Convention on Physical Protection of Nuclear Material". Accessed May 12, 2012. http://www.iaea.org/Publications/Documents/Conventions/cppnm.html

[18] The United Nations. "International Convention for the Suppression of Acts of Nuclear Terrorism". United Nations (2005).

[19] Signatory and State Party List for the International Convention for the Suppression of Acts of Nuclear Terrorism. Accessed May 25, 2012. http://treaties.un.org/Pages/ViewDetailsIII.aspx?&src=UNTSONLINE&mtdsg_no=XVIII~15&chapter=18&Temp=mtdsg3&lang=en#Participants

[20] "Resolution 1540 (2004). United Nations Security Council. S/Res/1540 (2004).
[21] The International Atomic Energy Agency. "The Physical Protection of Nuclear Material and Facilities". INFCIRC/225/Rev. 5 (2011)

[22] The International Atomic Energy Agency. "Code of Conduct on the Safety and Security of Radioactive Sources". IAEA/CODEOC/2004 (2004).

[23] International Atomic Energy Agency. "Nuclear Safety and Security: Adherence to International Legal Instruments" Updated Feb 17, 2012. Accessed May 25, 2012. http://www-ns.iaea.org/security/legal_instruments.asp?s=4&l=29.

[24] International Atomic Energy Agency. "Nuclear Safety and Security: Nuclear Security". Updated March 26, 2012. Accessed May 25, 2012. http://www-ns.iaea.org/security/.

[25] United States Government Accountability Office (GAO). "Nuclear Nonproliferation: IAEA has Strengthened Its Safeguards and Nuclear Security Programs, but Weaknesses Need to Be Addressed". GAO-06-93 Nuclear Nonproliferation (2005).

[26] Boureston, Jack and Andrew K. Semmel. "The IAEA and Nuclear Security: Trends and Prospects". *Policy Analysis Brief*, The Stanley Foundations (2010).

[27] International Atomic Energy Agency. "Nuclear Security - Measures to Protect Against Nuclear Terrorism: Progress report and Nuclear Security Plan for 2006-2009". (2005) GC(49)/17.

[28] Garcia, M.L. (2001). *The Design and Evaluation of Physical Protection Systems.* Boston :Butterworth- Heinemann.

[29] Hayns, M.R. "The Evolution of Probabilistic Risk Assessment in the Nuclear Industry". *Trans IChemE* 77, Part B (1999) 117-142

[30] Kaplan, Stanley and B. John Garrick. "On the Quantitative Definition of Risk". *Risk Analysis* 1, No. 1 (1981).

[31] Apostolakis, George. "The Nuclear News Interview - Apostolakis: On PRA." Nuclear News, (2000), 27-31.

[32] Ezell, C.B., Bennett, S.P. von Winterfeldt, D., Sokolowski, & J. Collins, A.J. "Probabilistic Risk Analysis and Terrorism Risk". *Risk Analysis* 30, No. 4 (2010) 575-589.

[33] Stamatelatos, Michael. "Probablistic Risk Assessment: What Is It and Why Is It Worth Performing It?". NASA Office of Safety and Mission Assurance. (2000).

[34] Federal Aviation Administration. "Guide to Reusable Launch and Reentry Vehicle Reliability Analysis". (2004) Version 1.0.

[35] Willis, Henry. "Guiding Resource Allocations Based on Terrorism Risk". RAND Center for Terrorism Risk Management Policy. (2006).

[36] Garrick, B. J. , Hall, J.E., Kilger, M., McDonald, J. C., O'Toole, T., Probst, P.S., Parker, E.R., Rosenthal, R., Trivelpiece, A.W., Van Arsdale, L.A. Zebroski, E.L. "Confronting the Risks of Terrorism: making the Right Decisions". *Reliability Engineering and System Safety,* 86 (2004) 129-176.

[37] Daniels, David C., Hudson, Linwood D., Laskey, Kathryn B., Mahoney, Suzanne M., Ware, Bryan S., Wright, Edward J. Chapter 14 of *Bayesian Networks: A Practical Guide to Applications*. (2008) John Wiley & Sons. West Sussex, England.

[38] Freeman, Corey Ross. "Bayesian Network Analysis of Nuclear Acquisitions". Texas A&M University. College Station, TX. Thesis. (2008).

[39] Keeney, Ralph L. "Modeling Values for Anti-Terrorism Analysis". *Risk Analysis,* 27, No 3 (2007) 585-596.

[40] Keeney, Ralph L. and Howard Raiffa. (1993) *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. New York: Cambridge University Press.

[41] Giangeli III, Donald D. "Development of the Fundamental Attributes and Inputs for Proliferation Resistance Assessments of Nuclear Fuel Cycles." Texas A&M University. College Station, TX. Thesis. (2007).

[42] Pate'-Cornell, Elisabeth and Seth Guikema. "Probablistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures". *Military Operations Research* 7, No 4 (2002) 5-20.

[43] Ezell, Charles B. "Infrastructure Vulnerability Assessment Model (I-VAM). Accessed 1/16/2012. http://create.usc.edu/assets/pdf/51834.pdf.

[44] Brown, G.B., Carlyle, W.M. & Wood, R.K. "Optimizing Department of Homeland Security Defense Investments: Applying Defender-Attacker (-Defender) Optimization to Terror Risk Assessment and Mitigation". Operations Research Department, Naval Postgraduate School. Appears as Appendix E of: National Research Council, "*Department of Homeland Security Bioterrorist Risk Assessment: A Call for Change*," National Academies Press, Washington, DC. (2008)

[45] Parnell, G.S., Smith, C.M. & Moxley, F.I., "Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model". *Risk Analysis* 30, No 1 (2010) 32-48.

[46] Baker, A.B., Eagan, R.J., Falcone, P.K., Harris, J.M.,Herrera, G.V., Hines, W.C., Hutchinson, R.L., Moonka, A.K., Swinson, M.L., Webb, E.K., Woodall, T.D., & Wyss, G.D. "A Scalable Systems Approach for Critical Infrastructure Security". Sandia National Laboratories, SAND2002-0877 (2002).

[47] Patterson, Sean A. "Identification of Critical Locations Across Multiple Infrastructures for Terrorist Actions". Massachusetts Institute of Technology. Cambridge, MA. Thesis. (2005).

[48] Michaud, David and George Apostolakis. "Methodology for Ranking the Elements of Water-Supply Networks". *Journal of Infrastructure Systems*. December 2006, 230-242.

[49] Woo, Gordon. "Quantitative Terrorism Risk Assessment". Risk Management Solutions, Ltd. Accessed May 12, 2012. http://isc.temple.edu/economics/wkpapers/Homeland/Quantitative_Terrorism_Risk_Assessment.pdf

[50] Blandford, E., Peterson, P., Powell, R. &Kim, L. "Protecting Critical Nuclear Infrastructure: Strategies for Security". Center for International Security and Cooperation, Stanford University, Stanford, CA (2010).

[51] Cuellar, L., Cleland, T., Kubicek, D., Kelton, T., Mathis, M., Roach, F., Roberts, R., Stroud, P., Saeger, K.J., & Smith, J.P. "Probabilistic Effectiveness Methodology: A holistic Approach on Risk Assessment of Nuclear Smuggling". *2011 IEEE International Conference on Technologies for Homeland Security(HST)*. November 2011, 325-331.

[52] Garcia, Mary L. (2005) *Vulnerability Assessment of Physical Protection Systems.* Boston: Butterworth-Heinermann.

[53] International Atomic Energy Agency (IAEA). "Design Basis Threat". Accessed January 15, 2012. http://www-ns.iaea.org/security/dbt.asp?s=4

[54] Duran, Felicia A. "Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Materials". University of Texas at Austin. Dissertation (2010)

[55] Conchewski, Curtis. "Physical Protection System Sensitivity to DBT Perturbations". Texas A&M University. College Station, TX. Thesis. (2012).

[56] McGill, W.L., Ayyub, B.M., & Kaminskiy, M. "Risk Analysis for Critical Asset Protection". *Risk Analysis* 27, No 5 (2007) 1265-1281.

[57] International Atomic Energy Agency. "IAEA Safeguards Glossary 2001 Edition". International Nuclear Verification Series No 3. Vienna (2002).

[58] Cochran, Thomas B. and Christopher E. Paine. "The Amount of Plutonium and Highly-Enriched Uranium Needed for Pure Fission Nuclear Weapons". Natural Resources Defense Council Inc., Washington DC (1995).

[59] Albright, David and Kimberly Kramer. "Neptunium 237 and Americium: World Inventories and Proliferation Concerns". Institute for Science and International Security (2005).

[6060] Glaser, Alexander. "On the Proliferation Potential of Uranium Fuel for Research Reactors at Various Enrichment Levels". *Science and Global Security* 14 (2006) 1-24.

[61] Choi, J-S., Lee, C.K., Ebbinghaus, B.B. "Effects of Plutonium Quality on Critical Mass". American Nuclear Society Winter Meeting and Nuclear Technology Expo. UCRL-CONF-204868. Lawrence Livermore National Laboratory (2004).

[62] Devolpi, A. "Fissile Materials and Nuclear Weapons Proliferation". *Ann. Rev. Nucl. Part. Sci.* 36 (1986) 83-114.

[63] United States General Accounting Office. "Quick and Secret Construction of Plutonium reprocessing Plants: A Way to Nuclear Weapons Proliferation?". Report by the Comptroller General of the United States. EMD-78-104 (1978).

[64] Steinhausler, Friedrich. "What It Takes to Become a Nuclear Terrorist". *American Behavioral Scientist* 46 (2003) 782-795. Sage Publications.

[65]International Atomic Energy Agency. "Categorization of Radioactive Sources". (2003) TECDOC-1344.

[66] International Atomic Energy Agengy. "Identification of Vital Areas at Nuclear Facilities (Draft)". IAEA Nuclear Security Series. (2007) Version 4.

[67] Johnson, Roger G. and Warner, Jon S. "Handbook of Security Blunders". *Proceedings of the 51st Annual INMM Meeting*. Baltimore, MD. July 11-15 2010.

[68]Cuellar, L., Cleland, T., Kubicek, D., Kelton, T., Mathis, M., Roach, F., Roberts, R., Stroud, P., Saeger, K.J., & Smith, J.P. "Probabilistic Effectiveness Methodology: A holistic Approach on Risk Assessment of Nuclear Smuggling". *2011 IEEE International Conference on Technologies for Homeland Security(HST)*. November 2011, 325-331.

[69] C. Bathke, B. Ebbinghaus, B. Sleaford, R. Wallace, B. Collins, K. Hase, G. Jarvinen, K. Bradley, J. Ireland, M. Johnson, A. Prichard, B. Smith, “The Attractiveness of

Materials in Advanced Nuclear Fuel Cycles for Various Proliferation and Theft Scenarios," Los Alamos National Laboratory (2009) LA-UR-09-02466.

[70] Mark, J. Carson, Hippel, Frank von, Lyman, Edward. "Explosive Properties of Reactor-Grade Plutonium". *Science and Global Security,* 17 (2009) 270-285.

APPENDIX A

Nuclear Terrorism Motivations and Disincentives
Kristen Childress
Texas A&M University
The Bush School of Government and Public Service

A.1. Motivations for Sub-state Groups to Pursue the Nuclear Threat

1. Prestige of Successful Capabilities (Peaceful): Possessing the capability for terrorism demonstrates an organization's viability and legitimacy. The group believes that simply possessing the ability to successfully complete a nuclear terrorist threat will achieve its goals, and finds the actual event to be unnecessary. It is also possible that the group may detonate a weapon as a show of strength in a non-populated area.
   - Al Qaeda – "Osama bin Laden would… think in terms of how best to leverage possession of a nuclear weapon to serve the longer term goal of an Islamic revival and restoration." "too valuable to detonate.. used as blackmail or deterrent"[g]

2. Prestige of Successful Capabilities (Non-Peaceful): Possessing the capability for terrorism demonstrates an organization's viability and legitimacy. The group clearly has no problem using nuclear terrorism to achieve their goals.

[g] Dunn, Lewis. "Can Al Qaeda be Deterred from Using Nuclear Weapons?" *Center for the Study of Weapons of Mass Destruction, Occasional Paper 3.* July 2005. <http://www.ndu.edu/inss/Occassional_Papers/CSWMD/OP3.pdf> p.18.

- Al Qaeda – “the mere possession of one nuclear weapon would make bin Laden’s little army of exiles a force to be reckoned with.”[h]

3. Manipulate Adversaries: A group pursues nuclear terrorism to use as leverage against or to demonstrate a weakness in other organizations or nations.
    - Al Qaeda – Remove U.S. presence from Saudi Arabia and Middle East[i]
        - Also establish Palestinian state[j]
        - Demonstrate weakness – sabotage
    - Ramzi Yousef – punish American people for the U.S. Government’s support of Israel – convince the people to force the government to stop supporting Israel.[k]
    - Chechen president Dzhokhar Dudayev’s personal archive. The archive contained a detailed plan to hijack a Russian atomic submarine, calling for seven Slavic-looking fighters to seize a submarine from the Russian Navy’s Pacific Fleet sometime in 1995 or 1996 and coerce Moscow into withdrawing troops from Chechnya.7 Dudayev’s archive also contained plans to blow up installations at nuclear power stations

[h] Jenkins, Brian Michael. Will Terrorists Go Nuclear? Amherst: Prometheus Books, 2008: 93. Note: pre-1996, so maybe this changed when his organization switched to mainly religious motives?

[i] Hayes, Laura, Borgna Brunner, and Beth Rowan. “Al Qaeda: Osama bin Laden’s Network of Terror.” 2007. Infoplease. 25 March 2009. <http://www.infoplease.com/spot/al-qaeda-terrorism.html>.

[j] Hoffman, Bruce. Inside Terrorism. 2nd ed. New York: Columbia University Press, 2006: 82.

[k] Parachini, John. “Comparing Motives and Outcomes of Mass Casualty Terrorism Involving Conventional and Unconventional Weapons.” *Studies in Conflict and Terrorism* Sept.-Oct. 2001, p.389-406.

4. Apocalyptic Beliefs: The organization believes that the end of the world is near and is motivated to take an active role in promoting the event.
    - Aum Shinrikyo – members would be the only ones to survive the apocalypse[l]
5. War on Own Nation: Separatist or nationalist group that wants to use nuclear terrorism to combat, overthrow, or undermine the current government of a country.
    - Nationalist – FARC[m]
    - Separatist – ETA[n]
    - Separatist – LTTE[o]
    - Separatist – PKK/Kongra Gel[p]
    - Timothy McVeigh – Oklahoma City bombing to incite a new American revolution against the U.S. Government[q]

[l] Aum Shinrikyo. 28 May 2008. Council on Foreign Relations. 25 March 25, 2009. <http://www.cfr.org/publication/9238/aum_shinrikyo_japan_cultists.html>.

[m] "Colombia: The Multi-faceted Motivation of the FARC and Prospects of Peace." Political Affairs Magazine. 11 October 2007. Council on Hemispheric Affairs. 25 March 2009. <http://www.politicalaffairs.net/article/view/5981/1/289/>.

[n] - http://www.geocities.com/CapitolHill/8864/ingle.htm (1995)

Basque Democratic Alternative. 1995. 25 March 2009. <http://www.geocities.com/CapitolHill/8864/ingle.htm>.

[o] *Tamil Tiger "Martyrs": Regenerating Divine Potency?* -Michael Roberts p.495 – (2005) - http://texasamcolstattx.library.ingentaconnect.com/content/routledg/uter/2005/00000028/00000006/art00003

[p] Inside the Kurdistan Workers Party. 17 October 2007. Council on Foreign Relations. 25 March 2009. <http://www.cfr.org/publication/14576/inside_the_kurdistan_workers_party_pkk.html>.

[q] Parachini, John. "Comparing Motives and Outcomes of Mass Casualty Terrorism Involving Conventional and Unconventional Weapons." *Studies in Conflict and Terrorism* Sept.-Oct. 2001, p.389-406.

6. War on Another Nation: The organization has a deep hatred for a particular people or nation and they feel compelled to use nuclear terrorism to combat or enact revenge upon their adversary.
    - Al Qaeda – "is dedicated to such broad goals as the overthrow of all corrupt Muslim governments..", "… bin Laden supplemented his publicly declared war on the United States… with a fatwa."[r]
    - Hezbollah – on Israel[s]

7. Redress Conventional Military Asymmetry: An organization has a finite amount of people and resources to combat a nation, and seeks to use nuclear terrorism to redress this imbalance.
    - Al Qaeda – Does not have the same access to resources and population as U.S. so has to use other means

8. Ensure Security: A group pursues nuclear terrorism in order to protect citizens/members of a certain group (religious, political, ethnic, etc.) from attack or persecution. The "guarantor of security."
    - Hamas – Israel has nuclear weapons, so Hamas needs weapons to protect the Palestinian Muslims[t]

[r] Hoffman, Bruce. "Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations." RAND. 1999. <http://www.rand.org/pubs/papers/2007/P8039-1.pdf> p.32.

