Towards a Unified
Homeland Security Strategy:
An Asset Vulnerability Model

University of Colorado at
Colorado Springs

College of Engineering and
Applied Science
Computer Science Department

Dissertation Submittal
v3.1, November 3, 2013

Richard L. White

Faculty Advisors:
  Dr. C. Edward Chow (chair)
  Dr. Terrance Boult
  Dr. Xiaobo Zhou
  Dr. Scott Trimboli
  Dr. Stan Supinski
TOWARDS A UNIFIED
HOMELAND SECURITY STRATEGY

by

Richard L. White

Dissertation submitted to the Faculty of
the College of Engineering and Applied Science
Computer Science Department
University of Colorado at Colorado Springs
in partial fulfillment of requirements for the degree of
Doctor of Philosophy
2013

Advisory Committee:
Dr. C. Edward Chow (chair)
Dr. Terrance Boult
Dr. Xiaobo Zhou
Dr. Scott Trimboli
Dr. Stan Supinski
Abstract

The attacks of September 11, 2001 made manifest the unprecedented threat of domestic catastrophic attack by small groups subverting the nation’s critical infrastructure. Tasked with protecting the nation’s critical infrastructure, the Department of Homeland Security still seeks an effective risk formulation to guide the efficient allocation of scarce national resources. Without an adequate performance measure, DHS is unable to justify taxpayer expenditures to Congress answering 1) how safe are we, 2) how much safer can we be, and 3) how much will it cost? Moreover, internal audits and external reviews reveal a program that is fragmented and uncoordinated. In the absence of historical data, the current threat-driven approach suffers from statistical outliers making the current risk formulation an ill-behaved problem. This research uniquely proposes risk criteria to help condition the problem and make it more amenable. Key insights include 1) the viability of an asset-driven approach, 2) reducing threat prediction to threat localization, 3) eschewing complexity for transparency and repeatability, 4) addressing the five phases of emergency management, and 5) capturing the national impact of consequences. Similarly, this research makes novel application of earlier work in game theory to propose a basic metric for guiding strategic investments by answering the question, how much risk is acceptable. Within this framework, an Asset Vulnerability Model is developed to 1) perform baseline analysis, 2) conduct cost-benefit analysis, and 3) provide decision support tools. AVM works with the DHS Risk Management Framework to 1) assess critical assets, 2) evaluate proposed measures, and 3) guide strategic investments. It demonstrates how such guidance might be accomplished by using AVM to evaluate six alternative risk reduction investment strategies. In this manner, AVM unifies DHS programs while delivering quantifiable results justifying taxpayer expenditures to Congress. Critical infrastructure, however, is not the only
threat to homeland security. Weapons of mass destruction in the form of chemical, biological, radiological, and nuclear agents also present the means for asymmetric attack. The same research in game theory contends that a coordinated defensive strategy is more efficient than an uncoordinated one. WMD protection is the responsibility of federal agencies outside DHS. Interagency coordination is facilitated through National Security Council and National Security Strategy. This research significantly suggests that current strategy is misdirected by its focus on terrorism, which is but one possible motive for precipitating domestic catastrophic attack. Consequently, a new definition is proposed for homeland security to provide a supporting policy framework leading towards a unified homeland security strategy.
Acknowledgement

In great appreciation for the patience, guidance, and understanding of my Advisory Committee, family, and friends. This wouldn’t have been possible without your support.
# Table of Contents

Abstract.............................................................................................................................................. v
Acknowledgement ............................................................................................................................... vii
Table of Contents ................................................................................................................................. ix
List of Figures ....................................................................................................................................... xiii
List of Tables ......................................................................................................................................... xv

Chapter 1. Introduction .......................................................................................................................... 1
  1.1. Motivation and Problem Description ......................................................................................... 1
  1.2. Objectives and Scope .................................................................................................................. 2
  1.3. Outline of Dissertation ................................................................................................................ 3

Chapter 2. Literature Review ............................................................................................................... 7
  2.1. An Unprecedented Threat ......................................................................................................... 7
  2.2. Critical Infrastructure Vulnerability .......................................................................................... 8
  2.3. The WMD Threat ...................................................................................................................... 11
  2.4. The CI Threat ............................................................................................................................ 15
  2.5. WMD Protection ....................................................................................................................... 28
  2.6. CI Protection ............................................................................................................................. 36
  2.7. Assessing Protection Efforts ..................................................................................................... 41
  2.8. Risk Analysis ............................................................................................................................. 46
  2.9. Risk Management ..................................................................................................................... 47
  2.10. Related Research .................................................................................................................... 49
  2.11. Summary ................................................................................................................................. 54
  2.12. Contributions ........................................................................................................................... 55

Chapter 3. Methodology ...................................................................................................................... 57
  3.1. Overview ..................................................................................................................................... 57
  3.2. Design Criteria .......................................................................................................................... 58
  3.3. An Asset Vulnerability Model .................................................................................................... 68
  3.4. Model Instantiation .................................................................................................................... 80
  3.5. Sensitivity Analysis .................................................................................................................... 88
  3.6. Model Comparisons .................................................................................................................. 96
  3.7. Summary .................................................................................................................................... 98
  3.8. Contributions .......................................................................................................................... 99
# Chapter 4. Implementation

4.1. Overview ........................................................................................................... 101
4.2. Strategy Coordination ...................................................................................... 101
4.3. AVM Implementation ...................................................................................... 108
4.4. Analyzing Investment Strategies .................................................................... 112
4.5. Summary .......................................................................................................... 142
4.5. Contributions .................................................................................................. 142

# Chapter 5. Contributions and Future Work

5.1. Research Contributions .................................................................................. 143
5.2. Future Research .............................................................................................. 145
5.3. Conclusion ....................................................................................................... 147

# Appendix A: Glossary

A.1. BIRR .................................................................................................................. 149

# Appendix B: CI Protection Models

B.1. BIRR .................................................................................................................. 155
B.2. BMI .................................................................................................................... 157
B.3. CAPRA .............................................................................................................. 160
B.4. CARVER2 ...................................................................................................... 161
B.5. CIMS ................................................................................................................ 162
B.6. CIPDSS ......................................................................................................... 163
B.7. CIPMA ............................................................................................................. 165
B.8. CommAspen ................................................................................................... 166
B.9. COUNTERACT ............................................................................................ 169
B.10. DECRIS .......................................................................................................... 171
B.11. EURACOM ................................................................................................... 172
B.12. FAIT ............................................................................................................... 173
B.13. MIN ................................................................................................................ 175
B.14. MDM .............................................................................................................. 176
B.15. N-ABLE ......................................................................................................... 177
B.16. NEMO ............................................................................................................ 178
B.17. NSRAM ........................................................................................................ 179
B.18. RAMCAP-Plus ............................................................................................. 181
B.19. RVA ............................................................................................................... 182
B.20. SRAM ............................................................................................................ 183
B.21. RMCIS .......................................................................................................... 184
(This Page Intentionally Blank)
List of Tables

Table 2-1: Critical Infrastructure Sectors ........................................................................... 15
Table 3-1: Homeland Security Risk Analysis Challenges/Criteria........................................ 62
Table 3-2: Domestic Catastrophic Threats (Infrastructure) ....................................................... 64
Table 3-3: Risk Formulation Criteria ....................................................................................... 68
Table 3-4: List of Program Models ......................................................................................... 81
Table 3-5: Asset Record Values and Bounds for Simulated Baseline Analysis ......................... 81
Table 3-6: Critical Infrastructure Risk Assessment Models ..................................................... 96
Table 3-7: Comparison of CI Models to Risk Criteria .............................................................. 97
Table 4-1: Protective Improvement Investment Strategies ....................................................... 114
Table 4-2: AVM Investment Strategy Simulation Program Models ........................................ 120
Table 4-3: AVM Investment Strategy Simulation Supporting Batch Files .............................. 122
Table 4-4: AVM Investment Strategy Simulation Data Sensitivity & Analysis Programs ......... 126
Table 4-5: Simulation Attack Results ....................................................................................... 133
Table C-1: CBA Output File Record Format .......................................................................... 188
Table C-2: AVM Strategy Simulation Program Files .............................................................. 196
Table C-3: AVM Strategy Simulation Result Files ................................................................. 197
Table C-4: Batch Execution & Output Files ........................................................................... 198
Table C-5: AVM Data Sensitivity Analysis Files ................................................................. 199
Table C-6: DSA Batch Execution & Output Files ................................................................. 200
List of Figures

Figure 2-1: CWMD Strategy Framework ................................................................. 29
Figure 2-2: DHS Risk Management Framework ...................................................... 38
Figure 3-1: Sandler & Lapan Model ........................................................................ 60
Figure 3-2.1: Unfiltered AVM Baseline Analysis Depicting Current Homeland Security Risk Profile .... 78
Figure 3-2.2: Baseline AVM Data Sorted by Theta Identifying Assets from Least to Most Vulnerable .... 78
Figure 3-2.3: Baseline AVM Data Sorted by Asset Type Identifying Vulnerabilities by Infrastructure Sector .. 78
Figure 3-2.4: Baseline AVM Data Sorted by Asset Location Identifying Vulnerabilities by Region .......... 78
Figure 3-3.1: Results from AVM Cost-Benefit Analysis Identifying Optimum Improvements in Order of Benefit (largest to smallest) ................................................................................................................................. 79
Figure 3-3.2: Results from AVM Cost-Benefit Analysis Identifying Optimum Improvements by Cost ........ 79
Figure 3-3.3: Results from AVM Cost-Benefit Analysis Identifying Optimum Improvements by Asset Type .. 79
Figure 3-3.4: Results from AVM Cost-Benefit Analysis Identifying Optimum Improvement by Region .... 79
Figure 3-3: BAM Sample Output / Baseline Data + Θ Calculation ................................. 82
Figure 3-4: PIM Sample Output / Simulated Asset Protective Measures Data .................. 85
Figure 3-5: Risk Reduction Worth vs. Θ .................................................................... 89
Figure 3-6: Θ Sensitivity Analysis ............................................................................ 93
Figure 3-7: Θ Sensitivity Without P .......................................................................... 94
Figure 3-8: Percent Change in ΔΘ ........................................................................... 95
Figure 4-1: Asset Identification ............................................................................... 109
Figure 4-2: AVM Investment Strategy Simulation Program Architecture ....................... 115
Figure 4-3: Probable Attack Model (PAM) ............................................................... 118
Figure 4-4: PAM Model of Expected Attacks Over 40 Years ...................................... 118
Figure 4-5: AVM Investment Strategy Simulation for Single Dataset over Ten Years .......... 123
Figure 4-6: AVM Investment Strategy Simulation for Single Asset over Ten Years .......... 124
Figure 4-7: AVM12 Comparison of Successful Attacks Across Investment Strategies ........ 127
Figure 4-8: AVM12 Comparison of Damages Across Investment Strategies .................. 128
Figure 4-9: AVM12 Comparison of Expenditures Across Investment Strategies .............. 128
Figure 4-10: AVM12 Comparison of Protection Purchases Across Investment Strategies ..... 129
Figure 4-11: AVM13 Comparison of Successful Attacks Across Investment Strategies ........ 130
Figure 4-12: AVM13 Comparison of Damages Across Investment Strategies .................. 130
Figure 4-13: AVM13 Comparison of Expenditures Across Investment Strategies .............. 130
Figure 4-14: AVM13 Comparison of Protection Purchases Across Investment Strategies ..... 130
Figure 4-15: AVM14 Comparison of Successful Attack Across Investment Strategies ....... 131
Figure 4-16: AVM14 Comparison of Damages Across Investment Strategies ..................... 131
Figure 4-17: AVM14 Comparison of Expenditures Across Investment Strategies ............. 131
Figure 4-18: AVM14 Comparison of Protection Purchases Across Investment Strategies ...... 131
Figure 4-19: PAM Attack Model .................................................................................. 132
Figure 4-20: AVM12 Average Computed Damages ......................................................... 133
Figure 4-21: AVM12 Adjusted Computed Damages ......................................................... 134
Figure 4-22: AVM12 Adjusted Damage Results ................................................................. 134
Figure 4-23: AVM12 Comparative Damage Results ......................................................... 135
Figure 4-24: AVM13 Damage Data Variation ................................................................. 136
Figure 4-25: AVM13 Adjusted Computed Damages ......................................................... 136
Figure 4-26: AVM13 Adjusted Damage Results ................................................................. 136
Figure 4-27: AVM13 Comparative Damages ................................................................. 136
Figure 4-28: AVM14 Damage Data Variation ................................................................. 137
Figure 4-29: AVM14 Adjusted Computed Damages ......................................................... 137
Figure 4-30: AVM14 Adjusted Damage Results ................................................................. 137
Figure 4-31: AVM14 Comparative Damages ................................................................. 137
Figure 4-32: Independent Damage Results Across Simulations ..................................... 138
Figure 4-33: Combined Damage Results Across Simulations ........................................ 138
Figure 4-34: Damage Results Across Simulations ......................................................... 139
Figure 4-35: Damage Variances Across Simulations ....................................................... 139
Figure 4-36: Data Normalization Across Simulations ...................................................... 139
Figure 4-37: Adjusted Damages Across Simulations ....................................................... 139
Figure 4-37: Final Simulation Results ............................................................................. 140
Figure C-1: AVM Baseline Program Architecture ......................................................... 188
Figure C-2: Sample AVM Baseline Execution ................................................................. 189
Figure C-3: AVM Baseline Extension for Investment Strategy Simulation ....................... 190
Figure C-4: Extended AVM Sample Execution ............................................................... 191
Figure C-5: 10-Year AVM Strategy Simulation ............................................................... 192
Figure C-6: Multiple Executions of 10-Year AVM Strategy Simulation over Varying Probabilities 194
Figure D-1: DSA Data for DTheta ................................................................................ 205
Figure D-2: DSA Data for Attacks ................................................................................. 205
Figure D-3: DSA Data for Damages ............................................................................. 205
Figure D-4: Percent Variation in Damages Across Simulations .................................... 206
Figure D-5: Normalized Damages Across Simulations ................................................ 206
Figure D-6: Normalized Damage Results Across Simulations

Figure D-7: Comparison of Damages Across Investment Strategies
(This Page Intentionally Blank)
Chapter 1. Introduction

1.1. Motivation and Problem Description

The Department of Homeland Security began operation on January 24, 2003. Yet after ten years and $542 billion, it can’t answer Congress’ questions asking 1) how safe are we, 2) how much safer can we be, and 3) how much will it cost? DHS was created in the wake of the September 11, 2001 attacks on New York and Washington DC killing nearly 3,000 people and causing over $41.5 billion in damages. On September 11, 2001, nineteen men hijacked four aircraft and turned them into guided missiles inflicting as much damage as the Imperial Japanese Navy on December 7, 1941. 9/11 exposed the vulnerability of the nation’s critical infrastructure to small groups or individuals seeking to inflict catastrophic damage. Prior to 9/11, most experts considered weapons of mass destruction the primary avenue for domestic catastrophic attack. The essential vulnerability of the nation’s critical infrastructure is that millions of lives depend on a network that’s not fully understood, riddled with weaknesses, and susceptible to malicious tampering. Accordingly, the 2002 Homeland Security Act made critical infrastructure protection a primary mission of the new department. In 2009, DHS released the National Infrastructure Protection Plan establishing a Risk Management Framework to 1) catalog critical assets, 2) assess their risk, and 3) prioritize protective investments. Risk is measured and protective improvements prioritized by the risk formula R=f(C,V,T) where C is the consequence of subverting the asset, V is its susceptibility to attack, and T is the probability the asset will be attacked. A number of internal reviews and external audits have since revealed serious flaws with the implementation of the Risk Management Framework indicating it is fragmented and uncoordinated. Moreover, a 2010 review by the National Research Council further concluded that DHS’ risk formulation is inadequate for guiding strategic investment decisions. The 1993
Government Performance Results Act requires all federal agencies to use performance measures to justify their taxpayer expenditures to Congress. In the absence of a guiding metric, DHS can’t say where we are, where we’re going, or even how we’ll get there.

Developing an appropriate metric is essential to guiding homeland security strategy and ensuring efficient allocation of scarce national resources. According to the 2010 National Research Council report, the DHS risk formulation suffers from two well-known problems affecting all threat-driven risk approaches: 1) statistical outliers called “black swans”, and 2) insufficient historical data. The report goes on to list ten challenges describing an ill-behaved problem whose risk calculations can fluctuate wildly depending on input that is not well understood. The National Research Council report concludes that DHS’ risk formulation and framework are “seriously deficient and in need of major revision” (National Research Council, 2010, p. 11).

1.2. Objectives and Scope

The purpose of this research is to develop a risk formulation to guide homeland security strategy in making informed national resource investments by 1) indicating current protection status, 2) demonstrating incremental improvement, and 3) assessing associated costs. The research begins by establishing criteria for an appropriate risk measure and its formulation. The chosen metric is $\Theta$, an attacker’s probability of failure suggested by earlier work in game theory by Sandler and Lapan. The proposed risk formulation is derived from criteria suggested in the 2010 National Research Council report. An Asset Vulnerability Model (AVM) is then introduced that works with the DHS Risk Management Framework to 1) provide a baseline estimation of critical infrastructure protection status, 2) perform cost-benefit analysis identifying
optimum resource investments, and 3) offer decision support tools helping decision makers at all levels make informed choices investing scarce national resources. As its name implies, AVM is an asset-driven risk methodology avoiding the problems of a threat-driven approach. Still, AVM addresses the problem of threat prediction through threat localization by scoping the target set. AVM formulations are transparent and repeatable employing data that is mostly already available. AVM formulations are comprehensive, capturing the broader effects of a disaster at a national level beyond the immediate damage. AVM decision support tools offer flexible presentation of results to inform decisions at different levels of management. Sensitivity analysis on AVM cost-benefit analysis demonstrates that it is stable. Critical infrastructure protection, though, is only half the homeland security problem; WMD protection is the other half. WMD protection is the responsibility of federal agencies outside the Department of Homeland Security and beyond the current reach of the Risk Management Framework. As determined by Sandler and Lapan’s research in game theory, a coordinated defense among all targets is more efficient than an uncoordinated one. Consequently, a policy framework is proposed that will accommodate combined AVM analysis of CI and WMD risks, leading towards a unified homeland security strategy.

1.3. Outline of Dissertation

Chapter 2 reviews current literature and primary sources to frame the homeland security threat, assess current protection efforts, and review related research in the area. Chapter 2 begins with the threat of critical infrastructure exposed by the 9/11 attacks. It describes how CI and WMD may be subverted or employed for domestic catastrophic attack. It then examines federal efforts to protect WMD and CI. An evaluation of DHS’ risk management approach to CI
protection reveals that it is fragmented, uncoordinated, and inadequate for guiding strategic investment decisions. A review of risk analysis and risk management methodologies reveals the general weakness of the threat-driven approach. Despite much research in terrorism risk modeling since 9/11, most methodologies suffer similar deficiencies, or have not yet been successfully adapted.

Chapter 3 introduces the Asset Vulnerability Model for CI protection. It begins by developing design criteria for selection of an appropriate metric and risk formulation. The key criteria in choosing a metric is one that can determine acceptable risk. Earlier research in game theory by Sandler and Lapan developed an attacker-defender model that determined the optimum defense strategy is to protect all targets equally, not necessarily maximally. The key determinant in their model was a value they designated as $\theta$, an attacker’s probability of failure. Sandler and Lapan’s $\theta$, however, represented an attacker’s perception. In its place, AVM uses $\Theta$ representing the defender’s true knowledge of the probability of attack failure. The switch from $\theta$ to $\Theta$ was precipitated by risk formulation criteria derived from the 2010 National Research Council review. The 2010 report listed ten challenges to developing a well-behaved risk model. These were evaluated to derive seven bounding criteria to help condition the problem. The seven criteria are summarized as 1) asset-driven approach, 2) threat localization, 3) transparency & reliability, 4) qualified results, 5) comprehensive scope, 6) national impact, and 7) applicable results. AVM develops a corresponding risk formulation for $\Theta$ within these bounding criteria. AVM works with the DHS Risk Management Framework to provide 1) baseline analysis, 2) cost-benefit analysis, and 3) decision support tools. Baseline analysis produces a risk profile of all critical assets based on $\Theta$. Cost-benefit analysis finds the optimum combination of protective improvement measure for each asset as determined by their $\Delta \Theta$ benefit and $D(\Delta \Theta)$ cost.
Decision support tools graphically portray the results of baseline and cost-benefit analysis in a flexible manner that best informs resource investment decisions. AVM program models were instantiated and evaluated using simulated data; critical infrastructure data collected by DHS is protected by the 2002 Homeland Security Act making it exempt even from release under the Freedom of Information Act. AVM program models and their parameters are described towards the end of this chapter. The chapter concludes by conducting sensitivity analysis on the AVM cost-benefit analysis program demonstrating its stability.

Chapter 4 addresses AVM implementation to address all sources of domestic catastrophic attack, including WMD. AVM works with the DHS Risk Management Framework to protect critical infrastructure. WMD protection is the responsibility of federal agencies outside the Department of Homeland Security, currently beyond the reach of RMF. However, coordination between federal agencies is directed from the National Security Council to achieve national objectives specified in the National Security Strategy. This chapter examines the policy framework needed to bring WMD into the AVM fold. It makes the case that the current homeland security definition and strategy objectives are unnecessarily restricted by their focus on terrorism. Terrorism is but one motive that may precipitate domestic catastrophic attack. It proposes a new homeland security definition and strategy statement to focus attention on the CI and WMD threats. Additional oversight by the National Security Council will be necessary to oversee this implementation. The chapter concludes by using AVM to examine alternative risk investment strategies, demonstrating how, with an appropriate supporting policy structure, AVM can objectively guide the nation towards a unified homeland security strategy.
Chapter 5 summarizes contributions and suggests areas for future research. It makes broad contributions to understanding the homeland security threat, developing a viable risk formulation, supporting informed risk management, and directing national efforts towards a unified strategy. And while it has endeavored to present a comprehensive framework for defining and improving homeland security, some important implementation details remain for future research including: 1) developing a comprehensive taxonomy of critical infrastructure, 2) assessing the gains of proposed improvement measures, 3) validating results, and 4) accounting for psychological impacts.
Chapter 2. Literature Review

2.1. An Unprecedented Threat

The United States was profoundly changed by the attacks of September 11, 2001. 9/11 instigated the longest war in US history, challenges to our civil liberties, and the most extensive government reorganization since World War II. On September 11, 2001, hijackers exploited elements of the aviation infrastructure to attack the World Trade Center and the Pentagon representing seats of US economic and military power (The White House, 2003, p. 8). They killed nearly 3,000 people and caused more than $41.5B in damage (Nanto, 2004, p. 2). On September 11, 2001, nineteen men inflicted as much damage on the United States as the Imperial Japanese Navy did on December 7, 1941. While by no means as threatening as Japan’s act of war, the 9/11 attack was in some ways more devastating. It was carried out by a tiny group of people, not even enough to fill a platoon, dispatched by an organization based in one of the poorest, most remote, and least industrialized countries on earth (National Commission on Terrorist Attacks Upon the United States, 2004, pp. 339-340). Most of the attackers spoke English poorly, some hardly at all. In groups of four or five, carrying with them only small knives, box cutters, and cans of Mace or pepper spray, they hijacked four planes and turned them into deadly guided missiles (National Commission on Terrorist Attacks Upon the United States, 2004, p. 2). Measured on a governmental scale, the resources behind it were trivial (National Commission on Terrorist Attacks Upon the United States, 2004, pp. 339-340) 9/11 was a “wake-up call” to the catastrophic potential of critical infrastructure (The White House, 2003, p. 5), and the unprecedented threat of small groups and individuals capable of wielding destructive power on a scale once only achievable through the combined might of a nation.
2.2. Critical Infrastructure Vulnerability

Prior to 9/11, most experts considered weapons of mass destruction (WMD) the primary avenue for domestic catastrophic attack (US House of Representatives, 1995). WMD encompasses a class of Chemical, Biological, Nuclear, and Radiological (CBRN) agents. These concerns were not unfounded. In 1995, the Japanese cult Aum Shinrikyo manufactured Sarin gas, a chemical nerve agent, and deployed it on the Tokyo subway killing 12 people and injuring hundreds more. Five people were killed in the weeks following 9/11 when envelopes containing anthrax were mailed to Washington DC, New York, and Florida (US Department of Justice, 2010, p. 1). While nuclear and radiological devices have yet to be employed, documents and interrogations from military operations in Afghanistan have reinforced the assessment that the Taliban sought, and al-Qaeda, continues to seek to obtain radioactive material for a radiological weapon (Bowman, 2002, p. 3). Experts cite the difficulty of acquiring, manufacturing, and deploying WMD as the main reason terrorists rely on conventional weapons (Bowman, 2002, p. 4). However, for those wishing to inflict catastrophic damage on the US, critical infrastructure offers an attractive alternative to WMD.

Critical infrastructure is defined by the 2001 USA Patriot Act as: “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” The vast majority of critical infrastructure is owned and operated by the private sector. The great diversity and redundancy of the nation’s critical infrastructure provides significant physical and economic resilience. However, this vast and diverse aggregation of highly interconnected assets, systems,
and networks may also present an attractive array of targets to terrorists, and magnify greatly the potential for cascading failure. (Department of Homeland Security, 2009, p. 11)

The essential vulnerability of today’s critical infrastructure is that little of it was centrally planned or designed, and virtually none of it was built to withstand deliberate attack. The result is that millions of lives depend upon a network that’s not fully understood, riddled with weaknesses, and susceptible to malicious tampering. A key concern of the federal government since 9/11 is that terrorists will target critical infrastructure to achieve three general types of effects: 1) Direct infrastructure effects: Cascading disruption or arrest of the functions of critical infrastructure through direct attacks on a critical node, system, or function; 2) Indirect infrastructure effects: Cascading disruption and financial consequences for government, society, and economy through public- and private-sector reactions to an attack; or 3) Exploitation of infrastructure: Exploitation of elements of a particular infrastructure to disrupt or destroy another target. (The White House, 2003, p. viii)

A cyber attack against the national electric grid is very unsettling prospect. Electric utilities rely on supervisory control and data acquisition (SCADA) systems to manage the nation’s power generation, transmission, and distribution networks. While generally protected from intrusion, SCADA systems operate over the Internet. The move to SCADA boosts efficiency at utilities because it allows workers to operate equipment remotely. But this access to the Internet exposes these once-closed systems to cyber attacks (Easyrider LAN Pro, 2011).

In 2006, the Department of Energy (DOE) and Department of Homeland Security jointly conducted Project Aurora to assess the potential vulnerability of the national electric grid. In a dramatic video-taped demonstration, engineers at Idaho National Labs showed how weaknesses could be exploited to cause a generator to physically self-destruct (Easyrider LAN Pro, 2011). As
a critical node in the infrastructure network, a cyber attack on the electric grid would produce cascading effects across most every other sector of critical infrastructure (Shea, 2004, p. 9).

Cascading failure within the electric grid itself can disrupt broad geographic regions affecting millions. On July 2, 1996, a cascade event left 2 million customers in 11 states and 2 Canadian provinces without power (Shea, 2004, p. 9). The August 2003 blackout of the northeastern United States and parts of Canada, has been invoked as indicative of the potential effects of a successful terrorist cyber attack on electrical utility control systems (Shea, 2004, p. 10). While widespread, these outages were not long term. The same might not be true of a targeted attack. The physical damage of certain system components (e.g. extra-high-voltage transformers) on a large scale could result in prolonged outages as procurement cycles for these components range from months to years (North American Electric Reliability Corporation, 2010, p. 11). Such an outage would be unprecedented, and the impact would be as great if not greater than those from CBRN agents.

Admittedly, a cyber attack on the electric grid, or any other critical infrastructure would not be easy. Yet, the sophistication required to infiltrate and compromise such systems has been amply demonstrated by the Stuxnet worm. Using thumb drives to bypass the Internet, a malicious software program known as Stuxnet infected computer systems that were used to control an Iranian nuclear power plant. Once inside the system, Stuxnet had the ability to degrade or destroy the software on which it operated. It was also able to spread throughout multiple countries worldwide (Kerr, Rollins, & Theohary, 2010, p. 2).

Many consider Stuxnet the type of risk that could seriously damage critical infrastructure basic to the functioning of modern society. A successful attack by a Stuxnet-like worm could
inflict long-term damage by ordering control systems to overload or otherwise destroy critical mechanical components. Long lead times to repair or replace such components could leave millions without life sustaining or comforting services for a long period of time. The resulting damage to the nation’s critical infrastructure could threaten many aspects of life, including the government’s ability to safeguard national security interests (Kerr, Rollins, & Theohary, 2010, p. 2).

The worst case terrorist attack envisioned in the 2004 Planning Scenarios estimates 450,000 people would be displaced after detonating a 10-kiloton improvised nuclear device in a major US city (Homeland Security Council, 2004, pp. 1-1). By comparison, a targeted terrorist attack on the national electric grid could disrupt millions of lives and have national strategic consequences.

9/11 exposed the vulnerability of critical infrastructure to anybody with the means, motive, and opportunity to inflict catastrophic damage on the US. Both weapons of mass destruction and critical infrastructure provide ready avenues of attack for small groups and individuals wishing to inflict catastrophic consequences.

2.3. The WMD Threat

Weapons of mass destruction are highly destructive. The homeland security concern is that they fall into the hands of malicious agents and are employed inside the US. Worldwide, the likelihood of non-state actors being capable of producing or obtaining WMD may be growing due to looser controls of stockpiles and technology in the former Soviet states specifically, and the broader dissemination of related technology and information in general. However, WMD remain significantly harder to produce or obtain than what is commonly depicted in the press.
The Central Intelligence Agency believes most hostile actors will continue to choose conventional explosives over WMD, but warns that the al-Qaeda network has made obtaining WMD capability a very high priority (Bowman, 2002, p. 2).

2.3.1. Chemical Agents

Toxic industrial chemicals such as chlorine or phosgene are easily available and do not require great expertise to be adapted into chemical weapons. Aerosol or vapor forms are the most effective for dissemination, which can be carried out by sprayers or an explosive device. Nerve agents are more difficult to produce, and require a synthesis of multiple precursor chemicals. They also require high-temperature processes and create dangerous by-products, which makes their production unlikely outside an advanced laboratory. Blister agents such as mustard can be manufactured with relative ease, but also require large quantities of precursor chemicals. The production and transfer of precursor chemicals is internationally monitored under the Chemical Weapons Convention and the informal international export control regime of the Australia Group, providing some degree of control over their distribution (Bowman, 2002, p. 6).

2.3.2. Biological Agents

Experts say malicious agents working outside a state-run laboratory would have to overcome extraordinary technical and operational challenges to effectively and successfully weaponize and deliver a biological agent to cause mass casualties. While many biological agents can be obtained or grown with relative ease, several significant steps remain on the way to weaponization and effective use of these agents. The main challenge is effective dissemination, which requires an aerosol form. The formulation of agents for airborne dispersal requires
dissolving optimal amounts of agent in a specific combination of different chemicals (with each agent requiring a unique formulation). Moreover, aerosol disseminators need to be properly designed for the agent used, and suitable meteorological conditions must be present to carry out a successful biological mass casualty attack. Of particularly great concern is the threat of highly contagious diseases, particularly smallpox. Anthrax is not contagious from person to person, consequently its spread can be relatively easily contained. With a disease like smallpox, however, contagion can spread very rapidly. The breath or coughing of an infected person at the fever stage of the disease is sufficient to infect those around him or her. The disease has an incubation period of 12-14 days, during which an infected person experiences no symptoms. Consequently, a clandestine smallpox release in a major transportation hub could infect hundreds, and would, in two weeks’ time, result in disease outbreaks wherever the passengers eventually traveled. Smallpox has been eradicated as a naturally occurring disease, and the only two known existing cultures of the virus are held by the United States and Russia. Even so, concerns over the security of the Russian samples and the possibilities of unknown samples, have kept smallpox in the forefront of threat considerations. Though the probability of hostile agents gaining access to the virus may be very low, the severity of the potential consequences has nevertheless led the federal government to stockpile 300 million smallpox vaccine doses (Bowman, 2002, pp. 5-6).

2.3.3. Radiological Agents

Explosive-driven “dirty bombs” are an often-discussed type of radiological dispersion device (RDD), though radioactive material can also be dispersed in other ways. Radioactive material is the necessary ingredient for an RDD. This material is composed of atoms that decay, emitting...
radiation. Some types and amounts of radiation are harmful to human health. Terrorist groups have shown some interest in RDDs. They could use them in an attempt to disperse radioactive material to cause panic, area denial, and economic dislocation. While RDDs would be far less harmful than nuclear weapons, they are much simpler to build and the needed materials are used worldwide. Accordingly, some believe RDDs are more likely to be employed than nuclear weapons. RDDs could contaminate areas with radioactive material, increasing long-term cancer risks, but would probably kill few people promptly compared to nuclear weapons which could destroy much of a city, kill tens of thousands of people, and contaminate much larger areas with fallout. Cleanup cost after an RDD attack could range from less than a billion dollars to tens of billions of dollars, depending on area contaminated, decontamination technologies used, and level of cleanup required (Medalia, 2011, p. 2). Despite the seeming ease of launching a successful RDD attack, to date this has not been done. The reasons are necessarily speculative, but may include difficulties in handling radioactive material, lack of sufficient expertise to fabricate material into an effective weapon, a shift to smaller-scale but simpler attacks using standard weapons and explosives, and improved security. Of course, such factors cannot guarantee that no attack will occur (Medalia, 2011, p. 2).

2.3.4. Nuclear Agents

While a nuclear weapon is the most destructive of all WMD, obtaining one poses the greatest difficulty for hostile non-state actors. The key obstacle to building such a weapon is the availability of a sufficient quantity of fissile material—either plutonium or highly enriched uranium. Some experts believe that if allowed access to the necessary quantities of fissile
material, extraordinarily capable groups could build a crude nuclear weapon (Bowman, 2002, p. 4).

2.4. The CI Threat

By itself, critical infrastructure is not destructive. Only through subversion by degrading, destroying, or diverting its intended function might it become destructive. At present, the government recognizes 16 distinct sectors of critical infrastructure as enumerated in Presidential Policy Directive #21 (PPD-21) (The White House, 2013).

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Commercial Facilities</td>
<td>10. Food &amp; Agriculture</td>
</tr>
<tr>
<td>5. Dams</td>
<td>13. Information Technology</td>
</tr>
<tr>
<td>7. Emergency Services</td>
<td>15. Transportation Systems</td>
</tr>
</tbody>
</table>

Table 2-1: Critical Infrastructure Sectors

2.4.1. Chemical Plants

The potential harm to public health and the environment from a sudden release of hazardous chemicals has long concerned the US Congress. The sudden, accidental release in December 1984 of methyl isocyanate in an industrial incident at the Union Carbide plant in Bhopal, India, and the attendant loss of thousands of lives and widespread injuries spurred legislative proposals to reduce the risk of chemical accidents in the United States (Schierow,
2004, p. 1). Potential hostile acts against chemical facilities might be classified roughly into two categories: direct attacks on facilities or chemicals on site, or efforts to use business contacts, facilities, and materials (e.g., letterhead, telephones, computers, etc.) to gain access to potentially harmful materials. In either case, agents may be employees (saboteurs) or outsiders, acting alone or in collaboration with others. In the case of a direct attack, traditional or nontraditional weapons may be employed, including explosives, incendiary devices, firearms, airplanes, computer programs, or weapons of mass destruction (nuclear, radiological, chemical, or biological). A hostile agent may intend to use chemicals as weapons or to make weapons, including but not limited to explosives, incendiaries, poisons, and caustics. Access to chemicals might be gained by physically entering a facility and stealing supplies, or by using legitimate or fraudulent credentials (e.g., company stationary, order forms, computers, telephones or other resources) to order, receive, or distribute chemicals (Schierow, 2004, p. 2).