[s] Sharp, Jeremy. "Lebanon: The Israel-Hamas-Hezbollah Conflict." Congressional Research Service Report. 15 September 2006. <http://www.fas.org/sgp/crs/mideast/RL33566.pdf>.

[t] Hamas. 7 January 2009. Council on Foreign Relations. 20 March 2009. <http://www.cfr.org/publication/8968/>.

- Lashkar-e-Toiba – Protect the people of Kashmir and Jammu from Indian rule – and more generally protect Muslims under non-Muslim rule[u]
- Al Qaeda – “We have the [chemical and nuclear] weapons as deterrent”, “I wish to declare that if America used chemical or nuclear weapons against us, then we may retort with chemical and nuclear weapons.” deter attack from US on Muslims/Al Qaeda[v]
- Jam’iyyat Ul-Islam Is-Saheeh – domestic US terrorist group wanting to “levy war against the government of the US through terrorism,” and indicate that the planned incidents are part of a “plight to defend and propagate traditional Islam in its purity” – 2006[w]

9. Mass Devastation/Chaos: The group is motivated to wreck economic, political and/or psychological havoc on a population, and thus devastate the nation’s infrastructure or population by nuclear terrorism. In this case, the violence is the end in itself.
    - Economic: Al Qaeda – “we will also aim to continue, by permission of Allah, the destruction of the American economy.” Al-Zawahiri[x]

[u] Lashkar-e-Toiba. 2006. South Asia Terrorism Portal. 25 March 2009. <http://satp.org/satporgtp/countries/india/states/jandk/terrorist_outfits/lashkar_e_toiba.htm>.

[v] Daly, Sarah, John Parachini, and William Rosenau. “Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism.” RAND (2005): 26.

[w] Mrozek, Thom. “Man Who Formed Terrorist Group that Plotted Attacks on Military and Jewish Facilities Sentenced to 16 Years in Federal Prison.” 6 March 2009. Department of Justice. 26 March 2009. < http://losangeles.fbi.gov/dojpressrel/pressrel09/la030609ausa.htm>.

[x] “Implementing the National Strategy.” U.S. Congressional Report. 15 December 2002. RAND. 26 March 2009. <http://www.rand.org/nsrd/terrpanel/terror4.pdf>.

- Psychological: 1995 - Chechen rebels planting dirty bomb in Moscow, calling media but not detonating – creating fear/psychological response from Russian population.[y]
- Psychological: Al Qaeda – as seen in the proliferation of analysts evaluating every recent threat in the media, and the shift in government policies as a result of these threats – "they want to see us sweat"[z]

10. Religious Imperative: Religious extremists that believe they have been given a religious mandate or imperative to pursue the nuclear threat.
    - "Religious Duty" – Al Qaeda (Bin Laden) [aa]
11. Manipulate Policy: A group seeks to use the nuclear threat to bring attention to and/or change a specific policy (political, economic, religious, etc) that it does not agree with.
    - Economic/political – FARC[bb]
    - Political/social – ETA[cc]
    - Political/religious – Jamaat al-Islamiyya[dd]

[y] Jenkins, Brian Michael. Will Terrorists Go Nuclear? Amherst: Prometheus Books, 2008: 125.

[z] Jenkins, Brian Michael. Will Terrorists Go Nuclear? Amherst: Prometheus Books, 2008: 126-129.

[aa] http://cns.miis.edu/pubs/reports/binladen.htm (1998), McCloud, Kimberly, and Matthew Osborne. "WMD Terrorism and Usama bin Laden." 20 November 2001. James Martin Center for Nuclear Nonproliferation. 26 March 2009. <http://cns.miis.edu/reports/binladen.htm>. Also in Hoffman – "Inside Terrorism" p. 82 (2006)

And Al Qaeda – "The United States is the world's biggest terrorist and rogue, and it is the duty of every Muslim to struggle for its annihilation." – Daly RAND article –p.25 –

[bb] http://www.politicalaffairs.net/article/view/5981/1/289/ (2007)

[cc] - http://www.geocities.com/CapitolHill/8864/ingle.htm (1995)

[dd] - http://www.cfr.org/publication/9156/ (2008)

- Political religious – Lashkar-e-Taiba[ee]
- Political/economic – ELF [ff]

12. Fascination With Nuclear Threat: Group leaders are fascinated by the threat of nuclear weapons, radiological weapons, or sabotage, or specific effects related to a threat, such as radiation
    - Asahara - Aum Shrinkyo's nuclear and chemical acquisition attempts were partially due to Asahara's fascination with poisons and the nuclear holocaust

A.2. Motivational Disincentives for Sub-state Groups to Pursue the Nuclear Threat

1. Fear of Retaliation on a Base of Support: Nuclear terrorism creates a fear of retribution on the group's perceived constituents. Usually more than likely applies to a group that has a well defined geographic territory or population. (Jenkins p.104)
    a. Hamas – Retribution on Palestinians
    b. Nationalist/Separatists[gg] – as a general group

[ee] – establish an Islamic state in India – advocate Islam worldwide http://satp.org/satporgtp/countries/india/states/jandk/terrorist_outfits/lashkar_e_toiba.htm (2006)

[ff] "a campaign of property destruction to cause economic damage to institutions responsible for practices harmful to the environment, and to destroy equipment being used in those activities." – Jeff Luers – "Extreme Action" 3/27/02 -http://www.freefreenow.org/jw_writings.html#extreme

[gg] Four Faces of Nuclear Terrorism p.19

2. Concern for Personnel Safety: Difficulty in protecting group members from exposure to radiation and difficulty of preventing radiation accidents deteriorates group's motivation to attempt nuclear terrorism.

3. Fear of Attracting Attention: Any news or hint of the group pursuing nuclear terrorism will put an international target on the group, making movement and success more difficult and threatening security.

    a. Provisional IRA – the discovery of IRA seeking nuclear material would bring out a severe crackdown from the British government and jeopardize the fragile peace process[hh]

4. Alienation: A display of nuclear terrorism would alienate the group's real or perceived base of support or actual financial supporters. (Jenkins p.103)
    a. Al Qaeda - Ackerman –"Nuclear Terrorism…" p.8
        i. Al Qaeda - "Can Al Qaeda be deterred from using nuclear weapons?" alienate the wider range of Muslims Osama bin Laden intends to use for his Islamic caliphate[ii]
    b. Nationalist/Separatists
        i. Tamil Tigers[jj]

[hh] Parachini, John. "Putting WMD Terrorism Into Perspective." *Washington Quarterly*. Autumn 2003. vol26:issue 4. P. 37.

[ii] Dunn, Lewis. "Can Al Qaeda be Deterred from Using Nuclear Weapons?" *Center for the Study of Weapons of Mass Destruction, Occasional Paper 3.* July 2005. <http://www.ndu.edu/inss/ Occassional_Papers/CSWMD/OP3.pdf> p.1.

c. Chechen Rebels[kk]

5. Contradict Goals of Group: Nuclear terrorism would contradict or directly prevent the fulfillment of the group's aims. (e.g. environmental groups)

    i. Hamas using nuclear weapons to defeat Israel would prevent it from being able to take over the then-contaminated land

    ii. Hamas leader Abu Shannab, for one, stated that the use of poison was contrary to Islamic teachings.22 Although Hamas is a religiously based organization, its struggle to establish a Palestinian state on Israeli territory and to eliminate Israel as a state is decidedly political. " Putting WMD Terrorism into Perspective"

b. Moral code: It would violate the group's moral code to carry out such an indiscriminate and mass-casualty attack.

    i. FARC

6. **Prohibitively Expensive or Difficult**: The extreme difficulty and expense of obtaining a weapon or material would prohibit the group from taking other desired actions. The relative cost of attempting nuclear terrorism is too high.

[jj] Four Faces of Nuclear Terrorism p.19
[kk] "The Threat of Nuclear Terrorism in Europe" *New Presence: The Prague Journal of Central European Affairs.*

    a. Ramzi Yousef – did not use a WMD in the 1993 world trade center attack because it was too difficult and too expensive – thought about using it in another attack[ll]

7. Risk-aversion: Nuclear terrorism does not have a high enough probability of success – group is not willing to risk a failure because it would hurt the credibility of its future threats. (Jenkins p.104)

8. Lack of religious mandate: A religiously-motivated group does not feel it has the necessary divine permission to carry out nuclear terrorism.

9. Internal Group Division: The group has divided opinions on the benefits of attempting nuclear terrorism, so progressing further would fracture group cohesion and significantly weaken the group. (Jenkins p. 103)

10. Current Security Adaquate: Group has confidence in current security situation because it has guaranteed protection from another state or entity whose "nuclear umbrella" will cover this group, and thus does not need nuclear weapons of its own.

    a. Hezbollah, Hamas - if Iran had nukes.

[ll] John Parachini – "Comparing motives and outcomes of mass casualty terrorism involving conventional and unconventional weapons." *Studies in Conflict and Terrorism* Sept.-Oct. 2001, p.389-406.

b. Pakistani militants in Kashmir – Council on Foreign Relations

A.3. Sources

Ackerman, Gary. “Nuclear Terrorism: Assessing the Threat to the Homeland.” United States Senate Committee on Homeland Security and Governmental Affairs. Hearing 2 April 2008. Accessed @ < http://hsgac.senate.gov/public/_files/040208Ackerman3.pdf>.

Ackerman, Gary. “WMD Terrorism Research: Whereto From Here?” Center for Nonproliferation Studies: Monterey Institute of International Studies, October 15, 2004. Accessed @ <http://www.cidcm.umd.edu/carnegie/papers/ackerman.pdf>.

Asal, Victor, Gary Ackerman, and R. Karl Rethemeyer. “Connections Can Be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Terrorism.” April 2008. Accessed @ < http://www.hks.harvard.edu/netgov/files/NIPS/Rethemeyer_ConnectionCanBeToxic_IDs.pdf>.

“Chemical, Biological, Radiological, and Nuclear Terrorism: The Threat According to the Current Unclassified Literature.” Center for Counterproliferation Research – National Defense University. 31 May 2002. Accessed @ <http://www.ndu.edu/centercounter/CBRN_Annotated_Bib.pdf>.

Ferguson, Charles, and William Potter. The Four Faces of Nuclear Terrorism. 1st ed. Monterey, CA: Monterey Institute of International Studies, 2004.

Jenkins, Brian Michael. Will Terrorists Go Nuclear? Amherst: Prometheus Books, 2008.

Kashmir Militant Extremists. 12 July 2006. Council on Foreign Relations. 08 May 2009. < http://www.cfr.org/publication/9135/>.

Van Vuuren, R. “Nuclear Non-Proliferation: The South African Experience in Global Context.” Library – University of South Africa. Thesis. p.65-102; accessed @ <http://etd.unisa.ac.za/ETD-db/theses/available/etd-05122005-104638/unrestricted/03chapter3.pdf>.

APPENDIX B

CONSEQUENCE UTILITY FUNCTIONS AND CALCULATIONS

Consequences of a terrorist attack are incredibly difficult to calculate because of the number of factors about the terrorist group that are unknown, which effect the reliability of any weapon they may attempt to detonate as well as the delivery method and locations they may target with the weapon. In addition a variety of unpredictable variables at the time of attack, such as weather patterns like wind direction and precipitation, can have a dramatic impact on the consequences. States have the resources to run detailed scenarios and determine the consequences of various attacks at potential target locations. These types of calculations are beyond the scope of this work.

For the purpose of this dissertation, we are more concerned with relative consequences between nuclear threats than absolute consequences. The worst case consequences for each consequence category for the State are set to unity, and the relative consequences of other threats are set to a value proportional to this consequence. The ratio of consequences between various threat scenarios are based on the State's utility function for that consequence category. The utility function determines the degree of loss each State feels based on the consequence. Table B.1 shows the economic loss in dollars from four threat scenarios and the corresponding utility value. A linear utility value assumes every dollar is equal, so a ten-thousand dollar loss is one-thousand times worse than a one-hundred dollar loss, a ten-million dollar loss is one-thousand times worse than a ten-thousand dollar loss, etc. However, over a the large range of consequence values presented in Table B.1, it is unlikely that the State's utility function will be linear. Examining the economic losses more closely, the loss of one-hundred dollars is essentially negligible to a State. Based on data from the CIA world fact book[mm], the yearly expenditures of many countries is on the order of billions of dollars. An annual expenditure of one-billion dollars equates to approximately 3 million dollars per day. In this context, one-hundred dollars accounts for a mere three-thousandths of one-percent of daily expenditures by the State. The consequences of Scenario 2 are more significant, but still only account for 3% of daily expenditures. Scenario 3 results in an economic loss equivalent to 10% of annual expenditures, which likely has a tangible negative effect on the State. Finally, the economic consequences from Scenario 4 are equivalent to one-hundred years worth of spending, which has the potential to economically cripple the State. In this situation, the utility of the threat scenarios may be more accurately portrayed by a non-linear utility function.

Table B.1. Example Utility Values for Various Scenarios

	Economic Loss ($)	U(linear)	U(non-linear)
Threat Scenario 1	1.00E+02	1.00E-09	1.00E-40
Threat Scenario 2	1.00E+05	1.00E-06	1.00E-20
Threat Scenario 3	1.00E+08	1.00E-03	1.00E-06
Threat Scenario 4	1.00E+11	1	1

[mm] The Central Intellegence Agency. "The World Factbook". https://www.cia.gov/library/publications/the-world-factbook/fields/2056.html

The utility values for each consequence category will vary based on the threat, weapon materials, target location, etc. To capture these variables in this work, we define the consequences for a nuclear terrorism event at each target location based on a 100 kT weapon for nuclear weapons, a 10 kT weapon for INDs, and an A/D value of 850 (which corresponds to 2295 Ci Cs-137, 687 Ci Co-60, 1380 Ci Am-241, or 1150 Ci Cm-244). These consequence utility values are then scaled based on the materials used in each specific scenario. For IND and Nuclear Weapon scenarios, the consequences are scaled based on destruction areas which are related to various overpressure ranges.[nn] These overpressure ranges are related to yield based on Equation B1,

$$R_{Xpsi}(W_1) = R_{Xpsi}(W_2) * (W_1)^{1/3} \tag{B1}$$

where:

R_{Xpsi} = the distance of overpressure X from the blast epicenter; and

W = the yield of the weapon in kT.

Using the relationship between overpressure distances in Equation B1, the relationship between yield and destruction area is given in Equation B2.

$$C(W_1) = C(W_2) * (W_1)^{2/3} \tag{B2}$$

[nn] Harney, Robert C. "Inaccurate Prediction of Nuclear Weapons Effects and Possible Adverse Influences on Nuclear Terrorism Preparedness". *Homeland Security Affairs*, Vol. V, No. 3, 1-19. (2009).

For nuclear weapons or INDs with different yields than the 10 kT or 100 kT defined consequence values, utility functions are scaled using Equation C2 assuming that the State's utility for consequences within the range of the scaling change is linear. For INDs, this assumption is used because the likely range of IND yields is less than 20 kT, corresponding to a scaling factor value near unity. The proportional scaling factor from a 10 kT yield IND to a 1 kT yield is 0.215 and from a 10 kT yield to a 20 kT yield is 1.587. For nuclear weapons, the linear utility scaling assumption is applied because the weapon yield must exceed 3 MT to cause a scaling factor increase of one order of magnitude from a 100 kT yield. This scaling factor is applied to all four consequence categories.

Scaling the consequences from IND and nuclear weapon scenarios is relatively straight forward because the consequences from these events are on the extreme end of the spectrum, capable of causing hundreds of thousands of deaths and hundreds of billions in economic losses. For RDD events, the consequences can range across the spectrum from relatively insignificant to severe. To scale RDD consequence categories, scaling functions were developed using A/D values and are given in Equations B3 to B6.

$$C_{A/D(2)}^{LL} = \begin{cases} C_{A/D(1)}^{LL} * 1250 * \left[9.41x10^{-7} * \left({}^{A}/_{D}\right)_2 - 2.4x10^{-13} * \left({}^{A}/_{D}\right)_2^{\ 2} + 1.85x10^{-20} * \left({}^{A}/_{D}\right)_2^{\ 3}\right], & \left({}^{A}/_{D}\right)_2 < 5x10^6 \\ C_{A/D(1)}^{LL} * 1250 * \sqrt{\frac{\left({}^{A}/_{D}\right)_2}{5x10^6}}, & \left({}^{A}/_{D}\right)_2 \geq 5x10^6 \end{cases} \tag{B3}$$

$$C_{A/D(2)}^{EL} = C_{A/D(1)}^{EL} * \left(\frac{\left({}^{A}\!/_{D}\right)_2}{850}\right)^{2/3} \tag{B4}$$

$$C_{A/D(2)}^{IL} = \begin{cases} C_{A/D(1)}^{IL} * \frac{\left({}^{A}\!/_{D}\right)_2}{850},\ \left({}^{A}\!/_{D}\right)_2 < 850 \\ C_{A/D(1)}^{IL} * \left[\frac{2x10^{-15} * \left({}^{A}\!/_{D}\right)_2{}^{2} + 1x10^{-8} * \left({}^{A}\!/_{D}\right)_2 + 0.0004}{0.000408}\right],\ \left({}^{A}\!/_{D}\right)_2 \geq 850 \end{cases} \tag{B5}$$

$$C_{A/D(2)}^{SC} = C_{A/D(1)}^{SC} * \left(\frac{\left({}^{A}\!/_{D}\right)_2}{850}\right)^{1/3} \tag{B6}$$

APPENDIX C

VERIFICATION TESTS INPUT DATA

C.1. Terrorist Inputs

The terrorist group modeled in the verification test has a slightly risk averse risk attitude and is known to have operated at approximately 30.283995º N and 97.7244533 º W. The terrorist group has a strong disincentive for causing mass casualties, so it would follow that their perceived benefit from completing a pathway would not include loss of life. They are not expected to have a preference between the other three consequence categories, as shown by their consequence weighting factors in Table C.1. The motivations and disincentive weighting factors are given in Table C.2.

Table C.1. Terrorist Consequence Weights

w_a^{LL}	w_a^{IL}	w_a^{EL}	w_a^{SC}
0	1	1	1

Table C.2. Terrorist Motivation and Disincentive Weights

Motivations	W_U^m
Prestige of Successful Capabilities	3
Manipulate Adversaries	5
Apocalyptic Beliefs	0
War on Own Nation	3
War on Another Nation	0
Redress Conventional Military Asymmetry	0
Ensure Security	0
Mass Devastation/Chaos	
-Deaths	0
-Other	5
Religious Imperative	0
Manipulate Policy	5
Fascination of Nuclear Weapons	0
Fascination of Radiological	0
Fascination of Sabotage	0
Disincentives	
Fear of Retaliation on Base of Support	3
Fear of Attracting Attention	0
Alienation	0
Contradict Goals of Group	
-Mass killings	5
-Contamination of territory or environment	0
Lack of Religious Mandate	0
Internal Group Division	0

The final adversary inputs are the assessed capabilities for each task, which are given in Table C.3.

Table C.3. Adversary Task Capabilities

Assessed Capabilities	P_B^{task}	P_U^{task}	β_D^{task}	N^{task}
Conversion	0.5	0.5	0.9	3
Reprocessing	1.00E-04	1.00E-02	1.00E-02	1
Enrichment	1.00E-09	1.00E-03	0.05	0
Machining	0.25	0.5	0.9	1
Metallurgy	0.5	0.75	0.75	2
IND Weaponization Gun-Type	0.7	0.7	0.5	1
RDD Weaponization	0.95	0.95	0.85	4
IND Weaponization Implosion	0.05	0.05	0.3	1

C.2. State Inputs

There are two facilities in the state that use nuclear and radiological materials. The first is a research reactor and the second is a hospital. The research reactor uses HEU fuel, and stores fresh fuel and spent fuel on site. The two sources analyzed at the hospital are a number of Cobalt-60 high dose rate (HDR) brachytherapy sources and the Cesium-137 blood irradiator. The inputs for the materials at each facility are given in Table C.4 and Table C.5.

Table C.4. Research Reactor Facility Inputs

Facility Name: Research Reactor					**Location:** 30.621609° N , 96.332141° W					$\bar{D}_{FAC}$	300	ε_{HR}	0.1		
SNM Material	**Type**	N_{SQ}	N_{I}	m_I	A_I	D_{SNM}	E_U	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Fresh Fuel	Uranium	1	225	0.9584	3.1E-4	1.60E-07	0.36	NONE	FALSE	FALSE	FALSE	TRUE	TRUE	0.8	0.05
Spent Fuel	Uranium	1.96	450	0.9584	625	4.00	0.34	NONE	TRUE	TRUE	FALSE	TRUE	TRUE	1	0.005

Table C.5. Hospital Facility Inputs

Facility Name: Hospital	**Location:** 31.1752681° N 95.175211° W				$\bar{D}_{FAC}$	350	ε_{HR}	0.01
Radiological Material	**Type**	D_{value}^{Rad}	N_{I}	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
HDR Brachytherapy Seeds	Co-60	0.03	50	7	10	2.1E-6	0.9762	1
Blood Irradiator	Cs-137	0.1	1	2200	7000	1.2E-6	1	0.05

The sabotage data for each facility is given in Table C.6 and Table C.7.

Table C.6. Research Reactor Sabotage Inputs

Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Containment	0.75	0.1	5.0E-12	4.50E-06	3.0E-06	5.0E-04
Reactor	Containment, Coolant Pump 1, Coolant Pump 2	0.4	0.3	1.0E-08	3.60E-06	1.0E-06	5.0E-04

Table C.7. Hospital Sabotage Inputs

Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Source Storage Vault	HDR Source Vault	1	0.001	0	1.0E-10	1.0E-10	5.0E-06
Irradiator Room	Lead Shielding	1	0.001	0	1.0E-08	1.0E-07	5.0E-06

The physical security system data at each facility is given in Table C.8 and Table C.9.

Table C.8. Research Reactor Physical Security System Inputs

Research Reactor PPS	P_{I}^{Layer}	P_{N}^{Layer}	Targets Under Layer
Layer 1	0.5	0.7	Fresh Fuel, Spent Fuel, Spent Fuel Pool, Containment, Coolant Pump 1, Coolant Pump 2
Layer 2	0.7	0.5	Spent Fuel, Spent Fuel Pool
Layer 3	0.9	0.7	Fresh Fuel Vault

Table C.9. Hospital Physical Security System Inputs

Hospital PPS	$\boldsymbol{P_I^{Layer}}$	$\boldsymbol{P_N^{Layer}}$	Targets Under Layer
Layer 1	0.5	0.1	1,3
Layer 2	0.7	0.1	2,4

In this problem, we analyze two potential targets. These are the capital city and the city with the highest population. The inputs corresponding to these target locations are given in Table C.10.

Table C.10. Target Inputs

Name	Location	$\boldsymbol{P^{targ}}$	$\boldsymbol{C_{IND}^{LL}}$	$\boldsymbol{C_{IND}^{IL}}$	$\boldsymbol{C_{IND}^{EL}}$	$\boldsymbol{C_{IND}^{SC}}$	$\boldsymbol{C_{RDD}^{LL}}$	$\boldsymbol{C_{RDD}^{IL}}$	$\boldsymbol{C_{RDD}^{EL}}$	$\boldsymbol{C_{RDD}^{SC}}$
Capital City	31.29733 ° N, 95.55902 ° W	0.3	0.7	1	0.6	1	7.0E-11	4.5E-06	3.0E-4	5.0E-4
Populous City	28.72913 ° N, 95.91065 ° W	0.5	1	0.8	1	1	1.0E-10	3.6E-06	5.0E-4	5.0E-4

The State consequence weights are given in Table C.11.

Table C.11. State Consequence Weights

w_S^{LL}	w_S^{IL}	w_S^{EL}	w_S^{SC}
1	1	0.5	0.1

The last data needed are the interdiction probabilities, which are given in table C.12.

Table C.12. State Interdiction Inputs

$\overline{D}_{Capt}^{BKG}$	$\overline{D}_{Capt}^{AS}$
0.0002	0.001

APPENDIX D

VALIDATION TESTS DATA

The SNM material data used in probability of attack validation tests are presented in Table D.1. The plutonium and uranium activity values are calculated using specific activity data.[oo,pp] Plutonium isotopics for each grade of material are derived from Mark et al.[qq] Uranium dose rates were estimated using an online calculator,[rr] and plutonium dose rates were calculated using specific dose rate data from Kang and von Hippel.[ss] Research reactor assembly information was based on information from Bretscher et al.[tt] Dose rate information for spent fuel was estimated based on data in Lloyd et al. [uu]

The normalized probability of attack results for the probability of attack validation tests are presented in Table D.2. for Group A and Table D.3 for Group B.

[oo] Argonne National Laboratory. "Plutonium". *Human Health Fact Sheet (2005)*

[pp] U.S. Department of Energy. "Characteristics of Uranium and Its Compounds". *Depleted Uranium Hexafluoride Fact Sheet* (2001).

[qq] Mark, J. Carson, Hippel, Frank von, Lyman, Edward. "Explosive Properties of Reactor-Grade Plutonium". *Science and Global Security,* 17 (2009) 270-285.

[rr] Uranium Radiation Individual Dose Calculator, http://www.wise-uranium.org/rdcu.html

[ss] Kang, Jungmin, von Hippel, Frank. "Limited Proliferation Resistance Benefits from Recycling Unseperated Transuranics and Lanthanides from Light-Water Reactor Spent Fuel". *Science and Global Security ,*

[tt] Bretscher, M. M., Hanan, N.A., Matos, J.E. Neutronic Performance of Several LEU Fuel Assembly Designs for the WWR-SM Research Reactor in Uzbekistan". *2002 International Meeting on Reduced Enrichment for Research and Test Reactors.* (2002)

[uu] Lloyd, W.R., Sheaffer, M.K., Sutcliffe, W.G. "Dose Rate Estimates from Irradiated Light Water Reactor Fuel Assemblies in Air". Lawrence Livermore National Laboratory. UCRL-ID-115199. (1994)

Table D.1 Material Properties

SNM Material	Type	N_S	N_I	m_I	A_I	D_{SNM}	E_U	Chemical Reactivity	Cooling	FP Rem.	Conv.	Metal.	Mach.
Super Grade Pu Metal	Plutonium	1	2	5	340	5.14E-06	0.97	Slow	FALSE	FALSE	FALSE	FALSE	TRUE
Weapons Grade Pu Metal	Plutonium	1	2	5	373	6.66E-06	0.93	Slow	FALSE	FALSE	FALSE	FALSE	TRUE
Fuel Grade Pu Metal	Plutonium	1	2	5	440	9.70E-06	0.85	Slow	FALSE	FALSE	FALSE	FALSE	TRUE
Reactor Grade Pu Metal	Plutonium	1	2	5	482	1.16E-05	0.8	Slow	FALSE	FALSE	FALSE	FALSE	TRUE
U WG metal	Uranium	1	3	10	2.07E-02	1.50E-05	0.93	Slow	FALSE	FALSE	FALSE	FALSE	TRUE
U HEU metal	Uranium	1	12	10	7.32E-03	3.57E-06	0.215	Slow	FALSE	FALSE	FALSE	FALSE	TRUE
U LEU metal	Uranium	1	39	10	6.95E-03	3.26E-06	0.195	Slow	FALSE	FALSE	FALSE	FALSE	TRUE
BWR assembly	Uranium	1	12	320	0.187	1.25E-05	0.035	None	FALSE	FALSE	TRUE	TRUE	TRUE
PWR assembly	Uranium	1	5	657	0.0725	3.45E-05	0.04	None	FALSE	FALSE	TRUE	TRUE	TRUE
LEU rsch rx assembly	Uranium	1	207	1.97	2.54E-04	5.70E-07	0.197	None	FALSE	FALSE	TRUE	TRUE	TRUE
HEU rsch rx assembly	Uranium	1	82	0.96	3.10E-04	1.60E-07	0.36	None	FALSE	FALSE	FALSE	TRUE	TRUE
Super Grade PU Oxide	Plutonium	1	2	7	300	4.53E-06	0.97	None	FALSE	FALSE	FALSE	TRUE	TRUE
Weapons Grade Pu Oxide	Plutonium	1	2	7	330	5.87E-06	0.93	None	FALSE	FALSE	FALSE	TRUE	TRUE
Fuel Grade Pu Oxide	Plutonium	1	2	7	388	8.55E-06	0.85	None	FALSE	FALSE	FALSE	TRUE	TRUE
Reactor Grade Pu Oxide	Plutonium	1	2	7	425	1.02E-05	0.8	None	FALSE	FALSE	FALSE	TRUE	TRUE
Weapons Grade UO2 cans	Uranium	1	7	7	9.11E-03	5.80E-06	0.93	None	FALSE	FALSE	FALSE	TRUE	TRUE
HEU (21.5%) UO2 cans	Uranium	1	24	7	3.22E-03	1.39E-06	0.215	None	FALSE	FALSE	FALSE	TRUE	TRUE
LEU (19.5%) UO2 cans	Uranium	1	77	7	3.06E-03	1.26E-06	0.195	None	FALSE	FALSE	TRUE	TRUE	TRUE
LEU (5%) UO2 cans	Uranium	1	300	7	1.86E-03	3.88E-07	0.05	None	FALSE	FALSE	TRUE	TRUE	TRUE
Natural (0.72%) UO2 Cans	Uranium	1	2384	7	1.51E-03	9.46E-08	0.0072	None	FALSE	FALSE	TRUE	TRUE	TRUE

Table D.2. Group A Probabilities of Attack for Various Materials

Material	U_a^{mat}	P_S	P_A
Uranium Weapons Grade Metal	3.94E-01	4.33E-03	3.31E-01
HEU (21.5%) metal	3.15E-01	4.33E-03	2.65E-01
Uranium Weapons Grade Metal (d)	1.92E-01	4.33E-03	1.61E-01
HEU (21.5%) metal (d)	6.60E-02	4.33E-03	5.54E-02
Weapons Grade UO_2 Cans	7.64E-01	3.61E-04	5.35E-02
Weapons Grade UO2 Cans (d)	7.57E-01	3.61E-04	5.30E-02
HEU (36%) Research Reactor Fresh Fuel Assembly	4.24E-01	3.61E-04	2.97E-02
HEU (36%) Research Reactor Fresh Fuel Assembly(d)	3.26E-01	3.61E-04	2.28E-02
HEU (21.5%) UO_2 Cans	3.11E-01	3.61E-04	2.17E-02
HEU (21.5%) UO_2 cans (d)	7.84E-02	3.61E-04	5.49E-03
Pu Metal Super Grade	4.18E-01	2.14E-06	1.74E-04
Pu Metal Weapons Grade	3.77E-01	2.14E-06	1.56E-04
Pu Metal Fuel Grade	3.34E-01	2.14E-06	1.39E-04
Pu Metal Reactor Grade	3.31E-01	2.14E-06	1.37E-04
Super Grade Pu Metal (d)	3.11E-01	2.14E-06	1.29E-04
Weapons Grade Pu Metal (d)	3.01E-01	2.14E-06	1.25E-04
Fuel Grade Pu Metal (d)	2.65E-01	2.14E-06	1.10E-04
Reactor Grade Pu Metal (d)	2.49E-01	2.14E-06	1.03E-04
PuO_2 Cans Super Grade	8.35E-01	1.78E-07	2.89E-05
PuO_2 Cans Super Grade (d)	8.35E-01	1.78E-07	2.89E-05
PuO_2 Cans Weapons Grade	7.53E-01	1.78E-07	2.61E-05
PuO_2 Cans Weapons Grade (d)	7.53E-01	1.78E-07	2.61E-05
PuO_2 Cans Fuel Grade	6.61E-01	1.78E-07	2.29E-05
PuO_2 Cans Fuel Grade(d)	6.61E-01	1.78E-07	2.29E-05
PuO_2 Cans Reactor Grade	6.22E-01	1.78E-07	2.15E-05
PuO_2 Cans Reactor Grade (d)	6.22E-01	1.78E-07	2.15E-05
Research Reactor Fresh Fuel Assembly LEU (19.5%)	1.08E-01	1.69E-27	3.56E-26
LEU (19.5%) UO_2 cans	8.20E-02	1.69E-27	2.69E-26
LEU (5%) UO_2 cans	9.07E-03	1.69E-27	2.98E-27
LEU (19.5%) Research Reactor Fresh Fuel Assembly(d)	7.91E-03	1.69E-27	2.60E-27
PWR Fresh Fuel assembly	6.04E-03	1.69E-27	1.98E-27
BWR Fresh Fuel assembly	4.59E-03	1.69E-27	1.51E-27
LEU (19.5%) UO_2 cans (d)	4.27E-03	1.69E-27	1.40E-27
Natural (0.72%) UO_2 Cans	3.70E-04	1.69E-27	1.22E-28
LEU (5%) UO_2 cans	1.10E-04	1.69E-27	3.61E-29
PWR Fresh Fuel assembly (d)	4.63E-05	1.69E-27	1.52E-29
BWR Fresh Fuel assembly (d)	3.01E-05	1.69E-27	9.88E-30
Natural (0.72%) UO_2 Cans (d)	6.35E-07	1.69E-27	2.09E-31