2.4.2. Commercial Facilities

About 460 skyscrapers are listed among concerns for attack among commercial facilities (The White House, 2003, p. 9). As was seen on 9/11, the collapse of the Twin Towers in New York City killed thousands of people and caused billions of dollars in damages. As places of aggregation, national symbols, and the potential for collateral damage, large facilities make lucrative targets.
2.4.3. *Communications*

The communications infrastructure is comprised of 2 billion miles of cable (The White House, 2003, p. 9) providing essential connectivity across the nation and around the globe. The central concern is the impact disrupting this network could have on all other infrastructures that depend on it. Damage or degradation of the communications network could have grave repercussions for the national economy.

2.4.4. *Critical Manufacturing*

Lean production systems based on just-in-time deliveries make manufacturers sensitive to supply disruptions. Attacks on critical manufacturing nodes could have cascading effects severely damaging the national economy.

2.4.5. *Dams*

The federal government has built hundreds of water projects, primarily dams and reservoirs for irrigation development and flood control, with municipal and industrial water use as an incidental, self-financed, project purpose. Many of these facilities are critically entwined with the nation’s overall water supply, transportation, and electricity infrastructure. The largest federal facilities were built and are managed by the Bureau of Reclamation (Reclamation) of the Department of the Interior and the U.S. Army Corps of Engineers (Corps) of the Department of Defense. Reclamation reservoirs, particularly those along the Colorado River, supply water to millions of people in southern California, Arizona, and Nevada via Reclamation and non-Reclamation aqueducts. Reclamation’s inventory of assets includes 471 dams and dikes that create 348 reservoirs with a total storage capacity of 245 million acre-feet of water. Reclamation
projects also supply water to 9 million acres of farmland and other municipal and industrial water users in the 17 western states. The Corps operates 276 navigation locks, 11,000 miles of commercial navigation channel, and approximately 1,200 projects of varying types, including 609 dams. It supplies water to thousands of cities, towns, and industries from the 9.5 million acre-feet of water stored in its 116 lakes and reservoirs throughout the country, including service to approximately 1 million residents of the District of Columbia and portions of northern Virginia. The largest Corps and Reclamation facilities also produce enormous amounts of power. For example, Hoover and Glen Canyon dams on the Colorado River represent 23% of the installed electrical capacity of the Bureau of Reclamation’s 58 power plants in the West and 7% of the total installed capacity in the Western United States. Similarly, Corps facilities and Reclamation’s Grand Coulee Dam on the Columbia River provide 43% of the total installed hydroelectric capacity in the West (25% nationwide). Still, despite its critical involvement in such projects, especially in the West, the federal government is responsible for only about 5% of the dams whose failure could result in loss of life or significant property damage. The remaining dams belong to state or local governments, utilities, and corporate or private owners. Attacks resulting in physical destruction to any of these systems could include disruption of operating or distribution system components, power or telecommunications systems, electronic control systems, and actual damage to reservoirs and pumping stations. Further, destruction of a large dam could result in catastrophic flooding and loss of life (Copeland, 2010, p. 2).
2.4.6. Defense Industrial Base

The Defense Industrial Base includes 250,000 firms in 215 distinct industries that manufacture and supply military equipment (The White House, 2003, p. 9). These too are susceptible to supply chain disruptions that could affect military readiness, or more insidiously, introduce vulnerabilities exploitable by an adversary.

2.4.7. Emergency Services

These encompass more than 87,000 tribal, state, county, and municipal First Responder jurisdictions (The White House, 2003, p. 9). Few are prepared to adequately cope with large-scale deployment of CBRN agents. The increased likelihood of catastrophic attack requires an unprecedented level of coordination and cooperation across jurisdictions. The ability of First Responders to operate together in a contaminated environment will greatly affect their capacity to save lives.

2.4.8. Energy

As was noted previously, electricity is vital to the commerce and daily functioning of United States. The modernization of the grid to accommodate today’s uses is leading to the incorporation of information processing capabilities for power system controls and operations monitoring. The “Smart Grid” is the name given to the evolving electric power network as new information technology systems and capabilities are incorporated. While these new components may add to the ability to control power flows and enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to computer-related attack since they are built around microprocessor devices whose basic functions are controlled by software.
programming (Campbell, 2011, p. 2). Industrial control systems are particularly vulnerable to cyber attack because of their intelligence and communications capabilities. Industrial control systems perform a number of functions in the electrical grid, ranging from microprocessor-based control systems which control the actuation and operation of one or more devices, to more sophisticated industrial control systems which can manage entire industrial processes or automated systems. SCADA systems are a well-known industrial control application to remotely monitor and control electric transmission system components. While cyber-intrusions into the US grid have been reported in recent years, no impairment or other damage has been publicly reported as a result of the attacks. By exploiting loopholes in cyber security, cyber attackers could breach the privacy of customer’s power usage data and access large numbers of meters, perhaps sending deliberately misleading information to the grid. This could potentially overload systems or cause grid operators to respond to false readings. However, concerns exist as to the potential damage that could result in the future from malware left behind by such intrusions or doorways created in systems which could be exploited. The revelation of the Stuxnet worm and the alleged targeting of the control systems of a nuclear power plant in Iran have raised additional concerns about the vulnerability of electric power systems worldwide (Campbell, 2011, p. 6).

2.4.9. Financial Services

Long before 9/11, analysts identified financial sector system vulnerabilities as elements of national economic security in the work of the President’s Commission on Critical Infrastructure Protection in 1996 and 1997. Financial institutions operate as intermediaries — accepting funds from various sources and making them available as loans or other investments to
those who need them. The test of their collective operational effectiveness is how efficiently the financial system as a whole allocates resources among suppliers and users of funds to produce real goods and services. America has grown far beyond a bank-centered financial economy: financial value has largely become resident on computers as data rather than physical means of payment. This element of the financial system is an area of particular vulnerability. Financial institutions face two categories of emergencies that could impair their functioning. The first is directly financial: danger of a sudden drop in the value of financial assets, whether originating domestically or elsewhere in the world, such that a global financial crisis might follow. The second is operational: failure of physical support structures that underlie the financial system. Either could disrupt the nation’s ability to supply goods and services and alter the behavior of individuals in fear of the disruption (or fear of greater disruption). They could reduce the pace of economic activity, or at an extreme, cause an actual contraction of economic activity. Financial regulators generally address the former set of problems through deposit insurance and other sources of liquidity to distressed institutions, safety and soundness regulation, and direct intervention. They address the latter, operational, set through remediation (as with the Y2K problem\textsuperscript{8}), redundancy, and other physical security. Under the worst case scenarios, the Federal Reserve (Fed) can relieve the economic effects of either set by acting as lender of last resort to supply liquidity to the financial system, employing monetary policy to expand domestic demand (as it did following the 9/11 terrorist attacks). In the Terrorism Risk Insurance Act of 2002 (TRIA), Congress expanded the Fed’s ability to act as lender of last resort to the financial and real economies. Congress may also legislate direct federal assistance to protect the financial infrastructure. It has done so to prevent troubled entities such as Chrysler, the Farm Credit System, and New York City from defaulting, thus harming their lenders, and potentially causing
failure in major parts of the financial system and the economy. Collapse of one prominent entity could evoke a contagion effect, in which sound financial institutions become viewed as weak — today’s equivalent of a bank run, in which panicked customers withdraw funds from many entities, probably causing others to fail as well (Jackson, 2003, pp. 1-2).

2.4.10. Food & Agriculture

The potential for malicious attacks against agricultural targets (agroterrorism) is increasingly recognized as a national security threat, especially after 9/11. Agroterrorism is a subset of bioterrorism, and is defined as the deliberate introduction of an animal or plant disease with the goal of generating fear, causing economic losses, and/or undermining social stability. The goal of agroterrorism is not to kill cows or plants. These are the means to the end of causing economic damage, social unrest, and loss of confidence in government. Human health could be at risk if contaminated food reaches the table or if an animal pathogen is transmissible to humans (zoonotic). While agriculture may not be the first choice of attack because it lacks the “shock factor” of more traditional targets, many analysts consider it a viable secondary target.

Agriculture has several characteristics that pose unique vulnerabilities. Farms are geographically dispersed in unsecured environments. Livestock are frequently concentrated in confined locations, and transported or commingled with other herds. Many agricultural diseases can be obtained, handled, and distributed easily. International trade in food products often is tied to disease-free status, which could be jeopardized by an attack. Many veterinarians lack experience with foreign animal diseases that are eradicated domestically but remain endemic in foreign countries (Monke, 2007, p. 2).
2.4.11. Government Facilities

The US government owns and operates some 3,000 facilities including the places where state and national representatives meet to conduct the peoples’ business (The White House, 2003, p. 9). Government facilities present an attractive target mostly for their symbolic value. While the catastrophic loss of a substantial portion of government would significantly affect the country, it would not lead to the collapse of the nation. Constitutions at all levels provide for succession of leadership, and plans for re-establishing central authority developed during the Cold War survive and are maintained to this day.

2.4.12. Healthcare & Public Health

This sector encompasses 5800 registered hospitals (The White House, 2003, p. 9). The situation here is similar to that for First Responders. The increased likelihood of catastrophic attack requires an unprecedented level of coordination and cooperation between medical facilities. And their ability to treat contaminated or contagious victims will greatly affect their capacity to save lives.

2.4.13. Information Technology

The FBI reports that cyber attacks attributed to hostile actors have largely been limited to unsophisticated efforts such as e-mail bombing of ideological foes, denial-of-service attacks, or defacing of websites. However, it says, their increasing technical competency is resulting in an emerging capability for network-based attacks. The FBI has predicted that hostile agents will either develop or hire hackers for the purpose of complementing large conventional attacks with cyber attacks. The Internet, whether accessed by a desktop computer or by the many available
handheld devices, is the medium through which a cyber attack would be delivered. However, for a targeted attack to be successful, the attackers usually require that the network itself remain more or less intact, unless the attackers assess that the perceived gains from shutting down the network entirely would offset the accompanying loss of their own communication. A future targeted cyber attack could be effective if directed against a portion of the US critical infrastructure, and if timed to amplify the effects of a simultaneous conventional physical or chemical, biological, radiological, or nuclear terrorist attack. The objectives of a cyber attack may include 1) loss of integrity, such that information could be modified improperly; 2) loss of availability, where mission-critical information systems are rendered unavailable to authorized users; 3) loss of confidentiality, where critical information is disclosed to unauthorized users; and 4) physical destruction, where information systems create actual physical harm through commands that cause deliberate malfunctions (Rollins, 2011, pp. 5-6).

2.4.14. Nuclear Reactors, Materials, & Waste

Protection of nuclear power plants from land-based assaults, deliberate aircraft crashes, and other hostile acts has been a heightened national priority 9/11 (Holt & Andrews, 2007, p. 1). The major concerns in operating a nuclear power plant are controlling the nuclear chain reaction and assuring that the reactor core does not lose its coolant and “melt down” from the heat produced by the radioactive fission products within the fuel rods. US plants are designed and built to prevent dispersal of radioactivity, in the event of an accident, by surrounding the reactor in a steel-reinforced concrete containment structure, which represents an intrinsic safety feature. Thee major accidents have taken place in power reactors, at Three Mile Island (TMI) in 1979\(^9\) at Chernobyl in the Soviet Union in 1986\(^{10}\), and the Fukushima Daiichi Nuclear Power Plant in
Japan\textsuperscript{11}. Although these accidents resulted from a combination of operator error and design flaws, TMI’s containment structure effectively prevented a major release of radioactivity from a fuel meltdown caused by the loss of coolant. In the Chernobyl accident, the reactor’s protective barriers were breached when an out-of-control nuclear reaction led to a fierce graphite fire that caused a significant part of the radioactive core to be blown into the atmosphere (Holt & Andrews, 2007, p. 4). In 2011, a combined earthquake and tsunami damaged cooling systems at the Fukushima Daiichi power plant causing reactor cores to melt and explosions to breach containment facilities, contaminating the surrounding area out to 20 km. US nuclear power plants were designed to withstand hurricanes, earthquakes, and other extreme events. But deliberate attacks by large airliners loaded with fuel, such as those that crashed into the World Trade Center and Pentagon, were not analyzed when design requirements for today’s reactors were determined. A taped interview shown September 10, 2002, on Arab TV station al-Jazeera, which contains a statement that Al Qaeda initially planned to include a nuclear plant in its 2001 attack sites, intensified concern about aircraft crashes. According to former Nuclear Regulatory Commission (NRC) Chairman Nils Diaz, NRC studies “confirm that the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low.” Even so, NRC announced in April 2007, that it would issue a proposed rule requiring license applicants for new reactors to assess potential design improvements that would improve protection against impact by large commercial aircraft. However, even if the reactor is secure from aircraft impact, the same may not be true for spent fuel. When no longer capable of sustaining a nuclear chain reaction, “spent” nuclear fuel is removed from the reactor and stored in a pool of water in the reactor building and at some sites later transferred to dry casks on the plant grounds. Because both types of storage are located outside the reactor containment
structure, particular concern has been raised about the vulnerability of spent fuel to attack by aircraft or other means. If hostile agents could breach a spent fuel pool’s concrete walls and drain the cooling water, the spent fuel’s zirconium cladding could overheat and catch fire (Holt & Andrews, 2007, p. 5). The National Academy of Sciences released a report in April 2005 that found that “successful terrorist attacks on spent fuel pools, though difficult, are possible,” and that “if an attack leads to a propagating zirconium cladding fire, it could result in the release of large amounts of radioactive material.” (Holt & Andrews, 2007, p. 6)

2.4.15. Transportation Systems

The nation’s air, land, and marine transportation systems are designed for accessibility and efficiency, two characteristics that make them highly vulnerable to attack. Aviation security has been a major focus of transportation security policy following 9/11. In the aftermath of these attacks, the 107th Congress moved quickly to pass the Aviation and Transportation Security Act (ATSA; P.L. 107-71) creating the Transportation Security Administration (TSA) and mandating a federalized workforce of security screeners to inspect airline passengers and their baggage. The act gave the TSA broad authority to assess vulnerabilities in aviation security and take steps to mitigate these risks. The July 2005 bombing of trains in London and the bombings of commuter trains and subway trains in Madrid and Moscow in 2004 highlighted the vulnerability of passenger rail systems to attacks. The volume of ridership and number of access points make it impractical to subject all rail passengers to the type of screening airline passengers undergo. A leading issue with regard to securing truck, rail, and waterborne cargo is the desire of government authorities to track a given freight shipment at a particular time. Most of the attention with regard to cargo vulnerability concerns the tracking of marine containers as they are
trucked to and from seaports. Security experts believe this is a particularly vulnerable point in the container supply chain. Hazardous materials (HAZMAT) transportation raises numerous security issues. There are issues regarding routing of hazmat through urban centers, and debate persists over the pros and cons of rerouting high hazard shipments (Peterman, 2006, p. 3).

2.4.16. Water and Wastewater Systems

Damage to or destruction of the nation’s water supply and water quality infrastructure by hostile attack or natural disaster could disrupt the delivery of vital human services, threatening public health and the environment, or possibly causing loss of life. Across the country, water infrastructure systems extend over vast areas, and ownership and operation responsibility are both public and private, but are overwhelmingly non-federal. Since the attacks, federal dam operators and local water and wastewater utilities have been under heightened security conditions and are evaluating security plans and measures. There are no federal standards or agreed-upon industry practices within the water infrastructure sector to govern readiness, response to security incidents, and recovery. Efforts to develop protocols and tools are ongoing since the 9/11 terrorist attacks (Copeland, 2010, p. 1). A fairly small number of large drinking water and wastewater utilities located primarily in urban areas (about 15% of the systems) provide water services to more than 75% of the U.S. population. Arguably, these systems represent the greatest targets of opportunity for terrorist attacks, while the larger number of small systems that each serve fewer than 10,000 persons are less likely to be perceived as key targets by those who might seek to disrupt water infrastructure systems. However, the more numerous smaller systems also tend to be less protected and, thus, are potentially more vulnerable to attack. A successful attack on even a small system could cause widespread panic, economic impacts,
and a loss of public confidence in water supply systems (Copeland, 2010, p. 2). Since 9/11, many water and wastewater utilities have switched from using chlorine gas as disinfection to alternatives which are believed to be safer, such as sodium hypochlorite or ultraviolet light. However, some consumer groups remain concerned that many wastewater utilities, including facilities that serve heavily populated areas, continue to use chlorine gas. Damage to a wastewater facility prevents water from being treated and can impact downriver water intakes. Destruction of containers that hold large amounts of chemicals at treatment plants could result in release of toxic chemical agents, such as chlorine gas, which can be deadly to humans if inhaled and, at lower doses, can burn eyes and skin and inflame the lungs (Copeland, 2010, pp. 4-5).

2.5. WMD Protection

US efforts to keep WMD out of the hands of hostile agents are collectively termed Counter-WMD (CWMD) strategy. CWMD strategy is a shared responsibility between the Department of Defense (DOD), Department of Energy (DOE), and the Department of State (DOS), in coordination with the Department of Justice (DOJ) and the Department of Homeland Security (Counterproliferation Program Review Committee, 2011, p. 3). Strategy coordination between executive departments is conducted at the highest-level in the National Security Council (NSC) (DEFENSE REPORT, 2009). The NSC has responsibility to “assess and appraise the objectives, commitments, and risks of the United States” and to “consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security” (Whittaker, Brown, Smith, & McKune, 2011, p. 25). The NSC has four statutory members (the President, Vice President, Secretary of State and Secretary of Defense) and also includes the National Security Advisor, the Secretary of the Treasury, the Director of National
Intelligence, the Chairman of the Joint Chiefs of Staff and other department secretaries, agency directors and advisors designated by the President. The NSC staff numbers 240 personnel located within the Executive Office of the President (EOP) and is managed by the President’s National Security Advisor, also known as the Assistant to the President for National Security Affairs (DEFENSE REPORT, 2009). The NSC is supported by a hierarchical collection of committees designed to screen policy matters and oversee their implementation. The Principals Committee (PC) is the “senior interagency forum for consideration of policy issues affecting national security” while the Deputies Committee (DC) “reviews and monitors the work of the NSC interagency process” and is “responsible for day-to-day crisis management.” Further management of the development and implementation of national security policies are overseen by Interagency Policy Committees (IPCs) that can be established to address specific issues (Best, 2011, pp. 23-24). At the highest levels of government, CWMD strategy is coordinated by the WMD-Terrorism Principals Committee (Whittaker, Brown, Smith, & McKune, 2011, p. 18).

Current CWMD strategy is rooted in National Security Strategy (Counterproliferation Program Review Committee, 2011, p. 3). The 2010 National Security Strategy established the objective of reversing the spread of nuclear and biological weapons, and securing nuclear materials to preclude their use by terrorist agents and rogue states (The White House, 2010, p. 23). The 2002 National Strategy to Combat Weapons of Mass Destruction provides the basic blueprint for pursuing this national security objective.

![Figure 2-1: CWMD Strategy](image-url)
(Counterproliferation Program Review Committee, 2011, p. 3). CWMD strategy is founded on three pillars: nonproliferation (NP), counterproliferation (CP), and consequence management (CM). Nonproliferation seeks to dissuade or impede both state and non-state actors from acquiring CBRN weapons. Counterproliferation seeks to develop both active and passive measures to deter and defend against the employment of CBRN weapons. Consequence management seeks to develop measures to quickly respond and recover against a domestic CBRN attack (The White House, 2002, p. 2). CWMD strategy is further refined in the 2010 Nuclear Posture Review Report and the 2009 National Strategy for Countering Biological Threats supporting the overall National Biodefense Strategy (HSPD-10/NSPD-33). These national-level documents provide strategic guidance for US government departments and agencies to develop goals and objectives, identify capability requirements, and ultimately provide material and nonmaterial solutions for CWMD (Counterproliferation Program Review Committee, 2011, p. 3).

2.5.1. Nonproliferation

Nonproliferation employs an array of international agreements, multilateral organizations, national laws, regulations, and policies to prevent the spread of dangerous weapons and technologies. The nuclear nonproliferation regime is presently the most extensive, followed by those dealing with chemical and biological weapons (Nikitin, Kerr, & Hildreth, 2010, p. 1).

The nuclear nonproliferation regime encompasses several treaties, extensive multilateral and bilateral diplomatic agreements, multilateral organizations and domestic agencies, and the domestic laws of participating countries (Commission on the Prevention of Weapons of Mass
Although the Nuclear Nonproliferation Treaty (NPT) is perhaps the most visible aspect of the nuclear nonproliferation regime, the success of nonproliferation efforts relies on the functioning of national export control laws and effective inspections conducted by the International Atomic Energy Agency (IAEA). Technical assistance in the peaceful uses of nuclear energy is also an important tool for nuclear nonproliferation (Nikitin, Kerr, & Hildreth, 2010, p. 16).

The cornerstone of international efforts to prevent biological weapons proliferation and terrorism is the 1972 Biological Weapons Convention (BWC). This treaty bans the development, production, and acquisition of biological and toxin weapons and the delivery systems specifically designed for their dispersal (Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, 2008, p. xviii). In 1969, the United States declared a unilateral end to its offensive biological weapons program (Nikitin, Kerr, & Hildreth, 2010, p. 27). But because biological activities, equipment, and technology can be used for good as well as harm, BW-related activities are exceedingly difficult to detect, rendering traditional verification measures ineffective. In addition, the globalization of the life sciences and technology has created new risks of misuse by states and terrorists (Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, 2008, p. xviii). The 2008 WMD Commission report concluded that terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon. (Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, 2008, p. xv).

Prohibitions against the use of chemical weapons date back to the International Peace Conferences that met at the Hague in 1899 and 1907; these pre-World War I prohibitions were reaffirmed in the 1919 Versailles Treaty and further expanded in the 1925 Geneva Protocol.
Controls on exports of chemical and biological agents with military applications have been regulated under the Arms Export Control Act (AECA) of 1968, and their dual-use technologies have been regulated under the Export Administration Act (EAA) of 1979 and its predecessors (Nikitin, Kerr, & Hildreth, 2010, p. 1).

A key aspect of all nonproliferation regimes is their attempt to control exports of sensitive goods and technologies through supplier agreements. These are the Nuclear Suppliers Group and the Zangger Committee for nuclear technology, and the Australia Group for chemical and biological weapons technology (Nikitin, Kerr, & Hildreth, 2010, p. 1). Although proliferation control regimes are a useful tool in preventing dangerous technology transfers, several factors undermine their effectiveness. One is the difficulty of addressing underlying motivations of countries to acquire WMD. Regional security conditions as well as the desire to compensate for other countries’ superior conventional or unconventional forces have been common motivations for WMD programs. Some countries may want WMD to dominate their adversaries. Prestige is another reason why certain countries seek WMD. Another factor working against the regimes is the steady diffusion of technology over time—much of the most significant WMD technology is 50 years old, and growing access to dual-use equipment makes it easier for countries or groups to build their own WMD production facilities from commonly available civilian equipment (Nikitin, Kerr, & Hildreth, 2010, pp. 1-2).

2.5.2. Counterproliferation

Since 9/11, significant US government interest has focused on counterproliferation programs—that is, military measures against weapons of mass destruction (Nikitin, Kerr, & Hildreth, 2010, p. 20). Defense cooperation and arms transfers to US allies can ease concerns
about security that can lead them to consider acquiring WMD, and also signal potential adversaries that acquisition or use of WMD may evoke a strong military response. US conventional and nuclear military capabilities and the threat of retaliation help deter WMD attacks against US forces, territory, and allies. One key tool of counterproliferation has been interdiction of WMD-related equipment shipments at sea, on land, and by air through the Proliferation Security Initiative (Nikitin, Kerr, & Hildreth, 2010, p. 5).

In recent years, counterproliferation capabilities were expanded to include more advanced “passive” and “active” defense measures. Passive counterproliferation tools include protective gear such as gas masks and detectors to warn of the presence of WMD. Active measures include missile defenses to protect US territory, forces, and allies; precision-guided penetrating munitions and special operation forces to attack WMD installations; and intelligence gathering and processing capabilities (Nikitin, Kerr, & Hildreth, 2010, p. 5). Although counterproliferation is a main pillar of CWMD strategy, political and technical hurdles (hidden underground bunkers, locations near civilians, etc.) tend to make counterproliferation a method of last resort, after other options have failed (Nikitin, Kerr, & Hildreth, 2010, p. 5).

2.5.3. Consequence Management

Management Agency (FEMA) is the coordinating agency within the Department of Homeland Security for federal disaster response (Federal Emergency Management Agency). The DHS guide for responding to all-hazard incidents is the National Response Framework (NRF) (Department of Homeland Security, 2008, p. 2). The NRF organizes federal response capabilities into 15 Emergency Support Functions (ESFs). ESFs align categories of resources and provide strategic objectives for their use (Department of Homeland Security, 2008, p. 29). FEMA coordinates response support across the federal government by calling up, as needed, one or more of the 15 ESFs (Department of Homeland Security, 2008, p. 57). ESF requirements for specific incidents are anticipated in NRF Incident Annexes. The NRF currently includes annexes for 1) Biological Incidents, 2) Catastrophic Incidents, 3) Food and Agriculture Incidents, 4) Mass Evacuation, 5) Nuclear/Radiological Incidents, 6) Cyber Incidents, and 7) Terrorism Incident / Law Enforcement and Investigation (Federal Emergency Management Agency).

The Catastrophic Incident Annex to the National Response Framework (NRF-CIA) establishes the context and overarching strategy for implementing and coordinating an accelerated, proactive national response to a catastrophic incident (Federal Emergency Management Agency). A catastrophic incident is characterized as any natural or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions (Department of Homeland Security, 2008, p. 42). The NRF-CIA establishes protocols to pre-identify and rapidly deploy key essential resources (e.g., medical teams, search and rescue teams, transportable shelters, medical and equipment caches, etc.) that are expected to be urgently needed to save lives and contain incidents (Department of Homeland Security, 2008, pp. CAT-1). Presumably such incidents include chemical attack as
the annex incorporates victim decontamination under ESF #8, Public Health and Medical Services (Department of Homeland Security, 2008, pp. CAT-4). Biological, radiological, and nuclear attacks are separately addressed under different annexes.

The Biological Incident Annex outlines actions, roles, and responsibilities associated with response to a human disease outbreak of known or unknown origin requiring federal assistance. This annex outlines biological incident response actions including threat assessment notification procedures, laboratory testing, joint investigative/response procedures, and activities related to recovery (Federal Emergency Management Agency). A key component of the government’s strategy is the Strategic National Stockpile (SNS). The Project BioShield Act of 2004 authorized the Secretary of Health and Human Services (HHS), among other things, to procure medical countermeasures in advance of a potential infectious disease outbreak (Gottron, Project BioShield: Purposes and Authorities, 2009, p. 1). The Centers for Disease Control and Prevention (CDC) maintains the SNS, and when requested, delivers it to state and local governments for distribution. State and local governments are responsible for developing and exercising distribution plans (Gottron & Shea, Federal Efforts to address the Threat of Bioterrorism: Selected Issues and Options for Congress, 2011, pp. 13-14).

The Nuclear/Radiological Incident Annex (NRIA) to the National Response Framework addresses federal response to a nuclear or radiological incident including: (1) inadvertent or otherwise accidental releases and (2) releases related to deliberate acts. The second category includes, but is not limited to, deliberate attacks with radiological dispersal devices (RDDs), nuclear weapons, or INDs (Department of Homeland Security, 2008, pp. NUC-2). The Department of Defense is expected to play a significant role in response to a domestic IND or RDD incident. In 2008, Secretary of Defense Robert M. Gates launched a plan to train
and equip three CBRNE Consequence Management Forces (CCMRFs) for domestic response (Le Jeune, 2010, p. 4). The first CCMRF just became operational in 2010 when plans were scrapped in favor of a new CBRN Enterprise replacing the three CCMRFs with a single Defense CBRN Response Force (DCRF). The DCRF is a 5,200 personnel federal military rapid response force composed of two force packages. The first force package is comprised of 2,100 personnel prepared to deploy within 24 hours. The second force package consists of 3,100 personnel and is prepared to deploy within 48 hours of notification. The new structure also consists of two Command and Control CBRN Consequence Response Elements (C2CRE) composed of 1,500 personnel each. The DCRF may be deployed to augment one of 10 regional Homeland Response Forces (HRFs) (United States Army) comprised of National Guardsmen. HRFs provide regional capabilities able to respond within six to 12 hours, and function alongside other National Guard assets belonging to state governors including 57 WMD civil support teams (WMD-CSTs) and 17 CBRNE enhanced response force packages (CERFPs). This new construct is considered more responsive compared to the CCMRFs, with a better match of lifesaving capabilities that allows for an improved balance between state and federal control (Le Jeune, 2010, pp. 4-5).

2.6. CI Protection

The Secretary of Homeland Security is vested by statute and Presidential directive with coordinating national efforts to secure and protect critical infrastructure and key resources, which the Department does currently through the National Protection and Programs Directorate (NPPD) (Department of Homeland Security, 2010, p. 7). Current critical infrastructure protection traces its roots back to President Clinton’s PDD-63\(^\text{12}\) which set a national goal to protect the nation’s critical infrastructure from intentional attacks, both physical and cyber by the
In December 2003, the Bush Administration released HSPD-7 establishing a critical infrastructure protection policy framework based on PDD-63 but with added emphasis on physical infrastructure. (Moteff, Critical Infrastructures: Background, Policy, and Implementation, 2011, p. 11) In June 2006, the Bush Administration released a National Infrastructure Protection Plan (NIPP) outlining the process by which the Department of Homeland Security would work with private industry to identify and protect the nation’s critical infrastructure. In 2009, the Obama Administration released an updated version of the National Infrastructure Protection Plan, and, for the most part, continues to follow the basic organizational structures and strategy of prior administrations. (Moteff, Critical Infrastructures: Background, Policy, and Implementation, 2011, p. Summary)

According to DHS, the NIPP meets the requirements set forth in HSPD-7 and provides the overarching approach for integrating the Nation’s many critical infrastructure protection initiatives into a single national effort (Department of Homeland Security, 2009, p. i). The NIPP classifies critical infrastructure into sectors and assigns a federal Sector-Specific Agency (SSA) to represent each (Department of Homeland Security, 2009, pp. 18-19). The cornerstone of the NIPP is its Risk Management Framework. The RMF is an iterative process comprised of six steps: 1) Set Goals and Objectives, 2) Identify Assets, Systems, and Networks, 3) Assess Risks, 4) Prioritize, 5) Implement Programs, and 6) Measure Effectiveness. (Department of Homeland Security, 2009, p. 27) Step Two is supported by the National Critical Infrastructure Prioritization Program (NCIPP) which conducts an annual data call to state and federal partners to identify and update an inventory of high priority infrastructure (Government Accountability Office, 2012, p. 14). Step Three is supported by the Enhanced Critical Infrastructure Protection (ECIP) program
whereby DHS Protective Security Advisors (PSAs) conduct voluntary security surveys and vulnerability assessments across the designated sectors (Government Accountability Office, 2012, pp. 3-4). Beginning in FY2009, DHS expanded its vulnerability assessments to consider collections of infrastructure, or clusters, as part of its Regional Resiliency Assessment Program (RRAP) (Moteff, Critical Infrastructures: Background, Policy, and Implementation, 2011, p. 25). Risk is assessed as a function of consequence, vulnerability, and threat, according to the formulation \( R = f(C,V,T) \) (Department of Homeland Security, 2009, p. 32). Step Four is also supported by the NCIPP which classifies infrastructure as priority level 1 or level 2 based on the consequence to the nation in terms of loss of life or economic impact (Government Accountability Office, 2012, p. 2). In Step Five, federal resources are spent in a number of ways, including agencies’ internal budgets for operations and programs, grants to states and localities, and research and development funding for universities and industry (Moteff, Critical Infrastructures: Background, Policy, and Implementation, 2011, p. 28). Working with public and private industry representatives, SSAs are responsible for applying the Risk Management Framework to develop Sector Specific Plans (SSPs) (Department of Homeland Security, 2009, p. 27) to implement risk reduction activities, with timelines and responsibilities identified, and tied to resources (Moteff, Critical Infrastructures: Background, Policy, and Implementation, 2011, p. 22).
In conjunction with the RMF, SSAs participate in a Strategic Homeland Infrastructure Risk Assessment (SHIRA) to build a National Risk Profile (NRP) (Department of Homeland Security, 2009, p. 33). Each year, the NRP identifies the highest relative risks to critical infrastructure and serves as the foundation of the National Critical Infrastructure and Key Resources Protection Annual Report (NAR) (Department of Homeland Security, 2009, p. 42). The NAR provides a summary of national infrastructure protection priorities and requirements and makes recommendations for prioritized resource allocation across the federal government (Department of Homeland Security, 2012). The NAR is submitted to the Executive Office of the President together with the DHS budget, on or before September 1st each year (Department of Homeland Security, 2009, p. 99). Funding for DHS critical infrastructure protection programs are identified within the DHS budget as Infrastructure Protection and Information Security (IPIS) programs. Funding for all CIKR protection programs across federal government are categorized by the Office of Management and Budget (OMB) as programs to “protect the American people, our critical infrastructure and key resources” (Moteff, Critical Infrastructure: The National Asset Database, 2007, pp. 33-36).

Presumably, the NIPP guides critical infrastructure protection investments towards the HSPD-8 National Preparedness Goal (NPG), (Government Accountability Office, 2012, pp. 7-8) first enunciated in 2005: “To engage federal, state, local, and tribal entities, their private and nongovernmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and economy” (Department of Homeland Security, 2005, p. 3). In 2011, HSPD-8 was replaced by PPD-8, (The White House, 2011, p. 1) and a new National Preparedness Goal formulated: “A secure and resilient Nation with capabilities
required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk” (Department of Homeland Security, 2011, p. 1). PPD-8 also directed development of a National Preparedness System (NPS) to achieve the National Preparedness Goal. The FEMA National Preparedness Directorate administers NPS (Federal Emergency Management Agency, 2012). The National Preparedness System provides an incremental development plan for achieving the National Preparedness Goal by building twenty “core capabilities” across five mission areas: prevent, protect, mitigate, respond, and recover (Department of Homeland Security, 2011, p. 2). The core capabilities were derived from a 2007 Target Capabilities List (TCL) of 37 capabilities representing a “consensus of the community” of more than 120 national associations, non-governmental organizations, and the private sector (Department of Homeland Security, 2007, p. 2). The National Preparedness System entails its own process to 1) identify and assess risk, 2) estimate current capabilities, 3) build and sustain capabilities, 4) plan to deliver capabilities, and 5) validate capabilities (Department of Homeland Security, 2011, p. 1). Steps One and Two are supported by a web-based Threat and Hazard Identification and Risk Assessment (THIRA) system (FEMA, 2012, p. 2). Step Three is supported by FEMA State and Local Grant Programs (SLGP), which in 2012 Congress was asked to repackage as the National Preparedness Grant Program (Federal Emergency Management Agency, 2012, p. 5). Step Four requires federal agencies to develop and maintain a family of plans to deliver identified capabilities. And Step Five propose validating capabilities through the FEMA administered National Exercise Program (NEP) (Department of Homeland Security, 2011, pp. 4-5).
2.7 Assessing Protection Efforts

Assessing WMD protection efforts is beyond the scope and classification of this research. For now, suffice it to say that responsible agencies maintain CBRN weapons and materials under tight security to prevent them from falling into the wrong hands. Assessing CI protection efforts is also limited by security concerns as infrastructure data collected by DHS is protected under the 2002 Homeland Security Act from disclosure even under the Freedom of Information Act. CI analysis is further complicated by the fact it has been in constant evolution since the founding of DHS, making some programs such as the National Preparedness System too new to gauge performance. However, a series of internal audits and Congressionally mandated reviews provide some insight and indicate some serious flaws, starting with the basic task of identifying critical infrastructure.