Table D.3. Group B Probabilities of Attack for Various Materials

Material	$\boldsymbol{U_a^{mat}}$	P_S	Normalized P_A
Super Grade Pu Metal	4.18E-01	4.33E-03	9.82E-02
Weapons Grade U Metal	3.94E-01	4.33E-03	9.27E-02
Weapons Grade Pu Metal	3.77E-01	4.33E-03	8.86E-02
Super Grade Pu Metal (d)	3.34E-01	4.33E-03	7.86E-02
Fuel Grade Pu Metal	3.31E-01	4.33E-03	7.78E-02
Weapons Grade U metal (d)	3.15E-01	4.33E-03	7.42E-02
Reactor Grade Pu Metal	3.11E-01	4.33E-03	7.31E-02
Weapons Grade Pu Metal (d)	3.01E-01	4.33E-03	7.08E-02
Fuel Grade Pu Metal (d)	2.65E-01	4.33E-03	6.22E-02
Reactor Grade Pu Metal (d)	2.49E-01	4.33E-03	5.85E-02
HEU (21.5%) Metal	1.92E-01	4.33E-03	4.50E-02
Super Grade PuO$_2$	8.35E-01	3.61E-04	1.64E-02
Super Grade PuO$_2$ (d)	8.35E-01	3.61E-04	1.64E-02
HEU (21.5%) Metal (d)	6.60E-02	4.33E-03	1.55E-02
Weapons Grade UO$_2$ cans	7.64E-01	3.61E-04	1.50E-02
Weapons Grade UO$_2$ cans (d)	7.57E-01	3.61E-04	1.48E-02
Weapons Grade PuO$_2$	7.53E-01	3.61E-04	1.48E-02
Weapons Grade PuO$_2$ (d)	7.53E-01	3.61E-04	1.48E-02
Fuel Grade PuO$_2$	6.61E-01	3.61E-04	1.30E-02
Fuel Grade PuO$_2$ (d)	6.61E-01	3.61E-04	1.30E-02
Reactor Grade PuO$_2$	6.22E-01	3.61E-04	1.22E-02
Reactor Grade PuO$_2$ (d)	6.22E-01	3.61E-04	1.22E-02
HEU Research Reactor Fresh Fuel Assembly	4.24E-01	3.61E-04	8.31E-03
HEU Research Reactor Fresh Fuel Assembly (d)	3.26E-01	3.61E-04	6.39E-03
HEU (21.5%) UO$_2$ cans	3.11E-01	3.61E-04	6.09E-03
HEU (21.5%) UO$_2$ cans (d)	7.84E-02	3.61E-04	1.54E-03
LEU Research Reactor Fresh Fuel Assembly	1.08E-01	1.69E-27	9.97E-27
LEU (19.5%) UO2 cans	8.20E-02	1.69E-27	7.55E-27
LEU (5%) UO2 cans	9.07E-03	1.69E-27	8.35E-28
LEU Research Reactor Fresh Fuel Assembly (d)	7.91E-03	1.69E-27	7.28E-28
PWR Fresh Fuel Assembly	6.04E-03	1.69E-27	5.55E-28
BWR Fresh Fuel Assembly	4.59E-03	1.69E-27	4.22E-28
LEU (5%) UO2 cans (d)	4.27E-03	1.69E-27	3.93E-28
Natural (0.72%) UO2 Cans	3.70E-04	1.69E-27	3.41E-29
LEU (5%) UO2 cans (d)	1.10E-04	1.69E-27	1.01E-29
PWR Fresh Fuel Assembly (d)	4.63E-05	1.69E-27	4.26E-30
BWR Fresh Fuel Assembly (d)	3.01E-05	1.69E-27	2.77E-30
Natural (0.72%) UO2 Cans (d)	6.35E-07	1.69E-27	5.84E-32

APPENDIX E

BEHAVIORAL TESTS DATA

Table E.1. Terrorist Consequence Weights

w_a^{LL}	w_a^{IL}	w_a^{EL}	w_a^{SC}
1	1	1	1

Table E.2. Adversary Task Capabilities

Assessed Capabilities	P_B^{task}	P_U^{task}	β_D^{task}	N^{task}
Conversion	0.6	0.8	0.95	1
Reprocessing	1.00E-04	1.00E-04	1.00E-02	1
Enrichment	1.00E-09	1.00E-09	0.05	1
Machining	0.5	0.5	0.9	1
Metallurgy	0.2	0.2	0.2	5
IND Weaponization Gun-Type	0.9	0.1	0.3	2
RDD Weaponization	0.95	0.95	0.75	3
IND Weaponization Implosion	0.45	0.05	0.15	2

Table E.3. Terrorist Motivation and Disincentive Weights

Motivations	$\boldsymbol{W_U^m}$
Prestige of Successful Capabilities	3
Manipulate Adversaries	5
Apocalyptic Beliefs	0
War on Own Nation	5
War on Another Nation	0
Redress Conventional Military Asymmetry	0
Ensure Security	5
Mass Devastation/Chaos	
-Deaths	0
-Other	5
Religious Imperative	0
Manipulate Policy	5
Fascination of Nuclear Weapons	0
Fascination of Radiological	0
Fascination of Sabotage	0
Disincentives	
Fear of Retaliation on Base of Support	3
Fear of Attracting Attention	0
Alienation	0
Contradict Goals of Group	
-Mass killings	3
-Contamination of territory or environment	0
Lack of Religious Mandate	0
Internal Group Division	0

Table E.4. Research Reactor Sabotage Inputs

Sabotage Event	Vital Areas	P^{Sab}_{Cons}	ε^{Ins}_{Sab}	C^{LL}_{Sab}	C^{IL}_{Sab}	C^{EL}_{Sab}	C^{SC}_{Sab}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.05	0.5	1.0E-08	3.6E-06	1.0E-06	5.0E-05
Reactor	Coolant Pump 1, Coolant Pump 2	0.05	0.5	1.0E-08	5.0E-12	4.5E-06	3.0E-06

Table E.5. One Target Case Target Inputs

Name	Location	P^{targ}	C^{LL}_{IND}	C^{IL}_{IND}	C^{EL}_{IND}	C^{SC}_{IND}	C^{LL}_{RDD}	C^{IL}_{RDD}	C^{EL}_{RDD}	C^{SC}_{RDD}
Target 1	40 ° N, 40 ° E	0.5	1	1	1	1	7.0E-11	4.5E-06	3.0E-4	5.0E-4

Table E.6 Two Target Case Target Inputs

Name	Location	P^{targ}	C^{LL}_{IND}	C^{IL}_{IND}	C^{EL}_{IND}	C^{SC}_{IND}	C^{LL}_{RDD}	C^{IL}_{RDD}	C^{EL}_{RDD}	C^{SC}_{RDD}
Target 1	40 ° N, 40 ° E	0.5	1	1	1	1	7.0E-11	4.5E-06	3.0E-4	5.0E-4
Target 2	40 ° N, 40 ° E	0.5	0.5	0.5	0.5	0.5	3.5E-11	2.25E-6	1.5-4	2.5E-4

Table E.7. Research Reactor Facility Inputs

Facility Name: Research Reactor					**Location:** 45° N , 45° W					$\bar{\boldsymbol{D}}_{\boldsymbol{FAC}}$	150	$\boldsymbol{\varepsilon}_{\boldsymbol{HR}}$	0.5		
SNM Material	**Type**	$\boldsymbol{N}_{\boldsymbol{SQ}}$	$\boldsymbol{N}_{\mathbf{I}}$	$\boldsymbol{m}_{\boldsymbol{I}}$	$\boldsymbol{A}_{\boldsymbol{I}}$	$\boldsymbol{D}_{\boldsymbol{SNM}}$	$\boldsymbol{E}_{\boldsymbol{U}}$	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	$\boldsymbol{\beta}_{\boldsymbol{MA}}$	$\boldsymbol{\beta}_{\boldsymbol{CS}}$
Fresh Fuel	Uranium	1.5	5	30	3.1E-4	5E-06	0.9	NONE	FALSE	FALSE	FALSE	TRUE	TRUE	0.2	0.35
Spent Fuel	Uranium	4.0	50	30	625	4.00	0.89	SLOW	TRUE	TRUE	FALSE	TRUE	TRUE	0.2	0.35

Table E.8. State Consequence Weights

w_S^{LL}	w_S^{IL}	w_S^{EL}	w_S^{SC}
1	1	0.5	0.05

Table E.9. Interdiction Inputs

$\bar{D}_{Capt}^{BKG}$	$\bar{D}_{Capt}^{AS}$
0.0001	0.00025

APPENDIX F

TEST CASES

F. 1. Adversary Inputs for Test Cases

Risk Attitude - Extremely Risk Averse

Table F.1. Terrorist Capabilities for Test Cases

Assessed Capabilities	P_B^{task}	P_U^{task}	β_D^{task}	N^{task}
Conversion	0.5	0.5	0.9	3
Reprocessing	1.00E-04	1.00E-02	1.00E-02	1
Enrichment	1.00E-09	1.00E-03	0.05	0
Machining	0.4	0.5	0.9	1
Metallurgy	0.25	0.75	0.75	2
IND Weaponization Gun-Type	0.35	0.5	0.75	1
RDD Weaponization	0.95	0.95	0.85	4
IND Weaponization Implosion	0.05	0.05	0.5	1

Table F.2 Terrorist Location for Test Cases

Latitude	Longitude
37.37619	-105.9228

Table F.3 Terrorist Consequence Weights for Test Cases

w_S^{LL}	w_S^{IL}	w_S^{EL}	w_S^{SC}
0.5	1	1	1

Table F.4 Terrorist Consequence Weights for Test Cases

Motivations/Disincentives	k_m	k_m
Prestige of Successful Capabilities	1	1
Manipulate Adversaries	5	5
Apocalyptic Beliefs	0	0
War on Own Nation	3	3
War on Another Nation	0	0
Redress Conventional Military Asymmetry	0	0
Ensure Security	0	0
Mass Devastation/Chaos		
-Deaths	0	5
-Other	5	3
Religious Imperative	0	0
Manipulate Policy	5	5
Fascination of Nuclear Weapons	0	0
Fascination of Radiological	0	0
Fascination of Sabotage	0	0
Fear of Retaliation on Base of Support	3	1
Fear of Attracting Attention	1	1
Alienation	0	0
Contradict Goals of Group		
-Mass killings	3	0
-Contamination of territory or environment	0	0
Lack of Religious Mandate	0	0
Internal Group Division	3	3

F.2. Small State Infrastructure

State Boundaries: 41^{o}00'48.62"N 109^{o}22'22.04" W, 36^{o}59'44.15"N 109^{o}22'22.04" W, 41^{o}00'48.62"N 102^{o}03'41.69" W, 36^{o}59'44.15"N 102^{o}03'41.69" W

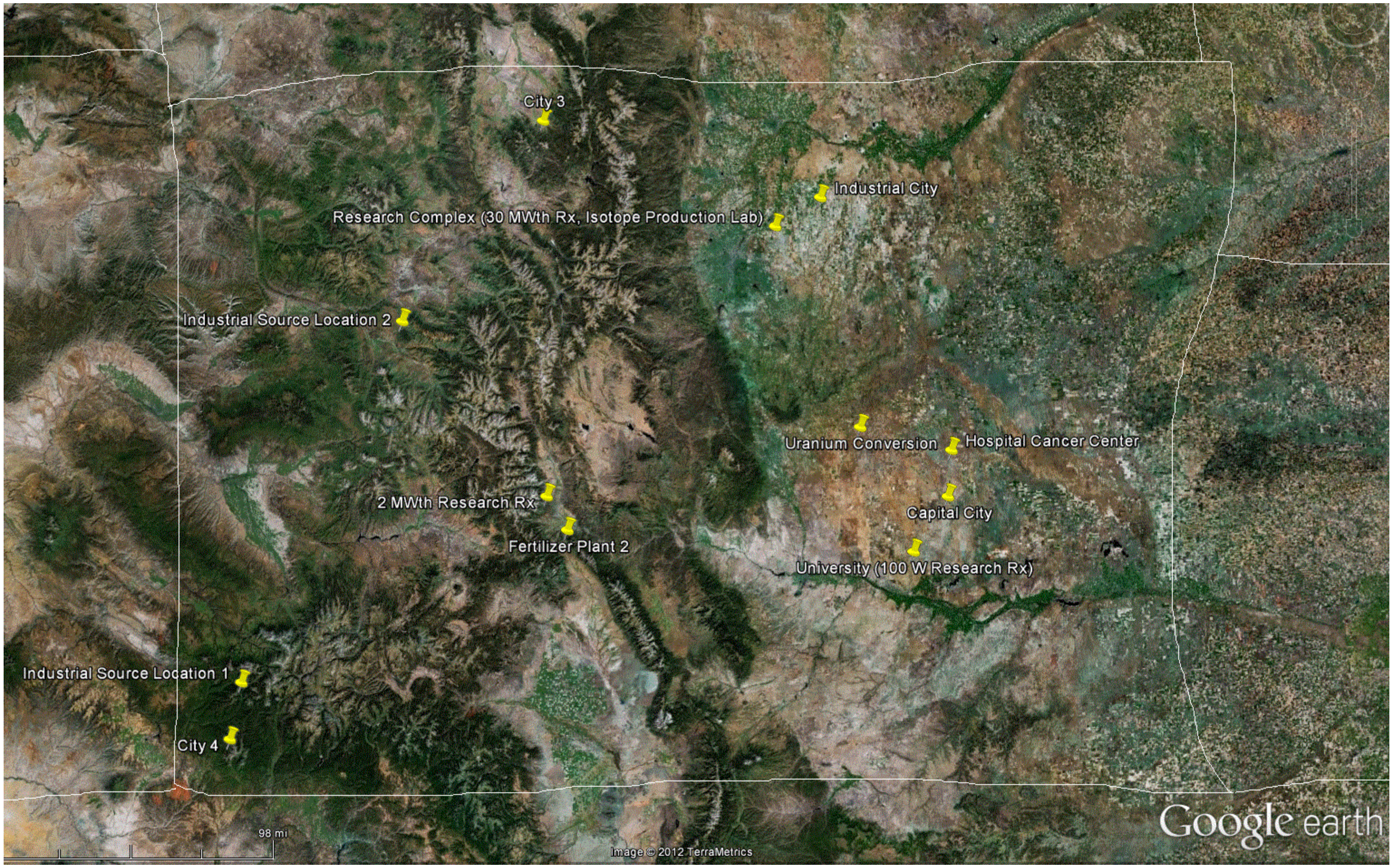

City 3
Industrial City
Research Complex (30 MWth Rx, Isotope Production Lab)
Industrial Source Location 2
Uranium Conversion
Hospital Cancer Center
2 MWth Research Rx
Capital City
Fertilizer Plant 2
University (100 W Research Rx)
Industrial Source Location 1
City 4
98 mi
Image © 2012 TerraMetrics
Google earth

Table F.5 30 MWth Research Reactor Facility Inputs

Facility Name: 30 MWth Research Reactor					**Location:** 39°51'37.79" N, 104°44'10.27" W					$\bar{D}_{FAC}$	256	ε_{HR}	0.2		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	E_U	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated LEU Fuel	Plutonium	1.00	301	2.4	625	4.24	0.6	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.9	0.25
Fresh LEU Fuel	Uranium	1.01	144	2.4	2.5E-04	5.70E-07	0.197	None	FALSE	FALSE	TRUE	TRUE	TRUE	0.95	0.25
Irradiated HEU Fuel	Uranium	1.02	47	0.9584	450	4.00	0.34	SLOW	TRUE	TRUE	FALSE	TRUE	TRUE	0.5	0.25

Table F.6 30 MWth Research Reactor Sabotage Inputs

Facility Name: 30 MWth Research Reactor							
Sabotage Event	Vital Areas	P^{Sab}_{Cons}	ε^{Ins}_{Sab}	C^{LL}_{Sab}	C^{IL}_{Sab}	C^{EL}_{Sab}	C^{SC}_{Sab}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.75	0.55	6.00E-09	1.00E-06	5.0E-05	9.50E-03
Reactor	Coolant Pump 1, Coolant Pump 2	0.85	0.55	1.0E-09	2.0E-07	3.0E-05	3.0E-03

Table F.7 30 MWth Research Reactor PPS Inputs

30 MWth Research Reactor PPS	P^{Layer}_{I}	P^{Layer}_{N}	Targets Under Layer
Layer 1	0.6	0.6	All Materials and Vital Areas
Layer 2	0.5	0.5	Irradiated LEU Fuel, Irradiated HEU Fuel, Spent Fuel Pool
Layer 3	0.5	0.35	Fresh LEU Fuel
Layer 4	0.1	0.1	Coolant Pump 1
Layer 5	0.01	0.01	Coolant Pump 2

Table F.8 2 MWth Research Reactor Facility Inputs

Facility Name: 2 MWth Research Reactor					**Location:** 38^{O}37'22.72" N, 106^{O}08'41.29" W					$\bar{D}_{FAC}$	263	ε_{HR}	0.05		
SNM Material	**Type**	N_{SQ}	N_{I}	m_{I}	A_{I}	D_{SNM}	Q_{PU}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated LEU Fuel	Plutonium	0.4	56	1.7	530	3.64	0.61	Slow	True	TRUE	TRUE	TRUE	TRUE	0.98	0.25

Table F.9 2 MWth Research Reactor Sabotage Inputs

Facility Name: 2 MWth Research Reactor							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.9	0.15	1.0E-11	1.00E-08	5.0E-07	1.20E-05
Reactor	Coolant Pump 1, Coolant Pump 2	0.72	0.15	2.0E-12	2.0E-09	3.0E-07	3.0E-06

Table F.10 2 MWth Research Reactor PPS Inputs

2 MWth Research Reactor PPS	P_{I}^{Layer}	P_{N}^{Layer}	Targets Under Layer
Layer 1	0.7	0.25	Irradiated LEU Fuel and Vital Areas
Layer 2	0.4	0.2	Irradiated LEU Fuel, Spent Fuel Pool
Layer 3	0.1	0.1	Coolant Pump 1
Layer 4	0.01	0.01	Coolant Pump 2

Table F.11 100 W Research Reactor Facility Inputs

Facility Name: 100 W Research Reactor					**Location:** 38°18'2.20"N, 103°57'36.38"W					$\bar{D}_{FAC}$	261	ε_{HR}	0.01		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	Q_{PU}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated LEU Fuel	Uranium	0.25	35	0.85	265	3.55	0.65	Slow	True	TRUE	TRUE	TRUE	TRUE	0.98	0.25

Table F.12 100 W Research Reactor Sabotage Inputs

Facility Name: 100 W University Research Reactor							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.9	0.05	5.0E-10	1.00E-08	5.0E-06	4.50E-06
Reactor	Coolant Pump 1, Coolant Pump 2	0.92	0.05	1.0E-10	2.0E-07	3.0E-06	7.2E-06

Table F.13 100 W Research Reactor Facility Inputs

100 W Research Reactor PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.4	0.3	Irradiated LEU Fuel and Vital Areas
Layer 2	0.1	0.1	Irradiated LEU Fuel, Spent Fuel Pool
Layer 3	0.1	0.1	Coolant Pump 1
Layer 4	0.01	0.01	Coolant Pump 2

Table F.14 Isotope Production Facility Inputs

Facility Name: Isotope Production Facility	**Location:** 39°51'37.79" N, 104°44'10.27" W				$\bar{D}_{FAC}$	256	ε_{HR}	0.02
Radiological Material	**Type**	D^{Rad}_{value}	N_{I}	m_I	A^{Rad}_I	D_{Rad}	β_{MA}	β_{CS}
Mo-99 Product	Mo-99	0.3	5	6	50	1.2e-4	0.8	0.95

Table F.15 Isotope Production Facility PPS Inputs

Isotope Production Facility PPS	P^{Layer}_I	P^{Layer}_N	Targets Under Layer
Layer 1	0.25	0.25	Moly-99
Layer 2	0.1	0.1	Moly-99

Table F.16 Hospital Cancer Center Facility Inputs

Facility Name: Hospital Cancer Center	**Location:** 38°46'37.17"N, 103°42'19.61"W				$\bar{D}_{FAC}$	262	ε_{HR}	0.02
Radiological Material	**Type**	D^{Rad}_{value}	N_{I}	m_I	A^{Rad}_I	D_{Rad}	β_{MA}	β_{CS}
LDR Brachytherapy Seeds	Ra-226	0.04	1750	7	0.015	2.1E-6	1	0.99999
HDR Brachytherapy Seeds	Ir-192	0.08	200	3	6	4.2e-7	1	0.995
Gamma Knife Multi-Beam	Co-60	0.03	1	3500	7000	1.2e-6	1	0.05
Nuclear Medicine Imaging	Mo-99/ Tc-99	0.3	1	20	75	1.1e-6	1	0.95

Table F.17 Hospital Cancer Center PPS Inputs

Hospital Cancer Center PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.1	LDR Brachytherapy Seeds
Layer 2	0.5	0.1	HDR Brachytherapy Seeds
Layer 3	0.75	0.25	Gamma Knife Source
Layer 4	0.3	0.1	Mo-99/Tc-99

Table F.18 Fertilizer Plant 1 Facility Inputs

Facility Name: Fertilizer Plant 1	**Location:** 40° 0'11.08"N, 104°27'15.79"W				$\bar{D}_{FAC}$	248	ε_{HR}	0.0001
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Phosphogypsum 1	Ra-226	0.04	1	2000	2.7e-8	1.7e-10	1	1

Table F.19 Fertilizer Plant 1 PPS Inputs

Fertilizer Plant 1 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.1	0.01	Phosphygypsum 1

Table F.20 Fertilizer Plant 2 Facility Inputs

Facility Name: Fertilizer Plant 2	**Location: Isolated Area** 38°27'2.39"N, 106° 3'30.31"W				$\bar{D}_{FAC}$	254	ε_{HR}	0.0001
Radiological Material	**Type**	D_{value}^{Rad}	N_{I}	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Phosphogypsum 2	Ra-226	0.04	1	5000	2.7e-8	1.7e-10	1	1

Table F.21 Fertilizer Plant 2 PPS Inputs

Fertilizer Plant 2 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.1	0.01	Phosphygypsum 2

Table F.22 Industrial Site 1 Facility Inputs

Facility Name: Industrial 1	**Location:** 37°43'29.79"N, 108° 3'10.28"W				$\bar{D}_{FAC}$	260	ε_{HR}	0.001
Radiological Material	**Type**	D_{value}^{Rad}	N_{I}	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Industrial Radiography Co 1	Co-60	0.03	5	4	60	1.2e-5	1	0.95
Industrial Radiography Ir	Ir-192	0.08	4	2	100	1.3e-5	1	0.95

Table F.23 Industrial Site 1 PPS Inputs

Industrial 1 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.1	Co Sources, Ir Sources
Layer 2	0.5	0.25	Co Sources

Table F.24 Industrial Site 2 Facility Inputs

Facility Name: Industrial 2	**Location: Isolated Area** 39°27'2.39"N, 107° 3'30.31"W				$\bar{D}_{FAC}$	251	ε_{HR}	0.001
Radiological Material	**Type**	D_{value}^{Rad}	N_{I}	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Industrial Radiography Co 2	Co-60	0.03	5	4	60	1.2e-5	1	0.75
Industrial Radiography Tm	Tm-170	20	8	1	150	1.4e-6	1	0.8

Table F.25 Industrial Site 2 PPS Inputs

Industrial 2 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.1	Co Sources, Tm Sources
Layer 2	0.5	0.25	Co Sources

Table F.26 Target Locations Inputs

Name	Location	P^{targ}	C_{IND}^{LL}	C_{IND}^{IL}	C_{IND}^{EL}	C_{IND}^{SC}	C_{RDD}^{LL}	C_{RDD}^{IL}	C_{RDD}^{EL}	C_{RDD}^{SC}
Target 1 - Capital City	38°33'24.19"N, 103°44'16.80"W	0.2	1.00	0.60	0.50	1.00	1.00E-11	6.00E-09	5.00E-07	1.00E-04
Target 2 - Industrial City	40° 0'11.08"N, 104°27'15.79"W	0.1	0.60	1.00	1.00	0.95	6.00E-12	1.00E-08	1.00E-06	9.50E-05
Target 3- City 3	40°23'54.52"N, 106°10'16.81"W	0.02	0.16	0.12	0.30	0.50	1.60E-12	1.20E-09	3.00E-07	5.00E-05
Target 4 - City 4	37°26'58.41"N, 108° 7'34.14"W	0.02	0.08	0.05	0.25	0.40	7.50E-13	5.00E-10	2.50E-07	4.00E-05

Table F.27 Small State Consequence Weights

w_S^{LL}	w_S^{IL}	w_S^{EL}	w_S^{SC}
1	1	1	0.001

Table F.28 Small State Interdiction Inputs

$\overline{D}_{Capt}^{BKG}$	$\overline{D}_{Capt}^{AS}$
5.00E-06	1.50E-05

Table F.29 Small State Consolidated Spent Fuel Facility Inputs

Facility Name: Consolidated Spent Fuel Facility					**Location:** 38^{O}37'22.72" N, 106^{O}08'41.29" W					$\bar{D}_{FAC}$	263	ε_{HR}	0.05		
SNM Material	**Type**	N_{SQ}	N_{I}	m_{I}	A_{I}	D_{SNM}	Q_{PU}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated LEU Fuel 30 MWth	Plutonium	1.00	301	2.4	625	4.24	0.6	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.9	0.25
Irradiated HEU Fuel 30 MWth	Uranium	1.02	47	0.9584	450	4.00	0.34	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.5	0.25
Irradiated LEU Fuel 2 MWth	Plutonium	0.4	56	1.7	530	3.64	0.61	Slow	True	TRUE	TRUE	TRUE	TRUE	0.98	0.25
Irradiated LEU Fuel 100W	Plutonium	0.25	35	0.85	265	3.55	0.65	Slow	True	TRUE	TRUE	TRUE	TRUE	0.98	0.25

Table F.30 Small State Consolidated Spent Fuel Facility Sabotage Inputs

Facility Name: Consolidated Spent Fuel Facility							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.5	0.5	6.00E-11	1.00E-07	5.00E-06	1.00E-05

Table F.31 Small State Consolidated Spent Fuel Facility PPS Inputs

Consolidated Spent Fuel Facility	P_{I}^{Layer}	P_{N}^{Layer}	Targets Under Layer
Layer 1	0.75	0.75	All materials and vital areas
Layer 2	0.75	0.75	All materials and vital areas

F.3. Intermediate State Infrastructure

State Borders - 40°59'38.70"N 111° 3'22.44"W, 40°59'38.70"N 111° 3'22.44"W, 44°59'36.84"N 104° 3'23.80"W, 44°59'36.84"N 104° 3'23.80" W

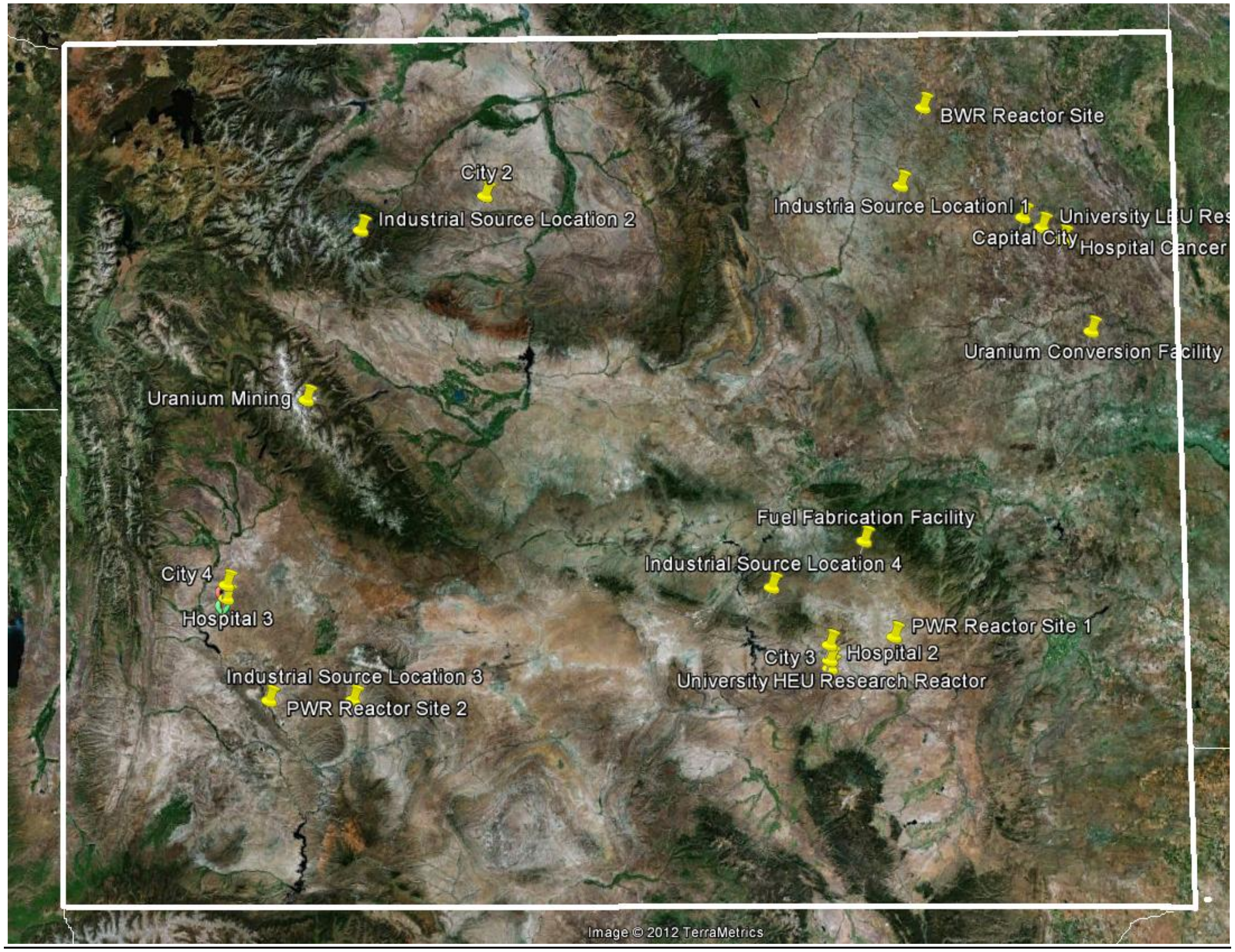

BWR Reactor Site
City 2
Industrial Source Location 2
Industria Source Locationl 1
University LEU Res
Capital City
Hospital Cancer
Uranium Conversion Facility
Uranium Mining
Fuel Fabrication Facility
Industrial Source Location 4
City 4
Hospital 3
PWR Reactor Site 1
City 3
Hospital 2
University HEU Research Reactor
Industrial Source Location 3
PWR Reactor Site 2
Image © 2012 TerraMetrics

Table F.32 BWR Reactor Site Facility Inputs

Facility Name: BWR Reactor Site					**Location: 44°22'17.77"N, 105°43'50.57"W**					$\bar{D}_{FAC}$	250	ε_{HR}	0.5		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	E_U/ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated Fuel	Plutonium	1.13	5	3.2E06	8.1E04	22	0.65	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
Fresh LEU Fuel	Uranium	1.02	12	320	2.5E-04	1.2E-05	0.03	None	FALSE	FALSE	TRUE	TRUE	TRUE	0.8	0.005

Table F.33 BWR Reactor Site Sabotage Inputs

Facility Name: BWR Reactor Site							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.15	0.85	1.00E-07	5.00E-04	1.00E-03	9.00E-03
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.05	0.92	5.00E-08	1.00E-04	5.00E-04	8.00E-03

Table F.34 BWR Reactor Site PPS Inputs

BWR Reactor Site PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump 1
Layer 4	0.01	0.01	Coolant Pump 1
Layer 5	0.01	0.01	Coolant Pump 2

Table F.35 PWR Reactor Site 1 Facility Inputs

Facility Name: PWR Reactor Site 1					**Location: 42° 0'59.30"N, 106° 1'39.65"W**					$\bar{\boldsymbol{D}}_{\boldsymbol{FAC}}$	262	$\boldsymbol{\varepsilon}_{\boldsymbol{HR}}$	0.5		
SNM Material	**Type**	$\boldsymbol{N}_{\boldsymbol{SQ}}$	$\boldsymbol{N}_{\mathbf{I}}$	$\boldsymbol{m}_{\boldsymbol{I}}$	$\boldsymbol{A}_{\boldsymbol{I}}$	$\boldsymbol{D}_{\boldsymbol{SNM}}$	$\boldsymbol{E}_{\boldsymbol{U}}/$ $\boldsymbol{Q}_{\boldsymbol{Pu}}$	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	$\boldsymbol{\beta}_{\boldsymbol{MA}}$	$\boldsymbol{\beta}_{\boldsymbol{CS}}$
Irradiated PWR Fuel	Plutonium	1.15	2	657	4.1E05	45	0.60	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
Fresh PWR Fuel	Uranium	1.23	5	657	2.5E-04	3.5E-05	0.04	None	FALSE	FALSE	TRUE	TRUE	TRUE	0.8	0.005

Table F.36 PWR Reactor Site 1 Sabotage Inputs

Facility Name: PWR Reactor Site **1**							
Sabotage Event	Vital Areas	$\boldsymbol{P}^{\boldsymbol{Sab}}_{\boldsymbol{Cons}}$	$\boldsymbol{\varepsilon}^{\boldsymbol{Ins}}_{\boldsymbol{Sab}}$	$\boldsymbol{C}^{\boldsymbol{LL}}_{\boldsymbol{Sab}}$	$\boldsymbol{C}^{\boldsymbol{IL}}_{\boldsymbol{Sab}}$	$\boldsymbol{C}^{\boldsymbol{EL}}_{\boldsymbol{Sab}}$	$\boldsymbol{C}^{\boldsymbol{SC}}_{\boldsymbol{Sab}}$
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.15	0.85	1.00E-9	2.00E-07	5.00E-05	1.00E-04
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.05	0.92	5.00E-10	1.00E-07	9.00E-06	8.00E-05