Taking an inventory of one’s assets is a standard first step for most risk management processes used to prioritize the protection of those assets (Moteff, Critical Infrastructure: The National Asset Database, 2007, p. 7). Step Two in the NIPP Risk Management framework specifies “a comprehensive inventory of assets, systems, and networks that make up the Nation’s critical infrastructure and key resources” (Department of Homeland Security, 2009, p. 29). Efforts to develop such a database trace their origin to Operation Liberty Shield, which developed a list of 160 “critical sites” as part of a national plan to protect the homeland during the 2003 US invasion of Iraq. Starting from this list, in 2003 DHS issued a data call to states yielding information on 28,368 more assets, from which it derived a Protected Measures Target List of 1,849 items judged to be in most need of additional protection from attack. In 2004 DHS issued another data call to states yielding even more information such that by 2006, DHS had compiled a list of 77,069 assets which it called the National Asset Database (NADB). Contained
within the NADB were 4,055 malls, shopping centers, and retail outlets, 224 racetracks, 539 theme parks and 163 water parks, 1,305 casinos, 234 retail stores, 514 religious meeting places, 127 gas stations, 130 libraries, 4,164 educational facilities, 217 railroad bridges, and 335 petroleum pipelines. Notably missing from the NADB were many other items from the defense industrial base, postal and shipping, banking and finance, and food and agriculture sectors. At the time, DHS officials acknowledged that only about 600 assets in the NADB were considered truly critical to the nation. The DHS Inspector General (IG) concluded that the NADB contained “many unusual or out-of-place assets whose criticality is not readily apparent, and too few assets in essential areas and may represent an incomplete picture.” The problem was attributed to the difficulty in defining critical infrastructure. Different definitions yielded widely varying results in the 2003 and 2004 data calls. As a result, additional assets of questionable national significance were added to the database (Moteff, Critical Infrastructure: The National Asset Database, 2007, pp. 1-7).

DHS responded to the IG report saying that the NADB was an inventory of assets from which critical assets could be drawn, and that it would not be possible or useful to develop a single definitive prioritized list of critical assets (Moteff, Critical Infrastructures: Background, Policy, and Implementation, 2011, p. 26). In response, Congress mandated the establishment of both a National Asset Database and a Prioritized Critical Infrastructure List (Public Law 110-53, 2007, p. Sec. 1001). Afterwards, the NADB evolved first into the Infrastructure Data Warehouse, then into the Infrastructure Information Collection Project. In 2009, the DHS IG released a follow-up report determining that while opportunities for improvement exist, DHS efforts were well conceived and maturing (Moteff, Critical Infrastructures: Background, Policy, and Implementation, 2011, pp. 26-27). Be that as it may, it does not explain what happened next.
In 2012, the Government Accountability Office (GAO) was asked to examine the DHS Enhanced Critical Infrastructure Protection program. Among their tasks was to identify how many security surveys and vulnerability analysis were being conducted on DHS identified high-priority critical infrastructure, essentially Step Three in the Risk Management Framework. According to GAO, DHS conducted about 2,800 combined surveys over a two-year period from 2009 to 2011. Of these, GAO was able to identify 179 assessments conducted on high-priority infrastructure. Because of discrepancies between lists, GAO acknowledged another 129 assessments might also have been done on high-priority infrastructure. Given the benefit of the doubt, only 11% (308) of DHS’ assessments were conducted on high-priority assets (Government Accountability Office, 2012, p. Summary). These results seem contrary to the NIPP assertion that “DHS works to ensure that appropriate vulnerability assessments for nationally critical CIKR” (Department of Homeland Security, 2009, p. 36). GAO acknowledged that DHS has little control over industry participation in the voluntary ECIP program, but it also noted that DHS 1) has not developed institutional performance goals to measure owner/operator participation, nor 2) is it positioned to assess why some high-priority asset owners and operators decline to participate (Government Accountability Office, 2012, p. 14). Granted, this problem may only be programmatic, but other reports indicate NIPP problems that are more systemic.

The NIPP identifies the risk formula $R = f(C,V,T)$ as an important component of vulnerability analysis conducted in Step Three of the Risk Management Framework. Yet, its one reported application seems more appropriate to Step Four, prioritization of assets. In 2004, the allocation of Homeland Security Grant Program (HSGP) funds raised debate when Wyoming received $28.34 per capita compared to $4.10 and $3.73 per capita allocated to New York and California respectively. The rationale behind the disbursement seemed counterintuitive. After
the 9/11 Commission weighed in on the issue, and spurred on by Congressional legislation, DHS undertook to develop a more risk-based approach for determining Homeland Security Grant Program allocations. Accordingly, the FY2007 HSGP grant guidance announced the adoption of the risk formula $R = T \times V \times C$ where $T$ is the likelihood of an attack occurring, and $V \times C$ is the relative impact of an attack. The problem with the formula as applied, however, was that DHS was unable to differentiate vulnerability across areas and states, and consequently assigned vulnerability a constant value of one (Masse, O'Neil, & Rollins, 2007, pp. 2-7). In effect, DHS treated all assets as equally vulnerable to make resource decisions about reducing vulnerability. As observed in one report: “While understandable at some level, this essentially eviscerates any interplay between vulnerability and consequence…” (Masse, O'Neil, & Rollins, 2007, p. 18).

The previous episode also indicates another systemic problem of adequate coordination within DHS. The establishment of the National Preparedness System in 2011 effectively divided infrastructure protection between the National Programs and Protection Directorate and FEMA. The NPPD is responsible for the NIPP, while FEMA is responsible for NPS. NPPD works with public and private institutions to improve infrastructure protection “inside the perimeter”, while FEMA works with state, local, and nonprofit agencies to improve infrastructure protection “outside the perimeter”. Yet, even before the NPS was established, the programs were split when authority for State and Local Grant Programs was transferred from NPPD to FEMA by the 2006 Post-Katrina Emergency Management Reform Act (Public Law 109-295, 2006, p. Sec. 505). According to a 2011 Congressional Research Service report, “it is not clear to what extent the NIPP process influences the allocation of resources to states and localities. DHS states that information contained in its list of high-priority sites is reviewed when making these grant allocation decisions. However, these grants are managed by FEMA which apparently assesses
risk independent of the NIPP. Similarly, port security grants, while managed by FEMA, are influenced largely by the review of vulnerability assessments and security plans performed by the Coast Guard.” (Moteff, Critical Infrastructures: Background, Policy, and Implementation, 2011, p. 29) In short, the NIPP is fragmented.

Perhaps the biggest indictment of DHS CI protection efforts is that the American public doesn’t know what it’s getting for its taxes. Between 2001 and 2008, DHS gave approximately $12 billion to state and local governments to prepare for and respond to terrorist attacks and other disasters. Yet, as the report notes: “A central question that may be asked is what has been the rate of return, as defined by identifiable and empirical returns on this $12 billion investment?” (Masse, O’Neil, & Rollins, 2007, p. 14). The first homeland security strategy stipulated that plans should “ensure that the taxpayers’ money is spent only in a manner that achieves specific objectives with clear performance-based measures of effectiveness” (Office of Homeland Security, 2002, p. xiii). The 2009 National Infrastructure Protection Plan affirms this commitment by stating it will “track progress toward a strategic goal by measuring beneficial results or outcomes” (Department of Homeland Security, 2009, p. 47). What’s more, it’s the law: the 1993 Government Performance and Results Act requires all federal agencies develop performance measures with respect to achieving their goals. But according to the same report, those metrics don’t exist, and nobody knows how much security was gained by the $12 billion investment. One DHS official attributed the lack of metrics to an “absence of methodology” (Masse, O’Neil, & Rollins, 2007, p. 14).
2.8. Risk Analysis

Risk analysis seeks to inform complex and difficult choices among possible measures to mitigate it (Masse, O'Neil, & Rollins, 2007, p. 16). Risk implies uncertain consequences. It is defined as the probability of loss or damage and its impact (Moteff, Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, 2007, p. 9). Accordingly, risk formulations are comprised of two elements: probability and magnitude. Combined, they provide an estimate of likelihood for a specified loss. Risk analyses may be roughly classified into two groups based on their probability component: 1) event- or threat-driven, or 2) asset-driven or asset-based methodologies. Event-driven methodologies begin with a predefined set of initiating events. Asset-driven methodologies begin with inherent susceptibilities of the system being evaluated focusing on finding and correcting vulnerabilities regardless what type of event occurred. A 2001 study indicated that 80% of risk assessment models are of the event- or threat-driven variety (McGill, 2008, pp. 15-16). The DHS risk formulation, \( f(T,V,C) \), includes both a threat and vulnerability component, but is properly classified as an event-driven methodology as \( T \) is the probability that an asset will be subjected to a particular threat or hazard (Department of Homeland Security, 2009, pp. 32-33). DHS estimates threat probabilities from attack scenarios developed through a formal elicitation process with subject matter experts based on analytic reports and past records (National Research Council of the National Academies, 2010, p. 33). There are two well-known deficiencies to this approach: 1) black-swans, and 2) insufficient historical data.

A “black swan” is a high-impact, large-magnitude attack that is a rare, hard-to-predict statistical outlier. Indeed, DHS recognizes that the use of generic attack scenarios based on today’s knowledge can leave risk analyses vulnerable to the unanticipated “never before seen”
attack scenario, a black swan, or to being behind the curve in emerging terrorist tactics and techniques (National Research Council of the National Academies, 2010, p. 59). Event-driven approaches are appropriate for studying initiating events that are well understood and whose rate of occurrence can be reliably predicted from historical data; however, they fail to consider emerging or unrecognized threats by an innovative adversary or those naturally-occurring events for which there is no human-record (McGill, 2008, pp. 15-16). In the insurance or financial sectors, the assessment of risk benefits from a rich and voluminous set of data which can be mined for patterns of historical behavior. While there are various governmental and non-governmental databases on terrorism, these data sources are relatively less robust (Masse, O'Neil, & Rollins, 2007, pp. 16-17). The National Research Council observed that: “with respect to exceedingly rare or never-observed events, the historical record is essentially nonexistent, and there is poor understanding of the sociological forces from which to develop assessment techniques.” They concluded: “Thus, it will rarely be possible to develop statistically valid estimates of attack frequencies (threat) or success probabilities (vulnerability) based on historical data” (National Research Council of the National Academies, 2010, pp. 45, 47).

2.9. Risk Management

Risk analysis supports risk management. Risk management is a continual process or cycle in which risks are identified, measured, and evaluated; countermeasures are then designed, implemented and monitored to see how they perform, with a continual feedback loop for decision-makers input to improve countermeasures and consider tradeoffs between risk acceptance and avoidance (Masse, O'Neil, & Rollins, 2007, p. 16). While the DHS Risk Management Framework ostensibly embraces these precepts, the 2010 National Research
Council report faulted the absence of a viable cost-benefit analysis capability to adequately inform resource investment decisions (National Research Council of the National Academies, 2010, p. 68). Risks can be reduced in a number of ways: by reducing threats (e.g., through eliminating or intercepting the adversary before he strikes); by reducing vulnerabilities (e.g., harden or toughen the asset to withstand the attack); or, by reducing the impact or consequences (e.g., build back-ups systems or isolate facilities from major populations). For each potential countermeasure, the benefit in risk reduction should be determined. More than one countermeasure may exist for a particular asset, or one countermeasure may reduce the risk for a number of assets. Multiple countermeasures should be assessed together to determine their net effects. The cost of each countermeasure must also be determined. Once a set of countermeasures have been assessed and characterized by their impact on risk and cost (assuming they’re feasible), priorities can be set (Moteff, Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, 2007, p. 11).

Even if a truly effective risk assessment tool were to be created to help decision makers, we are reminded that “management of risk is not elimination of risk”. Tools that attempt to quantify risk from human actions will always be inexact. “However, sound data, a well thought-out formula, and consistent application of the methodology are important when attempting to measure terrorism risk to the U.S. and systematically buy down the risk to a particular location or asset” (Masse, O'Neil, & Rollins, 2007, p. 23).
2.10. Related Research

Since 9/11, much research has been undertaken in terrorism risk modeling to help predict and subsequently deter or defeat terrorist actions. Terrorism risk modeling has been undertaken in various forms: 1) deterministic modeling, 2) stochastic games, 3) network analysis, and 4) game theory (Woo, 2003).

Deterministic modeling has long been used by the insurance industry to assess risk. For example, insurance companies calculate Probable Maximum Loss (PML) for earthquakes by 1) identifying the fault posing the greatest threat, 2) assigning the maximum credible earthquake to the fault, and 3) calculating portfolio loss assuming this size event occurs on this fault. PML estimation amounts to a series of problems in the domain of engineering, physical, chemical, and biological sciences. The same method can be applied to terrorist attacks such as evaluating the blast effect of a bomb detonation, the extent of fire from a fuel tanker explosion, the radiation fall-out from a radiological dispersal device, the spread of contagion from a smallpox outbreak, etc. These problems may still be technically complex and challenging, but the core mathematical models for blast analysis, conflagration, atmospheric dispersion, pollution transport, epidemiology, etc. are well established (Woo, 2003, p. 2). Notable is the research carried out by the RAND Center for Terrorism Risk Management Policy, which is a joint project of the RAND Institute for Civil Justice, RAND Public Safety and Justice, and Risk Management Solutions (RMS). A detailed RAND study based on the RMS model has developed an approach for making allocation decisions robust against uncertainty in model parameterization. A considerable volume of terrorism risk research has also been undertaken to support national public policy, notably at the University of Southern California’s Center for Risk and Economic Analysis of Terrorism Events (CREATE), a DHS University Center of Excellence (Woo, 2003,
Another method, Probabilistic Risk Analysis, initially developed for the purpose of assessing the safety of nuclear reactors has also been applied to terrorism risk modeling (Kardes, 2005, p. 11). Deterministic models, however, are packed with assumptions, and often resort to expert judgment to assign probabilities to terrorist attack scenarios, introducing a range of variability and subjectivity to the results. Furthermore, the deterministic approach largely removes the human behavioral component from estimation. The uncertainty introduced by assumptions is one reason why a deterministic approach can only be partially satisfactory (Woo, 2003, p. 3).

Unlike naturally occurring or accidental events, such as floods, earthquakes, or system failures, terrorism is fundamentally adversarial and adaptive (Kardes, 2005, p. 5). Randomness plays a significant part in any human conflict. But there are causal factors as well, which shape the conflict landscape, including the temporal pattern of successful attacks (Woo, 2003, p. 4). Stochastic games were first introduced to the literature by Lloyd S. Shapley in 1953. The first paper on stochastic games considers two-person zero-sum stochastic games. Two-person indicates that there are two players, and zero-sum denotes that a player’s gain is the cost to the other player. Play proceeds in stages, from one state to the other according to the transition probabilities controlled jointly by the two opponents. The game consists of states and actions associated with each player. Once in a state, each player chooses their respective action. The play then moves into another state with some probability that is determined by the actions chosen and by the state in which they are chosen. Given that opponents make their respective decisions in a given stage, a cost is incurred to each player. An opponent discounts his projected cost by a factor Beta. The usual interpretation of Beta is that decision makers consider that costs incurred in future stages have less value in the present stage. Another interpretation of Beta in homeland
security applications is the interest rate interpretation that determines the return on investment that could have been earned if the decision maker had not invested the funds in security investments (Kardes, 2005, p. 7). Similarly, the time development of the al-Qaeda conflict is a stochastic process which may be described by a controlled Markov chain model. At any moment in time, the predator (i.e., al-Qaeda) is in some specific state of attack preparedness, while the prey (i.e., USA) is in some corresponding state of defense preparedness. In a democracy, there are rigorous checks and balances imposed on law enforcement and security services. Accordingly, the counterterrorism response has to be commensurate with the terrorism threat: draconian measures (e.g., detention without trial) are only tolerable when the threat level is high. Democracies are prevented constitutionally from mounting an unlimited war on terrorism. Whatever state al-Qaeda occupies, police and security forces counter the prevailing threat with actions which aim to control terrorism. Because of these controlling counter-actions, the frequency of attack occurrence is not Poissonian, as is generally assumed for natural hazards. In mathematical terms, these counter-actions are termed Markov feedback policy (Woo, 2003, p. 4). Stochastic processes and Markov chains, however, require continual adjustment and parameter tuning to reflect observed behavior. The question of their utility, therefore, is whether they are best utilized as explanatory models rather than predictive tools.

Network analysis seeks to gain insight into the dynamics of a terrorist network by looking inside and analyzing the social network of interconnections between nodes corresponding to individual terrorists. Al-Qaeda has shown flexibility in adapting to counterterrorism action, and has been compared to the ability of a virus to mutate faster than its environment changes. This adaptation process can be simulated by evolving the social network according to a set of basic rules. Nodes communicate with one another to exchange information, financial and logistical
resources, subject to the risk that any communication might be detected by security services. Local cells are autonomous to a substantial degree, and recruit attack team members and carry out target reconnaissance. Large-scale attacks are planned, but the larger and more ambitious that an attack becomes, the higher the chance of it being compromised by one of the attack team. If any node is removed from the network, there is a chance that any node connected to it might also be named and removed. Thus the more hierarchical the network, the greater the chance of destabilization through the arrest of senior leaders (Woo, 2003, pp. 7-8). The opportunity for surveillance experts to spot a community of terrorists, and gather sufficient evidence for courtroom convictions, increases nonlinearly with the number of operatives; above a critical number, the opportunity improves dramatically. This nonlinearity emerges from analytical studies of networks using modern graph theory methods. Below the tipping point, the pattern of terrorist links may not necessarily betray much of a signature to the counterterrorism services. However, above the tipping point, a far more obvious signature may become apparent in the guise of a large connected network cluster of dots, which reveals the presence of a form of community. As exemplified by the audacious attempted replay in 2006 of the Bojinka plot\textsuperscript{16}, too many terrorists spoil the plot. Intelligence surveillance and eavesdropping of terrorist networks thus constrain the pipeline of planned attacks that logistically might otherwise seem almost boundless. For example, in the three years before the 7/7/05 London attack\textsuperscript{17}, eight plots were interdicted. Thanks to the diligence of the security services, which deter the planning of large numbers of attacks, and interdict most of those that are planned, the frequency of successful terrorist attacks is kept low. Only a small proportion of attacks succeed, and these tend to be those involving fewer operatives (Woo, 2003, pp. 5-6). Such network analysis, though, has to cope with the problem of missing data. Massive amounts of uncertainty and a dearth of data
plague network analysis (Woo, 2003, p. 8). The amount and type of data required to support network analysis comes at the cost of personal civil liberty. As happened after 9/11 and 7/7, after each major terrorist attack, democracies will respond by rebalancing the desire for liberty with the need for security (Woo, 2003, p. 6).

Unlike above methods, game theory incorporates human behavior directly into its mathematical analysis. The two fundamental precepts underlying game theory are 1) that protagonists are rational and 2) intelligent in strategic reasoning. In applying game theory to terrorism, it is important to leave behind popular notions of rationality, and to return to formal mathematical definitions of rational behavior, namely that actions are taken in accordance with a specific preference relation called “utility”. There is no requirement that a terrorist’s preference relation should involve economic advantage or financial gain. Nor is it necessary that a terrorist’s preference relation conform with those of society at large. Game theory is not restricted to any one cultural or religious perspective. The test of any mathematical risk model is its explanatory and predictive capability. Among its insights, game theory predicts that, as prime targets are hardened, rational terrorist will tend to substitute lesser softer targets. Explicit admission of this soft target strategy has since come from Khalid Sheikh Mohammed, the al-Qaeda operations chief and mastermind behind 9/11 after his capture in March 2003. As with burglar alarms, self-protection has the externality of shifting risk to one’s neighbors. Further validation of the terrorism target prioritization model is provided by analysis of the Irish Republican Army campaign in Ulster and England, and the GIA campaign in France. The success of this game theory model illustrates the future potential for quantitative terrorism model development (Woo, 2003, p. 7).
The 2010 National Research Council report recommends some of the preceding methods for potentially improving DHS risk analysis (National Research Council, 2010, p. 5), but apparently none have yet been successfully applied. The closest comparable research is a Critical Asset and Portfolio Risk Analysis for Homeland Security (CAPRA) by McGill. CAPRA is a threat-driven risk methodology comprised of six phases: 1) scenario identification, 2) consequence and severity assessment, 3) overall vulnerability assessment, 4) threat probability assessment, 5) actionable risk assessment, and 6) benefit-cost analysis (McGill, 2008, p. 44). Aside from the general difficulty of a threat-driven approach, which his research recognizes, it doesn’t seem to meet criteria for transparency or national impact that will be presented in the next chapter.

2.11. Summary

9/11 exposed the nation’s vulnerability to domestic catastrophic attack by small groups with limited means. Catastrophic damage may be inflicted within the US by employing weapons of mass destruction or subverting critical infrastructure. While DHS has adopted a risk management framework to protect critical infrastructure, an examination of their efforts reveals they are uncoordinated and uninformed by supporting metrics. A 2010 Review of the Department of Homeland Security’s Approach to Risk Analysis by the National Research Council of the National Academies determined that “DHS’s operationalization of that framework—its assessment of individual components of risk and their integration into a measure of risk—is in many cases seriously deficient and is in need of major revision” (National Research Council, 2010, p. 11).
2.12. Contributions

This chapter has provided a comprehensive review of the homeland security threat represented by critical infrastructure and weapons of mass destruction. Furthermore, it has drawn across a wide variety of sources to provide a consolidated view of what is being done to protect them. Similarly, it has provided a comprehensive analysis of DHS critical infrastructure protection programs that have been in a continual state of evolution since the department was created. The challenge of this research was in presenting a fair and balanced assessment based on authoritative sources addressing problems that remain relevant to current DHS operations.
Chapter 3. Methodology

3.1. Overview

The purpose of this research is to provide a quantitative risk methodology that will effectively and efficiently guide national investments protecting critical infrastructure and WMD agents that may be targeted to precipitate a domestic catastrophic attack. This chapter will focus on the CI component. The next chapter will examine integrating WMD into the methodology proposed here.

Recall from the previous chapter that the 2002 Homeland Security Act made critical infrastructure protection a priority mission for the Department of Homeland Security. DHS has since adopted a risk management approach to buy down risk through protective measure investments. A 2010 Review of the Department of Homeland Security’s Approach to Risk Analysis by the National Research Council of the National Academies concluded that “with the exception of risk analyses for natural disaster preparedness, the committee did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making… Moreover, it is not yet clear that DHS is on a trajectory for development of methods and capability that is sufficient to ensure reliable risk analyses other than for natural disasters” (National Research Council, 2010, pp. 2-3).

This chapter introduces an Asset Vulnerability Model (AVM) designed to work with the DHS Risk Management Framework to 1) provide a baseline estimation of critical infrastructure protection status, 2) perform cost-benefit analysis identifying optimum resource investments, and 3) offer decision support tools helping decision makers at all levels make informed choices investing scarce national resources. This chapter begins by proposing design criteria based upon analysis of current DHS efforts. It then derives a risk formulation and supporting methodology
based on the design criteria. It examines an instantiation of the model and assesses its performance. It concludes by comparing AVM with other critical infrastructure risk assessment methodologies against criteria developed in this section.

3.2. Design Criteria

The Government Performance and Results Act (GPRA) of 1993 seeks greater accountability of taxpayer expenditures by requiring federal agencies to set goals and use performance measures for management and budgeting. GPRA requires agencies to develop long-term goals and strategic plans to set specific performance goals (targets) based on the general goals, and to report annually on actual performance compared to the targets (Knezo, 1996, pp. ii, 5). DHS critical infrastructure protection programs are predicated on the risk formulation $R=f(C,V,T)$ where $C$ is the consequence that disrupting or destroying an asset will have on public health, safety, economy, and government; $V$ is the vulnerability of an asset to exploitation, disruption, or destruction, expressed as a probability it will succumb to a particular threat or hazard; and $T$ is the probability an asset will be subjected to a particular threat or hazard (Department of Homeland Security, 2009, pp. 32-33). This formula is central not only to the allocation of DHS grant programs, but to all of the department’s activities (Masse, O’Neil, & Rollins, 2007, p. 22), yet no such risk assessment is included in the annual DHS performance report accompanying its budget justification to Congress (Moteff, Critical Infrastructures: Background, Policy, and Implementation, 2011, p. 27). The GPRA requirement for accountability suggests three overarching requirements for any corresponding performance measure: 1) it must provide an indication of current status; 2) it must be able to demonstrate
incremental improvement; and 3) it must include associated costs. The choice of metric and corresponding risk formulation will be key to meeting these requirements.

3.2.1. Choosing A Metric

Insofar as measuring risk is concerned, it is essential to identify the primary drivers of risk and collect the most appropriate data to quantify those risks. Collecting and measuring data that is readily available, but not central to risk analysis yields quantifiable risk scores, but the results would be indefensible and meaningless. Accordingly, three questions frame the choice of choosing an appropriate metric: 1) what is the risk to, 2) what is the risk from, and 3) how much risk is acceptable (Masse, O'Neil, & Rollins, 2007, pp. 17-18). In answer to the first question, the 2002 Homeland Security Act establishes that the risk is to critical infrastructure, making its protection a priority mission of the Department of Homeland Security (107th United States Congress, 2002). In answer to the second question, Homeland Security Presidential Directive #7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, establishes that the risk is from attacks that could exploit or destroy infrastructure creating effects comparable to those from the use of a weapon of mass destruction (The White House, 2003). In answer to the third question we turn to earlier work in game theory.

Game theory has yielded fundamental insights into processes where indeterminate choice, either conscious or unconscious, is a critical element. Game theory derives its power by framing choice as an optimizing factor between competing agents with dependent relationships. The strength of this approach is that it reduces the many components comprising choice into a singular goal representing agents’ interests, or “utility”. Thus “winning” becomes the optimizing factor in strategy games, “profit” becomes the optimizing factor in economics, and “propagation” becomes the optimizing factor in evolution. Game theory lends understanding and prediction to
fields that were once thought unknowable and chaotic. Thus, it was not unexpected that game theory should yield valuable insights when it started to be applied to the problem of terrorism in the 1970s (Woo, 2003, p. 7).

![Figure 3-1: Sandler & Lapan Model](image)

In 1988, Todd Sandler and Harvey Lapan used game theory to examine the strategic relationship between terrorists’ choice of targets and targets’ investment decisions. They discovered that an investment decision by one target had a direct impact on the vulnerability, or likelihood of attack on the other. From this insight they concluded that 1) a coordinated defense policy among all targets is more efficient than an uncoordinated one, and 2) the optimum defense strategy is to protect all targets equally, not necessarily maximally (Sandler & Lapan, 1988, pp. 249-254). Sandler and Lapan’s findings, later confirmed and extended by the Center for Risk and Economic Analysis of Terrorism Events (CREATE) (Bier, Oliveros, & Samuelson, 2005, pp. 20-
were dependent on a particular value representing the terrorist’s probability of attack failure, which they designated as $\theta$.

Sandler and Lapan’s research suggest a metric based on $\theta$, an attacker’s probability of failure. If critical infrastructure is the designated target, then $\theta$ answers the questions what is the risk from, what is the risk to, and how much risk is acceptable. Assessing critical infrastructure in terms of its ability to withstand attack also satisfies the overarching requirement of determining current protection status. How to make this assessment is the next question.

3.2.2. Formulating Risk

In its 2010 Review of the Department of Homeland Security’s Approach to Risk Analysis, the National Research Council enumerated the many challenges to developing risk formulas amenable to homeland security in general, and critical infrastructure in particular. These challenges are summarized in Table 3-1. The first two challenges address the difficulty of reliably estimating threat as part of any formulation. The third and fourth challenges indicate the formulation should include some indication of tolerance or confidence in the results, and properly account for data dependencies within the calculation. The fifth, sixth, and seventh challenges require that the formulation be comprehensive in scope, addressing all significant consequence factors across human, temporal, and spatial dimensions. And the last three challenges stipulate that results must be meaningful to a wide variety of stakeholders in such a manner that will help them make appropriate decisions at different levels of management. The challenges listed by the National Research Council describe an ill-behaved problem whose risk calculation can fluctuate wildly depending on input that is not well understood. As with any ill-behaved problem, conditioning can help tame the calculations and provide insight through
approximate results. Accordingly, The National Research Council list of challenges suggest bounding criteria that may help condition an appropriate risk analysis.

| 1. Availability and reliability of data |
| 2. Modeling the decision making and behaviors of intelligent adversaries |
| 3. Appropriately characterizing and communicating uncertainty in models, data inputs, and results |
| 4. Methodological issues around implementing risk as a function of threats, vulnerabilities, and consequences |
| 5. Modeling cascading risks across infrastructures and sectors |
| 6. Incorporating broader social consequences |
| 7. Dealing with different perceptions and behaviors about terrorism versus natural hazards |
| 8. Providing analyses of value to multiple, distributed decision makers |
| 9. Varying levels of access to necessary information for analysis and decision making |
| 10. Developing risk analysis communication strategies for various stakeholders |

Table 3-1: Homeland Security Risk Analysis Challenges/Criteria  
(National Research Council of the National Academies, 2010, p. 51)

3.2.2.1. Asset-Driven Approach

As detailed in the previous chapter, an event-driven approach to risk analysis for malicious anthropic threats, such as that posed by the DHS risk formulation $R=f(C,V,T)$, suffers from two well-known problems: 1) statistical outliers called “black swans”, and 2) insufficient historical data to support robust statistical analysis. These shortcomings render traditional methods inadequate for accounting for human actions such as event-trees, event sequence diagrams, fault trees, and reliability block diagrams. Indeed, according to one report, “the threat element of the risk reduction formula is what differentiates terrorism from all other hazards” (Masse, O'Neil, & Rollins, 2007, p. 28). While the problem may be unique, the situation is not. In its 2010 report the National Research Council noted a similar inability for scientists to predict earthquakes. In response, local governments within affected regions have adopted an asset-driven risk approach implementing stringent seismic standards within their building codes.
The results have been palpable: “Prior to the implementation of codes, magnitude 6 earthquakes (on the Richter scale) were a major source of risk, whereas now the potential for loss given their occurrence is much less. Thus, from some decision makers’ point of view, a magnitude 6 earthquake afflicting southern California is no longer a threat despite having been so in the not too distant past” (McGill, 2008, p. 13). The observation here is that an asset-driven approach to risk analysis focusing on vulnerability can prove effective when an event-driven approach, focusing on threat, is not necessarily feasible.

3.2.2.2. Threat Localization

As noted by the National Research Council, “Terrorism risk analysis is hampered by datasets that are too sparse and targeted events that are too situation specific” (National Research Council, 2010, p. 50). By comparison, natural hazards have amassed a great deal of data and been subject to extensive statistical analysis. Even with this advantage, forecasters still can’t predict with certitude where or when a natural disaster will strike. The primary benefit of statistical analysis to hazard prediction has been in localizing their effects. Using statistical analysis, forecasters can assign reasonable probabilities that a given location will experience a given disaster over a given period. Localization is important to optimizing resource allocation by directing protection measures where they’re most needed. Thus, for example, while earthquakes are a national phenomenon, California incorporates more stringent seismic standards in its building codes than Connecticut. For similar reasons localization is also important to critical infrastructure protection: resources should be directed where they’re most needed. From this perspective, a large historical database is unnecessary. The potential target set has already been identified in HSPD-7: infrastructure that may be exploited or destroyed to create effects
comparable to those from the use of a weapon of mass destruction. Of the sixteen infrastructure sectors currently recognized by the federal government, the nine listed in Table 3-2 may be targeted to create catastrophic effects on such a scale.

<table>
<thead>
<tr>
<th>1. Chemical Plants</th>
<th>6. Information Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Dams</td>
<td>7. Nuclear Reactors, Materials, &amp; Waste</td>
</tr>
<tr>
<td>3. Energy</td>
<td>8. Transportation Systems</td>
</tr>
<tr>
<td>5. Food &amp; Agriculture</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-2: Domestic Catastrophic Threats (Infrastructure)

Not included in this list are commercial facilities, communications, critical manufacturing, defense industrial base, emergency services, government facilities, and healthcare and public health. As described in the previous chapter, commercial facilities include 460 skyscrapers, the loss of two of which proved particularly deadly on 9/11. But the collapse of the Twin Towers was due to subversion of the transportation sector turning passenger jets into guided missiles. The buildings themselves didn’t pose a catastrophic threat and had withstood a conventional bombing attack in 1993. The criticality of large buildings rests in their value as secondary targets where large numbers of people congregate. By themselves they cannot initiate catastrophic attack. The same holds true for government facilities whose attack would be mostly symbolic, and yet, as previously described, government would survive. Similarly, emergency services and healthcare and public health do not present targets for precipitating catastrophic attack. Their criticality rests with saving lives following an attack by preparing to coordinate mass rescue and care in a potentially contaminated environment. Conversely, an attack on communications, critical manufacturing, and the defense industrial base could have cascading
effects with broader consequences to the national economy and national defense. While certainly disruptive, they are unlikely to cause large scale deprivation of essential services comparable to a successful attack on the federal banking system. Their subversion is unlikely to be catastrophic, whereas a successful attack on the sectors listed in table 3-2 could be.

The essential insight of localization is that it has three significant impacts for homeland security. First, it is worth repeating, is that it overcomes prevailing concerns with developing strong statistical models similar to those for natural hazards. Second, it shifts attention from protecting the US population as the target of direct attack to the target of indirect attack. And third, as will be seen in the next chapter, it overcomes past problems with developing a definitive inventory of critical assets.

3.2.2.3. Transparency & Repeatability

In its 2010 Review of the Department of Homeland Security’s Approach to Risk Analysis, the National Research Council cautioned that a bad metric can be worse than no metric (National Research Council, 2010, p. 66). In this respect the National Research Council decried the oversimplification of the DHS risk formula reducing \( R=f(C,V,T) \) to \( R=C \times V \times T \), ignoring inherent dependencies among the terms (National Research Council, 2010, p. 46). By the same token, the National Research Council warned about undue complexity undercutting transparency, making it difficult to validate proposed formulations. The problem with developing high fidelity models is the same lack of historical data that troubles threat estimation. In the absence of hard data, assumptions must be made. The more complex the model, the more assumptions must be made, compounding potential errors. The middle ground, recommended by the National Research Council is to “ensure that vulnerability and consequence analyses for infrastructure
3.2.2.4. Qualified Results

In a similar fashion, the National Research Council expressed concern about fostering a blind faith in numbers. A metric without any qualification on its value can also lead to bad decisions. For example, there is a statistically significant difference between a measure that produces a 50% improvement compared to one with a 45% projected improvement; that is unless there’s a +/- 5% confidence in the first measure. To preclude such errors in false precision, the National Research Council recommended that “DHS should ensure that models undergo verification and validation—or sensitivity analysis at the least” (National Research Council, 2010, p. 12).