Table F.37 PWR Reactor Site 1 PPS Inputs

PWR Reactor Site PPS	$\boldsymbol{P}^{\boldsymbol{Layer}}_{\boldsymbol{I}}$	$\boldsymbol{P}^{\boldsymbol{Layer}}_{\boldsymbol{N}}$	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump 1
Layer 4	0.01	0.01	Coolant Pump 1
Layer 5	0.01	0.01	Coolant Pump 2

Table F.38 PWR Reactor Site 2 Facility Inputs

Facility Name: PWR Reactor Site 2					**Location:** 41°45'37.63"N, 109°46'49.19"W					$\bar{D}_{FAC}$	262	ε_{HR}	0.5		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	$E_U/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated Fuel	Plutonium	1	2	657	4.1E05	45	0.60	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
Fresh LEU Fuel	Uranium	1.5	5	657	2.5E-04	3.5E-05	0.04	None	FALSE	FALSE	FALSE	TRUE	TRUE	0.8	0.05

Table F.39 PWR Reactor Site 2 Facility Inputs

Facility Name: PWR Reactor Site 2							
Sabotage Event	Vital Areas	P^{Sab}_{Cons}	ε^{Ins}_{Sab}	C^{LL}_{Sab}	C^{IL}_{Sab}	C^{EL}_{Sab}	C^{SC}_{Sab}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.15	0.85	4.00E-12	1.00E-08	8.00E-06	1.00E-05
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.05	0.92	1.00E-12	4.00E-09	1.00E-06	8.00E-06

Table F.40 PWR Reactor Site 2 PPS Inputs

PWR Reactor Site 2 PPS	P^{Layer}_{I}	P^{Layer}_{N}	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump 1
Layer 4	0.01	0.01	Coolant Pump 1
Layer 5	0.01	0.01	Coolant Pump 2

Table F.41 Uranium Mining & Milling Facility Inputs

Facility Name: Uranium Mine & Milling					**Location:** 43° 6'17.06"N , 109°34'0.31"W					$\bar{D}_{FAC}$	262	ε_{HR}	0.001		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	$E_U/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Uranium ore (0.2% grade)	Uranium	0.02	1	1.0E5	1.4E-05	4.1E-05	0.0072	None	False	FALSE	TRUE	TRUE	TRUE	1	1
U_3O_8	Uranium	1	1	14000	7E-3	4.2E-04	0.0072	None	FALSE	FALSE	TRUE	TRUE	TRUE	1	0.05

Table F.42 Uranium Mining & Milling PPS Inputs

Uranium Mine PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.1	0.05	Uranium Ore and U_3O_8

Table F.43 Uranium Conversion Facility Inputs

Facility Name: Uranium Conversion					**Location:** 43°20'27.38"N, 104°44'52.13"W					$\bar{D}_{FAC}$	249	ε_{HR}	0.1		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	$E_U/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
U_3O_8	Uranium	1	1	14000	3.2	4.2E-04	0.0072	None	FALSE	FALSE	TRUE	TRUE	TRUE	1	0.05
UF_6 48Y Cylinders	Uranium	1.3	2	9500	2.75	5.8E-04	0.0072	None	FALSE	FALSE	FALSE	TRUE	TRUE	1	0.005

Table F.44 Uranium Conversion PPS Inputs

Uranium Conversion PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.1	0.05	48Y and U_3O_8

Table F.45 Fuel Fabrication Facility Inputs

Facility Name: Fuel Fabrication					**Location:** 42°26'53.73"N, 106°11'26.59"W					$\bar{D}_{FAC}$	255	ε_{HR}	0.1		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	E_U/ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
UF_6 30B Cylinder	Uranium	1.6	2	2200	0.61	5.6E-06	0.04	Slow	TRUE	FALSE	FALSE	TRUE	TRUE	1	0.005
BWR Assembly	Uranium	1.02	12	320	2.5E-04	1.2E-05	0.03	None	FALSE	FALSE	FALSE	TRUE	TRUE	0.8	0.005
PWR Assembly	Uranium	1.5	5	657	2.5E-04	3.5E-05	0.04	None	FALSE	FALSE	FALSE	TRUE	TRUE	0.8	0.005

Table F.46 Fuel Fabrication PPS Inputs

Fuel Fabrication PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.7	0.5	All Materials
Layer 2	0.8	0.4	BWR Assembly, PWR Assembly

Table F.47 Uranium HEU Research Reactor Facility Inputs

Facility Name: University HEU Research Reactor					**Location:** 41°55'17.43"N, 106°25'0.87"W					$\bar{D}_{FAC}$	267	ε_{HR}	0.15		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	E_U	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Fresh HEU Fuel	Uranium	1.03	46	0.9584	3.1E-4	1.60E-07	0.36	NONE	FALSE	FALSE	FALSE	TRUE	TRUE	0.98	0.98
Spent HEU Fuel	Uranium	1.02	47	0.9584	450	4.00	0.34	SLOW	TRUE	TRUE	FALSE	TRUE	TRUE	0.98	0.98

Table F.48 University HEU Research Reactor Sabotage Inputs

Facility Name: University HEU Research Reactor							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.5	0.25	5.00E-11	5.00E-07	1.00E-05	5.00E-04
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.375	0.25	1.20E-11	1.00E-07	5.00E-06	4.50E-04

Table F.49 University HEU Research Reactor PPS Inputs

PWR Reactor Site 2 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.35	0.35	All Materials and Vital Areas
Layer 2	0.2	0.2	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.01	0.01	Circulation Pump 1
Layer 4	0.01	0.01	Coolant Pump 1
Layer 5	0.01	0.01	Coolant Pump 2

Table F.50 University LEU Research Reactor Facility Inputs

Facility Name: University LEU Research Reactor					**Location:** 43°48'53.16"N, 105° 1'18.30"W					$\bar{D}_{FAC}$	255	ε_{HR}	0.1		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	E_U	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated LEU Fuel	Plutonium	1.00	301	2.4	625	4.24	0.6	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.99	0.99
Fresh LEU Fuel	Uranium	1.01	144	2.4	2.5E-04	5.70E-07	0.197	None	FALSE	FALSE	TRUE	TRUE	TRUE	0.99	0.99

Table F.51 University LEU Research Reactor Sabotage Inputs

Facility Name: University LEU Research Reactor							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.5	0.25	1.00E-08	1.00E-04	1.00E-03	5.00E-03
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.375	0.25	1.20E-08	1.00E-05	5.00E-04	4.50E-03

Table F.52 University LEU Research Reactor PPS Inputs

PWR Reactor Site 2 PPS	P_{I}^{Layer}	P_{N}^{Layer}	Targets Under Layer
Layer 1	0.5	0.5	All Materials and Vital Areas
Layer 2	0.25	0.25	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.01	0.01	Circulation Pump 1
Layer 4	0.01	0.01	Coolant Pump 1
Layer 5	0.01	0.01	Coolant Pump 2

Table F.53 Hospital Cancer Center Facility Inputs

Facility Name: Hospital Cancer Center	**Location:** 43°45'20.39"N, 104°53'46.57"W				$\overline{D}_{FAC}$	254	ε_{HR}	0.1
Radiological Material	**Type**	D_{value}^{Rad}	N_{I}	m_{I}	A_{I}^{Rad}	D_{Rad}	$\beta_{\square A}$	β_{CS}
LDR Brachytherapy Seeds	Ra-226	0.04	1750	3	0.015	2.1E-6	1	0.99999
HDR Brachytherapy Seeds	Ir-192	0.08	200	7	6	4.2E-6	1	0.995
Gamma Knife Multi-Beam	Co-60	0.03	1	3500	7000	1.2E-6	1	0.05
Nuclear Medicine Imaging	Mo-99/ Tc-99	0.3	1	20	75	1.1E-6	1	0.95

Table F.54 Hospital Cancer Center Facility Inputs

Hospital Cancer Center PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.1	LDR Brachytherapy Seeds
Layer 2	0.5	0.1	HDR Brachytherapy Seeds
Layer 3	0.75	0.25	Gamma Knife Source
Layer 4	0.3	0.1	Mo-99/Tc-99

Table F.55 Hospital 2 Facility Inputs

Facility Name: Hospital 2	**Location:** 41°59'25.77"N 106°25'0.87"W				$\bar{D}_{FAC}$	254	ε_{HR}	0.1
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
LDR Brachytherapy Seeds	Ra-226	0.04	1750	3	0.015	2.1E-6	1	0.99999
HDR Brachytherapy Seeds	Ir-192	0.08	200	7	6	4.2E-6	1	0.995
Nuclear Medicine Imaging	Mo-99/ Tc-99	0.3	1	20	75	1.1E-6	1	0.95

Table F.56 Hospital 2 Facility Inputs

Hospital 2 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.1	LDR Brachytherapy Seeds
Layer 2	0.5	0.1	HDR Brachytherapy Seeds
Layer 3	0.3	0.1	Mo-99/Tc-99

Table F.57 Hospital 3 Facility Inputs

Facility Name: Hospital 3	**Location:** 42°12'54.69"N 110° 2'39.65"W				$\bar{D}_{FAC}$	254	ε_{HR}	0.1
Radiological Material	**Type**	D_{value}^{Rad}	N_{I}	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
LDR Brachytherapy Seeds	Ra-226	0.04	1750	3	0.015	2.1E-6	1	0.99999
HDR Brachytherapy Seeds	Ir-192	0.08	200	7	6	4.2E-6	1	0.995
Nuclear Medicine Imaging	Mo-99/ Tc-99	0.3	1	20	75	1.1E-6	1	0.95

Table F.58 Hospital 3 Facility Inputs

Hospital 3	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.1	LDR Brachytherapy Seeds
Layer 2	0.5	0.1	HDR Brachytherapy Seeds
Layer 3	0.3	0.1	Mo-99/Tc-99

Table F.59 Industrial 1 Facility Inputs

Facility Name: Industrial 1	**Location:** 44° 1'30.54"N, 105°53'25.17"W				$\bar{D}_{FAC}$	260	ε_{HR}	0.001
Radiological Material	**Type**	D_{value}^{Rad}	N_{I}	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Industrial Radiography Co 1	Co-60	0.03	5	4	60	1.2e-5	1	0.85
Industrial Radiography Ir	Ir-192	0.08	4	2	100	1.3e-5	1	0.85

Table F.60 Industrial 1 PPS Inputs

Industrial 1 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.1	Co Sources, Ir Sources
Layer 2	0.5	0.25	Co Sources

Table F.61 Industrial 2 Facility Inputs

Facility Name: Industrial 2	**Location:** 43°51'46.66"N 109°14'23.00"W				$\bar{D}_{FAC}$	260	ε_{HR}	0.001
Radiological Material	**Type**	D_{value}^{Rad}	N_{I}	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Well Logging Am-Be	Am-241/Be	0.06	5	4	20	1.2e-5	1	0.95
Well Logging Cf	Cf-252	0.02	4	3	0.08	5.3e-5	1	0.95

Table F.62 Industrial 2 PPS Inputs

Industrial 2 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.3	Am-Be sources, Cf sources
Layer 2	0.5	0.25	Cf sources

Table F.63 Industrial 3 PPS Inputs

Facility Name: Industrial 3	**Location:** 41°46'1.95"N , 109°16'26.32"W				$\bar{D}_{FAC}$	248	ε_{HR}	0.25
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Food Irradiator	Co-60	0.03	1	5500	4.0E06	1.5E-05	1	0.005

Table F.64 Industrial 3 PPS Inputs

Industrial 3 PPS	$P_I^{L\square yer}$	P_N^{Layer}	Targets Under Layer
Layer 1	0.7	0.8	Food Irradiator
Layer 2	0.45	0.5	Food Irradiator

Table F.65 Industrial 4 Facility Inputs

Facility Name: Industrial 4	**Location:** 42°15'12.98"N 106°45'16.59"W				$\bar{D}_{FAC}$	255	ε_{HR}	0.1
Radiological Material	**Type**	D_{value}^{Rad}	N_{I}	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Blood Irradiator	Cs-137	0.1	1	2200	7000	1.2E-6	1	0.05

Table F.66 Industrial 4 PPS Inputs

Industrial 4 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.5	0.5	Blood Irradiator
Layer 2	0.5	0.25	Blood Irradiator

Table F.67 Intermediate State Target Inputs

Name	Location	$\boldsymbol{P^{targ}}$	$\boldsymbol{C_{IND}^{LL}}$	$\boldsymbol{C_{IND}^{IL}}$	$\boldsymbol{C_{IND}^{EL}}$	$\boldsymbol{C_{IND}^{SC}}$	$\boldsymbol{C_{RDD}^{LL}}$	$\boldsymbol{C_{RDD}^{IL}}$	$\boldsymbol{C_{RDD}^{EL}}$	$\boldsymbol{C_{RDD}^{SC}}$
Target 1 - Capital City	43°51'48.62"N, 105° 8'10.74"W	0.3	1	1	1	1	5.00E-12	5.00E-08	5.00E-05	1.00E-04
Target 2 - City 2	44° 0'53.49"N, 108°28'12.78"W	0.1	0.35	0.01	0.05	0.7	1.65E-12	5.00E-10	2.50E-07	7.00E-05
Target 3- City 3	41°53'9.67"N 106°25'0.87"W	0.05	0.15	0.001	0.005	0.3	7.2 E-13	5.00E-11	2.50E-08	3.00E-05
Target 4 - City 4	42°16'30.37"N, 110° 2'39.65"W	0.05	0.10	0.001	0.005	0.2	7.2 E-13	5.00E-11	2.50E-08	3.00E-05

Table F.68 State Interdiction Inputs

$\bar{D}_{Capt}^{BKG}$	$\bar{D}_{Capt}^{AS}$
5.00-05	1.50E-04

F.4. Complex State Infrastructure

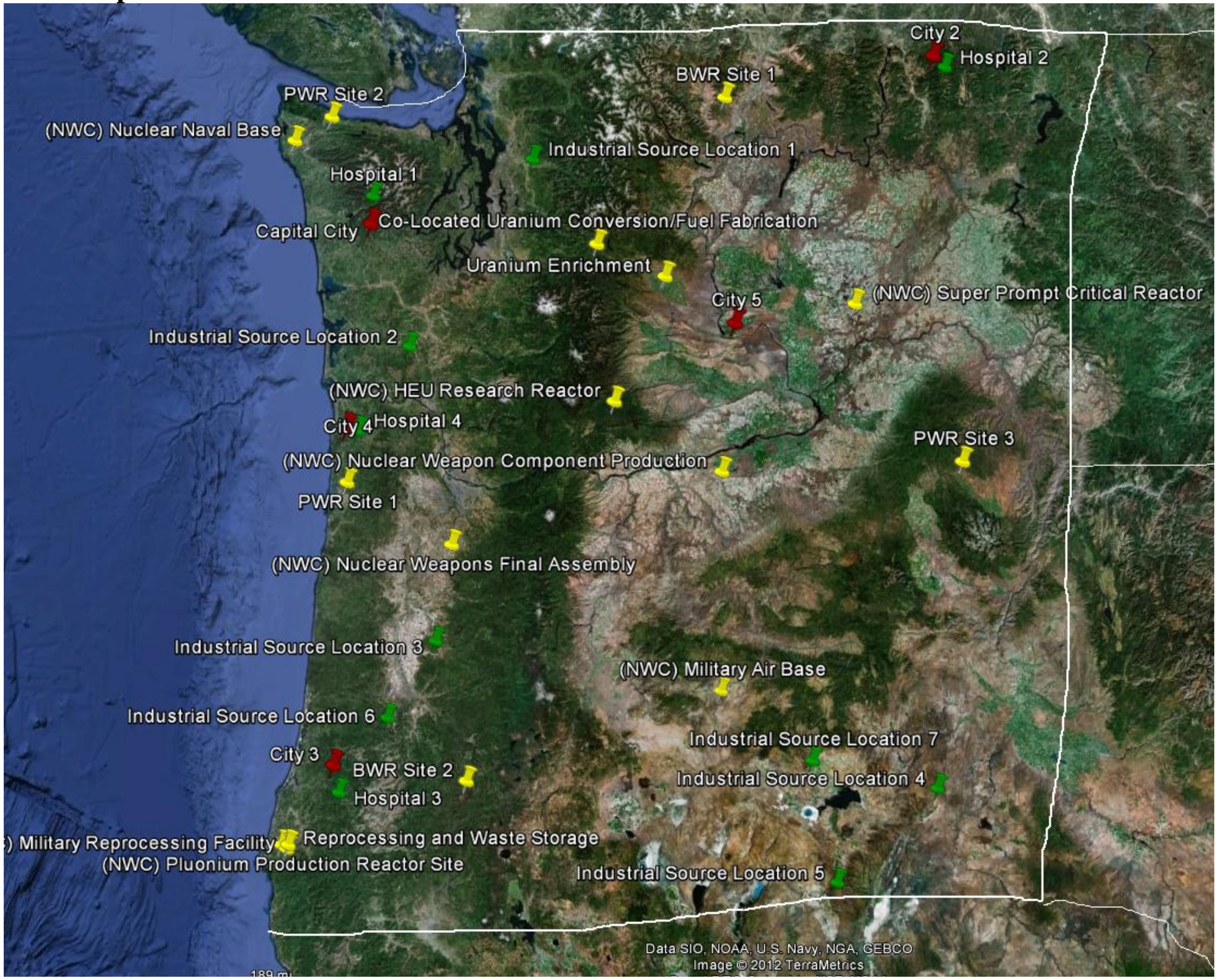

City 2
Hospital 2
BWR Site 1
PWR Site 2
(NWC) Nuclear Naval Base
Industrial Source Location 1
Hospital 1
Capital City
Co-Located Uranium Conversion/Fuel Fabrication
Uranium Enrichment
City 5
(NWC) Super Prompt Critical Reactor
Industrial Source Location 2
(NWC) HEU Research Reactor
City 4
Hospital 4
PWR Site 3
(NWC) Nuclear Weapon Component Production
PWR Site 1
(NWC) Nuclear Weapons Final Assembly
Industrial Source Location 3
(NWC) Military Air Base
Industrial Source Location 6
Industrial Source Location 7
City 3
BWR Site 2
Industrial Source Location 4
Hospital 3
) Military Reprocessing Facility
Reprocessing and Waste Storage
(NWC) Pluonium Production Reactor Site
Industrial Source Location 5
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image © 2012 TerraMetrics
189 mi

Table F.69 BWR Reactor Site 1 Facility Inputs

Facility Name: BWR Reactor Site 1					**Location: 48°15'14.87"N, 119°55'8.89"W**					$\bar{D}_{FAC}$	336	ε_{HR}	0.8		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	$E_U/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated BWR Fuel	Plutonium	1.13	5	320	8.1E04	22	0.65	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
Fresh LEU Fuel	Uranium	1.02	12	320	2.5E-04	1.2E-05	0.03	None	FALSE	FALSE	TRUE	TRUE	TRUE	0.8	0.005

Table F.70 BWR Reactor Site 1 Sabotage Inputs

Facility Name: BWR Reactor Site 1							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	$C_{Sab}^{\square L}$	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.2	0.9	1.00E-08	5.00E-05	6.20E-05	1.00E-05
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.01	0.95	5.00E-09	5.00E-05	4.50E-05	1.00E-05

Table F.71 BWR Reactor Site 1 PPS Inputs

BWR Reactor Site 1 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.9	0.93	All Materials and Vital Areas
Layer 2	0.9	0.9	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.9	Circulation Pump 1
Layer 4	0.75	0.75	Coolant Pump 1
Layer 5	0.75	0.75	Coolant Pump 2

Table F.72 BWR Reactor Site 2 Facility Inputs

Facility Name: BWR Reactor Site 2					**Location:** 43°21'55.75"N 122°32'11.43"W					$\bar{D}_{FAC}$	341	ε_{HR}	0.8		
SNM Material	**Type**	N_{SQ}	N_{I}	m_I	A_I	D_{SNM}	$E_U/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated Fuel	Plutonium	1.13	5	320	8.1E04	22	0.65	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
Fresh LEU Fuel	Uranium	1.02	12	320	2.5E-04	1.2E-05	0.03	None	FALSE	FALSE	TRUE	TRUE	TRUE	0.8	0.005

Table F.73 BWR Reactor Site 2 Facility Inputs

Facility Name: BWR Reactor Site 2							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.2	0.9	1.00E-08	5.00E-05	6.20E-05	1.00E-05
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.01	0.95	5.00E-09	5.00E-05	4.50E-05	1.00E-05

Table F.74 BWR Reactor Site 2 PPS Inputs

BWR Reactor Site 2 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump 1
Layer 4	0.75	0.75	Coolant Pump 1
Layer 5	0.75	0.75	Coolant Pump 2

Table F.75 PWR Reactor Site 1 Facility Inputs

Facility Name: PWR Reactor Site 1					**Location 45°28'19.71"N 123°49'13.30"W**					$\bar{D}_{FAC}$	303	ε_{HR}	0.8		
SNM Material	**Type**	N_{SQ}	N_{I}	m_{I}	A_{I}	D_{SNM}	$E_{U}/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated PWR Fuel	Plutonium	1.15	2	657	4.1E05	45	0.60	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
Fresh PWR Fuel	Uranium	1.23	5	657	2.5E-04	3.5E-05	0.04	None	FALSE	FALSE	TRUE	TRUE	TRUE	0.8	0.005

Table F.76 PWR Reactor Site 1 Sabotage Inputs

Facility Name: PWR Reactor Site 1							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.2	0.9	1.00E-08	5.00E-05	6.20E-05	2.50E-05
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.01	0.95	5.00E-09	5.00E-05	4.50E-05	2.50E-05

Table F.77 PWR Reactor Site 1 PPS Inputs

PWR Reactor Site 1 PPS	P_{I}^{Layer}	P_{N}^{Layer}	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump 1
Layer 4	0.75	0.75	Coolant Pump 1
Layer 5	0.75	0.75	Coolant Pump 2

Table F.78 PWR Reactor Site 2 Facility Inputs

Facility Name: PWR Reactor Site 2					**Location:** **48° 5'36.14"N 124° 9'35.46"W**					$\bar{D}_{FAC}$	317	ε_{HR}	0.8		
SNM Material	**Type**	N_{SQ}	N_{I}	m_I	A_I	D_{SNM}	E_U/Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated PWR Fuel	Plutonium	1.15	2	657	4.1E05	45	0.60	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
Fresh PWR Fuel	Uranium	1.23	5	657	2.5E-04	3.5E-05	0.04	None	FALSE	FALSE	TRUE	TRUE	TRUE	0.8	0.005

Table F.79 PWR Reactor Site 2 Sabotage Inputs

Facility Name: PWR Reactor Site							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.2	0.9	5.00E-08	9.00E-05	6.20E-05	3.50E-05
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.01	0.95	9.00E-09	8.00E-05	4.50E-05	3.50E-05

Table F.80 PWR Reactor Site 2 PPS Inputs

PWR Reactor Site PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump 1
Layer 4	0.75	0.75	Coolant Pump 1
Layer 5	0.75	0.75	Coolant Pump 2

Table F.81 PWR Reactor Site 3 Facility Inputs

Facility Name: PWR Reactor Site 3					**Location:** **45°36'44.90"N 117°32'41.62"W**					$\bar{D}_{FAC}$	328	ε_{HR}	0.8		
SNM Material	**Type**	N_{SQ}	N_{I}	m_{I}	A_{I}	D_{SNM}	$E_{U}/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated PWR Fuel	Plutonium	1.15	2	657	4.1E05	45	0.60	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
Fresh PWR Fuel	Uranium	1.23	5	657	2.5E-04	3.5E-05	0.04	None	FALSE	FALSE	TRUE	TRUE	TRUE	0.8	0.005

Table F.82 PWR Reactor Site 3 Sabotage Inputs

Facility Name: PWR Reactor Site 3							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	$C_{Sab}^{L\square}$	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pool	Spent Fuel Pool, Circulation Pump 1	0.2	0.9	1.00E-08	5.00E-05	6.20E-05	1.00E-05
Reactor	Coolant Pump 1, Coolant Pump 2, Containment	0.01	0.95	5.00E-09	5.00E-05	4.50E-05	1.00E-05

Table F.83 PWR Reactor Site 3 PPS Inputs

PWR Reactor Site 3 PPS	P_{I}^{Layer}	P_{N}^{Layer}	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump 1
Layer 4	0.75	0.75	Coolant Pump 1
Layer 5	0.75	0.75	Coolant Pump 2

Table F.84 (NWC) Military Reprocessing Facility Inputs

Facility Name: (NWC) Military Reprocessing					**Location: 42°50'44.73"N 124°18'21.71"W**					$\bar{D}_{FAC}$	349	ε_{HR}	0.95		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	E_U/Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Spent Pu Fuel Pin	Plutonium	10	4000	3	1200	24	0.93	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.99	0.005
Plutonium Oxide Weapons Grade Cans	Plutonium	18.2	10	7	300	4.2E-06	0.93	None	FALSE	FALSE	FALSE	TRUE	TRUE	0.5	0.005

Table F.85 (NWC) Military Reprocessing Sabotage Inputs

Facility Name: (NWC) Military Reprocessing							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Pin Storage	Spent Fuel Shielding	0.2	0.9	1.00E-09	9.00E-06	5.00E-05	5.00E-06

Table F.86 (NWC) Military Reprocessing PPS Inputs

(NWC) Military Reprocessing	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.75	0.75	Spent Fuel Pins, Spent Fuel Shielding
Layer 3	0.75	0.75	Spent Fuel Shielding
Layer 4	0.9	0.9	Plutonium Oxide Cans
Layer 5	0.85	0.88	Plutonium Oxide Cans

Table F.87 Commercial Reprocessing and Waste Storage Facility Inputs

Facility Name: Commercial Reprocessing and Waste Storage					**Location: 42°48'54.74"N 124°19'10.43"W**					$\bar{D}_{FAC}$	328	ε_{HR}	0.85		
SNM Material	**Type**	N_{SQ}	N_{I}	m_I	A_I	D_{SNM}	$E_U/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Irradiated PWR Fuel	Plutonium	1.15	2	657	4.1E05	45	0.60	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
Irradiated BWR Fuel	Plutonium	1.13	5	320	8.1E04	22	0.65	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.8	0.005
PuO_2 Cans Reactor Grade	Plutonium	25	45	7	425	1.02E-05	0.62	None	FALSE	FALSE	FALSE	TRUE	TRUE	0.2	0.005

Table F.88 Commercial Reprocessing and Waste Storage Facility Inputs

Facility Name: Commercial Reprocessing and Waste Storage							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Storage	Spent Fuel Pool, Circulation Pump 1	0.2	0.9	1.00E-08	6.00E-06	6.20E-05	1.00E-05

Table F.89 Commercial Reprocessing and Waste Storage Facility Inputs

Commercial Reprocessing and Waste Storage PPS	P_I^{Layer}	$P_N^{Laye\square}$	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuels, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump 1
Layer 4	0.9	0.9	PuO_2 Cans
Layer 5	0.9	0.85	PuO_2 Cans

Table F.90 (NWC) MAGNOX Pu Production Reactor Facility Inputs

Facility Name: (NWC) MAGNOX Pu Production Reactor					**Location: 42°50'44.73"N 124°18'21.71"W**					$\bar{D}_{FAC}$	349	ε_{HR}	0.95		
SNM Material	**Type**	N_{SQ}	N_{I}	m_I	A_I	D_{SNM}	E_U/Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Spent Pu Production Fuel Pin	Plutonium	2	800	3	1200	24	0.93	Slow	TRUE	TRUE	FALSE	TRUE	TRUE	0.99	0.005

Table F.91 (NWC) MAGNOX Pu Production Reactor Sabotage Inputs

Facility Name: (NWC) MAGNOX Pu Production Reactor							
Sabotage Event	Vital Areas	P^{Sab}_{Cons}	ε^{Ins}_{Sab}	C^{LL}_{Sab}	C^{IL}_{Sab}	C^{EL}_{Sab}	C^{SC}_{Sab}
Reactor	Containment, Coolant Pump 1, Coolant Pump 2	0.2	0.95	4.20E-10	5.50E-05	5.00E-06	5.00E-06

Table F.92 (NWC) MAGNOX Pu Production Reactor PPS Inputs

MAGNOX Reactor PPS	P^{Layer}_{I}	P^{Layer}_{N}	Targets Under Layer
Layer 1	0.94	0.92	All Materials and Vital Areas
Layer 2	0.92	0.9	Spent Fuel Pins
Layer 3	0.9	0.9	Coolant Pump 1
Layer 4	0.9	0.9	Coolant Pump 2

Table F.93 (NWC) HEU Research Reactor Facility Inputs

Facility Name: (NWC) HEU Research Reactor					**Location: 46° 5'11.79"N 121° 4'58.01"W**					$\bar{D}_{FAC}$	329	ε_{HR}	0.85		
SNM Material	**Type**	N_{SQ}	N_{I}	$m_{\square}$	A_I	D_{SNM}	$E_U/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Fresh HEU Fuel	Uranium	1.03	46	0.9584	3.1E-4	1.60E-07	0.36	NONE	FALSE	FALSE	FALSE	TRUE	TRUE	1	0.005
Spent HEU Fuel	Uranium	1.02	47	0.9584	450	4.00	0.34	SLOW	TRUE	TRUE	FALSE	TRUE	TRUE	1	0.005

Table F.94 (NWC) HEU Research Reactor Sabotage Inputs

Facility Name: (NWC) HEU Research Reactor							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Storage	Spent Fuel Pool, Circulation Pump	0.2	0.9	4.20E-10	5.50E-05	5.00E-06	1.00E-06
Reactor	Coolant Pump 1, Coolant Pump 2	0.1	0.9	3.00E-10	5.50E-05	5.00E-06	1.00E-06

Table F.95 (NWC) HEU Research Reactor PPS Inputs

(NWC) HEU Research Reactor PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump
Layer 4	0.9	0.9	Fresh HEU Fuel
Layer 5	0.9	0.85	Coolant Pumps

Table F.96 (NWC) Weapon Component Production Inputs

Facility Name: (NWC) Weapon Component Production					**Location:** 45°35'3.28"N 119°59'17.27"W					$\bar{D}_{FAC}$	334	ε_{HR}	0.95		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Plutonium Oxide Weapons Grade Cans	Plutonium	18.2	10	7	300	4.2E-06	0.93	None	FALSE	FALSE	FALSE	TRUE	TRUE	0.5	0.005
Pu Metal Product	Plutonium	25	100	2.0	149	2.66E-06	0.93	SLOW	FALSE	TRUE	FALSE	FALSE	TRUE	0.5	0.005
Pu Machined Metal	Plutonium	50	100	4.0	299	5.33E-06	0.93	SLOW	FALSE	TRUE	FALSE	FALSE	FALSE	0.5	0.005

Table F.97 (NWC) Weapon Component PPS Inputs

(NWC) Weapon Component Production	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.9	0.9	All Materials
Layer 2	0.9	0.8	All Materials
Layer 3	0.8	0.75	PuO_2
Layer 4	0.9	0.85	Pu Metal Product
Layer 5	0.9	0.9	Pu Machined Metal

Table F.98 (NWC) Super Prompt Critical Reactor Facility Inputs

Facility Name: (NWC) Super Prompt Critical Reactor					**Location:** 46° 5'11.79"N 121° 4'58.01"W					$\bar{D}_{FAC}$	332	ε_{HR}	0.9		
SNM Material	**Type**	N_{SQ}	N_{I}	m_I	A_I	D_{SNM}	$E_U/$ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Fresh HEU Fuel	Uranium	1.003	59	0.9584	3.1E-4	1.60E-07	0.85	NONE	FALSE	FALSE	FALSE	TRUE	TRUE	1	0.005
Irradiated HEU Fuel	Uranium	1.008	60	0.9584	450	4.00	0.84	SLOW	TRUE	TRUE	FALSE	TRUE	TRUE	1	0.005

Table F.99 (NWC) Super Prompt Critical Reactor Sabotage Inputs

Facility Name: (NWC) HEU Research Reactor							
Sabotage Event	Vital Areas	P_{Cons}^{Sab}	ε_{Sab}^{Ins}	C_{Sab}^{LL}	C_{Sab}^{IL}	C_{Sab}^{EL}	C_{Sab}^{SC}
Spent Fuel Storage	Spent Fuel Pool, Circulation Pump	0.2	0.9	2.20E-10	1.50E-05	5.00E-05	1.00E-06
Reactor	Coolant Pump 1, Coolant Pump 2	0.1	0.9	2.20E-10	1.50E-05	5.00E-05	1.00E-06

Table F.100 (NWC) Super Prompt Critical Reactor PPS Inputs

(NWC) HEU Research Reactor PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.9	0.9	All Materials and Vital Areas
Layer 2	0.9	0.8	Irradiated Fuel, Spent Fuel Pool
Layer 3	0.8	0.75	Circulation Pump
Layer 4	0.9	0.9	Fresh HEU Fuel
Layer 5	0.9	0.85	Coolant Pumps