3.2.2.5. Comprehensive Scope

While endorsing the DHS risk formulation $R=f(C,V,T)$, the National Research Council contends that the DHS implementation is deficient in scope omitting key contributing factors to vulnerability. Specifically, the report states that “vulnerability is much more than physical security; it is a complete systems process consisting at least of exposure, coping capability, and longer term accommodation or adaptation” (National Research Council, 2010, p. 62). In other words, vulnerability needs to consider mitigating factors both before and after an attack; or put more colloquially, “to the left of the boom and the right of the boom”. This suggests that risk analysis draw on lessons from the Federal Emergency Management Agency (FEMA) Integrated
Emergency Management System (IEMS). IEMS was derived from the Comprehensive Emergency Management (CEM) system proposed by the National Governor’s Association in 1978. CEM was based on observations by the Disaster Research Center that both manmade and natural catastrophes placed similar response-generated demands on society. CEM consequently proposed a common framework for addressing all phases of all types of disaster. The current IEMS identifies those phases as prevent, protect, mitigate, respond, and recover (Lindell, Prater, & Perry, 2006, pp. 23-26). A comprehensive vulnerability analysis should accordingly address mitigating factors across the five phases of emergency management.

3.2.2.6. National Impact

The National Research Council also faulted deficiencies in DHS’ current assessment of consequence. “The fundamental challenge for analyzing the consequences of a terrorist event is how to measure the intangible and secondary effects. DHS’s consequence analyses tend to limit themselves to deaths, physical damage, first-order economic effects, and in some cases, injuries and illness. Other effects, such as interdependencies, business interruptions, and social and psychological ramifications, are not always modeled, yet for terrorism events these could have more impact than those consequences that are currently included” (National Research Council, 2010, p. 51). Put more succinctly, consequence needs to consider the broader effects of a disaster beyond the immediate damage, both in time and space. As homeland security concerns impacts to the nation’s welfare, it suggests that consequence should be assessed in similar terms. Currently, the federal government assesses the welfare of the nation in terms of economic vitality and individual longevity. The two key measures are Gross Domestic Product (GDP) and national mortality. In their detailed formulation by the Department of Commerce and Centers
for Disease Control and Prevention, they capture the broader effects of impacts to national welfare both in time and space. Indeed, in 2001 the gross domestic product dropped 47%\(^{22}\), and the national homicide rate increased 20%\(^{23}\), registering the impact of 9/11.

### 3.2.2.7. Applicable Results

Ultimately, the effectiveness of any risk analysis is judged by its usefulness to decision makers in managing resources. According to the National Research Council, the attributes of a good risk analysis includes the ability to 1) convey current risk levels, 2) support cost-benefit analysis, 3) demonstrate risk reduction effects across multiple assets at different levels of management, and 4) measure and track investments and improvement in overall system resiliency over time (National Research Council, 2010, pp. 68-70).

<table>
<thead>
<tr>
<th>1. Asset-Driven Approach</th>
<th>5. Comprehensive Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Transparency &amp; Repeatability</td>
<td>7. Applicable Results</td>
</tr>
<tr>
<td>4. Qualified Results</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-3: Risk Formulation Criteria

### 3.3. An Asset Vulnerability Model

An Asset Vulnerability Model is now introduced to 1) reasonably define and measure risk, 2) provide a means for measuring how developing capabilities are reducing that risk, and 3) illustrate how to identify specific capability gaps which might serve as an input for allocation of homeland security grants. AVM is comprised of 1) baseline analysis, 2) cost-benefit analysis, and 3) decision support tools. AVM analysis is predicated on a risk measure designated as Θ representing an attacker’s probability of failure based on the Sandler and Lapan value θ. The
two values differ in that the Sandler and Lapan θ represents an attacker’s perception while the AVM Θ represents the defender’s known understanding. AVM is not concerned whether or not the attacker knows the true value of Θ. The switch in perspective value was made to accommodate transparency and repeatability criteria thus reducing error margins.

3.3.1. Baseline Analysis

Baseline analysis produces a risk profile of all critical assets based on Θ. The Greek capital theta (hereafter referred to as “theta”) represents the probability of attack failure on a given asset. Theta is calculated in an asset-based risk formula (criteria 1) addressing the five phases of emergency management (criteria 2). A separate Θ is calculated for every critical infrastructure asset that may be exploited or destroyed to created WMD effects, as listed in Table 3-2 (criteria 2). The proposed risk formulation for Θ is as follows:

$$\Theta = P(\text{dis}) \times P(\text{def}) \times P(\text{den}) \times P(\text{dim}) \times \% (\text{dam})$$

(3-1)

where:

- \(P(\text{dis})\) = Probability an attack can be detected/disrupted
- \(P(\text{def})\) = Probability an attack can be defeated
- \(P(\text{den})\) = Probability a worst case disaster can be averted
- \(P(\text{dim})\) = Probability 100% survivors can be saved
- \(\% (\text{dam})\) = % decrease in economic output* % increase in mortality rate

3.3.1.1. Probability of Disrupting an Attack

\(P(\text{dis})\) corresponds to the “prevent” phase of emergency management. As noted by former Secretary Chertoff, “…our best solution is a solution that prevents a terrorist act before it
actually comes about” (Masse, O’Neil, & Rollins, 2007, p. 27). P(dis) is the probability an attack can be detected and disrupted before it is launched. P(dis) differentiates threat warning from threat prediction. Threat warning is short-term based on current indicators compared to threat prediction which is long term based on historical data. The distinction is analogous to the difference between hurricane warning and hurricane prediction, except where it is impossible to stop a hurricane, it may be possible to stop an attack. As noted by Secretary Chertoff, “a critical element in that is our early warning system, which is intelligence…” (Masse, O’Neil, & Rollins, 2007, p. 27). P(dis) may be calculated from historical intelligence data for past attempts to attack domestic critical infrastructure. The basic calculation divides the number of attempts that were thwarted by the sum of the attempts that were both thwarted and executed. The calculation should be specific to each CI sector.

3.3.1.2. Probability of Defeating an Attack

P(def) corresponds to the “protect” phase of emergency management. P(def) is the probability an attack that is launched can be defeated. This term examines the amount and type of security protecting the CI target in question. P(def) may be derived from the Protective Measure Index (PMI) assessed from security surveys and vulnerability assessments currently conducted by DHS. Trained Protective Security Advisors (PSAs) work with owners and operators to examine more than 1,500 variables covering six major components – information sharing, security management, security force, protective measures, physical security, or dependencies – as well as 42 more specific subcomponents within those categories) (Government Accountability Office, 2012, p. 9). Vulnerability analysis is predicated on about 25 attack scenarios generated for each sector. The attack scenarios are developed through a
structured process by intelligence analysts drawing on experts, previous attacks, and reporting (National Research Council, 2010, p. 33). Again, the threat estimation is not being used to predict the probability of attack but rather the type of attack in order to assess current defensive measures. While this too may be imperfect, it has the advantage of consistency (criteria 3) as survey results are turned over to the Argonne National Laboratory to produce a Protective Measures Index score ranging from 0 (low protection) to 100 (high protection) (Government Accountability Office, 2012, p. 9). The PMI is normalized for use in the AVM risk formulation. Of course it will take time to conduct vulnerability assessments on all assets making a default PMI necessary for baseline analysis. The default P(def) value may calculated from historical data by dividing the number of thwarted attacks by the total number of attacks on a particular type of asset.

3.3.1.3. Probability of Denying Success

P(den) corresponds to the “mitigate” phase of emergency management. P(den) is the probability that the worst case disaster can be averted, even if an attacker successfully breaches an asset’s security. P(den) examines the failure mode and/or redundancy built into the asset. An asset that is failsafe or redundant, as applicable, may be assigned a P(den) of 1 meaning no consequences result, that the attack was for naught. Lesser values may be assigned to P(den) using the same data and methodologies for producing the Protective Measure Index (see 3.3.1.2.). The default value should be some constant greater than zero.
3.3.1.4. Probability of Diminishing Consequences

P(dim) corresponds to the “response” phase of emergency management. P(dim) is the probability that 100% of survivors can be saved from the consequences of the worst case disaster. In 2012, FEMA deployed a web-based Threat and Hazard Identification and Risk Assessment (THIRA) system and made it a requirement for states and territories competing for funds under the Homeland Security Grant Program (FEMA, 2012). THIRA assists states and territories with examining their “core capabilities” established in the 2011 National Preparedness Goal. THIRA collects data on regional response capabilities in critical transportation, environmental response, fatality management services, mass care services, mass search and rescue operations, on-scene security and protection, operational communications, public and private services and resources, and public health and medical services (Department of Homeland Security, 2012, pp. 3-4). This database could assist in assessing regional capabilities within 72-hours of an incident, the critical window for saving lives (Federal Emergency Management Agency, 2011, p. 11). P(dim) may be calculated many different ways, but the central concept is to divide available capacity by the number of anticipated casualties. The calculation may take into account a reduction in capacity due to losses among the responding agencies due to the incident. A default value may be calculated from historical data on similar size incidents independent of cause.

3.3.1.5. Percent Damages

The %(dam) parameter simultaneously represents the “recovery” phase of emergency management and the magnitude component of the risk assessment formula. It captures the national impact on lives and the economy for incidents of both mass destruction and disruption.
(criteria 6) by tapping the extensive capabilities already invested by the federal government to collect this information. Just as important, both sets of data can be expressed as percentages, facilitating mathematical manipulation while avoiding awkward value judgments comparing the loss of lives and property.

3.3.2. Cost-Benefit Analysis

AVM baseline analysis identifies CI assets with highest risk scores. The next step is to identify protective measures expected to result in the greatest reduction of risk for any given investment. Protective measures should include actions that can prevent, deter, or mitigate a threat, reduce a vulnerability, minimize the consequences, or enable timely and efficient response and recovery (Moteff, Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, 2007, p. 17). Cost-benefit analysis finds the optimum combination of protective improvement measures proposed for each asset.

Cost-benefit analysis is conducted using $\Delta \Theta$ and $D(\Delta \Theta)$ estimations for each improvement measure. Delta theta is the estimated increase in $\Theta$ for the proposed security measure. Delta theta is provided in component form as $P(\Delta\text{dis})$, $P(\Delta\text{def})$, $P(\Delta\text{den})$, and $P(\Delta\text{dim})$. The magnitude component, $\%\text{dam}$ remains constant for $\Theta$ and $\Delta \Theta$ as it represents the worst case disaster if the asset is subverted or disrupted. An associated cost component is provided for each $\Delta \Theta$ in the form of $D(\Delta\text{dis})$, $D(\Delta\text{def})$, $D(\Delta\text{den})$, and $D(\Delta\text{dim})$. Each proposed security improvement has an associated set of paired $\Delta \Theta$ and $D(\Delta \Theta)$ data tuples. Only the $P(\Delta\text{def})$ and $P(\Delta\text{den})$ tuples are directly associated with an asset. $P(\Delta\text{dis})$ and $P(\Delta\text{dim})$ representing national and regional improvement proposals are proportionally assigned to affected assets. The given
$\Delta \Theta$ and $D(\Delta \Theta)$ values are discrete, representing specific capabilities for purchase. The choice whether to buy them or not is also discrete; there are no fractional solutions. For this reason, values are provided in tabular format as opposed to polynomial curves. The data sets associated with each improvement measure are also independent. This stipulation simplifies the estimation of $\Delta \Theta$ by eliminating dependency analysis. Estimating $\Delta \Theta$ will be sufficiently difficult using either expert analysis or computer modeling. Consistency will be key (criteria 3), suggesting that $\Delta \Theta$ should be estimated by a central source. Precision can be gradually improved by comparing estimated and actual performance data over time. Thus, each asset may have a number of tables representing corresponding improvement measures. Cost-benefit analysis evaluates each proposed measure to determine which provides the greatest return on investment. First, the combined $\Delta \Theta$ and $D(\Delta \Theta)$ is calculated for each measure according to the formulations shown in 3-2 and 3-3. Then a proportional value is calculated for each measure by dividing $\Delta \Theta$ by $D(\Delta \Theta)$. The measure with the highest proportional value representing the “biggest bang for the buck” and is nominated for that asset.

\[
\Delta \Theta = P(\Delta \text{dis}) P(\Delta \text{def}) P(\Delta \text{den}) P(\Delta \text{dim}) \times \% \text{dam} \tag{3-2}
\]

where:

\[
P(\Delta \text{dis}) = \text{Increased probability an attack can be detected/disrupted} \tag{3-2.1}
\]

\[
P(\Delta \text{def}) = \text{Increased probability an attack can be defeated} \tag{3-2.2}
\]

\[
P(\Delta \text{den}) = \text{Increased probability Worst Case Disaster can be averted} \tag{3-2.3}
\]

\[
P(\Delta \text{dim}) = \text{Increased probability 100% survivors can be saved} \tag{3-2.4}
\]

\[
\% \text{dam} = \% \text{decrease in economic output} \times \% \text{increase in mortality rate} \tag{3-2.5}
\]
\[ D(\Delta \Theta) = D(\Delta \text{dis}) + D(\Delta \text{def}) + D(\Delta \text{den}) + D(\Delta \text{dim}) \]  

(3-3)

where:

\[ D(\Delta \text{dis}) = \text{Cost of proposed national prevention measures} \]  

(3-3.1)

\[ D(\Delta \text{def}) = \text{Cost of proposed asset protection measures} \]  

(3-3.2)

\[ D(\Delta \text{den}) = \text{Cost of proposed asset mitigation measures} \]  

(3-3.3)

\[ D(\Delta \text{dim}) = \text{Cost of proposed regional response measures} \]  

(3-3.4)

3.3.2.1. Prevention Measures

Prevention measures are national intelligence capabilities for detecting and disrupting planned attacks on CI assets. Each proposed measure must be assessed for its estimated risk reduction value \( P(\Delta \text{dis}) \) and cost \( D(\Delta \text{dis}) \).

3.3.2.2. Protection Measures

Protection measures are asset-specific capabilities enhancing the defenses of WMD and CI assets to withstand attack. The Protective Measure Index currently calculated by Argonne Laboratories based on DHS security surveys and vulnerability analyses offers an available method for estimating \( P(\Delta \text{def}) \). The PMI as currently calculated is presented in a “dashboard” depicting an asset’s overall protective measure score, the score for each of the six major components, the mean protective measures score and major component scores for all like assets in the sector. The dashboard is an interactive program that allows asset owners/operators to see the effect of making security upgrades to its asset. For example, if the dashboard shows a low score for physical security relative to those of other like assets, the owner/operator can add data on perimeter fencing to see how adding or improving a fence would increase an asset’s score.
In this manner a P(Δdef) value can be derived from the PMI, and associated costs D(Δdef) identified.

3.3.2.3. *Mitigation Measures*

Mitigation measures are asset-specific capabilities reducing the likelihood of catastrophic failure if an attacker breaches their security. For example, nuclear weapons employ Permissive Action Links that prevent their detonation except as authorized by the President (Bellovin, 2005). Similarly, passive safety systems for nuclear reactors, those relying only on natural forces such as gravity, buoyancy, convection, and conduction, could prevent core meltdowns such as what happened to the Fukushima Daiichi power plant in Japan. Each proposed measure must be assessed for its estimated risk reduction value P(Δden) and cost D(Δden).

3.3.2.4. *Response Measures*

Response measures are regional capabilities of First Responders for reducing the consequences of a worst case disaster. Perhaps a similar technique for assessing PMI can be developed to estimate P(Δdim) using THIRA data.

3.3.2.5. *Recovery Measures*

AVM does not analyze recovery measures by virtue of the fact that estimated recovery costs are already aggregated into the magnitude component, % (dam) of the ΔΘ formulation in 3-2.
3.3.3. Decision Support Tools

Decision support tools in the form of spreadsheets graphically portray the results of baseline and cost-benefit analyses and facilitate easy manipulation to present the information in a manner most meaningful to a decision maker. Figure 3-2.1 portrays the unfiltered results from baseline analysis using simulated data. Various spreadsheet tabs present different views of the same information. For example, Figure 3-2.2 shows the baseline data sorted by Θ, identifying the most protected to the least protected assets. Alternatively, Figure 3-2.3 sorts baseline data by asset type, depicting the relative protection of assets within the same sector. Baseline data may also be sorted by location, as in Figure 3-2.4, indicating the relative protection of assets within a given geographic region. Other views may be created as desired. The significance of this tool is that it provides decision makers a snapshot of the current homeland security profile in a manner that is most useful to them.

Similarly, the results from cost-benefit analysis can be graphically portrayed to assist decision makers in allocating resources. If the main concern is getting the most protection for a given investment, then a decision maker may refer to Figure 3-3.1 which sorts proposed improvements from largest to smallest gains in Θ. If the main concern is cost, a decision maker may refer to Figure 3-3.2 which sorts proposed improvement from smallest to largest cost. If the decision maker wishes to concentrate on protecting a particular sector, then improvements can be sorted by asset type as in Figure 3-3.3. If the decision maker wishes to concentrate on protecting a particular region, then improvements can be sorted by asset location as in Figure 3-3.4. The significance of this tool is that it can inform resource allocation decision based on any number of different homeland security strategies.
Figure 3-2.1: Unfiltered AVM Baseline Analysis Depicting Current Homeland Security Risk Profile

Figure 3-2.2: Baseline AVM Data Sorted by Theta Identifying Assets from Least to Most Vulnerable

Figure 3-2.3: Baseline AVM Data Sorted by Asset Type Identifying Vulnerabilities by Infrastructure Sector

Figure 3-2.4: Baseline AVM Data Sorted by Asset Location Identifying Vulnerabilities by Region
Figure 3.1: Results from AVM Cost-Benefit Analysis identifying optimum improvements in order of benefit (largest to smallest)

Figure 3.2: Results from AVM Cost-Benefit Analysis identifying optimum improvements by cost

Figure 3.3: Results from AVM Cost-Benefit Analysis identifying optimum improvements by asset type

Figure 3.4: Results from AVM Cost-Benefit Analysis identifying optimum improvement by region
3.4. Model Instantiation

As indicated in the previous chapter, critical infrastructure data collected by DHS is protected by the 2002 Homeland Security Act which makes it exempt from release even under the Freedom of Information Act (DHS even refused my request to see an unclassified guide for conducting risk assessments despite the fact I have a government security clearance). As a result, program models for AVM baseline analysis, cost benefit analysis, and decision support tools were developed using simulated data.

Program models developed in support of this research were created in the C programming language using Microsoft Visual C++ 2010 Express. Each program was built as a Win32 Console Application compatible with the Windows 7 operating system. Executable files are launched from the Windows Command Prompt by typing the name of the file plus any accompanying arguments. Where indicated, output files were generated in Comma Delimited Format (CDF). The CDF format accommodated easy data upload into corresponding Microsoft Excel 2010 spreadsheets. Excel spreadsheets were used to format, display, and analyze program data. A significantly large data set would warrant a database. Microsoft Access 2010 proved too limited for this research and was abandoned in favor of Microsoft Excel. Excel seemed an appropriate choice for a proposed business application. The list of program models is identified in Table 3-4.
### Table 3-4: List of Program Models

<table>
<thead>
<tr>
<th>Function</th>
<th>Type</th>
<th>File Name</th>
<th>Arguments/Inputs</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Generator/Baseline Analysis</td>
<td>C Program</td>
<td>BAM.c</td>
<td>(1) # of assets to generate (2) Output file name (CDF)</td>
<td>P-1</td>
</tr>
<tr>
<td>Baseline Decision Support Tool</td>
<td>Spreadsheet</td>
<td>Theta1.xls</td>
<td>Formats and analyzes output from BAM</td>
<td>P-2</td>
</tr>
<tr>
<td>Protective Measures Generator</td>
<td>C Program</td>
<td>PIM.c</td>
<td>(1) Input from Test20b (2) Output file name</td>
<td>P-3</td>
</tr>
<tr>
<td>Cost-Benefit Analysis Program</td>
<td>C Program</td>
<td>CBA.c</td>
<td>(1) Input from PIM (2) Output file name (CDF)</td>
<td>P-4</td>
</tr>
<tr>
<td>CBA Decision Support Tool</td>
<td>Spreadsheet</td>
<td>Theta2.xls</td>
<td>Formats and analyzes output from CBA</td>
<td>P-5</td>
</tr>
<tr>
<td>Sensitivity Analysis Generator</td>
<td>C Program</td>
<td>Test23e.c</td>
<td>(1) Input from CBA (2) Output file name (CDF)</td>
<td>P-6</td>
</tr>
<tr>
<td>Sensitivity Analysis Evaluator</td>
<td>Spreadsheet</td>
<td>Theta3.xls</td>
<td>Formats and analyzes output from Test23e</td>
<td>P-7</td>
</tr>
</tbody>
</table>

3.4.1. Baseline Analysis

Baseline analysis calculated $\Theta$ on a list of simulated assets generated by a Baseline Asset Model (BAM) (P-1). This program generated a CDF file of asset records with bounded random values assigned as shown in Table 3-5. BAM was used to generate a sample list of 1,000 assets and baseline $\Theta$ values as shown in Figure 3-3. The output file with sample data was named assets.txt.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Range</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Asset Unique Identifier</td>
<td>1 - n</td>
<td>Sequential order asset generated.</td>
</tr>
<tr>
<td>Type</td>
<td>Asset Type</td>
<td>1-13</td>
<td>Type of identifier.</td>
</tr>
<tr>
<td>Location</td>
<td>Asset Location</td>
<td>1-50</td>
<td>Location identifier.</td>
</tr>
<tr>
<td>P(dis)</td>
<td>P(Disrupt Attack)</td>
<td>.001-.01</td>
<td>National intelligence efforts.</td>
</tr>
<tr>
<td>P(def)</td>
<td>P(Defeat Attack)</td>
<td>.001-.70</td>
<td>Asset on-site security.</td>
</tr>
<tr>
<td>P(den)</td>
<td>P(Mitigate Effects)</td>
<td>.001-.10</td>
<td>Asset fault mitigation measures.</td>
</tr>
<tr>
<td>P(dim)</td>
<td>P(Diminish Effects)</td>
<td>.001-.50</td>
<td>Regional response capabilities.</td>
</tr>
<tr>
<td>% (dam)</td>
<td>% (Damages)</td>
<td>.001-.01</td>
<td>Economic &amp; mortality impact.</td>
</tr>
<tr>
<td>Theta</td>
<td>P(Attack Failure)</td>
<td>.001-1.0</td>
<td>Product of above values.</td>
</tr>
</tbody>
</table>

Table 3-5: Asset Record Values and Bounds for Simulated Baseline Analysis
ID, Type, Location, P(dis), P(def), P(den), P(dim), % (dam), Θ
1, 3, 9, 0.001848, 0.443307, 0.060176, 0.238462, 0.005561, 6.535791E-008
2, 7, 17, 0.005834, 0.463551, 0.083017, 0.105515, 0.008981, 2.127581E-007
3, 8, 37, 0.004957, 0.369710, 0.014895, 0.215984, 0.007050, 4.156483E-008
4, 3, 45, 0.001848, 0.144503, 0.091580, 0.079733, 0.004445, 8.666376E-009
5, 2, 15, 0.006196, 0.676620, 0.096093, 0.022168, 0.004093, 3.655105E-008
6, 3, 50, 0.001848, 0.194293, 0.062517, 0.445405, 0.003918, 3.916215E-008
7, 9, 2, 0.0001534, 0.402668, 0.016799, 0.244051, 0.001928, 4.882477E-009
8, 8, 39, 0.004957, 0.519613, 0.039404, 0.238462, 0.008510, 2.059483E-007
9, 11, 12, 0.008182, 0.668769, 0.012261, 0.254117, 0.006944, 8.465554E-008
... 

Figure 3-3: BAM Sample Output / Baseline Data + Θ Calculation

3.4.2. Baseline Decision Support Tool

Spreadsheet Thetal (P-2) formats and displays asset records generated by the baseline analysis program BAM (P-1). Thetal can import the CDF output from BAM. Data is imported to the Input Data tab and automatically displayed in a bar graph (Figure 3-2.1) indicating current theta values for each asset in the order they’re imported from the input file (corresponding to the order they were generated in BAM). The data is automatically copied to three subsequent tabs: 1) Sort by Theta, 2) Sort by Type, and 3) Sort by Location. Each tab has its own bar graph displaying asset data as indicated (Figures 3-2.2 to 3-2.4). Each tab also displays average Θ calculated across the aggregate data. Conceptually, Thetal depicts the nation’s ability to contend with a domestic catastrophic attack, simultaneously identifying areas of potential strength and weakness. This spreadsheet provides decision makers a snapshot and various views of the current protection levels across all critical assets.
3.4.3. Protective Measures Generator

A Protective Improvement Model (PIM) (P-3) generates simulated results from collecting data on proposed asset protection measures. Protection measures are represented by two values, \( \Delta \Theta \) and \( D(\Delta \Theta) \) indicating the expected gain in protection (i.e., increased probability of attack failure) and its associated cost. As expressed, \( \Delta \Theta \) is a relative value representing an increase over the current \( \Theta \) assigned to the asset being examined. Delta-theta is a randomly generated value between \( \Theta \) and an arbitrary maximum \( \Theta \) value indicated in Table 3-5. Associated costs were independently generated with a random value between 10 and 10,000. The cost range was chosen to provide values with relatively differing magnitudes, and do not represent actual expected values.

Random tuples of \( \Delta \Theta \) and \( D(\Delta \Theta) \) may be generated for each protection area representing \( P(\Delta \text{dis}) \), \( P(\Delta \text{def}) \), \( P(\Delta \text{den}) \), and \( P(\Delta \text{dim}) \). No more than ten tuples are generated for each area, an arbitrary limit representing real-world constraints on collecting such data. Similarly, some areas are randomly selected to receive no data at all, indicating that no protection measures are proposed in this round of analysis (this does not preclude values from being added during some later iteration). Indeed, some assets are randomly assigned no values whatsoever indicating they have no proposed protection improvements at this time. PIM allows the user to specify what percentage of records will receive no protection improvement data.

Generated tuples are independent of each other and output in no particular order. Data independence is important because it relieves data collectors from performing dependency analysis on proposed protective measures. This presents a significant complication that may not be viable and introduce another source for approximation errors.
No data is generated for \( \% \text{dam} \). This value is constant representing worst case damages from a successful attack on the given asset. \( P(\Delta \text{dis}) \) and \( P(\Delta \text{dim}) \) are also treated as special cases. \( P(\Delta \text{dis}) \) represents a national capability related to asset type. \( P(\Delta \text{dim}) \) represents a regional capability related to asset location. Consequently, \( P(\Delta \text{dis}) \) and \( P(\Delta \text{dim}) \) values are the same across all assets with similar types and locations. This treatment presented a particular problem for the overall methodology regarding \( P(\Delta \text{dis}) \) and \( P(\Delta \text{dim}) \) costs. If \( P(\Delta \text{dis}) \) represents a national capability, that cost is absorbed once and should not be counted across multiple assets. This creates a problem, however, in assessing an individual asset’s \( \Theta \) value for comparison against other assets. While a number of alternatives presented themselves, the chosen solution was to assign each asset a fractional proportion of the \( P(\Delta \text{dis}) \) cost value. The same was done for \( P(\Delta \text{dim}) \). To accommodate these calculations required a prescreening of the input file to conduct a tally on the number of assets with similar types and locations.

The input to PIM was a CDF file of asset records named assets.txt. The output from PIM was a data file of assets and associated \( \Delta \Theta \) and \( D(\Delta \Theta) \) cost tuples as shown in Figure 3-4. The output file was named dtheta.dat.

3.4.4 Cost-Benefit Analysis

The Cost-Benefit Analysis (CBA) (P-4) model takes simulated protective improvement data and finds the optimum cost combination of protective improvements across the five areas of protection for each asset. Finding the optimum combination begins by computing a proportional value for all \( \Delta \Theta \) and \( D(\Delta \Theta) \) data tuples across the four improvement areas \( P(\Delta \text{dis}) \), \( P(\Delta \text{def}) \), \( P(\Delta \text{den}) \), and \( P(\Delta \text{dim}) \) (remember, \( \% \text{dam} \) remains constant). The proportional value represents the relative cost benefit of each proposed protective measure. The larger the proportional value
7 3 10 0.0097 0.6276 0.0831 0.2911 0.0065 9.559908E-007
0
0
0
4
0.157590 47.652172
0.149352 149.782608
0.134496 137.260864
0.029189 280.913055
8 10 44 0.0067 0.4166 0.0329 0.0419 0.0022 8.515869E-009
4
0.002590 49.253166
0.002978 35.658226
0.002252 72.000000
0.003243 47.189873
5
0.006989 5119.000000
0.115040 1167.000000
0.206759 7875.000000
0.183602 6985.000000
0.205098 2542.000000
1
0.002338 4760.000000
4
0.063407 126.666664
0.272673 329.500000
0.339366 21.611111
0.396607 117.666664
...
11 10 1 0.0067 0.1682 0.0705 0.3004 0.0016 3.769868E-008
4
0.002590 49.253166
0.002978 35.658226
0.002252 72.000000
0.003243 47.189873
0
0
0
0
...

Figure 3-4: PIM Sample Output / Simulated Asset Protective Measures Data
the greater the cost/benefit. The ΔΘ and D(ΔΘ) tuple with the highest proportional value is selected from each protection area. Protection areas with no corresponding data have no corresponding improvement. Their ΔΘ and D(ΔΘ) are zero. The selected ΔΘs are added to the asset’s previous component values to produce new P(dis), P(def), P(den), and P(dim) values. A new Θ is then computed as the product of P(dis) * P(def) * P(den) * P(dim) * %(%(dam)). The combined ΔΘ is computed by subtracting the previous Θ (theta prime) from the new Θ. The results and supporting data are written to a CDF output file. The file output was named otheta.txt.

This program was originally conceived to input improvement/cost data (ΔΘ & D(ΔΘ)) in the form of polynomial equations representing cost curves, and to find the optimum combination using polynomial interpolation. It quickly became apparent, however, that this method produced significant fluctuations due to the resolution of the polynomial approximations, and was therefore unsuitable for performing meaningful comparisons. Polynomial interpolation was thus discarded in favor of linear interpolation to improve fidelity of the results. The problem with any interpolation method, though, is that it assumes costs are continuous and can be divisible. This does not necessarily correspond with reality. You can’t walk onto a car lot and purchase 1.5 automobiles. Consequently, it was decided to treat costs as discrete values. Based on the previous work, it was assumed the data would still be provided in terms of increasing benefits Θ and costs D(Θ). Interpolation was replaced by permutation on all data tuples for a given asset to find the optimum combination of improvement/costs. It was later realized that producing cost tables in increasing order of Θ and D(Θ) placed a significant burden on data collection. Specifically, each proposed protection measure would have to be assessed against every other in its category to determine a dependent Θ value. This requirement would be particularly difficult
for protection measures offered by competing contractors, and introduce an additional
opportunity for approximation errors. Consequently it was decided to replace dependent tuples
of Θ and D(Θ) with independent tuples of ΔΘ and D(ΔΘ). This change also facilitated
simplification of the current analysis model to only seek the highest proportional value within
each protection area.

3.4.5. CBA Decision Support Tool

The results from cost-benefit analysis are presented in spreadsheet Theta2 (P-5). This
spreadsheet formats and displays asset records generated by program CBA (P-4). Theta2 is
similar to Theta1 in that data is imported to the Input Data tab and automatically copied to other
worksheets to format and display in various ways. Input data was imported from otheta.txt.
Each graph displays current Θ for every asset as the sum of the original Θ (theta prime) and ΔΘ.
Each graph displays the information differently based upon the primary sort field: 1) Sort by
Theta Prime, 2) Sort by Theta, 3) Sort by Delta Theta, 4) Sort by Cost, 5) Sort by Location (See
Figures 3-3.1 to 3-3.4). Each graph provides a different profile that a decision maker may find
useful in helping select protection measures for implementation. Sort by Theta Prime shows the
relationship of proposed protection measures against the current protection profile. Sort by
Theta demonstrates how full implementation can change the current protection profile. Sort by
Delta Theta indicates which protection measures provide the greatest protection improvement,
independent of cost. Sort by Cost identifies protection measures solely based on cost, and may
be a politically viable method for ensuring the greatest distribution of federal protection funds.
Sort by Type may help direct protection efforts towards sectors most in need. And Sort by
Location may help direct protection efforts towards regions most in need.
A cumulative cost total of protection measures is presented in corresponding sort order next to each graph. Conceptually, a decision maker can look down the column and draw a line representing a budget ceiling. Every measure above the line would be a candidate for implementation. Ultimately it remains for Congress to decide what protection measures will be implemented. However, for the first time, DHS will be able to demonstrate how much protection is currently available, how much more can be gained, and how the nation will benefit from the investment.

3.5. Sensitivity Analysis

Two measures of risk importance are identified which are useful in characterizing the risk properties and in aiding decision making. The two risk measures are termed the “risk achievement worth” and the “risk reduction worth”. The risk achievement worth of a feature such as a safety system is the worth of the feature in achieving the present level of risk. The risk reduction worth of the feature is the worth of the feature in further reducing the risk. To maintain the present level of risk, the features having the highest risk achievement worths will be of most interest. To reduce the risk, the features having the highest risk reduction worths will be of most interest. The two risk worth measures thus complement one another with regard to their characterization of what is important to risk (Vesely, Davis, & Denning, 1986, p. 1).
To measure the worth of a feature in reducing the present risk, a logical approach is to “optimize” the feature and then determine how much the risk has been decreased. Thus, the risk reduction worth is formally defined to be the decrease in risk if the feature were assumed to be optimized for were assumed to be made perfectly reliable. Risk reduction worth $D_i$ may be measured as either a ratio or an interval (Vesely, Davis, & Denning, 1986, p. 5):

$$D_i = \frac{R_0}{R_i} \quad \text{or}$$

$$D_i = R_0 - R_i$$

where:

$R_0 = \text{Present risk level.}$

$R_i = \text{Decreased risk level}$

The risk achievement worth and risk reduction worth are included in the broad class of importance measures defined by Engelbrecht-Wiggins and Strip. Another generally applied
importance measure is the factional contribution of i to the risk, or the Fussell-Vesly measure of importance, I_i, which can be expressed as (Vesely, Davis, & Denning, 1986, p. 7):

\[ I_i = \frac{R_0 - R_i}{R_0} \quad (3-6) \]

Equation 3-6 expresses the fractional risk reduction worth. This may be modified to derive a simple expression of determining sensitivity, S:

\[ S_i = \frac{1}{p} \frac{\Delta_p R_i}{R} \quad (3-7) \]

where:

\[ \Delta_p R_i = R_0 - R_i = \text{Change in the representative value of risk due to a favorable percentage change } p \text{ in the value of the } i\text{-th risk contributor.} \]

\[ \text{And } R = R_0 \]

Equation 3-7 yields the ratio of fractional reduction in risk due to a fixed percentage change in the value of each risk contributor, which is a generalization of the risk reduction worth importance measure (McGill, 2008, p. 84). Equation 4-4 can be rewritten in terms of Θ thus:

\[ S_i = \frac{1}{p} \frac{1 - \theta - \Delta \theta}{1 - \theta} \quad (3-8) \]

Equation 3-8 provides a relative measure of Θ sensitivity due to changes in risk contributors P(Δdis), P(Δdef), P(Δden), P(Δdim), and %Δdam). The higher the value of S, the greater the sensitivity.