Table F.101 (NWC) Nuclear Weapon Assembly Facility Inputs

Facility Name: (NWC) Nuclear Weapon Assembly Facility					**Location: 45° 3'10.55"N 122°43'38.76"W**					$\bar{D}_{FAC}$	332	ε_{HR}	0.95		
SNM Material	**Type**	N_{SQ}	N_I	m_I	A_I	D_{SNM}	E_U/ Q_{Pu}	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
Pu Machined Metal	Plutonium	50	100	4.0	300	5.33E-06	0.93	SLOW	FALSE	TRUE	FALSE	FALSE	FALSE	0.5	0.005

Table F.102 (NWC) Nuclear Weapon Assembly Nuclear Weapons Inputs

Facility Name: (NWC) Nuclear Weapon Assembly Facility				
# Nuclear Weapons	Y_E (kT)	P_{NSU}^{NW}	β_{MA}	β_{CS}
25	2000	0.005	0.25	0.001

Table F.103 (NWC) Nuclear Weapon Assembly PPS Inputs

(NWC) Nuclear Weapon Assembly Facility	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.9	0.94	All Materials
Layer 2	0.9	0.8	Pu Machined Metal
Layer 3	0.9	0.9	Nuclear Weapons
Layer 4	0.9	0.85	Nuclear Weapons
Layer 5	0.9	0.85	Nuclear Weapons

Table F.104 (NWC) Military Air Base Inputs

Facility Name: (NWC) Military Air Base			$\boldsymbol{\varepsilon_{HR}}$	0.95
Location: 44° 2'15.61"N 120° 0'55.52"W				
# Nuclear Weapons	$\mathrm{Y_E}$ (kT)	$\boldsymbol{P_{NSU}^{NW}}$	$\boldsymbol{\beta_{MA}}$	$\boldsymbol{\beta_{CS}}$
30	2000	0.005	0.25	0.001

Table F.105 (NWC) Military Air Base PPS Inputs

(NWC) Military Air Base PPS	$\boldsymbol{P_I^{Layer}}$	$\boldsymbol{P_N^{Layer}}$	Targets Under Layer
Layer 1	0.95	0.95	Nuclear Weapons
Layer 2	0.95	0.95	Nuclear Weapons

Table F.106 (NWC) Nuclear Naval Base Nuclear Weapons Inputs

Facility Name: (NWC) Nuclear Naval Base			$\boldsymbol{\varepsilon_{HR}}$	0.95
Location: 47°54'48.38"N 124°33'5.02"W				
# Nuclear Weapons	$\mathrm{Y_E}$ (kT)	$\boldsymbol{P_{NSU}^{NW}}$	$\boldsymbol{\beta_{MA}}$	$\boldsymbol{\beta_{CS}}$
30	2000	0.005	0.25	0.001

Table F.107 (NWC) Nuclear Naval Base PPS Inputs

(NWC) Nuclear Naval Base PPS	$\boldsymbol{P_I^{Layer}}$	$\boldsymbol{P_N^{Layer}}$	Targets Under Layer
Layer 1	0.7	0.5	All Materials
Layer 2	0.8	0.4	BWR Assembly, PWR Assembly

Table F.108 Uranium Conversion and Fuel Fabrication Facility Inputs

Facility Name: Uranium Conversion and Fuel Fabrication					**Location:** 47°12'21.27"N , 121°16'27.76"W					$\bar{D}_{FAC}$	332	ε_{HR}	0.1		
SNM Material	**Type**	N_{SQ}	N_{I}	m_I	A_I	D_{SNM}	E_U	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
U_3O_8	Uranium	1	1	14000	3.2	4.2E-04	0.0072	None	FALSE	FALSE	TRUE	TRUE	TRUE	1	0.05
UF_6 30B Cylinder	Uranium	1.6	2	2200	0.61	5.6E-06	0.04	Slow	FALSE	FALSE	TRUE	TRUE	TRUE	1	0.05
BWR Assembly	Uranium	1.02	12	320	2.5E-04	1.2E-05	0.03	None	FALSE	FALSE	FALSE	TRUE	TRUE	0.8	0.005
PWR Assembly	Uranium	1.5	5	657	2.5E-04	3.5E-05	0.04	None	FALSE	FALSE	FALSE	TRUE	TRUE	0.8	0.005

Table F.109 Uranium Conversion and Fuel Fabrication Facility Inputs

Uranium Conversion and Fuel Fabrication PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.7	0.5	All Materials
Layer 2	0.8	0.4	BWR Assembly, PWR Assembly

Table F.110 Uranium Enrichment Facility Inputs

Facility Name: Uranium Enrichment					**Location:** 46°58'28.68"N, 120°33'33.85"W					$\bar{D}_{FAC}$	329	ε_{HR}	0.1		
SNM Material	**Type**	N_{SQ}	N_{I}	m_I	A_I	D_{SNM}	E_U	**Chemical Reactivity**	**Cooling**	**FP Rem.**	**Conv.**	**Metal.**	**Mach.**	β_{MA}	β_{CS}
UF_6 48Y Cylinders	Uranium	1.3	2	9500	2.75	5.8E-04	0.0072	None	FALSE	FALSE	FALSE	TRUE	TRUE	1	0.005
UF_6 30B Cylinder	Uranium	1.6	2	2200	0.61	5.6E-06	0.04	None	FALSE	FALSE	FALSE	TRUE	TRUE	1	0.005

Table F.111 Uranium Enrichment PPS Inputs

Uranium Enrichment PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.75	0.75	All Materials

Table F.112 Hospital 1 Facility Inputs

Facility Name: Hospital 1	**Location:** 47°32'22.55"N 123°39'48.85"W				$\bar{D}_{FAC}$	317	ε_{HR}	0.05
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
LDR Brachytherapy Seeds	Ra-226	0.04	1750	3	0.015	2.1E-6	1	0.99999
HDR Brachytherapy Seeds	Ir-192	0.08	200	7	6	4.2E-6	1	0.995
Gamma Knife Multi-Beam	Co-60	0.03	1	3500	7000	1.2E-6	1	0.05
Nuclear Medicine Imaging	Mo-99/ Tc-99	0.3	1	20	75	1.1E-6	1	0.95

Table F.113 Hospital 1 PPS Inputs

Hospital 1 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.1	LDR Brachytherapy Seeds
Layer 2	0.5	0.1	HDR Brachytherapy Seeds
Layer 3	0.75	0.25	Gamma Knife Source
Layer 4	0.3	0.1	Mo-99/Tc-99

Table F.114 Hospital 2 Facility Inputs

Facility Name: Hospital 2	**Location:** 48°26'40.42"N 117°32'32.27"W				$\bar{\boldsymbol{D}}_{\boldsymbol{FAC}}$	322	$\boldsymbol{\varepsilon}_{\boldsymbol{HR}}$	0.05
Radiological Material	**Type**	$\boldsymbol{D}_{\boldsymbol{value}}^{\boldsymbol{Rad}}$	$\boldsymbol{N}_{\mathbf{I}}$	$\boldsymbol{m}_{\boldsymbol{I}}$	$\boldsymbol{A}_{\boldsymbol{I}}^{\boldsymbol{Rad}}$	$\boldsymbol{D}_{\boldsymbol{Rad}}$	$\boldsymbol{\beta}_{\boldsymbol{MA}}$	$\boldsymbol{\beta}_{\boldsymbol{CS}}$
LDR Brachytherapy Seeds	Ra-226	0.04	1750	3	0.015	2.1E-6	1	0.99999
HDR Brachytherapy Seeds	Ir-192	0.08	200	7	6	4.2E-6	1	0.995
Nuclear Medicine Imaging	Mo-99/ Tc-99	0.3	1	20	75	1.1E-6	1	0.95

Table F.115 Hospital 2 PPS Inputs

Hospital 1 PPS	$\boldsymbol{P}_{\boldsymbol{I}}^{\boldsymbol{Layer}}$	$\boldsymbol{P}_{\boldsymbol{N}}^{\boldsymbol{Layer}}$	Targets Under Layer
Layer 1	0.2	0.1	LDR Brachytherapy Seeds
Layer 2	0.5	0.1	HDR Brachytherapy Seeds
Layer 3	0.3	0.1	Mo-99/Tc-99

Table F.116 Hospital 3 Facility Inputs

Facility Name: Hospital 3	**Location:** 43°15'17.43"N 123°48'23.56"W				$\bar{\boldsymbol{D}}_{\boldsymbol{FAC}}$	323	$\boldsymbol{\varepsilon_{HR}}$	0.05
Radiological Material	**Type**	$\boldsymbol{D_{value}^{Rad}}$	$\boldsymbol{N_{\mathrm{I}}}$	$\boldsymbol{m_I}$	$\boldsymbol{A_I^{R\square d}}$	$\boldsymbol{D_{Rad}}$	$\boldsymbol{\beta_{MA}}$	$\boldsymbol{\beta_{CS}}$
LDR Brachytherapy Seeds	Ra-226	0.04	1750	3	0.015	2.1E-6	1	0.99999
HDR Brachytherapy Seeds	Ir-192	0.08	200	7	6	4.2E-6	1	0.995
Gamma Knife Multi-Beam	Co-60	0.03	1	3500	7000	1.2E-6	1	0.05
Nuclear Medicine Imaging	Mo-99/ Tc-99	0.3	1	20	75	1.1E-6	1	0.95

Table F.117 Hospital 3 PPS Inputs

Hospital 3 PPS	$\boldsymbol{P_I^{Layer}}$	$\boldsymbol{P_N^{Layer}}$	Targets Under Layer
Layer 1	0.2	0.1	LDR Brachytherapy Seeds
Layer 2	0.5	0.1	HDR Brachytherapy Seeds
Layer 3	0.75	0.25	Gamma Knife Source
Layer 4	0.3	0.1	Mo-99/Tc-99

Table F.118 Hospital 4 Facility Inputs

Facility Name: Hospital 4	**Location:** 45°51'23.72"N 123°43'9.78"W				$\bar{\boldsymbol{D}}_{FAC}$	321	$\boldsymbol{\varepsilon}_{HR}$	0.05
Radiological Material	**Type**	D^{Rad}_{value}	N_{I}	m_I	A^{Rad}_I	D_{Rad}	β_{MA}	β_{CS}
LDR Brachytherapy Seeds	Ra-226	0.04	1750	3	0.015	2.1E-6	1	0.99999
HDR Brachytherapy Seeds	Ir-192	0.08	200	7	6	4.2E-6	1	0.995
Gamma Knife Multi-Beam	Co-60	0.03	1	3500	7000	1.2E-6	1	0.05
Nuclear Medicine Imaging	Mo-99/ Tc-99	0.3	1	20	75	1.1E-6	1	0.95

Table F.119 Hospital 4 PPS Inputs

Hospital 4 PPS	P^{Layer}_I	P^{Layer}_N	Targets Under Layer
Layer 1	0.2	0.1	LDR Brachytherapy Seeds
Layer 2	0.5	0.1	HDR Brachytherapy Seeds
Layer 3	0.75	0.25	Gamma Knife Source
Layer 4	0.3	0.1	Mo-99/Tc-99

Table F.120 Industrial 1 Facility Inputs

Facility Name: Industrial 1	**Location:** 47°49'29.89"N, 121°57'58.21"W				$\bar{\boldsymbol{D}}_{FAC}$	325	$\boldsymbol{\varepsilon}_{HR}$	0.01
Radiological Material	**Type**	D^{Rad}_{value}	N_{I}	m_I	A^{Rad}_I	D_{Rad}	β_{MA}	β_{CS}
Blood/Tissue Irradiator	Cs-137	0.1	4	3500	3.0E06	5.1e-6	1	0.05

Table F.121 Industrial 1 PPS Inputs

Industrial 1 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.5	0.5	Blood/Tissue Irradiator
Layer 2	0.5	0.5	Blood/Tissue Irradiator

Table F.122 Industrial 2 Facility Inputs

Facility Name: Industrial 2	**Location:** 46°28'6.23"N, 123°12'58.41"W				$\bar{D}_{FAC}$	322	ε_{HR}	0.01
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Food Irradiator	Co-60	0.03	2	5500	4.0E06	1.5E-05	1	0.005

Table F.123 Industrial 2 PPS Inputs

Industrial 2 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.7	0.8	Food Irradiator
Layer 2	0.45	0.5	Food Irradiator

Table F.124 Industrial 3 Facility Inputs

Facility Name: Industrial 3	**Location:** 42°27'2.90"N, 122°38'37.00"W				$\bar{D}_{FAC}$	322	ε_{HR}	0.001
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Industrial Radiography Co 1	Co-60	0.03	5	4	60	1.2e-5	1	0.85
Industrial Radiography Ir	Ir-192	0.08	4	2	100	1.3e-5	1	0.85

Table F.125 Industrial 3 PPS Inputs

Industrial 3 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.1	Co Sources, Ir Sources
Layer 2	0.5	0.25	Co Sources

Table F.126 Industrial 4 Facility Inputs

Facility Name: Industrial 4	**Location:** 43°18'15.16"N, 117°54'24.23"W				$\bar{D}_{FAC}$	318	ε_{HR}	0.001
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	$D_{Ra□}$	β_{MA}	β_{CS}
Well Logging Am-Be	Am-241/Be	0.06	5	4	20	1.2e-5	1	0.95
Well Logging Cf	Cf-252	0.02	4	3	0.08	5.3e-5	1	0.95

Table F.127 Industrial 5 Facility Inputs

Industrial 4 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.3	Am-Be sources, Cf sources
Layer 2	0.5	0.25	Cf sources

Table F.128 Industrial 5 Facility Inputs

Facility Name: Industrial 5	**Location:** 42°38'51.88"N, 118°54'35.09"W				$\bar{D}_{FAC}$	322	ε_{HR}	0.001
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Well Logging Am-Be	Am-241/Be	0.06	5	4	20	1.2e-5	1	0.95
Well Logging Cf	Cf-252	0.02	4	3	0.08	5.3e-5	1	0.95

Table F.129 Industrial 5 PPS Inputs

Industrial 5 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.2	0.3	Am-Be sources, Cf sources
Layer 2	0.5	0.25	Cf sources

Table F.130 Industrial 6 Facility Inputs

Facility Name: Industrial 6	**Location:** 43°48'29.26"N, 123°20'10.80"W				$\bar{D}_{FAC}$	331	ε_{HR}	0.01
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Food Irradiator	Co-60	0.03	2	5500	4.0E06	1.5E-05	1	0.005

Table F.131 Industrial 6 PPS Inputs

Industrial 6 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.7	0.8	Food Irradiator
Layer 2	0.45	0.5	Food Irradiator

Table F.132 Industrial 7 Facility Inputs

Facility Name: Industrial 7	**Location:** 43°31'43.91"N, 119° 7'36.30"W				$\bar{D}_{FAC}$	324	ε_{HR}	0.0001
Radiological Material	**Type**	D_{value}^{Rad}	N_I	m_I	A_I^{Rad}	D_{Rad}	β_{MA}	β_{CS}
Radio-thermo Generator	Sr-90	1	2	6600	2.0E04	1E-02	1	0.99

Table F.133 Industrial 7 PPS Inputs

Industrial 7 PPS	P_I^{Layer}	P_N^{Layer}	Targets Under Layer
Layer 1	0.001	0.001	Radio-thermo Generator
Layer 2	0.001	0.001	Radio-thermo Generator

Table F.134 Complex State Targets Inputs

Name	Location	P^{targ}	C_{NW}^{LL}	C_{NW}^{IL}	C_{NW}^{EL}	C_{NW}^{SC}	C_{IND}^{LL}	C_{IND}^{IL}	$C_{IND}^{E\square}$	C_{IND}^{SC}	C_{RDD}^{LL}	C_{RDD}^{IL}	C_{RDD}^{EL}	C_{RDD}^{SC}
Target 1 - Capital City	43°51'48.62"N, 105° 8'10.74"W	0.3	1	1	1	1	2.15E-01	2.15E-01	2.15E-01	2.15E-01	1.08E-12	1.08E-08	1.08E-05	2.15E-05
Target 2 - City 2	44° 0'53.49"N, 108°28'12.78"W	0.1	0.35	0.01	0.05	0.7	7.54E-02	2.15E-03	1.08E-02	1.51E-01	8.89E-14	1.08E-12	2.69E-09	1.06E-05
Target 3- City 3	41°53'9.67"N 106°25'0.87"W	0.05	0.15	0.001	0.005	0.3	3.23E-02	2.15E-04	1.08E-03	6.50E-02	1.55E-14	1.08E-14	2.69E-11	1.94E-06
Target 4 - City 4	42°16'30.37"N, 110° 2'39.65"W	0.05	0.10	0.001	0.005	0.2	2.15E-02	2.15E-04	1.08E-03	4.30E-02	1.55E-14	1.08E-14	2.69E-11	1.29E-06
Target 4 - City 4	46°38'18.18"N 119°50'9.57"W	0.05	0.10	0.001	0.005	0.2	2.15E-02	2.15E-04	1.08E-03	4.31E-02	1.55E-14	1.08E-14	2.69E-11	1.29E-06