3.5.1. Sensitivity Analysis Data Generator

Data for sensitivity analysis was generated by program Test23e listed in table 3-4 (P-6). At the heart of the program is a copy of the dtheta cost-benefit analysis from CBA. This
program segment is wrapped within a loop that controls how many runs are conducted on the model as specified by the user. The purpose of conducting multiple runs is to average out statistical deviations in the results. The results of interest are average $\Theta$ and average $\Delta \Theta$ as they are affected by controlled deviations to $P(\Delta \text{dis})$, $P(\Delta \text{def})$, $P(\Delta \text{den})$, and $P(\Delta \text{dim})$. Deviations are controlled by an outer loop which starts at 0% deviation and steps up to 100% deviation by 10% increments. The user may select which parameters and what percentage of them are deviated (i.e., “coverage”). The program semi-randomly picks which points to deviate within the given range. So, for example, if a user specifies 100 runs with deviations to 10% of $P(\Delta \text{dis})$ points, Test23e will start by calculating the average $\Theta$ and $\Delta \Theta$ resulting from 100 runs with 0% deviation to 10% of semi-randomly selected $P(\Delta \text{dis})$ values, and step next to find average $\Theta$ and $\Delta \Theta$ resulting from 100 runs with 10% deviation to 10% of semi-randomly selected $P(\Delta \text{dis})$ values, and continue to step upward to 100% deviation to 10% of semi-randomly selected $P(\Delta \text{dis})$ values averaged over 100 runs. The results from each step are printed to a CDF file, in this case s1.txt. Test23e operates on the same input as CBA, in this case dtheta.dat.

3.5.2. Sensitivity Analysis Data Evaluator

Spreadsheet Theta3 listed in table 3-4 (P-7) accepts formatted input from Test23e and graphs the results from corresponding sensitivity analysis. Theta3 conducts two separate sensitivity tests: 1) run sensitivity and 2) data sensitivity.

Run sensitivity compares average $\Delta \Theta$ values resulting from 10, 100, and 1,000 runs respectively. Sensitivity data was generated by executing Test23e fifteen times, once for each protection parameter ($P(\Delta \text{dis})$, $P(\Delta \text{def})$, $P(\Delta \text{den})$, $P(\Delta \text{dim})$, and $\%(\Delta \text{dam})$) running 10, 100, and
1000 times respectively. The resulting $\Delta \Theta$ averages are displayed in a bar graph for each set of runs.

Data sensitivity calculates the Risk Reduction Worth of $\Theta$ and $\Delta \Theta$ resulting from increasing deviation coverage. Sensitivity data was generated by executing Test23e fifty times, once for each protection parameter running 100 times with 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, and 100% coverage respectively. The number of runs was set at 100 because the previous run sensitivity indicated no difference in average $\Theta$ and $\Delta \Theta$ values over 100 runs compared to 1000 runs. The resulting Risk Reduction Worth based on increasing deviation is displayed in an area chart for each parameter and all combined parameters.

3.5.3. Sensitivity Analysis Results

Sensitivity analysis was conducted on a simulated set of data representing 1,000 assets with proposed protection $\Delta \Theta$ and cost $D(\Delta \Theta)$ improvements. Cost-benefit analysis was conducted to find the optimum combination of new measures and calculate corresponding $\Theta$ ($\Theta'$) and $\Delta \Theta$ values resulting from their implementation. The results were averaged over 1,000 executions, each examining a different parameter as it was incrementally deviated 10% from 0% to 100%. The combined results are shown in figure 3-6.
As might be expected, the analysis indicates a greater sensitivity to smaller deviations as these affect a greater proportion of the remaining risk. Figure 3-6 also indicates that the model is fairly stable as the results from independent analysis of $P(\Delta\text{dis})$, $P(\Delta\text{def})$, $P(\Delta\text{den})$, $P(\Delta\text{dim})$, and $\%(\Delta\text{dam})$ almost perfectly overlap. This holds true even when deviations are made to less than 100% of the parameters. This stability may be attributed to the fact that $p$, the percent deviation is a much greater magnitude (x5) than $\Theta$ and $\Delta\Theta$. Even so, removing this factor does not reveal any fluctuations as shown in figure 3-7.
Yet another view may be more informative. Figure 3-8 shows the percent change in $\Delta \Theta$ as the result of parameter deviations the same as previously. From this chart it becomes apparent that the $\%$(dam) parameter is susceptible to the greatest amount of change. This is because $\%$(dam) is a constant. Any change in this value essentially indicates that the asset was replaced by something else. In effect, it is a new asset. Interestingly, this suggests that the greatest security gains may be made by replacing current assets with ones with smaller damage profiles. Perhaps this is something to be investigated later. By the same token, the remaining parameters, $P$(dis), $P$(def), $P$(den), and $P$(dim) don’t exhibit as a great a change because deviations were enacted on their $\Delta \Theta$ improvements, not their total $\Theta$ value as was the case with $\%$(dis). The slight variations among the remaining parameters may be attributed to arbitrary limits placed on
their maximum values. For example, \( P(\text{def}) \) and \( P(\text{dis}) \) were assigned maximum values of 0.70 and 0.10 respectively, assuming a greater chance of defeating an attack-in-progress through improved site security measures compared to developing intelligence and thwarting an attack before it occurs. These assumptions are an artifact of the simulated data and are not necessarily expected to manifest themselves in real data. Otherwise, the parameters are well behaved in that they demonstrate a linear relationship between input and output. Small changes are unlikely to produce large results.

![Figure 3-8: Percent Change in \( \Delta \Theta \).](image)
3.6. Model Comparisons

By one estimate there are more than 250 proposed risk assessment methodologies for critical infrastructure alone (Lewis T. G., Darken, Mackin, & Dudenhoeffer, 2012, p. 4). A 2006 survey identified 30 CI models specializing in interdependency analysis (Pederson, Dudenhoeffer, Hartley, & Permann, 2006). A 2012 survey identified 21 CI models for informing strategic decisions (Giannopoulos, Filippini, & Schimmer, 2012). Together, the two surveys identified 41 distinct models representing the “state-of-the-art” in CI risk modeling (Table 3-6).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Athena</td>
<td>12. COUNTERACT</td>
<td>22. KM&amp;V</td>
<td>32. PFNAM</td>
<td></td>
</tr>
<tr>
<td>3. BIRR</td>
<td>13. DECRIS</td>
<td>23. MDM</td>
<td>33. RAMCAP-Plus</td>
<td></td>
</tr>
<tr>
<td>4. BMI</td>
<td>14. DEW</td>
<td>24. MIN</td>
<td>34. RMCIS</td>
<td></td>
</tr>
<tr>
<td>5. CARVER2™</td>
<td>15. EMCAs</td>
<td>25. MUNICIPAL</td>
<td>35. RMF</td>
<td></td>
</tr>
<tr>
<td>7. CIP</td>
<td>17. FAIT</td>
<td>27. NEMO</td>
<td>37. SRAM</td>
<td></td>
</tr>
<tr>
<td>10. CISIA</td>
<td>20. IEISS</td>
<td>30. NGtools</td>
<td>40. UIS</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-6: Critical Infrastructure Risk Assessment Models

A detailed comparison of all the models is beyond the scope of this research, and the 2006 survey did not provide sufficient information to make an analysis. However, the 2012 survey did provide sufficient insight to make at least a cursory attempt. The CAPRA model (McGill, 2008) was also included in this analysis together with AVM, making a total of 23 CI risk methodologies (models summarized in Appendix B). Given the available information, each model was compared against the risk analysis formulation and risk management criteria established at the outset of this chapter. The seven risk formulation criteria are 1) asset-drive approach, 2) threat localization, 3) transparency & repeatability, 4) qualified results, 5)
comprehensive scope, 6) national impact, and 7) applicable results. The three risk management criteria include the ability to 1) perform baseline analysis, 2) conduct cost-benefit analysis, and 3) provide decision management tools. Each model was assessed “Y” if it explicitly met the criteria, “N” if it explicitly didn’t meet the criteria, and “U” if there was insufficient information to make a determination. The results of the analysis are shown in table 3-7.

<table>
<thead>
<tr>
<th>Model</th>
<th>RA Criteria</th>
<th>Risk Mgmt</th>
<th>Score</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. AVM</td>
<td>Y Y Y Y Y Y</td>
<td>Y Y Y Y</td>
<td>10</td>
<td>0 0 N</td>
</tr>
<tr>
<td>2. NEMO</td>
<td>Y U U U U U U</td>
<td>U U U 1 0 9 Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. CIFMA</td>
<td>Y Y U U U U U</td>
<td>U Y Y 4 1 5 Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. CIMS</td>
<td>Y Y U U U U U</td>
<td>U U Y 2 1 7 Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. COUNTERACT</td>
<td>N Y U U U U U</td>
<td>U Y U 2 1 7 U</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. FAIT</td>
<td>Y U U U U U U U</td>
<td>U U U Y 2 1 7 Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. NSRAM</td>
<td>N U U U U U U U</td>
<td>U U Y Y 2 1 7 Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. RAMCAP-Plus</td>
<td>N U Y U U U U U</td>
<td>U U Y 2 1 7 Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. EURACOM</td>
<td>U U U U U U U U</td>
<td>U U Y 1 1 8 U</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. MDM</td>
<td>U U N U U U U U</td>
<td>U U Y 1 1 8 Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. CIPDSS</td>
<td>N U U U N Y U U U Y Y 3 2 5 Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. DECIRS</td>
<td>N Y Y U N U U U U U Y 3 2 5 N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. CommAspen</td>
<td>Y Y Y N U N U U U U U U 2 2 6 Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. MIN</td>
<td>Y U N U N U U U U Y U U 2 2 6 Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. SRAM</td>
<td>N U N U U U U U U Y Y 2 2 6 U</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16. BMI</td>
<td>N U U U U U U U U N Y 1 2 7 Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17. N-ABLE</td>
<td>Y U N U U U U U U U U N 1 2 7 Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18. RVA</td>
<td>N U U U U U U U U U U Y 1 2 7 U</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19. CARVER2</td>
<td>Y N Y U N Y U U U N Y 4 3 3 N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20. RMCIS</td>
<td>N U U U U U U U U U U N 0 3 7 Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21. BIRR</td>
<td>N N N U Y Y Y U Y Y N Y 4 5 1 N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22. CAPRA</td>
<td>N N N Y N N U Y Y N 3 6 1 N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23. RMF</td>
<td>N N N N N N N N N N N 0 10 0 Y</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3-7: Comparison of CI Models to Risk Criteria

The models in table 3-7 are listed in order from most compatible to least compatible with the stated criteria. The list was sorted based on their composite scores with fewest number of “N” counts given first priority, then greatest number of “Y” counts, and finally greatest number of “U” counts. “N” counts were given first priority because they are a disqualifying factor. The biggest disqualifying factor was “comprehensive scope” (CS). Sixty-one percent of the models scored “N” in this category mostly because they didn’t account for “resilience” in their formulation. Resilience is a vaguely defined term, but the 2012 survey indicated that it included mitigation, response, and recovery efforts. These are explicitly accounted for in the AVM.
baseline formulation in the form of $P(\text{den})$, $P(\text{dim})$, and $\%(\text{dam})$. The second biggest disqualifier was “asset-driven approach” (ADA). Fifty-two percent of the models scored “N” against this criteria. Except for AVM, only one other model, NEMO, had no disqualifying scores. This was primarily due to incomplete information. In fact, NEMO is not even a critical infrastructure protection model. It is a targeting tool developed for the military to identify critical nodes in enemy critical infrastructure. The methodology was mentioned because of its potential application in identifying key nodes in domestic critical infrastructure (Giannopoulos, Filippini, & Schimmer, 2012, pp. 28-29). While such a capability could be useful, similar to CARVER+Shock, it does not present a full risk management capability.

The last column in table 3-7 indicates whether a model includes interdependency analysis. Interdependency analysis determines the impact of attack on one asset on other assets, accounting for cascading effects through the infrastructure network. This factor was not counted in the previous scoring because it was not part of the formulated criteria. AVM does not include interdependency analysis. While the concept is attractive, it adds an additional set of assumptions complicating transparency and repeatability criteria. It may be further argued that an aggregation of assets could provide similar insight, something AVM can support.

3.7. Summary

Inherent vulnerabilities in critical infrastructure may be leveraged by small groups or individuals to inflict catastrophic damage on the nation. While the Department of Homeland Security has adopted a risk management approach to protecting critical infrastructure, a 2010 review by the National Research Council determined that none of its methods were adequate for informing decision making. The same report summarized the challenges to developing an
adequate risk methodology. From this list a set of criteria was derived to guide development of an Asset Vulnerability Model to provide adequate risk management. AVM is predicated on a measure of risk designated as $\Theta$, an attacker’s probability of failure, based on earlier work in game theory. AVM provides baseline analysis, cost-benefit analysis, and decision support tools using a risk formulation informed by National Research Council criteria. The derived criteria essentially provide conditioning on an ill-behaved problem to provide approximate results. A sensitivity analysis on the instantiated model exhibits strong stability. A cursory analysis of other CI protection models indicates that AVM uniquely complies with the formulated risk criteria. Most importantly, AVM informs decision making by providing 1) an indication of current CI protection status, 2) demonstrating incremental improvement, and 3) evaluating associated costs.

3.8. Contributions

This research makes significant contributions in 1) proposing homeland security risk formulation criteria, and 2) developing a compatible methodology answering fundamental questions and providing strategic direction in homeland security.

This research uniquely proposes substantiated criteria for conditioning ill-behaved homeland security risk formulations. It justifies an asset-based approach to overcome well-known problems with threat-driven methods and based on successful application to earthquakes. It reduces the problem of threat prediction to threat localization, helping focus resource investments where needed without the benefit of a robust statistical database. By the same token it shifts attention from protecting the US population as the target of direct attack to the target of indirect attack. It substantiates a middle-ground approach to risk formulation favoring
transparency and repeatability over complexity. It establishes an imperative for qualifying results. It justifies a comprehensive risk formulation based on the five phases of emergency management. It uniquely quantifies risk magnitude in terms of GDP and national mortality rates, well-developed indicators of national welfare capturing the broader consequences of a disaster while avoiding awkward value comparisons between life and property. Thus the derived criteria provide bounding conditions and requirement standards for any suitable homeland security risk formulation.

This research developed an Asset Vulnerability Model consistent with the previous homeland security risk formulation criteria. AVM uniquely applies game theory to develop a risk measure answering the question “how much risk is acceptable?” AVM offers distinct capabilities currently absent from DHS to 1) concisely convey critical infrastructure risk levels, 2) conduct protective measure cost-benefit analysis, 3) demonstrate risk reduction across multiple assets at different levels of management, and 4) measure and track investments and improvements over time. The AVM baseline formulation 1) distinguishes between threat prediction and threat warning making appropriate use of what limited historical data is available, 2) suggests a novel adaptation of the DHS Protective Measure Index to indicate both current protection status and improvement potential, 3) reduces assumptions and unpredictability through transparency and repeatability, to provide 4) a profile of current critical infrastructure protection status. AVM cost-benefit analysis provides a stable method for selecting optimum protective investments at the asset, region, and national levels. AVM decision support tools graphically present results affording flexible insight to inform homeland security resource investment decisions. AVM offers the capability to answer questions currently unanswerable and provide strategic direction now absent from DHS.
Chapter 4. Implementation

4.1. Overview

Chapter 3 proposed an Asset Vulnerability Model to work with the DHS Risk Management Framework to inform resource investment decisions protecting the nation’s critical infrastructure from being leveraged by small groups or individuals to precipitate domestic catastrophic attack. But as was detailed in Chapter 2, CI is only half the problem; WMD is the other half. WMD protection is the responsibility of federal agencies outside the Department of Homeland Security and beyond the current reach of the Risk Management Framework. As determined by Sandler and Lapan’s research in game theory, a coordinated defense among all targets is more efficient than an uncoordinated one. This chapter will examine the policy framework needed to bring WMD into the AVM fold. It will then demonstrate how AVM can be integrated into the DHS Risk Management Framework leading towards a unified homeland security strategy.

4.2. Strategy Coordination

As described in Chapter 2, strategy coordination between executive departments is conducted at the highest-level in the National Security Council. The National Security Council is supported by an NSC staff, organized and administered by a National Security Advisor appointed by the President. While the president clearly holds final decision-making authority in the executive branch, over the years the NSC staff has emerged as a major factor in the formulation (and at times in the implementation) of national security policy. Similarly, the head of the NSC staff, the National Security Adviser, has played important, and occasionally highly public, roles in policymaking issues (Best, 2011, p. 2). Since 1986, the National Security
Advisor has assisted the president with publishing National Security Strategy (Dale, 2008, p. 3) formally identifying national security objectives and the means for attaining them. This congressionally-mandated document helps guide Congress in determining national funding priorities. The National Security Strategy also serves as a coordinating framework for federal agencies to prioritize resources and schedule activities to work towards common national goals (Dale, 2008, p. 2). In the immediate aftermath of 9/11, President Bush established a parallel Homeland Security Council and Homeland Security Advisor responsible for developing a corresponding Homeland Security Strategy. In 2009, President Obama re-integrated the Homeland Security Council into the National Security Council and made homeland security strategy a part of national security strategy (Hsu, 2009). In 2010, the Obama Administration released the current National Security Strategy identifying four national security objectives: 1) security, 2) prosperity, 3) values, and 4) international order. Embedded within national security strategy is a homeland security strategy built upon 1) strengthening security and resilience at home, 2) disrupting, dismantling and defeating al-Qaeda and its affiliates, 3) reversing the spread of nuclear and biological weapons and securing nuclear materials, 4) advancing peace, security, and opportunity in the greater Middle East, and 5) securing cyberspace (The White House, 2010, p. 15). That same year, the Obama Administration also released the Quadrennial Homeland Security Review defining homeland security as “a concerted national effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive” (Department of Homeland Security, 2010, p. 13). As statements of national objectives, the goals are necessarily lofty, but this also makes them unfortunately vague for coordinating efforts between the federal departments. Moreover, the
Terrorism and hazards are not the homeland security problem. To suggest they are is to ignore the historical significance of 9/11. Homeland security was not thrust to the forefront of national concern until the attacks of September 11, 2001. As a result of 9/11, the federal government underwent its largest reorganization since the end of World War II, including creation of the Department of Homeland Security. The first National Strategy for Homeland Security in 2002 squarely laid the blame on terrorism (Office of Homeland Security, 2002, p. 2); natural disasters didn’t enter consideration until after Hurricane Katrina in 2005 (Homeland Security Council, 2007, p. 10). If terrorism is the problem, then why didn’t the 1993 attacks on the World Trade Center25 (National Commission on Terrorist Attacks Upon the United States, 2004, pp. 71-73) or 1983 attacks killing 241 Marines in Beirut, Lebanon26 (National Commission on Terrorist Attacks Upon the United States, 2004, p. 96) result in a similar shakeup of US government? Statistically, terrorism and hazards don’t even register as a threat. Heart disease, cancer, respiratory disease, and vascular disease collectively kill more than 1.5 million Americans annually, occupying the top four positions in the Centers for Disease Control and Prevention National Vital Statistics Report (Kochanek, Murphy, Xu, Minino, & Kung, 2011, p. 5). Unintentional deaths due to accident rank fifth on the list with 117,176 fatalities. Deaths due to terrorism are classified under Assault (homicide), and rank 15th (out of 16) near the bottom of the list with 16,591 deaths (2009 data) (Kochanek, Murphy, Xu, Minino, & Kung, 2011, p. 35).

What is homeland security? What was unique about 9/11 that’s that made it a watershed in the nation’s history? According to the 9/11 Commission, it was the “surpassing disproportion” of the attack that made it unique. On September 11, 2001, nineteen men inflicted as much damage
on the United States as the Imperial Japanese Navy on December 7, 1941 (National Commission

Domestic catastrophic attack precipitated by small groups and individuals employing asymmetric means is the homeland security problem. As detailed in Chapter 2, critical infrastructure and weapons of mass destruction provide such means. The preoccupation with terrorism is unnecessarily restrictive as it couples means with motive. Terrorism is a tactic implying a particular motive, specifically “any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments” (Office of Homeland Security, 2002, p. 2). While terrorism may be a motive, it may be only one of any innumerable possible motives for instigating domestic catastrophic attack. The term is actually a misnomer. It was meant to convey that the attackers are independent agents not affiliated or sponsored by a foreign nation. This distinguishes homeland security from homeland defense which seeks to preserve the sovereignty of the United States among the community of nations. In this realm, the federal government employs instruments of national power including diplomatic, economic, and military means to achieve national objectives as expressed in National Security Strategy. Differentiating the actions of individuals from those of nations, particularly acts within US territory, makes them subject to US law, no matter what the person’s nationality. Assault is a crime, thus homeland security is a specific concern of law enforcement at all levels of US government. What distinguishes homeland security, however, is the magnitude of the crime. The consequences of domestic catastrophic attack can have repercussions affecting the health and welfare of the entire nation.
4.2.1. Redefining Homeland Security

The current focus of national policy on terrorism and hazards diverts attention from the root problem of domestic catastrophic attack. A more precise definition of homeland security is needed to better focus interagency coordination. The following is proposed:

**Safeguard the US from domestic catastrophic attack.**

This definition is more precise because it focuses on the specific problem of domestic catastrophic attack, directing attention to those means that make it possible. This definition is more comprehensive because it doesn’t restrict the motives of the attackers. This definition is more discriminate because it distinguishes the principal concern from other forms of crime such as the mass killings at Newtown, Virginia Tech, and Columbine. Supported by AVM, the corresponding homeland security strategy becomes:

**Maximize protective investments that minimize the probability of successful domestic catastrophic attack.**

The preceding statement offers a concise strategy specifying “ends”, “ways”, and “means”. The “ends” are “minimize the probability of successful domestic catastrophic attack.” The “ways” are “Maximize protective investments.” The “means” are “protective investments”. By implication, protective investments should be directed towards means of catastrophic attack; i.e., weapons of mass destruction and critical infrastructure. Also implied within this strategy is exclusive concern with malicious anthropic events in the form of deliberate attack.

Natural hazards are not specifically addressed by this strategy. There is precedent supporting this approach. During much of the Cold War, programs for natural disasters were treated separately from programs for Civil Defense. Then, with the creation of the Defense Civil
Preparedness Agency in 1972, federal funding began to give priority to “dual use” capabilities, those that could be useful in both natural disasters and nuclear attack. Unintentionally, this policy built an empirical body of evidence for common requirements. The Disaster Research Center (DRC) conceptualized the similarities as response-generated demands on society. These demands were deemed to be similar for various disasters, both natural and manmade. This insight gave rise to Comprehensive Emergency Management (CEM) proposed by the National Governor’s Association (NGA) in 1978 as a common framework for addressing all phases of all types of disaster. CEM was adopted by FEMA in 1983 as the Integrated Emergency Management System (IEMS) (Lindell, Prater, & Perry, 2006, pp. 23-26). The implication is that protection measures designed for malicious anthropic events will also benefit response to natural disasters. Moreover, the 2010 National Research Council report advised that “The risks presented by terrorist attack and natural disasters cannot be combined in one meaningful indicator of risk, so an all hazards risk assessment is not practical. DHS should not attempt an integrated risk assessment across its entire portfolio of activities at this time because of the heterogeneity and complexity of the risks within its mission” (National Research Council, 2010, p. 84)

4.2.2. NSC Reform

It is widely understood that the security environment of the early 21st century differs significantly from the one the US national security system was created to manage. The character of the actors has changed; the diversity of state capabilities is greater; and the international norms delimiting legitimate behaviors have shifted as well. Exchanges of goods, information, ideas, and people are also far denser and more variable than they were even a dozen years ago,
let alone when the National Security Council was created in 1947 (Project on National Security Reform, 2008, p. Executive Summary). Although much progress has been made since 9/11, one of the central criticisms leveled by virtually every commission and panel that studied what went wrong leading up to the attacks of 9/11 was that the US government suffered from a serious lack of coordination among the various agencies whose job it is to keep us safe (Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, 2008, p. 83). These concerns have led to various calls for reform to the national security system.

Perhaps the most thorough analysis and critical assessment of the policy processes for national security was conducted by the Project on National Security Reform (PNSR). Headed by a board of senior, experienced former government officials, the project evaluated the national security policy development and execution process in various administrations and identified the organizational strengths and weaknesses of those processes (Whittaker, Brown, Smith, & McKune, 2011, p. 24). In its November 2008 report, Forging a New Shield, PNSR reviewed the functions of the NSC along with other parts of the “national security system” and determined that the current organizational structure is ill-coordinated, potentially placing the nation at risk in an international environment that requires agile and coordinated efforts by all instruments of power (Best, 2011, p. 31). In place of the NSC, PNSR recommended creating a President’s Security Council and a Senate-confirmed Director of National Security who would have broader responsibilities than the existing National Security Adviser. The Director would “direct the implementation of national security missions identified by the present as inherently interagency.” The office of the new Director of National Security would be comprised of some 500 people. To date, none of these sweeping changes have been adopted. (Best, 2011, p. 31)
While not embracing the more radical suggestions of the PNSR, the Obama administration did demonstrate an interest in reforming the national security process. In February 2009, President Obama issued Presidential Study Directive #1 ordering a 60-day interagency review of the White House homeland security and counterterrorism organization. Following the review, the President announced the integration of the HSC into a broader NSC organization and national security staff. The Homeland Security Advisor became a deputy to the NSA but retained direct access to the President (DEFENSE REPORT, 2009). The presidential directive also created new offices to deal with cybersecurity, preventing WMD terrorist attacks, transborder security, information sharing and national resilience (i.e., preparedness for and response to WMD attack, health pandemics and natural disasters), and WMD Coordinator (Loukianova, 2009). While the new WMD Coordinator provides consolidated oversight for counter-WMD and counter-terrorism policy, it does not include CI protection as well. Unless security policy is consolidated for both WMD and CI, Sandler and Lapan’s work in game theory predicts an imbalance of deterrence increasing the likelihood of their employment for domestic catastrophic attack.

4.3. AVM Implementation

AVM is fully compatible with the DHS Risk Management Framework. With an appropriate supporting policy structure, RMF can be extended to encompass both CI and WMD. Thus AVM can help guide the nation towards a unified homeland security strategy.
Recognizing critical infrastructure as the root problem and defining homeland security in related terms can help scope a definitive list of assets requiring protection in Step Two of the Risk Management Framework. The DHS IG attributed the questionable results from previous attempts to difficulties defining the problem set. In the 2003 data call, states and localities were asked to identify “any system or asset that, if attacked, would result in catastrophic loss of life and/or catastrophic economic loss.” The 2004 data call described more thresholds, such as refineries with certain capacities, or commercial centers with potential economic loss impact of $10 billion or more than 35,000 people (Moteff, Critical Infrastructure: The National Asset Database, 2007, p. 4). None of these definitions would include a passenger jet, only four of which proved devastating on 9/11. The new definition of homeland security can help rectify this oversight by making the problem set evident: those things that can be employed in domestic catastrophic attack. Passenger jets fall in this category. Shopping malls do not. Certainly the destruction of a major shopping mall and the resulting casualties would be catastrophic. But the shopping mall itself is inert. It didn’t create the casualties. The culprit would be what caused the catastrophe; possibly a passenger jet, more likely a CBRN agent. These are the things that need to be protected, not shopping malls, gas stations, or whatever. Thus the new definition of homeland security can reduce the problem set.
dramatically, and even further with additional analysis (Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, 2006).

AVM baseline analysis is conducted in Step Three of the Risk Management Framework. Data collection is conducted on all catastrophic assets previously identified and a corresponding $\Theta$ value calculated. Data collection will have to change to meet the requirements of the new risk assessment formulation. The forms and tools separately employed for security surveys, vulnerability analysis, and state and local grant programs will have to be integrated and possibly augmented. This is not to suggest they need to be combined. Security surveys and vulnerability analysis remain most effective in assessing protection and mitigation measures “inside the perimeter”. THIRA, likewise, is most appropriate for assessing prevention, response, and recovery measures “outside the perimeter”. There is the question, though, of voluntary versus mandatory data collection. THIRA is mandatory for state and local grant eligibility (FEMA, 2012). Security surveys and vulnerability analysis are voluntary on the part of private industry (Government Accountability Office, 2012, p. 3). Most sectors identified as part of the new homeland security definition, though, are federally regulated. It would not require much regulatory change to institute mandatory collection of data essential to a more coherent homeland security strategy (Lewis & Darken, Potholes and Detours in the Road to Critical Infrastructure Protection Policy, 2005, p. 7). At the conclusion of Step Three, DHS would have something it has never had before: a definitive list of catastrophic assets and their relative levels of protection. The baseline decision support tool presents the data in a spreadsheet that may be sorted on various fields to provide better insight. For example, the data may be sorted by $\Theta$ to gain perspective on relative protection across all assets as shown in Figure 3-2.2. Alternatively,
the data may be sorted based on asset type or location to assess relative protection across sectors or regions as shown in Figures 3-2.3 and 3-2.4.

AVM provides cost-benefit analysis in Step Four in the Risk Management Framework. For each asset, any number of protection measures can be nominated from across the five phases of emergency management. Each measure is evaluated and assigned a $\Delta \Theta$ value indicating its expected improvement contribution. Associated costs, $D(\Delta \Theta)$, are also captured. The resulting data is processed to find the highest proportional value of cost versus protection for each asset. The results of cost-benefit analysis can then be used to inform resource investment decisions based on multiple criteria.

Cost-effectiveness may serve as one set of criteria to guide resource investments in countermeasures that yield the greatest risk reduction or provide the maximum reduction for a fixed cost. Alternatively, resource investments may be guided by various attributes of critical assets including geographic distribution or potential loss consequences (Moteff, Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, 2007, pp. 11-12). ISO 31000:2009, Risk Management, gives the following preference order for addressing risk: 1) avoid the risk, 2) take on increased risk to pursue an opportunity, 3) remove the risk source, 4) change the likelihood, 5) change the consequence, 6) share the risk with another party (e.g., insurance), and 7) accept the risk by informed decision. The DHS approach according to the 2009 National Infrastructure Protection Plan is to target protective programs and resiliency strategies to aggregations of systems, networks, and sectors with the highest risk (Department of Homeland Security, 2009, p. 41).
Results from AVM cost-benefit analysis are presented in a spreadsheet as shown in figures 3.1 to 3.4 to inform resource investment decisions based on the desired criteria. The data may be included in the DHS Annual Performance Report together with its budget justification to Congress. Subsequent protection grants need to be equally offered “inside the perimeter” as well as “outside the perimeter”. Currently, protective measure grants are allocated almost exclusively to government and nonprofit agencies. The chief argument for not including private industry is that government subsidies may confer unfair advantages and upset market forces. Another concern is that industry may abdicate its security responsibility entirely to the government. While both concerns are justifiable, they are not inevitable. Responsible investments can keep government from unnecessarily shouldering a disproportionate security burden, and the potential effect on market forces can be weighed against the potential impact of their disruption (Cordes, Yezer, Young, Foreman, & Kirschner, 2006). 28

4.4. Analyzing Investment Strategies

AVM decision support tools provide the flexibility allowing a decision maker to choose among a variety of resource investment strategies. This section will examine seven possible investment strategies and compare their performance over a simulated ten-year period using a probable attack model.

4.4.1. Strategy Alternatives

AVM cost-benefit analysis provides decision makers an investment choice among protective improvement measures that have already been selected for their optimum cost/performance gains. The decision maker’s choice is constrained by their available budget.
The question is how to allocate limited funds and purchase protective improvement measures that will provide the maximum protection? Previous discussion on AVM implementation suggests seven different investment strategies: 1) Least Cost (LC), 2) Least Protected (LP), 3) Region Protection (RP), 4) Sector Protection (SP), 5) Highest DTheta (HD), 6) Highest Consequence (HC), or 7) Random Protection (RAN).

The Least Cost investment strategy purchases all protective improvement measures based on lowest cost. Given a fixed budget, this strategy attempts to purchase as many measures as possible, regardless of their individual protective gain. The advantage of this strategy is that it affords the purchase of the most protective measures, which may make it politically attractive “sharing the wealth” among more congressional districts.

The Least Protected investment strategy purchases protective improvement measures for the least protected assets as determined by their Θ value. This strategy has the intuitive advantage of allocating resources where they are most needed, or at least towards assets that are most vulnerable. In a sense, it is an implementation of the Sandler and Lapan strategy of protecting all assets equally by making them all equally vulnerable.

The Region Protection investment strategy purchases protective improvement measures for regions of the country that may be deemed more susceptible to attack than others. The RP strategy is similar to the Urban Area Security Initiative (UASI) grant program already administered by DHS. UASI grants are distributed to the 100 most populous metropolitan areas in the United States as prescribed by the 2002 Homeland Security Act. Grant eligibility is determined by the current DHS risk formulation R=f(T,V,C) (Federal Emergency Management Agency, 2013).
The Sector Protection investment strategy allocates funds to a specific sector that may be deemed more susceptible to attack or whose incapacitation or destruction is considered significantly damaging. Again, this may be considered a variation of the Sandler and Lapan strategy of protecting all assets of a specific sector equally by making them equally vulnerable.

The Highest DTheta investment strategy allocates funds to protective improvement measures that provide the highest protection gain regardless of cost. This may be considered a cost optimization scheme by purchasing protective measures that provide the highest return on investment.

The Highest Consequence investment strategy allocates funds to assets with the highest magnitude component in terms of national economic and mortality consequences. Similar to LP, this strategy has the intuitive advantage of allocating resources where they are most needed in terms of most damaging effects.

The Random Protection investment strategy essentially simulates current practices. Without the advantage of a guiding metric, there is can be no determination of how to systematically apply protective improvement measures. Simulation of this strategy provides a baseline for comparing investment strategies with and without the benefit of AVM.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. LC – Least Cost</td>
<td>5. HD – Highest DTheta</td>
</tr>
<tr>
<td>2. LP – Least Protected</td>
<td>6. HC – Highest Consequence</td>
</tr>
<tr>
<td>3. RP – Region Protection</td>
<td>7. RAN – Random Protection</td>
</tr>
<tr>
<td>4. SP – Sector Protection</td>
<td></td>
</tr>
</tbody>
</table>

Table 4-1: Protective Improvement Investment Strategies
4.4.2. Strategy Simulation

Do any of the preceding cost investment strategies confer an advantage against domestic catastrophic attack? Can a consistent allocation of a fixed budget reduce probable damages over time? This section details an AVM investment strategy simulation program and experiments conducted to test the hypothesis.

The AVM strategy simulation program architecture is depicted in Figure 4-2. It begins with the three AVM program models BAM, PIM, and CBA. The Baseline Asset Model (BAM) generates 100 assets at random, as constrained by the value ranges in table 3-5. While BAM is
capable of generating any number of specified assets, only 100 assets were generated in a tradeoff between creating a representative sample and charting resolution. The Protective Improvement Model (PIM) takes the BAM output and generates corresponding protection measures conforming to parameters specified at execution. The three parameters are: 1) percent of assets not receiving protective measures, 2) percent of asset types not receiving protective measures, and 3) percent of asset locations not receiving protective measures. The parameters were designed to represent the situation where not every asset will request funding for protective improvement measures every year. In all subsequent executions, the parameters were set to 40%, 40%, and 40% respectively. The Cost-Benefit Analysis (CBA) program takes the combined asset/improvement output from PIM and selects the optimum combination of improvements that provide the greatest protection increase at the least cost. To conduct the AVM strategy simulation, two new programs were developed: 1) the Selective Improvement Program (SIP) to purchase protective measures based on one of the preceding six strategies, and 2) the Probable Attack Model (PAM) for calculating the consequences of a successful attack.

The Selective Improvement Program simulates one of six investment strategies numerically specified at execution: 1 = Least Cost, 2 = Least Protected, 3 = Region Protection, 4 = Sector Protection, 5 = Highest DTheta, 6 = Highest Consequence, and 7 = Random Protection. For the Region and Sector investment strategies, the protected region and protected sectors must also be specified at execution, 1-50 and 1-13 respectively. As there was no particular advantage to specifying a specific region or sector, the values 44 and 9 were indiscriminately chosen for all subsequent simulations. SIP reads in the assets and associated protective improvement measures recommended by Cost-Benefit Analysis. For LC simulations, asset records are sorted in ascending order based on the total cost of recommended protective improvement measures. For
LP simulations, asset records are sorted in ascending order of their current Θ value. For RP and SP simulations, asset records are sorted in ascending order of their location and type values respectively. For HD simulations, asset records are sorted in descending order of their protective improvement ΔΘ value. For HC simulations, asset records are sorted in descending order of their consequence indicated by the % (dam) value. For RAN simulations, asset records are sorted in ascending order of a randomly generated key. After sorting asset records by investment strategy, SIP purchases as many corresponding protective improvement measures as it can afford within a fixed budget. For all simulations, the budget was set at $50,000, calculated at 20% of the purchase price for all protective improvement measures recommended by CBA on the initial 100 assets generated by BAM. In the absence of real-world data, 20% was indiscriminately chosen as a reasonable size budget that was not too big and not too small. SIP concludes by writing modified and unmodified asset records to output for PAM. SIP expenditures and ΔΘ purchases are recorded to a separate output file for later analysis.

The Probable Attack Model computes the estimated damages of a successful attack based on 1) the probability of attack, and 2) the attacker’s perception of Θ (i.e., θ). The probability of attack is specified at program execution in terms of likelihood over a given period of years. Using these values, standard quantitative risk assessment methodologies compute an annualized rate of occurrence, in this case termed the annual attack expectancy (AAE), by dividing the probability of attack by the given period of years. So, for example, an estimated 30% probability of attack over 10 years has an AAE of 3% or 0.03. PAM keeps a cumulative probability of attack (CPA) based on the AAE. PAM maintains a state vector so it can restore the CPA between executions. At the beginning of the attack period, PAM sets the CPA to the AAE. It then calculates the probability of attack by generating a random number between 0.001 and 1.0
and comparing it to the CPA. If the random number is within range of the CPA, i.e., “less than” the CPA, then an attack is deemed to have occurred. If the random number is outside the range of the CPA, i.e., “greater than” the AAE, then no attack occurred. If no attack occurs, then the cumulative probability of attack is incremented by the AAE. If an attack does occur, then the cumulative probability is reset to the AAE. The attack model is illustrated in figure 4-3.

How accurately does the model reflect reality? A 2012 paper by Clauset and Woodard claims to have developed a probabilistic model for global catastrophic attack. By their estimation, there was a 11%-35% chance of a 9/11-sized attack in the 40 year period between 1968 and 2007. Using the PAM model, an analysis was conducted on the expected number of attacks over a 40 year period using increasing probabilities of attack. As shown in Figure 4-4, PAM calculates between 1.3 and 2.6 attacks over that period, in close agreement with Clauset and Woodard’s research. By the same token, they estimate a 19%-46% chance of another similar attack over the next 10 years (Clauset & Woodard, 2012, p. 1&8). Please note that the similarity between the two models does not constitute proof of either, nor does it repudiate earlier observations about the
shortcomings of estimating attack probabilities. At best, it provides a basis for comparison
demonstrating that PAM is “in the ballpark” with respect to other research.

Calculating the probability of attack is only the first step in calculating the probability of
success. Calculating the probability of success depends on which target is attacked, and this
depends on the attacker’s own perception of success. As already detailed, AVM calculates a Θ
value representing an attacker’s probability of failure for a given asset. Capital theta is based on
the Sandler and Lapan model which postulates θ, an attacker’s perceived probability of failure.
To reiterate, according to Sandler and Lapan, an attacker will choose the target that offers the
least probability of failure, or in other words, the greatest probability of success (1-θ). Since the
attacker’s perceptions are unknown, PAM derives a value for θ as a percentage of Θ. The
maximum Θ deviation is specified at program execution. Again, PAM uses a random number
generator to assign a deviation no greater than + or – the maximum specification. Thus, for
example, a 20% Θ deviation will produce a θ value between 80% and 120% of the “known” Θ
value. PAM reads in asset records and sorts them in ascending order according to the derived θ
value. The first record in the list has the lowest θ value of all assets, and according to the
Sandler and Lapan model, becomes the attacker’s target of choice.

PAM uses asset information from the selected target to next compute a probability of
successful attack. Each asset record contains the component values of the Θ risk formulation in
3-1. While the asset may have been targeted based on an attacker’s perception θ, the probability
of successful attack will be determined by the known Θ values. The first three terms in the Θ
risk formulation are related to the prevent and protect phases of emergency management, “to the
left of the boom”, and thus are pertinent to determining the outcome of an attack. PAM
calculates a probability of failure (PF) as the product of P(dis), P(def), and P(den). Afterwards, it
calls on the random number generator one last time to produce an attacker’s probability of
success (PS) between 0.001 and 1.0. If PS is greater than PF, then PAM designates the attack a
success. A successful attack will result in PAM removing the targeted asset from the list and
further simulation processing, but not before it calculates the damages.

PAM calculates damages as a product of P(dim) and % (dam) corresponding to the
response and recovery phases of emergency management, actions taken after an incident has
occurred, or “to the right of the boom”. In addition to the amount of damage, PAM records the
identification of the attacked asset and the year it was attacked for later analysis. Both PAM and
SIP programs are summarized in table 4-2.

<table>
<thead>
<tr>
<th>Function</th>
<th>Type</th>
<th>File Name</th>
<th>Arguments/Inputs</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selective Improvement Program</td>
<td>C Program</td>
<td>SIP.c</td>
<td>1. Simulation Type</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = LC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 = LP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 = RP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 = SP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 = HD</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6 = HC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7 = RAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Simulation Key</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RP = 1-50</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SP = 1-13</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LC, LP, HD, &amp; HC = 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Budget ($50,000)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. Input Asset File (from CBA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5. Output Asset File (to PAM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6. Output Expenditure File (to MAP)</td>
<td></td>
</tr>
<tr>
<td>Problem Attack Model</td>
<td>C Program</td>
<td>PAM3.c</td>
<td>1. Maximum Probability of Attack 10% - 100%</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Attack Probability Period (10 years)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Theta Deviation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. PAM State File (store CPA &amp; year)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5. Input Asset File (from SIP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6. Output Asset File (to PIM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7. Output Damages File (to MAP)</td>
<td></td>
</tr>
</tbody>
</table>

Table 4-2: AVM Investment Strategy Simulation Program Models
Investment strategy simulation is facilitated by a series of batch files. To recap, BAM produces a list of assets and corresponding Θ values; PIM generates proposed protective improvement measures with associated ΔΘ protection gains and D(ΔΘ) costs; CBA identifies protective improvement measures offering the greatest proportional value in protective gains compared to costs; SIP simulates one of six investment strategies to purchase optimum improvements within a fixed budget; and PAM calculates damages from a successful attack based on a given probability of attack and Θ deviation, and removes the targeted asset of a successful attack from further simulation. BAM, PIM, CBA, SIP, and PAM are standard C executable files. When executed in sequence, and the output from one is fed in as input to the next, they simulate a single, one-year investment cycle. Windows batch files facilitate correct sequence execution and repetitive runs to 1) examine each investment strategy individually, 2) with respect to changing probabilities of attack and Θ deviation, 3) over multiple executions to derive average results, and 4) over multiple years corresponding to the estimated attack probability period. Table 4-3 lists the supporting batch files and their execution parameters. AVM12 executes all seven strategy simulations for 100 assets over a 10 year probability period repeated 100 times recording expenditures and damages related to a changing probability of attack from 10%-100% by 10% increments. Theta deviation remains constant at 20%. AVM13 does the same as AVM12, except it varies the Θ deviation from 10%-100% while keeping the attack probability constant at 32%, corresponding to the median probability of attack predicted by Clauset and Woodard. AVM14 also does the same as AVM12, except it replaces the Sandler and Lapan model (PAM3) for selecting targeted assets based on smallest θ (as a deviation of Θ) with one that chooses targets whose destruction will cause the most damage (PAM4).
<table>
<thead>
<tr>
<th>Master File</th>
<th>Simulation</th>
<th>Batch Calls</th>
<th>Execution Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVM12.bat</td>
<td>Range of Attack Probabilities + Target Selection by θ (PAM3)</td>
<td>AVM100LC_100.bat AVM100LP_100.bat AVM100R44_100.bat AVM100S9_100.bat AVM100HD_100.bat AVM100HC_100.bat AVM100RAN_100.bat</td>
<td>BAM: Number of Assets Generated = 100 PIM: Percent Unimproved Assets = 40% PIM: Percent Unimproved Asset Types = 40% PIM: Percent Unimproved Locations = 40% SIP: Annual Improvement Budget = $50,000 PAM3: Maximum Probability of Attack = 10%-100% PAM3: Probable Period of Attack = 10 years PAM3: Attacker’s Theta Deviation = 20% AVM: Number of Simulations = 100</td>
</tr>
<tr>
<td>AVM13.bat</td>
<td>Range of Θ Deviations + Target Selection by θ (PAM3)</td>
<td>AVM100LC_100.bat AVM100LP_100.bat AVM100R44_100.bat AVM100S9_100.bat AVM100HD_100.bat AVM100HC_100.bat AVM100RAN_100.bat</td>
<td>BAM: Number of Assets Generated = 100 PIM: Percent Unimproved Assets = 40% PIM: Percent Unimproved Asset Types = 40% PIM: Percent Unimproved Locations = 40% SIP: Annual Improvement Budget = $50,000 PAM3: Maximum Probability of Attack = 32% PAM3: Probable Period of Attack = 10 years PAM3: Attacker’s Theta Deviation = 10%-100% AVM: Number of Simulations = 100</td>
</tr>
<tr>
<td>AVM14.bat</td>
<td>Range of Attack Probabilities + Target Selection by Consequence (PAM4)</td>
<td>AVM100LC_100.bat AVM100LP_100.bat AVM100R44_100.bat AVM100S9_100.bat AVM100HD_100.bat AVM100HC_100.bat AVM100RAN_100.bat</td>
<td>BAM: Number of Assets Generated = 100 PIM: Percent Unimproved Assets = 40% PIM: Percent Unimproved Asset Types = 40% PIM: Percent Unimproved Locations = 40% SIP: Annual Improvement Budget = $50,000 PAM4: Maximum Probability of Attack = 10%-100% PAM4: Probable Period of Attack = 10 years PAM4: Attacker’s Theta Deviation = 20% AVM: Number of Simulations = 100</td>
</tr>
</tbody>
</table>

Table 4-3: AVM Investment Strategy Simulation Supporting Batch Files

AVM14/PAM4 was motivated by a report on The Impact of Home Burglar Alarm Systems on Residential Burglaries. The report is often cited by home security companies attesting to the benefits of burglar alarms. Indeed, the author concluded there was a statistically significant correlation between burglar alarm installations and a decrease in residential burglaries (Lee, 2008, p. 295). However, the data also indicated that while fewer homes with alarms were subject to burglaries, they were more likely to be targeted, 3.75% compared to 2.32% for homes without alarms (Lee, 2008, pp. 131-133). The 359-page report written for the Alarm Industry Research & Educational Foundation did not explain the unintended finding. Perhaps it can be explained by what some ascribe as Sutton’s Law for first considering the obvious choice, mistakenly attributed to Willie Sutton who reportedly answered the question why he robbed...
banks saying: “That’s where the money is.” Despite their obvious high security, 5,014 banks were robbed in 2011 (Federal Bureau of Investigation, 2013). The circumstantial evidence does not invalidate Sandler and Lapan’s findings how attackers choose targets based on their expected probability of failure, but, it does offer an alternative target selection model for consideration.

Figure 4-5: AVM Investment Strategy Simulation for Single Dataset over Ten Years.
Each AVM simulation captures the expenditures and damages to 100 assets over a period of 10 years, as depicted in figure 4-5. A ten-year profile for a single asset is shown in figure 4-6. Simulations were executed in Windows 7 on a dedicated Dell® Vostro™ 3300 laptop computer with an Intel® Core™ i3, 2.4GHz processor, 4.0GB RAM, and 285GB hard disk drive. Each simulation performed 60,000 executions (6 strategies x 10 iterations x 100 sims x 10 years) on 100 asset records. Altogether, the three AVM simulations took 18 hours to execute from the time the master batch file was launched. Much of this time can be attributed to data collection for sensitivity analysis.

![Asset #98 Changing Theta Value Over 10 Years](image)

Figure 4-6: AVM Investment Strategy Simulation for Single Asset over Ten Years.
Data sensitivity analysis was facilitated by data collection between the CBA and SIP program modules. A Data Sensitivity Collector (DSC) was inserted to write asset records and recommended improvements to disk storage. A disk file was created for every 1,000 executions capturing up to 100,000 assets records (~14MB) containing data on 1) strategy type, 2) PAM execution options (i.e., % probability of attack and % Θ deviation), and 3) number of simulations over 10 years (100 assets x 10 years x 100 sims). The DSC program was created to capture data after system copy commands proved much too slow. Each investment strategy simulation produced ten data files for a total of 70 data files per AVM simulation. Data reduction and analysis was accomplished by the Data Sensitivity Analysis (DSA) program. DSA tallied asset records and calculated average results across each 10-year dataset and across all 10 datasets corresponding to 10% increments in attack probability or Θ deviation. The data averages were written to a CDF file and uploaded to a spreadsheet for analysis (DSA.xlsx).

In a similar fashion, simulation results were collected and analyzed using the Model Assessment Program (MAP). As previously detailed, SIP wrote cost and improvement purchase data to an expense output file and PAM did the same for damages and attacks. Again, each investment strategy simulation produced ten data files for a total of 140 data files per AVM simulation. These files weren’t nearly so large, averaging only 9kb in size. MAP took the two data files, Expended and Damages, and matched up data records and tallied results and recorded averages to a CDF output file, which was also uploaded to a spreadsheet for analysis (MAP.xlsx). Both DSA and MAP components are depicted in figure 4-2 and summarized in table 4-3. See Appendix C for a more detailed description of these programs.
<table>
<thead>
<tr>
<th>Function</th>
<th>Type</th>
<th>File Name</th>
<th>Arguments/Inputs</th>
<th>Ref.</th>
</tr>
</thead>
</table>
| Data Sensitivity Collector | C Program | DSC.c     | 1. Input Asset File (from CBA)  
2. Output Data Collection File (to DSA) | P-10 |
| Data Reduction             | C Program | DSA.c     | 1. Input Data Collection File (from DSC)  
2. Output Data Reduction File | P-11 |
| DSA Control                | Batch File| DSA.bat   | Call dsalc.bat  
Call dsalp.bat  
Call dsar44.bat  
Call das9.bat  
Call sahd.bat  
Call sahc.bat | |
| DSA Execution              | Batch File| DSAxx.bat | DSA dsaxx_10.txt dsaxx.txt  
DSA dsaxx_20.txt dsaxx.txt  
DSA dsaxx_30.txt dsaxx.txt  
DSA dsaxx_40.txt dsaxx.txt  
DSA dsaxx_50.txt dsaxx.txt  
DSA dsaxx_60.txt dsaxx.txt  
DSA dsaxx_70.txt dsaxx.txt  
DSA dsaxx_80.txt dsaxx.txt  
DSA dsaxx_90.txt dsaxx.txt  
DSA dsaxx_100.txt dsaxx.txt | |
| Data Analysis              | Spreadsheet| DSA.xlsx | Output from DSA.c | P-12 |
| Data Reduction             | C Program | MAP.c     | 1. Input Damages File (from PAM)  
2. Input Expenditures File (from SIP)  
3. Output Data Reduction File | P-13 |
| MAP Control                | Batch File| MAP.bat   | Call maplc.bat  
Call maplp.bat  
Call mapr44.bat  
Call maps9.bat  
Call maphd.bat  
Call maphc.bat | |
| MAP Execution              | Batch File| MAPxx.bat | MAP damagesxx_10.txt expendedxx_10.txt mapxx.txt  
MAP damagesxx_20.txt expendedxx_20.txt mapxx.txt  
MAP damagesxx_30.txt expendedxx_30.txt mapxx.txt  
MAP damagesxx_40.txt expendedxx_40.txt mapxx.txt  
MAP damagesxx_50.txt expendedxx_50.txt mapxx.txt  
MAP damagesxx_60.txt expendedxx_60.txt mapxx.txt  
MAP damagesxx_70.txt expendedxx_70.txt mapxx.txt  
MAP damagesxx_80.txt expendedxx_80.txt mapxx.txt  
MAP damagesxx_90.txt expendedxx_90.txt mapxx.txt  
MAP damagesxx_100.txt expendedxx_100.txt mapxx.txt | |
| Data Analysis              | Spreadsheet| MAP.xlsx | Output from MAP.c | P-14 |

**Table 4-4: AVM Investment Strategy Simulation Data Sensitivity & Analysis Programs**

### 4.4.3. Simulation Results

AVM12 conducted a simulation of the 7 investment strategies over 10 years using 100 executions to average out the results for a varying probability of attack from 10% to 100%.

Theta deviation was set at 20% for all executions. The Model Assessment Program examined
each strategy with respect to 1) the number of successful attacks, 2) total number of damages, 3) protective improvement expenditures, and 4) amount of protection ($\Delta \Theta$) purchased.

![AVM12 Successful Attacks](image)

Figure 4-7: AVM12 Comparison of Successful Attacks Across Investment Strategies.

As detailed previously, PAM3 calculated the probability of successful attack in stepwise fashion by first determining the probability of attack, then identifying the probable target, and finally examining the probability of failure against that target. The results for all six strategies are charted in figure 4-7. As would be expected, the number of attacks increases as the probability of attack increases. The number of expected attacks over 10 years ranges from 0.35 to 2.26 given a varying probability of attack from 10% to 100%. Overall, the Highest Consequence strategy suffered the fewest number of attacks.
Given a successful attack, PAM3 calculates damages as the product of $P(dim)$ and $\% (dam)$. As expected, damages increase as the probability of attack rises as shown in figure 4-8. The raw simulation results indicate that the Least Protected strategy suffered the least amount of damages.
As seen in figure 4-9, expenditures remained fairly constant within a given investment strategy, but varied considerably across investment strategies. While each investment strategy was given the same fixed budget every year ($50,000), their purchases were affected by 1) the cost of protective improvements, and 2) purchasing restrictions. In particular, the Region Protection and Sector Protection strategies (R44 and S9 in chart) restricted protective improvement purchases to specific regions and sectors, significantly constraining their expenditures. In the AVM12 simulation, RP had the lowest overall expenditures.

![AVM12 DTTheta Purchases](image)

**Figure 4-10**: AVM12 Comparison of Protection Purchases Across Investment Strategies.

The amount of protection purchased also varied across investment strategies. The Highest DTTheta strategy purchased the greatest amount of protective gain, as it was designed to do. Again, constrained by expenditure restrictions, both the RP and SP investment strategies purchased the least amount of protective gain.
AVM13 conducted the same simulations as AVM12 except it varied Theta deviation from 10% to 100%. Recall that Theta deviation is the attacker’s perception of probable failure, $\theta$, as a percentage of known $\Theta$. The smaller the deviation, the closer $\theta$ is to $\Theta$. The probability of attack was set at 32%, the median value of Clauset & Woodard’s prediction, for all executions. As might be expected, the number of attacks depicted in figure 4-11 remains fairly constant as a result of the fixed probability of attacks. Interestingly, figure 4-12 appears to show
a slightly decreasing trend in damages as an attacker’s perception varies farther away from known $\Theta$.

AVM14 is the same as AVM12 except it uses a different attack model, PAM4. As previously discussed, unlike PAM3, PAM4 selects targets based on highest consequence value not least probability of failure. At a glance, AVM14 simulation results depicted in figures 4-15 through 4-18 appear similar to AVM12. How closely they actually match and what conclusions can be safely drawn will be examined in the next section.
4.4.4. Simulation Analysis

This section will examine the results from three simulations, AVM12, AVM13, and AVM14, taking into account data variances in order to draw some conclusions on the seven protective measure investment strategies. The best strategy will be the one that results in the least amount of damages over time.

![Expected Number of Attacks Over 10 Years Given Increasing Attack Probabilities](image)

**Figure 4-19: PAM Attack Model.**

Analysis will begin by looking at the simulation attack model. As indicated previously in figure 4-4, the PAM model compares favorably with recent estimates of attack probabilities over the 40-year period from 1968 to 2007. Figure 4-19 shows the PAM profile for expected attacks over a 10-year period using the same methodology as previously. The model projects between 0.04 and 2.49 attacks occurring within this period. The average number of attacks for each
simulation falls comfortably within this range as shown in table 4-5. Please note that the narrow range of minimum and maximum attacks for AVM13 is a result of the probability of attack being held constant at 32% while varying Θ deviation from 10%-100%.

<table>
<thead>
<tr>
<th></th>
<th>PAM Model</th>
<th>AVM12</th>
<th>AVM13</th>
<th>AVM14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min # Attacks</td>
<td>0.48</td>
<td>0.35</td>
<td>1.22</td>
<td>0.34</td>
</tr>
<tr>
<td>Max # Attacks</td>
<td>2.49</td>
<td>2.51</td>
<td>1.49</td>
<td>2.14</td>
</tr>
</tbody>
</table>

Table 4-5: Simulation Attack Results

Damages will be the key determinant in differentiating investment strategies. The investment strategy that results in the fewest damages over ten years will obviously be best. The baseline results from AVM12 in figure 4-8 indicate that allocating resources to the Least Protected assets produces the fewest damages over time. The results, however, are skewed. Sensitivity data collected during simulation execution in figure 4-20 shows a variance between computed damages for each of the six investment strategies. To make an accurate comparison it is necessary to adjust simulation results to account for the variances.

Figure 4-20: AVM12 Average Computed Damages.
To make any accurate comparisons, the simulation results need to be adjusted to account for the data variances. This can be done by normalizing the results using the variance data itself. Figure 4-21 shows the adjusted computed damages after normalization. The same variances are now used to normalize the simulation results.

Figure 4-21: AVM12 Adjusted Computed Damages.

Figure 4-22: AVM12 Adjusted Damage Results.
Figure 4-22 shows the adjusted damage results for simulation AVM12. The AVM12 baseline and adjusted results are shown together in figure 4-23 for comparison. In this case, adjusting for simulation data variances did not affect the final outcome. The Least Protected investment strategy remains the best candidate.

Figure 4-23: AVM12 Comparative Damage Results.

Figure 4-22 shows the adjusted damage results for simulation AVM12. The AVM12 baseline and adjusted results are shown together in figure 4-23 for comparison. In this case, the Least Protected investment strategy remains the best candidate. Normalization of AVM13 data as shown in figures 4-24 through 4-27, however, shows a switch from Random Protection to the Least Cost investment strategy causing the least amount of damages. Similarly, AVM14 baseline data indicates Highest Consequence as the best investment strategy, but normalization gives the advantage to the Least Cost investment strategy, as shown in figure 4-31.
Figure 4-24: AVM13 Damage Data Variation.

Figure 4-25: AVM13 Adjusted Computed Damages.

Figure 4-26: AVM13 Adjusted Damage Results.

Figure 4-27: AVM13 Comparative Damages.
Figure 4-28: AVM14 Damage Data Variation.

Figure 4-29: AVM14 Adjusted Computed Damages.

Figure 4-30: AVM14 Adjusted Damage Results.

Figure 4-31: AVM14 Comparative Damages.
After adjusting for data variances, the results thus far favor two different investment strategies: Least Cost and Least Protected. These findings, however, are independent of each other. To make a comparison across strategies, it is necessary to normalize variances across strategies. This was done as shown in figures 4-34 through 4-37. The tabulated results are shown in figure 4-33.

Figure 4-32: Independent Damage Results Across Simulations.

Figure 4-33: Combined Damage Results Across Simulations.
Figure 4-34: Damage Results Across Simulations.

Figure 4-35: Damage Variances Across Simulations.

Figure 4-36: Data Normalization Across Simulations.

Figure 4-37: Adjusted Damages Across Simulations.
Interestingly, data normalization across simulations doesn’t change the preference order for investment strategies: LP (AVM12), LC (AVM13), and LC (AVM14). It should be noted as indicated in figure 4-33 that AVM14 produces substantially more damages than when attackers select a target based on their perceived probability of failure. Still, the question remains which investment strategy offers the best return on investment. Now that the damages are normalized across simulations, it is possible to take the average to determine the aggregate best strategy. The final result shown in figure 4-37 shows a clear preference for the Least Cost investment strategy with 13.7% fewer damages than Least Protection, the investment strategy with the next fewest damages.

Figure 4-37: Final Simulation Results.
4.4.5. Simulation Findings

This section used AVM to examine seven alternative investment strategies under varying probabilities of attack, attacker perceptions, and attack models. Not surprisingly, it found that the potential for catastrophic damage increases as the probability of attack increases. Interestingly, though, it appears that damages decrease as attackers’ perceptions of their own failure drifts farther from the known Θ value. An exception appears to occur, though, if attackers use some other criteria for selecting targets, such as highest consequences. This finding deserves further investigation. The aggregate results, however, after data variations across simulations have been accounted, favor the Least Cost investment strategy. As mentioned at the outset, this strategy offers the advantage over the other strategies of purchasing more protective improvements for more assets. As far as which strategies proved least effective, the Region Protection and Sector Protection strategies exhibited the highest damages. As previously explained, these are probably an artifice of the simulation since it only allocated funding to one region (#44) and one sector (#9). As described earlier, DHS Urban Areas Security Initiative grants are not nearly so restrictive, encompassing some 100 major metropolitan areas. For this reason, these results should be discounted. Overlooking the RP and SP strategy results leaves RAN with the highest proportion of damages. This is interesting because without a metric to guide current homeland security strategy, current protective improvement purchases may be considered essentially random. These results demonstrate the advantage of having a performance measure such as that provided by AVM to more effectively guide homeland security strategy. Are these results conclusive? Unlikely. There are many more variables and refinements worth investigating, including different attack models. However, this investigation demonstrates the ability of AVM to provide objective guidance for strategic decisions.
4.5. Summary

The Asset Vulnerability Model works with the DHS Risk Management Framework to inform resource investment decisions protecting the nation’s critical infrastructure. WMD protection is the responsibility of federal agencies outside the Department of Homeland Security and beyond the current reach of the Risk Management Framework. As determined by Sandler and Lapan’s research in game theory, a coordinated defense among all targets is more efficient than an uncoordinated one. Interagency coordination is directed from the National Security Council towards strategic objectives specified in National Security Strategy. Homeland security strategy is a subset of national security strategy. Current homeland security definitions and strategy focus on terrorism and hazards. A new definition and strategy is proposed focusing interagency efforts on domestic catastrophic attack. With an appropriate supporting policy structure, RMF can be extended to encompass both CI and WMD. Thus AVM can help guide the nation towards a unified homeland security strategy.

4.5. Contributions

This research offers circumstantial evidence that domestic catastrophic attack is the homeland security threat. It proposes a significant national policy shift away from terrorism to concentrate on the catastrophic threats presented by critical infrastructure and weapons of mass destruction. In this manner, it uniquely answers the question “what is homeland security?” It also provides a unifying policy framework for coordinating protection among CI and WMD, which game theory suggests is most efficient. It also demonstrates the effective ability of an appropriate metric to objectively guide strategic decisions.
Chapter 5. Contributions and Future Work

5.1. Research Contributions

This research has made significant contributions to understanding the homeland security threat, developing a viable risk formulation, supporting informed risk management, and directing national efforts towards a unified strategy.

1. Understanding. This research provides a comprehensive review of the homeland security threat represented by critical infrastructure and weapons of mass destruction.

2. Understanding. This research provides a comprehensive analysis of CI and WMD protection efforts.

3. Risk Management. This research proposes substantiated criteria for conditioning an ill-behaved problem.

4. Risk Management. This research provides substantiated justification for choosing an asset-based approach over event-driven approaches for anthropic threats.

5. Risk Management. This research uniquely solves the problem of reliable threat estimation by reducing it to threat localization through a defined target set.

6. Risk Management. This research provides substantiated justification for structuring a risk formulation based on the five phases of Integrated Emergency Management.

7. Risk Management. This research uniquely solves the problem of quantifying catastrophic consequences across time and space using well-developed national indicators.

8. Risk Management. This research uniquely developed a homeland security risk methodology that 1) concisely conveys current risk levels, 2) supports cost-benefit analysis, 3) demonstrates risk reduction effects across multiple assets at different levels of management, and 4) measures and tracks investments and improvements over time.
9. Risk Formulation. This research uniquely proposes a homeland security risk measure
designated as \( \Theta \), probability of attack failure, based on earlier work in game theory.

10. Risk Formulation. This research uniquely distinguishes between threat prediction and threat
warning for homeland security.

11. Risk Formulation. This research uniquely adapts the DHS Protective Measure Index as both
an indication of current status and potential improvement.

12. Risk Formulation. This research uniquely proposes a homeland security risk formulation that
is transparent and repeatable.

13. Risk Management. This research uniquely developed a cost-benefit analysis capability for
choosing optimum homeland security resource investments.

14. Risk Management. This research uniquely developed decision support tools providing
flexible insight to informing homeland security resource investment decisions.

15. Risk Management. This research uniquely provides unifying direction to a currently
fragmented and uncoordinated CI protection program.

16. Risk Management. This research provides a vertically integrated solution and is uniquely
compatible with current DHS organizations and programs.

17. Policy. This research provides substantiated justification why CI and WMD are the homeland
security problem.

18. Policy. This research uniquely proposes a national policy framework leading towards a
unified homeland security strategy encompassing both CI and WMD threats.

19. Policy. This research uniquely answers the question “what is homeland security?”
20. **Policy.** This research provides an unprecedented capability to answer the fundamental homeland security questions: how safe are we, how much safer can we be, and how much will it cost?

In short, the this research 1) offers criteria for developing an appropriate risk methodology for the challenging problem of homeland security, 2) demonstrates a compatible risk model to provide quantitative direction that has so far eluded DHS, and 3) answers the fundamental question “what is homeland security” to develop a coordinating policy framework leading towards a unified homeland security strategy.

### 5.2. **Future Research**

While this research has endeavored to present a comprehensive framework for defining and improving homeland security, some important implementation details remain for future research.

First, a definitive taxonomy must be developed to help identify those things that can create a domestic catastrophic attack. DHS previously developed a taxonomy for its National Asset Database. (Moteff, Critical Infrastructure: The National Asset Database, 2007, p. 9) Perhaps it can be adopted for this application. CARVER+Shock analysis has also been employed and may be sufficiently useful (Food and Drug Administration, 2012). Related to this effort is defining “catastrophic attack.” In 2002, the term “macroterrorism”, was coined as “an act of terrorism causing at least 500 deaths, and/or property damage or economic loss exceeding $1 billion” (Williams, 2002, p. 9). For reasons stated in this research, the word “terrorism” should be avoided as part of any definition of “catastrophic attack.” As concern for homeland
security began with 9/11, maybe it should become the benchmark: “Any deliberate act inflicting over 3,000 deaths or $40 billion in damages.” This remains an area to be explored.

Perhaps the biggest challenge to AVM is developing acceptable estimates for $\Delta \Theta$ on proposed improvement measures. Accuracy is the objective, but this requires a foundation of data that is currently (and fortunately) not present. In its absence, the next best objective is consistency. In this respect, modeling would be the preferred solution. It will be extremely difficult, though, to build a model capable of evaluating all the novel solutions it is likely to encounter. Difficult, but not impossible if each solution can be methodically deconstructed into a set of underlying principles on which the model is based. Whether such principles exist and how they may be extracted is another area for potential research. In the absence of such models, expert elicitation may be the most practical method, so long as it is adequately structured and formally conducted as recommended by the National Research Council (National Research Council, 2010, p. 49).

Understandably, the National Research Council also placed a premium on verifying and validating model results (National Research Council, 2010, p. 12). Again, the availability of historical data is problematic. In this regard, the National Research Council suggests one possible method recommended by the JASON scientific advisory group to “address smaller, well-defined, testable pieces of the larger problem” (National Research Council, 2010, p. 48). How this might be accomplished is also an area for research.

Finally, AVM does not address the psychological impact of domestic catastrophic attack, which the National Research Council deemed “significant and may be the primary goal of terrorists” (National Research Council, 2010, p. 5). From this remark it is inferred that the chief psychological concern is a public outcry provoking a major policy shift, administration change,
or reformation of US government placing the nation in greater international peril or undermining the constitutional principles upon which it is founded. AVM indirectly addresses these concerns on the assumption that intangible effects proceed from tangible ones. Whether this assumption is valid, and examining the relationship between public sentiment and national welfare remains an area for future research.

5.3. Conclusion

Developing an appropriate metric is essential to guiding homeland security policy and ensuring efficient allocation of national resources. While the Department of Homeland Security has adopted a risk management approach, an extensive review by the National Research Council concluded that none of their models are adequate for supporting decision making. This research draws on that review to propose criteria for developing an appropriate metric and introduces an Asset Vulnerability Model. AVM consists of baseline analysis, cost-benefit analysis, and decision support tools predicated on a measure of Θ, and attacker’s probability of failure. AVM is unique in a number of respects, particularly in avoiding the problem of reliable threat estimation while meeting criteria suggested by the National Research Council review. AVM is also compatible with current DHS processes and organizations. With the right supporting framework, AVM can lead the nation towards a unified homeland security strategy and answer the fundamental questions: how safe are we, how much safer can we be, and how much will it cost.
(This Page Intentionally Blank)
### Appendix A: Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAE</td>
<td>Annualized Attack Expectancy</td>
</tr>
<tr>
<td>AECA</td>
<td>Arms Export Control Act</td>
</tr>
<tr>
<td>ATSA</td>
<td>Aviation and Transportation Security Act</td>
</tr>
<tr>
<td>AVM</td>
<td>Asset Vulnerability Model</td>
</tr>
<tr>
<td>BAM</td>
<td>Baseline Asset Model</td>
</tr>
<tr>
<td>BIRR</td>
<td>Better Infrastructure Risk and Resilience</td>
</tr>
<tr>
<td>BMI</td>
<td>Protection of CI – Baseline Protection Concept</td>
</tr>
<tr>
<td>BWC</td>
<td>Biological Weapons Convention</td>
</tr>
<tr>
<td>C2CRE</td>
<td>Command and Control CBRN Consequence Response Element</td>
</tr>
<tr>
<td>CAPRA</td>
<td>Critical Asset and Portfolio Risk Analysis for Homeland Security</td>
</tr>
<tr>
<td>CBA</td>
<td>Cost-Benefit Analysis</td>
</tr>
<tr>
<td>CBRN</td>
<td>Chemical, Biological, Radiological, and Nuclear Agents</td>
</tr>
<tr>
<td>CCMRF</td>
<td>CBRN Consequence Management Response Force</td>
</tr>
<tr>
<td>CDC</td>
<td>Centers for Disease Control and Prevention</td>
</tr>
<tr>
<td>CDF</td>
<td>Comma Delimited Format</td>
</tr>
<tr>
<td>CEM</td>
<td>Comprehensive Emergency Management</td>
</tr>
<tr>
<td>CERFP</td>
<td>CBRN Enhanced Response Force Package</td>
</tr>
<tr>
<td>CIKR</td>
<td>Critical Infrastructure and Key Resources</td>
</tr>
<tr>
<td>CIMS</td>
<td>Critical Infrastructure Modeling Simulation</td>
</tr>
<tr>
<td>CIPDSS</td>
<td>Critical Infrastructure Protection Decision Support System</td>
</tr>
<tr>
<td>CIPMA</td>
<td>Critical Infrastructure Protection Modeling and Analysis</td>
</tr>
<tr>
<td>CM</td>
<td>Consequence Management</td>
</tr>
<tr>
<td>CP</td>
<td>Counterproliferation</td>
</tr>
<tr>
<td>CPA</td>
<td>Cumulative Probability of Attack</td>
</tr>
<tr>
<td>CREATE</td>
<td>Center for Risk and Economic Analysis of Terrorism Events</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>CRS</td>
<td>Congressional Research Service</td>
</tr>
<tr>
<td>CWMD</td>
<td>Counter-WMD</td>
</tr>
<tr>
<td>DC</td>
<td>Deputies Committee</td>
</tr>
<tr>
<td>DCRF</td>
<td>Defense CBRN Response Force</td>
</tr>
<tr>
<td>DECRIS</td>
<td>Risk and Decision Systems for Critical Infrastructure</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOE</td>
<td>Department of Energy</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
</tr>
<tr>
<td>DOS</td>
<td>Department of State</td>
</tr>
<tr>
<td>DRC</td>
<td>Disaster Research Center</td>
</tr>
<tr>
<td>DSA</td>
<td>Data Sensitivity Analysis</td>
</tr>
<tr>
<td>DSC</td>
<td>Data Sensitivity Collector</td>
</tr>
<tr>
<td>EAA</td>
<td>Export Administration Act</td>
</tr>
<tr>
<td>ECIP</td>
<td>Enhanced Critical Infrastructure Protection Program</td>
</tr>
<tr>
<td>EOP</td>
<td>Executive Office of the President</td>
</tr>
<tr>
<td>ESF</td>
<td>Emergency Support Function</td>
</tr>
<tr>
<td>EURACOM</td>
<td>European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks</td>
</tr>
<tr>
<td>FAIT</td>
<td>Fast Analysis Infrastructure Tool</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Agency</td>
</tr>
<tr>
<td>FY</td>
<td>Fiscal Year</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>GDP</td>
<td>Gross Domestic Product</td>
</tr>
<tr>
<td>GPRA</td>
<td>Government Performance and Results Act</td>
</tr>
<tr>
<td>HAZMAT</td>
<td>Hazardous Materials</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>HC</td>
<td>Highest Consequence</td>
</tr>
<tr>
<td>HD</td>
<td>Highest DTheta</td>
</tr>
<tr>
<td>HHS</td>
<td>Department of Health and Human Services</td>
</tr>
<tr>
<td>HRF</td>
<td>Homeland Response Force</td>
</tr>
<tr>
<td>HSC</td>
<td>Homeland Security Council</td>
</tr>
<tr>
<td>HSGP</td>
<td>Homeland Security Grant Program</td>
</tr>
<tr>
<td>HSPD</td>
<td>Homeland Security Presidential Directive</td>
</tr>
<tr>
<td>IEMS</td>
<td>Integrated Emergency Management System</td>
</tr>
<tr>
<td>IG</td>
<td>Inspector General</td>
</tr>
<tr>
<td>IND</td>
<td>Improvised Nuclear Device</td>
</tr>
<tr>
<td>IPC</td>
<td>Interagency Policy Committee</td>
</tr>
<tr>
<td>IPIS</td>
<td>Infrastructure Protection and Information Security Programs</td>
</tr>
<tr>
<td>JASON</td>
<td>No Acronym Given</td>
</tr>
<tr>
<td>LC</td>
<td>Least Cost</td>
</tr>
<tr>
<td>LP</td>
<td>Least Protected</td>
</tr>
<tr>
<td>MAP</td>
<td>Model Assessment Program</td>
</tr>
<tr>
<td>MDM</td>
<td>Modular Dynamic Model</td>
</tr>
<tr>
<td>MIN</td>
<td>Multiyear Infrastructure Network</td>
</tr>
<tr>
<td>N-ABLE</td>
<td>Agent-Based Laboratory for Economics</td>
</tr>
<tr>
<td>NADB</td>
<td>National Asset Database</td>
</tr>
<tr>
<td>NAR</td>
<td>National CIKR Resources Protection Annual Report</td>
</tr>
<tr>
<td>NCIPP</td>
<td>National Critical Infrastructure Prioritization Program</td>
</tr>
<tr>
<td>NEMO</td>
<td>Net-Centric Effects-based Operations Model</td>
</tr>
<tr>
<td>NEP</td>
<td>National Exercise Program</td>
</tr>
<tr>
<td>NGA</td>
<td>National Governor’s Association</td>
</tr>
<tr>
<td>NIPP</td>
<td>National Infrastructure Protection Plan</td>
</tr>
<tr>
<td>NISAC</td>
<td>National Infrastructure Simulation and Analysis Center</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NP</td>
<td>Nonproliferation</td>
</tr>
<tr>
<td>NPG</td>
<td>National Preparedness Goal</td>
</tr>
<tr>
<td>NPPD</td>
<td>National Protection Programs Directorate</td>
</tr>
<tr>
<td>NPS</td>
<td>National Preparedness System</td>
</tr>
<tr>
<td>NPT</td>
<td>Nuclear Nonproliferation Treaty</td>
</tr>
<tr>
<td>NRC</td>
<td>National Research Council</td>
</tr>
<tr>
<td>NRC</td>
<td>Nuclear Regulatory Commission</td>
</tr>
<tr>
<td>NRF</td>
<td>National Response Framework</td>
</tr>
<tr>
<td>NRF-CIA</td>
<td>National Response Framework Catastrophic Incident Annex</td>
</tr>
<tr>
<td>NRIA</td>
<td>Nuclear/Radiological Incident Annex</td>
</tr>
<tr>
<td>NRP</td>
<td>National Risk Profile</td>
</tr>
<tr>
<td>NSC</td>
<td>National Security Council</td>
</tr>
<tr>
<td>NSPD</td>
<td>National Security Presidential Directive</td>
</tr>
<tr>
<td>NSRAM</td>
<td>Network Security Risk Assessment Modeling</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>PAM</td>
<td>Probable Attack Model</td>
</tr>
<tr>
<td>PC</td>
<td>Principals Committee</td>
</tr>
<tr>
<td>PIM</td>
<td>Protective Improvement Model</td>
</tr>
<tr>
<td>PL</td>
<td>Public Law</td>
</tr>
<tr>
<td>PMI</td>
<td>Protective Measure Index</td>
</tr>
<tr>
<td>PML</td>
<td>Probable Maximum Loss</td>
</tr>
<tr>
<td>PNSR</td>
<td>Project on National Security Reform</td>
</tr>
<tr>
<td>PPD</td>
<td>Presidential Policy Directive</td>
</tr>
<tr>
<td>PSA</td>
<td>Protective Security Advisor</td>
</tr>
<tr>
<td>RAMCAP-Plus</td>
<td>Risk Analysis and Management for Critical Asset Protection</td>
</tr>
<tr>
<td>RDD</td>
<td>Radiological Dispersion Device</td>
</tr>
<tr>
<td>RMCIS</td>
<td>Risk Management for Critical Infrastructure Sectors</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>RMF</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>RMS</td>
<td>Risk Management Solutions</td>
</tr>
<tr>
<td>RP</td>
<td>Region Protection</td>
</tr>
<tr>
<td>RRAP</td>
<td>Regional Resiliency Assessment Program</td>
</tr>
<tr>
<td>RVA</td>
<td>Risk and Vulnerability Analysis</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SHIRA</td>
<td>Strategic Homeland Infrastructure Risk Assessment</td>
</tr>
<tr>
<td>SIP</td>
<td>Selective Improvement Program</td>
</tr>
<tr>
<td>SLGP</td>
<td>State and Local Grant Programs</td>
</tr>
<tr>
<td>SP</td>
<td>Sector Protection</td>
</tr>
<tr>
<td>SRAM</td>
<td>Sandia Risk Assessment Methodology</td>
</tr>
<tr>
<td>SSA</td>
<td>Sector-Specific Agency</td>
</tr>
<tr>
<td>SSP</td>
<td>Sector Specific Plan</td>
</tr>
<tr>
<td>TCL</td>
<td>Target Capabilities List</td>
</tr>
<tr>
<td>THIRA</td>
<td>Threat and Hazard Identification and Risk Assessment</td>
</tr>
<tr>
<td>TMI</td>
<td>Three Mile Island</td>
</tr>
<tr>
<td>TRIA</td>
<td>Terrorism Risk Insurance Act</td>
</tr>
<tr>
<td>TSA</td>
<td>Transportation Security Administration</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>WMD</td>
<td>Weapons of Mass Destruction</td>
</tr>
<tr>
<td>WMD-CST</td>
<td>WMD Civil Support Team</td>
</tr>
<tr>
<td>Y2K</td>
<td>Year 2000</td>
</tr>
</tbody>
</table>
(This Page Intentionally Blank)
Appendix B: CI Protection Models

In 2012, the Joint Research Centre of the European Commission conducted a survey of critical infrastructure risk methodologies to inform the European Programme for Critical Infrastructure Protection (Giannopoulos, Filippini, & Schimmer, 2012, p. 5). The survey examined twenty-one models providing insight for the comparative analysis conducted in Chapter 3. With two exceptions, a quick summary of each model is provided in this appendix. The DHS Risk Management Framework is not included because it is examined extensively in Chapter 2. By the same token, CAPRA, which was not included in the 2012 survey, is briefly summarized here. The models are listed in alphabetical order.

B.1. BIRR

Better Infrastructure Risk and Resilience (BIRR)

Argonne National Laboratory

Argonne National Laboratory has provided key technical support to a U.S. Department of Homeland Security (DHS) program by developing a methodology for assessing infrastructure risk and resilience to a variety of natural and man-made hazards. These include energy facilities, transportation assets, water treatment plants, financial institutions, and commercial office buildings. Argonne also developed statistical and data-mining procedures to analyze and display the data collected in easy-to-use "dashboards."

The program, called the Enhanced Critical Infrastructure Protection (ECIP) Program, relies on information collected by 93 DHS Protective Security Advisors (PSAs) who are located throughout the United States. The PSAs use a Web-data collection template that Argonne
developed for DHS. The ECIP template - and underlying methodology - has more than 1,500 variables covering six major security-related components (e.g., physical security and security management) and 42 subcomponents (e.g., access control). Data collected as part of the ECIP Program undergo extensive quality assurance and quality control processes.

To facilitate comparisons among critical assets across the 18 critical infrastructure sectors (e.g., Energy, Critical Manufacturing, Transportation Systems, and Water), Argonne has developed a procedure to use the collected data to estimate a vulnerability index (VI). The process for developing a VI begins with the creation of a protective measures index (PMI). The PMI is constructed so that it increases as protective measures are added. The gathered information is used to assist DHS in analyzing sector (e.g., Energy) and subsector (e.g., electricity, oil, and natural gas) vulnerabilities to identify potential ways to reduce vulnerabilities and to assist in preparing sector risk estimates. The owner/operator of infrastructure facilities also receives a dashboard, which analyzes the data collected for a specific asset. To date, more than 1,800 interactive "what if" analysis dashboards have been delivered to facilities across the United States. The dashboards show a comparison of the facility's protection posture with that of similar sector/subsectors visited. This comparison gives the operator a feel for the asset's security strengths and weaknesses, which may be contributing factors to its vulnerability and protection posture.

The development of the PMI and the associated VI is intended to assist DHS in conducting analyses of the vulnerabilities associated with the nation's critical infrastructure and to explore cost-effective ways to reduce those vulnerabilities. In addition, the approach can provide valuable information to owners and operators about where they stand relative to similar assets and protective measures that they may want to consider to reduce their vulnerability. The
applications and uses of the PMI are at a very early stage in the ECIP Program, and improvements in concept and approach are expected as the program matures. ECIP results, however, have been prominently featured in DHS reports on progress in protecting the nation's critical infrastructure.

Recently, work has begun on developing a resiliency index from the question set of the ECIP that will assess the robustness, resourcefulness (pre-event and post-event), and recovery of a facility based on the same concept.

(Argonne National Laboratories)

B.2. BMI

Protection of Critical Infrastructures – Baseline Protection Concept (BMI)

German Federal Ministry of Interior

The aim of this baseline protection concept is to reduce the vulnerability of critical infrastructures to natural events and accidents as well as terrorist attacks and criminal acts. In this context it focuses on building-related, organizational, personal and technical protection measures.

The need for a baseline protection concept arises from statutory regulations and generally recognized standards, as well as generally recognized business principles of anticipatory risk management and strategic business planning geared to success and continuity – in the form of so-called business continuity management (BCM), for example.
The initial target group for the development of strategic concepts for danger analysis, risk management systems and risk minimization measures is top level management at infrastructure operators, who should bear the business risk and, where appropriate, liability risks in case of contraventions. The security officers are generally the points of contact at the companies for implementation of these strategic concepts. Implementation of the baseline protection concept is ultimately a task for the entire business in question, requiring support from all levels.

Trusting co-operation between the state and infrastructure operators is a prerequisite for clearly defining comprehensive protection measures. It is the operators who possess an adequate detailed knowledge of their infrastructures and are in a position to implement concrete protection measures in an effective manner. Agreement thus first of all requires to be reached as to what level of protection is desired and acceptable.

The starting point is a multi-stage analysis and planning process covering identification of the given risks and a subsequent review, together with the adaptation of protective measures, where necessary. This process can be structured as follows:

- The establishment of danger categories, differentiated according to the areas of natural disasters, accident, terrorism/crime,
- based on the above, definition of the respective protection levels,
- the development of damage and threat scenarios,
- the analysis of weak points,
- the formulation of protection objectives as a basis for the definition of protection measures and counter-measures,
• definition of the required scope of action (coordination between public- and private-sector measures),
• implementation of the defined required scope of action and
• regular reviews of this analysis and planning process for the purposes of quality management.

Potential dangers for critical infrastructures are outlined as initial points of reference. These essentially cover dangers resulting from natural events, technical failure or human error and terrorism/criminal acts. On the basis of these defined dangers, particularly endangered areas at companies can be identified and generalized baseline protection recommendations can be drawn up.

Where this process is considered to be too cost-intensive or difficult to implement, such as at small and medium-sized enterprises (SME), it may well be expedient to approach the matter in small steps, initially addressing aspects of the baseline protection concept that are considered especially urgent.

A questionnaire and a checklist (Appendix 1), have been developed as an aid to operators of infrastructure facilities in implementing the baseline protection concept. The questionnaire and the checklist are designed as interdisciplinary instruments and are intended primarily to initiate a discussion process within companies on how to enhance and effectively control security. Both the questionnaire and the checklist are to be considered only as samples, rather than definitive inventories. This means that missing items require to be added in the course of the process and any inappropriate questions are to be modified or deleted accordingly.
The aim of this development process is to jointly set priorities from the perspective of internal security in close consultation with the infrastructure operators and to operationalize measures for the protection of critical infrastructures.

(German Federal Ministry of the Interior, p. Summary).

**B.3. CAPRA**

**Critical Asset and Portfolio Risk Analysis for Homeland Security (CAPRA)**

University of Maryland, College Park

CAPRA supports operational and strategic resource allocation decisions at any level of leadership or system abstraction. The CAPRA methodology consists of six analysis phases: scenario identification, consequence and severity assessment, overall vulnerability assessment, threat probability assessment, actionable risk assessment, and benefit-cost analysis. The results from the first four phases of CAPRA combine in the fifth phase to produce actionable risk information that informs decision makers on where to focus attention for cost-effective risk reduction. If the risk is determined to be unacceptable and potentially mitigable, the sixth phase offers methods for conducting a probabilistic benefit-cost analysis of alternative risk mitigation strategies. Several case studies are provided to demonstrate the methodology, including an asset-level analysis that leverages systems reliability analysis techniques and a regional-level portfolio analysis that leverages techniques from approximate reasoning.

CARVER2™

National Infrastructure Institute (NI2)

The NI2 Centre for Infrastructure Expertise is working closely with operators, government, private industry in order to ensure the protection of critical infrastructures in US. CARVER2 is a tool that has been developed in order to serve the needs of critical infrastructure analysis mostly from the policy maker point of view. CARVER stands for Criticality Accessibility Recoverability Vulnerability Espyability Redundancy. NI2 states that it is a non-technical method for comparing and ranking critical infrastructure and key resources and also claims CARVER2 to be the only assessment tool that ranks critical infrastructure across sectors. A stand-alone PC tool and a server/client version (CARVER2Web) have been developed for the implementation of this methodology. The methodology is supposed to cover both terrorist threats as well as natural disasters, thus implementing an all-hazards approach.

CARVER2 assess infrastructure using six different criteria. The criticality is in fact the impact assessment part of the methodology. It is remarkable that it is in good agreement with the cross-cutting criteria of the EPCIP Directive in terms of impact categories (users affected, direct economic loss and cost to rebuild, potential casualties). Accessibility refers to the possibility that terrorists can enter the infrastructure to provoke destruction, it is thus mostly an assessment of the vulnerability of the infrastructure in terms of physical security. The recoverability in fact partially covers resilience since it refers to the bouncing back capability of the infrastructure after failure. The vulnerability covers part of the potential infrastructure vulnerabilities, the ones related to terrorist attacks and more specifically to explosions and chemical/biological threats.
Clearly at this point the claimed all hazards approach is not evident. The Espyability criterion refers to the function of an infrastructure as an icon (e.g. cultural site) with indirect impact. However, the implementation to quantify this is not thoroughly explained. Finally the Redundancy refers to the alternatives that exit for the asset in consideration.


**B.5. CIMS**

**Critical Infrastructure Modeling Simulation (CIMS)**

Idaho National Laboratory

Developed in 2005 by four INL infrastructure protection engineers, the Critical Infrastructure Modeling System (CIMS) is a software application that visually portrays the interoperability of numerous infrastructure sectors. The CIMS program relies on an easy-to-use graphical user interface, which allows a decision maker to build models on the fly and which supports rapid model construction from limited, open-source information.

Using only a simple map or aerial photo, CIMS users can start construction of an infrastructure model. As additional information, changing circumstances or intelligence data becomes available, the model can be updated to create a real-time view of dynamic environments similar to those after a hurricane or terrorist attack. External data sources such as Web links including webcam or direct sensor feeds can also be built into the model.

CIMS seeks to provide emergency planners with a high-level analysis of infrastructure interoperabilities without requiring detailed engineering data to support the model. In this way,
users can quickly construct three-dimensional models of cities and counties and run multiple infrastructure failure scenarios.

By identifying which infrastructures affect the greatest number of people, resources such as utility companies, first responders and government agencies can plan ahead and prioritize resources to return the region to a normal operating state.

In 2006, CIMS was licensed for commercial production to Massachusetts-based Priority 5 Holdings, Inc.

(Idaho National Laboratory, 2013)

\textit{B.6. CIPDSS}

\textbf{Critical Infrastructure Protection Decision Support System (CIPDSS)}

Los Alamos National Laboratory, National Infrastructure Simulation and Analysis Center

The Critical Infrastructure Protection Decision Support System (CIPDSS) provides information and decision support for the protection of critical infrastructures based on an assessment of risks appropriately accounting for the likelihood of threat, vulnerabilities, and uncertain consequences associated with terrorist activities, natural disasters, and accidents.

Model Characteristics

- High-level, aggregated model of national and metropolitan scales
- System dynamics-based
- Represents 17 CIKR and primary interdependencies
CIPDSS is a computer simulation and decision analytic tool that informs users when making difficult choices between alternative mitigation measures and operational tactics, or when allocating limited resources to protect the nation’s critical infrastructures against existing and future threats. CIPDSS integrates event simulation with a risk assessment process, explicitly accounting for uncertainties in threats, vulnerabilities, and the consequences of terrorist acts and natural disasters. CIPDSS models the primary interdependencies that link 17 CIKR together and calculates the impacts that cascade into these interdependent infrastructures and into the national economy.

Where Is the Tool Applied? CIPDSS can be applied to almost any infrastructure disruption. CIPSS has been demonstrated on several case studies: pandemic influenza, accidental chemical release, biological attack, telecommunications disruption, and dam breach.

CIPDSS Application to Infrastructure Disruption Analysis. NISAC’s CIPDSS team has interviewed critical infrastructure protection decision makers and stakeholders to identify requirements for the decision support system, scope out the decision environment, and quantify the prioritization of consequences. The taxonomy of decision metrics includes fatalities, injuries, economic loss, and public confidence.

Model Confidence. An independent panel comprised from academia, industry, and government conducted a technical review of CIPDSS. Selected submodels have been reviewed by experts and results of disruption scenario analyses have been presented at workshops for peer review. Some submodels have been compared to high-resolution models (Los Alamos National Laboratory, 2013).
B.7. CIPMA

Critical Infrastructure Protection Modeling and Analysis (CIPMA)

Australia Attorney General’s Department

Overview. The Critical Infrastructure Protection Modeling and Analysis program (CIPMA) is a computer based tool to support business and government decision making for critical infrastructure (CI) protection, counter-terrorism and emergency management, especially with regard to prevention, preparedness, and planning and recovery. CIPMA is designed to examine the relationships and dependencies within and between critical infrastructure systems, and to demonstrate how a failure in one sector can greatly affect the operations of critical infrastructure in other sectors. CIPMA uses a vast array of data and information from a range of sources to model and simulate the behavior and dependency relationships of critical infrastructure systems. The capability will include a series of impact models to analyze the effects of a disruption to CI services. The CIPMA Program currently focuses on three priority sectors: banking and finance, communications, and energy. The capability was launched by the Attorney-General in February 2006. “Proof of concept” of the capability was successfully demonstrated to key business and government stakeholders in May 2006. Although CIPMA is still in development, results from the capability are already assisting the development and direction of government policy in national security and critical infrastructure protection (CIP), and helping owners and operators to better protect their critical infrastructure.

Development goals – The current focus is on broadening and deepening CIPMA coverage of the three priority sectors, the Sydney commercial business district (CBD) precinct, and development of impact models for the Decision Support Module. The impact models will assess the flow-on
consequences of a CI service disruption, the economic impacts of the disruption, the effects on population, time/duration and area of the disruption, and the behavior of networks and clusters of infrastructure as a result of the service interruption. Work on a fourth sector will commence by July 2007.

Intended users – Users include CI owners and operators and Australian local governments.

System output – Output will include geographic information system (GIS) functionality for data capture, management, and visualization. System behavior will determine dependencies and time-based impacts of disruptive events on infrastructure networks.

Maturity – In development, some tools are complete.

Areas modeled – Australian critical infrastructure networks and high priority precincts (e.g., capital cities).

Customers/sponsors – Australian government, state and territory governments, CI owners and operators.

(Pederson, Dudenhoeffer, Hartley, & Permann, 2006, p. 43)

**B.8. CommAspen**

**CommAspen**

Sandia National Laboratory

Overview – CommAspen is a new agent-based model for simulating the interdependent effects of market decisions and disruptions in the telecommunications infrastructure on other critical
infrastructures in the U.S. economy such as banking and finance, and electric power.

CommAspen extends and modifies the capabilities of Aspen-EE, an agent-based model previously developed by Sandia National Laboratories to analyze the interdependencies between the electric power system and other critical infrastructures. CommAspen has been tested on a series of scenarios in which the communications network has been disrupted, due to congestion and outages. Analysis of the scenario results indicates that communications networks simulated by the model behave as their counterparts do in the real world. Results also show that the model could be used to analyze the economic impact of communications congestion and outages.

Development goals – To analyze interdependent infrastructure systems in a more holistic way, Sandia and other research institutions have developed models of critical infrastructure systems using agent-based approaches. Sandia’s first agent-based model of the U.S. economy, developed in the mid-1990s, is called Aspen. This model is a Monte Carlo simulation that uses agents to represent various decision making segments in the economy, such as banks, households, industries, and the Federal Reserve. An agent is a computational entity that receives information and acts on its environment in an autonomous way; that is, an agent’s behavior depends at least partially on its own experience. Through the use of evolutionary learning techniques, Aspen allows us to examine the interactive behavior of these agents as they make real-life decisions in an environment where agents communicate with each other and adapt their behaviors to changing economic conditions, all the while learning from their past experience. In 2000, Sandia developed a new model of infrastructure interdependency called Aspen-EE. This model extended the capabilities of Aspen to include the impact of market structures and power outages in the electric power system, a critical infrastructure, on other infrastructures in the economy.
One of the limitations of agent-based models in current development at Sandia and other research institutions is that communication is treated simply as a message passing between agents. Effectively, the telecommunications infrastructure is not specifically represented. None of the models simulates the differences in communication over telephone, computer, wireless, or other networks and therefore cannot model the impact of specific communication failures on the whole system. Nor can current models simulate the impact of other infrastructure failures on telecommunications.

To address the communications deficiencies described above, Sandia revised and restructured the Aspen-EE model to include a more realistic representation of the telecommunications infrastructure. This new model of infrastructure interdependency is called CommAspen. In CommAspen, communication is treated as an integrated agent system capable of creating, transforming, sending, receiving, and storing information and messages over time and across distance. With CommAspen, we can model communication networks or medium-specific vulnerabilities to failures and their dependence on supporting infrastructures like power.

Intended users – Internal analyst.

System output – Not specified.

Maturity – Development.

Areas modeled – Not specified.

Customers/sponsors – Not specified.

(Pederson, Dudenhoeffer, Hartley, & Permann, 2006, p. 29)
B.9. COUNTERACT

COUNTERACT

European Commission Directorate-General for Research

This approach is closer to an organizational risk assessment methodology containing all the relevant items. Counteract (Cluster of User Networks in Transport and Energy relating to Anti-terrorist Activities) has been an FP6 funded project. This project is focused on the transport and energy sectors and it is focused on terrorist threats. Thus a priori this methodology is sectoral and covers a certain part of the threats spectrum. According to this consortium, security measures in the transport sector are applied in a non-structured and inconsistent manner, mostly on a case-by-case basis. In order to remediate this, the consortium proposed to adopt a security risk assessment methodology as the first and most important step towards securing transport infrastructure in a consistent way.

The risk assessment methodology presented in this project is focused on assets and operators of any size, thus excluding an approach at the systems level. The security risk assessment is divided in two parts, the risk analysis and the vulnerability assessment. The risk analysis focuses on the probability of an event and the impact it may have, while the vulnerability assessment evaluates the safeguards in place for the corresponding risks for the various assets. It is a rather different approach as to what is risk assessment with respect to what is widely acceptable.

The probability of realization of a threat (terrorist threat) is classified according to a 5 degree scale (very high, high, possible, low, very unlikely). It is important to mention that the classification of a threat according to this scheme mostly resides on past events within the limits
of this company or within the limits of similar companies in other areas of the world. It thus mainly relies on past experience.

The impact/severity assessment follows a similar approach and it is classified in escalating categories (Disastrous, Critical, Marginal, Uncritical). The combination of probability of threat realization with the impact provides the risk categories (20 categories, although both threat probability and impact categories can be modified and adapted according to the needs of the assessment).

The vulnerability assessment follows the probability assessment of a threat and the impact assessment. It is applied to detect gaps and weak points in the prevention and mitigation of threats and incidents as well as diagnosing potential for optimizing the safeguards in place. Basically the vulnerability assessment evaluates additional potential measures against the risks that have been diagnosed during the risk analysis process. These measures are analyzed considering the following parameters:

- Costs
- Effectiveness
- Time for implementation
- Insurance impact
- Impact on the daily basis operation

This part of the methodology can be classified within the limits of risk mitigation and risk management and less within the limits of a traditional risk assessment.

(Giannopoulos, Filippini, & Schimmer, 2012, pp. 21-23)
The DECRIS approach is the result of intensive research from SINTEF in the domain of hazard/risk assessment for critical infrastructures. The DECRIS project/approach builds on the existing capacities in the sectoral risk assessment methodologies that existed already in Norway. The main issue of these risk assessment methodologies, which is common at global level, is exactly the sectorial approach and the assessment of each sector independently. Thus DECRIS project aims to bridge the gap between the methodologies that exist in various sectors and propose an all-hazard generic Risk and Vulnerability Assessment methodology for cross-sector infrastructure analysis. The target group for this methodology is policy and decision makers.

The DECRIS methodology is based on a four-step procedure:

- Establishment of event taxonomies and risk dimensions.
- Simplified Risk and Vulnerability Analysis for the identified events.
- Selection of events to be further analyzed.
- Detailed analysis of selected events.

A proof of concept of this methodology has been setup for the city of Oslo. For each of the four categories of infrastructures that have been considered (Electricity, Water, Transport, ICT) a number of events have been identified. For each of these events, the above mentioned criteria are applied and a short list of scenarios to be further assessed is established. In principle
this methodology fosters the collaboration between the various stakeholders in the different sectors in order to widen their understanding on the interdependencies across sectors.

(Giannopoulos, Filippini, & Schimmer, 2012, pp. 23-24)

**B.11. EURACOM**

**European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks (EURACOM)**

European Commission Directorate-General for Research

EURACOM has been a 7th Framework program funded project. The aim of this project was to develop a holistic risk assessment methodology that covers all hazards for all sectors although the name of the project may be misleading. In fact it is not a methodology with developed supporting tools but rather a methodological framework. The implementation tools have still to be developed. Within the framework of this project a risk assessment methodologies state of the art study has been conducted focusing mainly on risk assessment methodologies at European level.

The methodology consists of seven well defined steps:

1. Set up an holistic team with an holistic view
2. Define the holistic scope
3. Define risk assessment scales
4. Understand the assets
5. Understand the threat context
6. Review security/Identify vulnerabilities
7. Evaluate and rank the risks

(Giannopoulos, Filippini, & Schimmer, 2012, pp. 24-25)

**B.12. FAIT**

**Fast Analysis Infrastructure Tool (FAIT)**

Sandia National Laboratory

Overview – National Infrastructure Simulation and Analysis Center (NISAC) analysts are regularly tasked by the Directorate for Preparedness in the Department of Homeland Security (DHS) with determining the significance and interdependencies associated with elements of the nation’s critical infrastructure. The Fast Analysis Infrastructure Tool (FAIT) has been developed to meet this need. FAIT utilizes system expert-defined object-oriented interdependencies, encoded in a rule-based expert systems software language (JESS), to define relationships between infrastructure assets across different infrastructures. These interdependencies take into account proximity, known service boundaries, ownership, and other unique characteristics of assets found in their associated metadata. In a similar fashion, co-location of assets can be analyzed based exclusively on available spatial data. The association process is dynamic, allowing for the substitution of data sets and the inclusion of new rules reflecting additional infrastructures, as data accuracy is improved and infrastructure analysis requirements expand. FAIT also utilizes established Input/Output (I/O) methods for estimating the economic consequence of the disruption of an asset. Each of these analysis elements (interdependency, co-
location, economic analysis) have been extended from their original ‘asset-level’ analysis, to allow for the analysis of a specified region. Here, rules written for individual assets are executed en masse on classes of demand infrastructures, like assets of the emergency services (e.g., fire and police stations) and public health (e.g., hospitals) infrastructures, which lie in a defined analysis area, such as a hurricane damage zone, to identify those elements of supply infrastructures (e.g., electric power and telecommunications) which serve the largest number of particular sets of demand infrastructures. FAIT’s regional economic analysis takes as input economic data (from the Bureau of the Census) for the disrupted area (as modeled by other NISAC capabilities). When coupled with other NISAC modeling results (estimates for the duration of the disruption and recovery, and the range of magnitude of disruption for the disrupted region), FAIT creates a regional economic analysis, an understanding of the direct and indirect economic consequences, for each sector of the economy in each county in the analysis area.

Development goals – The FAIT development team is constantly modifying their development goals to best support the requirements of NISAC analysts, in responding to questions from DHS. Current goals include the following:

- Expansion of existing FAIT capabilities to cover infrastructures not in the current analysis set;
- Enhancement of economic analysis capability to more accurately represent the consequences of the loss of infrastructure services on the performance of individual industrial sectors;
- Incorporation of infrastructure-specific models to define areas of consequence due to the failure of asset(s) in a given infrastructure; and
• Development of a network ‘metacrawler’ designed to associate sparse metadata (e.g., transportation system commodity throughput) with fragmented system elements (e.g., segments of the national rail network).

Intended users – Analysts on NISAC’s Fast Analysis and Simulation Team.

(Pederson, Dudenhoeffer, Hartley, & Permann, 2006, p. 55)

**B.13. MIN**

**Multilayer Infrastructure Network (MIN)**

Purdue School of Civil Engineering

Overview – This is a preliminary network flow equilibrium model of dynamic multi-layer infrastructure networks (MIN) in the form of a differential game involving two essential time scales. In particular, three coupled network layers—automobiles, urban freight, and data—are modeled as being comprised of Cournot-Nash dynamic agents. An agent-based simulation solution structure is introduced to solve the flow equilibrium and optimal budget allocation problem for these three layers under the assumption of a super authority that oversees investments in the infrastructure of all three technologies and thereby creates a dynamic Stackelberg leader-follower game.

Development goals – Continue to develop a generalized framework to address both equilibrium and disequilibrium scenarios.

Intended users – Community planners and engineers.
System output – Charts, graphs, behavioral trends.

Maturity – Research.

Areas modeled – Urban transportation (e.g., auto, urban freight, and data).

Customers/sponsors – The National Science Foundation sponsored the work.

(Pederson, Dudenhoeffer, Hartley, & Permann, 2006, p. 71)

**B.14. MDM**

**Modular Dynamic Model (MDM)**

Sandia National Laboratories

Sandia National Laboratories are involved in an important number of projects related to critical infrastructure protection. The Modular Dynamic Model is the outcome of one of these projects and it has been developed based on the issue of interdependencies. All sectors and infrastructures are falling within the scope of this methodology. The objective is to analyze the risk by modeling infrastructure interdependencies. The analysis outcome is the estimate of the consequences due to an applied perturbation.

The theoretical background is based on agent-based modeling and dynamic systems modeling. This methodology follows a kind of hierarchical modeling approach in the sense that it provides a first screening that can be followed by a more detailed analysis if the identified risks require such action. However, the whole approach is rather complicated and requires substantial
effort from the end user to obtain accurate and reliable results. In addition a huge data set is necessary that further complicates the analysis process.

The target group of this methodology is primarily CI operators and decision makers but with a certain level of expertise. Resilience is not explicitly addressed.

(Giannopoulos, Filippini, & Schimmer, 2012, p. 27)

**B.15. N-ABLE**

**Agent-Based Laboratory for Economics (N-ABLE)**

Sandia National Laboratory

Overview – The NISAC Agent-Based Laboratory for Economics (N-ABLE) is a software system for analyzing the economic factors, feedbacks, and downstream effects of infrastructure interdependencies. N-ABLE is a simulation environment in which hundreds of thousands to millions of individual economic actors simulate real-world manufacturing firms, households, and government agencies. NABLE can specifically address questions such as: 1. Which economic sectors are most vulnerable to infrastructure disruptions and interdependencies? 2. What firms are most affected who does well, poorly? 3. What are the different qualitative and quantitative ways in which economic sectors use the energy, transportation, financial, and communication sectors? 4. What short-run infrastructure changes affect economic performance (and vice versa)? 5. How do systems of firms and individuals respond and adapt over time and over regions? 6. What economic mechanisms do national, state, and local governments have or need to have to assist firms and other economic sectors in their regions?
Development goals – Developed to provide decision makers with a firm-level understanding of the interdependencies between infrastructure sectors and the economy.

Intended users – Economic Analysts.

System Output – Geographical charts and statistical output.

Maturity – Mature Internal.

Areas modeled – Examples: chemical, food, financial, manufacturing sectors.

Customers/sponsors – Department of Homeland Security

(Pederson, Dudenhoeffer, Hartley, & Permann, 2006, p. 89)

**B.16. NEMO**

**Net-Centric Effects-based Operations Model (NEMO)**

SPARTA Inc.

Overview – Net-Centric Effects-based operations MOdel (NEMO) is an effects-based planning and analysis application for modeling the cascading effects of events across multiple infrastructure networks. It is a Net-Centric compliant application, relying on a service oriented architecture (SOA) approach to access infrastructure models, data repositories, and mapping tools. NEMO models interactions across electrical power, water, gas, and road networks using an on/off interaction behavior between the components of the different networks, and provides a solid foundation for advancement. NEMO provides a first of its kind capability for observing second and higher order effects of operations against opponents’ infrastructure networks.
Development goals – Efforts are underway to integrate social/political networks into the effects-based operation (EBO) process. Future development needs to enhance the program capabilities for integrating additional relationship definitions, multi-agent capabilities, and optimization.

Intended users – Planners and analysts are the intended users.

System output – NEMO displays maps overlaid with nodes and linkages between various infrastructures. Disruptions and cascading effects are highlighted during simulations.

Maturity – This is a prototype system.

Areas modeled – Not specified.

Customers/sponsors – NEMO was internally developed by SPARTA.

(Pederson, Dudenhoeffer, Hartley, & Permann, 2006, p. 79)

B.17. NSRAM

Network Security Risk Assessment Modeling (NSRAM)

James Madison University Institute for Infrastructure and Information Assurance

Overview – The network security risk assessment model (NSRAM) tool is a complex network system simulation modeling tool that emphasizes the analysis (including risk analysis) of large interconnected multi-infrastructure models. It is designed to be portable, and uses portable and expandable database and model structures. The tool also provides a framework to simulate large networks and analyze their behavior under conditions where the network suffers failures or structural breakdowns. In order to accurately portray the severity of network failures, repair
variables (time to repair, cost to repair, repair priorities) must be considered. NSRAM’s unique repair element set consists of repair entities with specialized functions that allow users to accurately simulate any configuration of fault detection and repair schemes. The intent of these repair element sets is to more accurately model the human response to perceived system damage. The repair element sets identify symptoms, test the system to determine the elements that are damaged, attempt to repair the damage, and then attempt system recovery. If symptoms are still present, the repair elements repeat the above cycle until the system is recovered. Inspection routines will also be accommodated so that preventative maintenance effects are accurately incorporated. The tool is flexible and can be used to model different infrastructure networks, such as computers, electrical systems, and highway systems.

Development goals – James Madison University (JMU) is continuing development to add strong security features, improve the graphical user interface (GUI) and database efficiency, and to develop an emergency radio system element set. JMU is also developing the concept of sophisticated repair element sets that interact via predefined algorithms to more accurately simulate repair personnel reaction to system insults or malfunctions. These repair element sets are unique in that they interact with the simulation network model in a predetermined manner, but their operating rules can be changed to allow the user to optimize repair strategies.

Intended users – Analysts are the intended users.

System output – NSRAM contains a GUI for developing models and scenarios, and interpreting output. The data output is flexible to facilitate post simulation processing.

Maturity – NSRAM is currently in development as part of the CIP project.
Areas modeled – Not specified.

Customers/sponsors – Not specified.

(Pederson, Dudenhoeffer, Hartley, & Permann, 2006, p. 87)

**B.18. RAMCAP-Plus**

**Risk Analysis and Management for Critical Asset Protection (RAMCAP-Plus)**

American Society of Mechanical Engineers (ASME)

The RAMCAP-Plus methodology has been developed by ASME (American Society of Mechanical Engineers) as an all hazards risk and resilience assessment methodology. The scope of the methodology covers all infrastructures, with the objective of addressing protection of nations critical infrastructures (avoiding hazardous events or their consequences) and resilience (rapid return to full function after disruptive events).

The methodology is based on a seven step approach namely:

1. Asset characterization
2. Threat characterization
3. Consequence analysis
4. Vulnerability analysis
5. Threat assessment
6. Risk and Resilience assessment
7. Risk and Resilience Management
Risk and Vulnerability Analysis (RVA)

Danish Emergency Management Agency

Risk and vulnerability analysis is an important first step in the comprehensive civil preparedness planning process. DEMA has therefore developed a generic scenario-based model for risk and vulnerability analysis (the RVA Model). The model is developed for government agencies with responsibilities for society’s critical functions.

The model consists of tables which make the user identify and evaluate threats, risks and vulnerabilities. The underlying focus is to formulate suggestions for countermeasures.

The RVA Model consists of four parts, which each come in a MS Word document.

- In Part 1, the purpose and scope of the analysis is defined.
- In Part 2, the scenarios are developed. The users generate their own scenarios based on what is most relevant to them.
- In Part 3, users are asked to assess the risks and vulnerabilities associated with each scenario. Risks are assessed according to likelihood and consequences. Vulnerabilities are assessed according to existing capacities to prepare for, respond to, and recover from the type of incident in the scenario.
- In Part 4, the analyzed scenarios are presented graphically in a risk and vulnerability profile.
B.20. SRAM

Sandia Risk Assessment Methodology (SRAM)

Sandia National Laboratory

Sandia National Laboratories presented back in 2000 a risk assessment methodology for the protection of physical critical infrastructures. This work has been performed on behalf of an agency of the US Government, thus it has a clear orientation towards policy makers at national level.

What is particularly interesting is that in the abstract of the report there is a clear link between critical infrastructure and services and also continuation of service even after anthropogenic threats. This translated to modern critical infrastructure jargon would be increase the resilience of critical infrastructures against terrorist and man-made threats. Clearly resilience is within the objectives of the methodology although it is not explicitly mentioned.

The methodology comprises seven distinct steps:

- Characterize facility
- Identify undesired events ad critical assets
- Determine consequences of undesired events
- Define threats to the facility
- Analyze protection system effectiveness
- Estimate risks
- Suggest and evaluate upgrades to the system

Fault tree analysis is the main tool of this methodology to identify the vulnerabilities. This implies that the user of the methodology is in the position to master this methodology and apply it to assets of critical infrastructures. It is important to mention that fault tree analysis is mostly adapted for use in selected assets rather than complex networks, although this is also feasible by adapting the fault tree methodology. By applying fault tree analysis it is possible to identify failure scenarios and critical elements for the functioning of the asset (Giannopoulos, Filippini, & Schimmer, 2012, pp. 32-33).

**B.21. RMCIS**

**Risk Management for Critical Infrastructure Sectors (RMCIS)**

Public Safety Canada

One of the main elements of the action plan of the national strategy for critical infrastructure protection in Canada is the risk management framework that is mostly addressed to the operators and jurisdictions. Although the whole strategy and program fosters collaborative actions in order to improve resilience of critical infrastructures this particular element (risk management) is addressed to operators and local governments.

The risk management framework is based on three pillars:

- Sector risk profiles at national level
- Risk assessments
- Risk management tools and guidance
Concerning risk assessment, the framework sets out some guidelines for the elements of the methodologies but does not indicate which methodology should be implemented.

(Giannopoulos, Filippini, & Schimmer, 2012, pp. 35-36).
Appendix C: AVM Installation/Configuration

C.1. AVM Baseline Functional Description

The Asset Vulnerability Model is comprised of 1) baseline analysis, 2) cost-benefit analysis, and 3) decision support tools. Baseline analysis produces a risk profile of all critical assets based on Θ, the probability of attack failure. Theta is calculated as indicated in equation 3.1. AVM cost-benefit analysis finds the optimum combination of protective improvement measures proposed for critical assets. AVM decision support tools are Excel spreadsheets that graphically portray the results of baseline and cost-benefit analysis and facilitate easy manipulation to present the information in a manner most meaningful to a decision maker.

Because critical infrastructure data is protected by the 2002 Homeland Security Act, AVM baseline analysis, cost-benefit analysis, and decision support tool capabilities can only be demonstrated using simulated data. Baseline analysis is simulated by the Baseline Asset Model (BAM). BAM produces a list of simulated assets with associated AVM risk parameters and corresponding calculation of Θ. Asset records are written to a CDF file as shown in figure 3-3.

In a similar fashion, AVM cost-benefit analysis requires simulated protective improvement data to perform its function. Simulated protected improvements are generated by the Protective Improvement Model (PIM). PIM takes the output from BAM, generates simulated improvements, and produces a data file as depicted in figure 3-4. Strictly speaking, PIM is not a part of AVM, but is required to demonstrate its capabilities. As described in section 3.4.3, PIM allows the user to specify what percentage of asset records receive no protection improvement data. AVM Cost-benefit analysis is performed by the CBA program. It takes the output from PIM, finds the combination of protective improvements that provide the highest return on investment, and records the assets and proposed improvements to a CDF file in the format shown
in table C-1. Theta1 and Theta2 are spreadsheets that can format and display the output from BAM and CBA respectively. The AVM baseline program architecture is illustrated in figure C-1.

<table>
<thead>
<tr>
<th>Record Field</th>
<th>Description</th>
<th>Type</th>
<th>Range</th>
<th>Record Field</th>
<th>Description</th>
<th>Type</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Asset ID</td>
<td>Integer</td>
<td>#</td>
<td>9.</td>
<td>Theta</td>
<td>E-Notation</td>
<td>0-1.0</td>
</tr>
<tr>
<td>2.</td>
<td>Asset Type</td>
<td>Integer</td>
<td>1-13</td>
<td>10.</td>
<td>DTheta</td>
<td>E-Notation</td>
<td>0-1.0</td>
</tr>
<tr>
<td>3.</td>
<td>Asset Location</td>
<td>Integer</td>
<td>1-50</td>
<td>11.</td>
<td>Cost</td>
<td>Float</td>
<td>#</td>
</tr>
<tr>
<td>4.</td>
<td>P(dis)</td>
<td>Float</td>
<td>0-1.0</td>
<td>12.</td>
<td>P(Δdis)</td>
<td>Float</td>
<td>0-1.0</td>
</tr>
<tr>
<td>5.</td>
<td>P(def)</td>
<td>Float</td>
<td>0-1.0</td>
<td>13.</td>
<td>P(Δdef)</td>
<td>Float</td>
<td>0-1.0</td>
</tr>
<tr>
<td>6.</td>
<td>P(den)</td>
<td>Float</td>
<td>0-1.0</td>
<td>14.</td>
<td>P(Δden)</td>
<td>Float</td>
<td>0-1.0</td>
</tr>
<tr>
<td>7.</td>
<td>P(dim)</td>
<td>Float</td>
<td>0-1.0</td>
<td>15.</td>
<td>P(Δdim)</td>
<td>Float</td>
<td>0-1.0</td>
</tr>
<tr>
<td>8.</td>
<td>% (dam)</td>
<td>Float</td>
<td>0-1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table C-1: CBA Output File Record Format

Figure C-1: AVM Baseline Program Architecture.
C.2. AVM Baseline Execution

As described in section 3.4, AVM programs were developed in standard C using Microsoft Visual C++ 2010 Express. Each program was built as a Win32 Console Application compatible with the Windows 7 operating system. Executable files are launched from the Windows Command Prompt by typing the name of the file plus any accompanying arguments as identified in table 3-4. A sample baseline execution generating 100 assets is depicted in figure C-2 below.

```
c:\avm> bam 100 assets100.txt
  
c:\avm> pim assets100.txt pim100.dat 40 40 40
  
c:\avm> cba pim100.dat cba100.txt
```

Figure C-2: Sample AVM Baseline Execution.

C.3. AVM Strategy Simulation

As described in section 4.4, AVM was extended to investigate alternative protective improvement investment strategies. Two new program models were developed to facilitate strategy simulation. These were the Selective Improvement Program (SIP) and Probable Attack Model (PAM) described in section 4.4.2. As described, SIP simulates one of seven possible investment strategies: 1) Least Cost (LC), 2) Least Protected (LP), 3) Region Protection (RP), 4) Sector Protection (SP), 5) Highest DTheta (HD), 6) Highest Consequence, and 7) Random Purchase (RAN). When an asset is identified to receive upgrades using one of the previous purchase strategies, SIP will add the delta-theta values to the asset record’s component theta values, and compute a new theta value as the product of the revised terms as indicated in
equation 3-1. Asset records are then output to a CDF file in the same format as baseline analysis shown in figure 3-3. SIP separately records total expenditures and purchases to a separate results file for later analysis. PAM takes the asset file output from SIP and computes the estimated damages of a successful attack based on 1) the probability of attack, and 2) the attacker’s perception of $\Theta$. If an asset is successfully attacked, it is not written to output, effectively removing it from further simulation. By the same token, PAM will calculate and record damages to separate results file. Again, refer to section 4.4.2 for a complete description of PAM functionality. The extended AVM baseline architecture is depicted in figure C-3. A single execution of this program string will simulate a one-year asset investment cycle. A sample execution is illustrated in figure C-4.
As depicted in figure C-4, SIP will purchase $50,000 in protective improvements using the Least Cost investment strategy. The revised asset records are written to sip100.txt, and the results of the purchases are record in expended100.txt. Similarly, PAM simulates a 10% probability of attack over 10 years with a 20% deviation of an attacker’s perception of Θ. PAM writes the surviving assets to pam100.txt, and records attack results to damages100.txt. The file pam_state.dat supports attack modeling as described in section 4.4.2 by maintaining the Cumulative Probability of Attack (CPA) between PAM executions. This file must be initialized at the outset of a multi-year simulation. Initialization is accomplished by overwriting pam_state.dat with pam_state0.dat as shown in the first line of figure C-4.

As previously mentioned, the execution sequence in figure C-4 simulates a one-year investment cycle. In order to evaluate an investment strategy it is necessary to examine its cumulative results over a ten-year period. This will require taking the asset file output from PAM and feeding it back into the sequence at PIM. Batch file processing will facilitate repetitive execution of the AVM command sequence. Figure C-5 presents a sample batch file capable of executing a complete 10-year investment strategy simulation.
The sample batch file depicted in figure C-5 will execute the extended AVM program sequence over a simulated 10-year cycle. BAM generates an initial set of 100 assets at the outset of the script. These are fed into PIM to add proposed protective improvements. These are fed
into CBA which selects the combination of improvements offering the highest proportional value of protective gain compared to cost. The modified list of assets and recommended improvements are fed into SIP which uses the LC investment strategy to purchase as many improvements as it can within its $50,000 budget. The modified list of assets is then fed into PAM which calculates the probability of attack and removes the target of successful attack from the asset list. The PAM generated asset list is then fed back into PIM, and the cycle repeated ten times. Cumulative results are collected in the expended100lc.txt and damages100lc.txt files. Note that the batch file executes the SIP2 and PAM3 AVM program models. SIP2 is the current baseline version of SIP simulating all seven investment strategies. Likewise, PAM3 is the current implementation of the Probable Attack Model that targets assets with the smallest Θ value, corresponding to the Sandler & Lapan game theoretic model described in section 3.2.1.

The AVM simulation is not yet ready for execution. The batch file needs further modifications to conduct multiple simulations over varying conditions. To be more specific, it is necessary to conduct many executions of the 10-year simulation cycle in order to average out results. While 1000 repetitions were preferred, 100 repetitions were chosen to keep the execution time reasonable (i.e., 3 hours per strategy). It was also desired to observe PAM performance over varying probabilities of attack from 10%–100%. The sample batch file in figure C-6 makes the appropriate modifications to perform a complete simulation of a single investment strategy.
rem /* Initiate Do Loop for Attack Probability */
set /a k=0
:loop3
if %k%==100 goto end3
set /a k=%k%+10
rem
rem /* Initiate Do Loop for # of simulations */
set /a j=0
:loop2
if %j%==100 goto end2
set /a j=%j%+1
rem
    echo Initialize PAM State...
    cp pam_state0.dat pam_state.dat
rem
    echo Generate baseline assets...
    BAM 100 pam100lc.txt
rem
rem /* Initiate Do Loop for # of years */
set /a i=0
:loop1
if %i%==10 goto end1
set /a i=%i%+1
rem
    echo LC: Year %i% Sim %j%% Prob(Atk) %k%
    PIM pam100lc.txt pim100.dat 40 40 40 > exepim.txt
    CBA pim100.dat cba100.txt > execba.txt
    DSC cba100.txt dsalc.txt
    SIP2 1 0 50000 cba100.txt sip100lc.txt expended100lc.txt exedsa.txt > exesip.txt
rem
    PAM3 %k% 10 20 pam_state.dat sip100lc.txt pam100lc.txt damages100lc.txt > expam.txt
    goto loop1
:end1
del pim100.dat
del cba100.txt
del sip100lc.txt
del pam100lc.txt
del pam_state.dat
goto loop2
:end2
rem
    ren dsalc.txt dsalc_%k%.txt
    ren damages100lc.txt damages100lc_%k%.txt
    ren expended100lc.txt expended100lc_%k%.txt
    goto loop3
:end3

Figure C-6: Multiple Executions of 10-Year AVM Strategy Simulation over Varying Probabilities.
In addition to the previous modifications, it will be noticed that the script in figure C-6 pipes AVM program screen output to text files. This was done to speed execution by limiting output to the monitor while keeping information that may be useful for troubleshooting. Also note that an additional program, the Data Sensitivity Collector (DSC), was inserted into the AVM simulation sequence between CBA and SIP. DSC was created to capture CBA output for data sensitivity analysis. It was found that the C program facilitated faster simulation execution compared to using the system Copy command to concatenate files. With these additions, it is now possible to run a complete simulation of a single investment strategy. To simulate a different strategy, make a copy of the batch file and adjust the program parameters appropriately. Thus, for example, to simulate the Least Protected strategy, change the SIP simulation type from 1 to 2. To simulate the Region Protection strategy, change the SIP simulation type from 1 to 3, and the SIP simulation key from 0 to 44 in this case. In this manner, a separate batch file was created for each strategy simulation for a total of seven batch files. In addition to adjusting the SIP simulation designator, a global replace was done on the simulation type (e.g., “lc”) to differentiate simulation output files. Finally, a master batch file was created called AVMxx to sequence execution of the seven investment strategy simulations. As depicted in table 4-3, AVMxx calls each of the seven subordinate batch files in sequential order. AVM12.bat executed the described simulations examining seven different investment strategies over a ten-year probable attack period with varying probabilities of attack from 10% to 100%, simulated 100 times each while maintaining a fixed Θ deviation of 20%. The subordinate batch files in AVM13 were modified to maintain a fixed 32% probability of attack while varying the Θ deviation from 10% to 100%. AVM14 duplicated AVM12, except it replaced PAM3 with PAM4. Each simulation, AVM12, AVM13, and AVM14, was executed within its own
directory/folder to preclude overwriting the output files. To set up a simulation, create a corresponding directory/folder and copy over the files indicated in table C-2. Launch each simulation by first opening a Windows console command prompt. Set the console command prompt default location to the simulation directory/folder. Launch the simulation by entering the name of the master batch file at the console command prompt, e.g., AVM12.bat. Each simulation took approximately six hours to execute. In total it took eighteen hours to run all three simulations from start to finish.

<table>
<thead>
<tr>
<th>Application Files</th>
<th>Batch Files</th>
<th>Excel Spreadsheets</th>
<th>Data Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Execution Files</td>
<td>AVM12.bat</td>
<td></td>
<td>Theta1.xlsx</td>
</tr>
<tr>
<td></td>
<td>AVM130HC100_100.bat</td>
<td></td>
<td>Theta2.xlsx</td>
</tr>
<tr>
<td></td>
<td>AVM130HD100_100.bat</td>
<td>Theta1.xlsx</td>
<td>PAM_state0.dat</td>
</tr>
<tr>
<td></td>
<td>AVM130LC100_100.bat</td>
<td>Theta2.xlsx</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AVM130LP100_100.bat</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AVM130RAN100_100.bat</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AVM130R44100_100.bat</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AVM130S9100_100.bat</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model Analysis Program Files</th>
<th>MAP.bat</th>
<th>MAPHC.bat</th>
<th>MAP_AVM12.xlsx</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MAPHD.bat</td>
<td></td>
<td>Analysis.xlsx</td>
</tr>
<tr>
<td></td>
<td>MAPLC.bat</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAPLP.bat</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAPRAN.bat</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAPR44.bat</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAPS9.bat</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Sensitivity Program Files</th>
<th>DSA.bat</th>
<th>DSA_AVM12.xlsx</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DSAHC.bat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DSAHD.bat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DSALC.bat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DSALP.bat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DSARAN.bat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DSAR44.bat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DSAS9.bat</td>
<td></td>
</tr>
</tbody>
</table>

Table C-2: AVM Strategy Simulation Program Files
C.4. AVM Simulation Data Analysis

Each strategy simulation produces two sets of result files recording associated expenditures and damages. Each set includes ten files corresponding to the percent variation of the given simulation, whether attack probability or $\Theta$ deviation. Altogether, a simulation of the seven strategies produces 70 pairs of expenditure and damage files as shown in figure C-3.

<table>
<thead>
<tr>
<th>Expenditures</th>
<th>Damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>expended100hc_10.txt</td>
<td>damages100hc_10.txt</td>
</tr>
<tr>
<td>expended100hc_20.txt</td>
<td>damages100hc_20.txt</td>
</tr>
<tr>
<td>expended100hc_30.txt</td>
<td>damages100hc_30.txt</td>
</tr>
<tr>
<td>expended100hc_40.txt</td>
<td>damages100hc_40.txt</td>
</tr>
<tr>
<td>expended100hc_50.txt</td>
<td>damages100hc_50.txt</td>
</tr>
<tr>
<td>expended100hc_60.txt</td>
<td>damages100hc_60.txt</td>
</tr>
<tr>
<td>expended100hc_70.txt</td>
<td>damages100hc_70.txt</td>
</tr>
<tr>
<td>expended100hc_80.txt</td>
<td>damages100hc_80.txt</td>
</tr>
<tr>
<td>expended100hc_90.txt</td>
<td>damages100hc_90.txt</td>
</tr>
<tr>
<td>expended100hc_100.txt</td>
<td>damages100hc_100.txt</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expenditures</th>
<th>Damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>expended100hd_10.txt</td>
<td>damages100hd_10.txt</td>
</tr>
<tr>
<td>expended100hd_20.txt</td>
<td>damages100hd_20.txt</td>
</tr>
<tr>
<td>expended100hd_30.txt</td>
<td>damages100hd_30.txt</td>
</tr>
<tr>
<td>expended100hd_40.txt</td>
<td>damages100hd_40.txt</td>
</tr>
<tr>
<td>expended100hd_50.txt</td>
<td>damages100hd_50.txt</td>
</tr>
<tr>
<td>expended100hd_60.txt</td>
<td>damages100hd_60.txt</td>
</tr>
<tr>
<td>expended100hd_70.txt</td>
<td>damages100hd_70.txt</td>
</tr>
<tr>
<td>expended100hd_80.txt</td>
<td>damages100hd_80.txt</td>
</tr>
<tr>
<td>expended100hd_90.txt</td>
<td>damages100hd_90.txt</td>
</tr>
<tr>
<td>expended100hd_100.txt</td>
<td>damages100hd_100.txt</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expenditures</th>
<th>Damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>expended100lc_10.txt</td>
<td>damages100lc_10.txt</td>
</tr>
<tr>
<td>expended100lc_20.txt</td>
<td>damages100lc_20.txt</td>
</tr>
<tr>
<td>expended100lc_30.txt</td>
<td>damages100lc_30.txt</td>
</tr>
<tr>
<td>expended100lc_40.txt</td>
<td>damages100lc_40.txt</td>
</tr>
<tr>
<td>expended100lc_50.txt</td>
<td>damages100lc_50.txt</td>
</tr>
<tr>
<td>expended100lc_60.txt</td>
<td>damages100lc_60.txt</td>
</tr>
<tr>
<td>expended100lc_70.txt</td>
<td>damages100lc_70.txt</td>
</tr>
<tr>
<td>expended100lc_80.txt</td>
<td>damages100lc_80.txt</td>
</tr>
<tr>
<td>expended100lc_90.txt</td>
<td>damages100lc_90.txt</td>
</tr>
<tr>
<td>expended100lc_100.txt</td>
<td>damages100lc_100.txt</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expenditures</th>
<th>Damages</th>
</tr>
</thead>
<tbody>
<tr>
<td>expended100lp_10.txt</td>
<td>damages100lp_10.txt</td>
</tr>
<tr>
<td>expended100lp_20.txt</td>
<td>damages100lp_20.txt</td>
</tr>
<tr>
<td>expended100lp_30.txt</td>
<td>damages100lp_30.txt</td>
</tr>
<tr>
<td>expended100lp_40.txt</td>
<td>damages100lp_40.txt</td>
</tr>
<tr>
<td>expended100lp_50.txt</td>
<td>damages100lp_50.txt</td>
</tr>
<tr>
<td>expended100lp_60.txt</td>
<td>damages100lp_60.txt</td>
</tr>
<tr>
<td>expended100lp_70.txt</td>
<td>damages100lp_70.txt</td>
</tr>
<tr>
<td>expended100lp_80.txt</td>
<td>damages100lp_80.txt</td>
</tr>
<tr>
<td>expended100lp_90.txt</td>
<td>damages100lp_90.txt</td>
</tr>
<tr>
<td>expended100lp_100.txt</td>
<td>damages100lp_100.txt</td>
</tr>
</tbody>
</table>

Table C-3: AVM Strategy Simulation Result Files
Each file contains 1,000 records corresponding to the results from 10 years of executions repeated over 100 simulations. Given an associated pair of expenditure and damage files, e.g., expended100lc_10.txt and damages100lc_10.txt, the MAP executable program will match records, tabulate the totals for each year, and record the average results for each year to output. In this way, MAP reduces the 10,000 records for each strategy to 110 records providing the average values for each year, plus the average total for each ten year data set as the varying parameter, attack probability or Θ deviation, increases by 10% from 10% to 100%. Since MAP only works with two files at a time, a batch file is used to reduce the results from the 20 files associated with each strategy, as shown if table 4-4. A master batch file, MAP.bat, sequences data reduction across all seven simulations. To initiate data reduction following simulation execution, enter MAP.bat into the console command prompt (assuming your default is still in the same directory/folder). The master batch file will sequence data reduction of all investment strategies and produce the condensed results listed in table C-4.

<table>
<thead>
<tr>
<th>Batch Execution</th>
<th>Batch Output</th>
<th>Batch Execution</th>
<th>Batch Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAPHC.bat</td>
<td>MAPHC.txt</td>
<td>MAPRAN.bat</td>
<td>MAPRAN.txt</td>
</tr>
<tr>
<td>MAPHD.bat</td>
<td>MAPHD.txt</td>
<td>MAPR44.bat</td>
<td>MAPR44.txt</td>
</tr>
<tr>
<td>MAPLC.bat</td>
<td>MAPLC.txt</td>
<td>MAPS9.bat</td>
<td>MAPS9.txt</td>
</tr>
<tr>
<td>MAPLP.bat</td>
<td>MAPLP.txt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table C-4: Batch Execution & Output Files

MAP output files are created in CDF format. This makes them compatible for importing into the MAP_AVMxx spreadsheet. The spreadsheet includes tabs for each investment strategy. The corresponding MAP text file is imported into its matching tab; e.g., import MAPLC.txt into the LC tab. The MAP_AVMxx spreadsheet performs individual analysis on each investment
strategy within its tab. All supporting calculations and charts are automatically updated when
the text file is imported into the spreadsheet. A combined tab pools the results together across
investment strategies to provide consolidated analysis as described in section 4.4.3 and Appendix
D.

Just as MAP reduces simulation results, DSA reduces simulation data collected by DSC
during simulation execution. While there is half the number of DSA data files compared to their
MAP counterparts, they are substantially larger averaging 14MB each. That is because each file
contains 100,000 records capturing the 100 assets output by CBA over a simulated 10-year
period repeated for 100 executions. Each record is formatted as indicated in table C-1. Table C-
5 lists the simulation output files that provide input to the DSA data reduction program.

<table>
<thead>
<tr>
<th>dsahc_10.txt</th>
<th>dsahd_10.txt</th>
<th>dsalc_10.txt</th>
<th>dsalp_10.txt</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsahc_20.txt</td>
<td>dsahd_20.txt</td>
<td>dsalc_20.txt</td>
<td>dsalp_20.txt</td>
</tr>
<tr>
<td>dsahc_30.txt</td>
<td>dsahd_30.txt</td>
<td>dsalc_30.txt</td>
<td>dsalp_30.txt</td>
</tr>
<tr>
<td>dsahc_40.txt</td>
<td>dsahd_40.txt</td>
<td>dsalc_40.txt</td>
<td>dsalp_40.txt</td>
</tr>
<tr>
<td>dsahc_50.txt</td>
<td>dsahd_50.txt</td>
<td>dsalc_50.txt</td>
<td>dsalp_50.txt</td>
</tr>
<tr>
<td>dsahc_60.txt</td>
<td>dsahd_60.txt</td>
<td>dsalc_60.txt</td>
<td>dsalp_60.txt</td>
</tr>
<tr>
<td>dsahc_70.txt</td>
<td>dsahd_70.txt</td>
<td>dsalc_70.txt</td>
<td>dsalp_70.txt</td>
</tr>
<tr>
<td>dsahc_80.txt</td>
<td>dsahd_80.txt</td>
<td>dsalc_80.txt</td>
<td>dsalp_80.txt</td>
</tr>
<tr>
<td>dsahc_90.txt</td>
<td>dsahd_90.txt</td>
<td>dsalc_90.txt</td>
<td>dsalp_90.txt</td>
</tr>
<tr>
<td>dsahc_100.txt</td>
<td>dsahd_100.txt</td>
<td>dsalc_100.txt</td>
<td>dsalp_100.txt</td>
</tr>
</tbody>
</table>

Table C-5: AVM Data Sensitivity Analysis Files

The DSA executable program takes each data file and reduces it individually. DSA first
reduces data on each asset by tabulating averages over 100 simulations for each year. This
reduces the 100,000 records to only 1,000 representing the average value of each asset during a given year. DSA then reduces data on each year by tabulating the average record values for that year, and tabulating an average total over the ten-year period. This further reduces the data to only eleven records, the average data value of a record for each year over ten years plus the totals for the decade. Batch files listed in table C-6 sequence execution on each file related to a single strategy simulation to reduce data across vary parameters, whether probability of attack or Θ deviation. The end result of DSA data reduction is a file related to each investment strategy with 110 records listing the average aggregate value of assets during each year over a ten-year period over a range of the varying parameter from 10% to 100%. Data reduction across investment strategy simulation is controlled by the master batch file DSA.bat as described in table 4-4.

<table>
<thead>
<tr>
<th>Batch Execution</th>
<th>Batch Output</th>
<th>Batch Execution</th>
<th>Batch Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSAHC.bat</td>
<td>DSAHC.txt</td>
<td>DSARAN.bat</td>
<td>DSARAN.txt</td>
</tr>
<tr>
<td>DSAHD.bat</td>
<td>DSAHD.txt</td>
<td>DSAR44.bat</td>
<td>DSAR44.txt</td>
</tr>
<tr>
<td>DSALC.bat</td>
<td>DSALC.txt</td>
<td>DSAS9.bat</td>
<td>DSAS9.txt</td>
</tr>
<tr>
<td>DSALP.bat</td>
<td>DSALP.txt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table C-6: DSA Batch Execution & Output Files

DSA output files are created in CDF format. This makes them compatible for importing into the DSA_AVMxx spreadsheet. The spreadsheet includes tabs for each investment strategy. The corresponding DSA text file is imported into its matching tab; e.g., import DSALC.txt into the LC tab. The DSA_AVMxx spreadsheet performs individual analysis on each investment strategy within its tab. All supporting calculations and charts are automatically updated when the text file is imported into the spreadsheet. A combined tab pools the results together across
investment strategies to provide consolidated analysis as described in section 4.4.3 and Appendix D.

C.5. Summary

The complete AVM investment strategy simulation program architecture is depicted in figure 4-2. To setup a simulation, create a directory/folder and copy over the AVM files indicated in table C-2. The simulation is currently configured to execute 100 simulations on each of seven investment strategies over 10 years over a varying probability of attack and Θ deviation from 10% to 100%. Open a Windows command console and set default to the simulation directory/folder. Launch the simulation by entering the master batch file name, AVM12.bat at the console command prompt. Simulation execution will take as much as six hours. Upon completion, the AVM programs will have produced the result files listed in table C-3 and the data sensitivity files listed in table C-5. Launch the master batch file MAP.bat to reduce the results data and produce the output files listed in table C-4. Launch the master batch file DSA.bat to reduce the data sensitivity files and produce the output files listed in table C-6. Open the MAP_AVM12.xlsx spreadsheet and import each MAP-reduced data output file into its corresponding spreadsheet tab. In a similar manner, open the DSA_AVM12.xlsx spreadsheet and import each DSA-reduced data output file into its corresponding spreadsheet tab. The spreadsheets will automatically perform all subsequent processing and charting of the combined results. For a complete description of spreadsheet processing and analysis, see Appendix D.
Appendix D: AVM Strategy Simulation Demonstration

D.1. Introduction

As described in section 4.3, the Asset Vulnerability Model is designed to work within the DHS Risk Management Framework. AVM baseline analysis provides the means to develop a risk profile of all critical assets during Step Three of the RMF process. Using the AVM risk formula for $\Theta$, a risk profile may be generated and examined using the AVM Theta1.xlsx spreadsheet as shown in figures 3-2.1 through 3-2.4. AVM cost-benefit analysis is applied in Step Four of the RMF process. CBA examines proposed protection improvement measures in terms of $\Delta\Theta$ protective gain and $D(\Delta\Theta)$ component costs to find the combination of measures providing the greatest protective gain at least cost. The AVM Theta2.xlsx spreadsheet presents the results of cost-benefit analysis in a flexible form supporting strategic investment decisions to buy down risk as measured by $\Theta$. AVM does not recommend a specific investment strategy, but does provide a means for comparing alternatives. This was done by performing a simulation and comparing results across seven different strategies over a ten-year period examining variable probabilities of attack and attacker perceptions as a percent deviation of $\Theta$. Section 4.4.3 presented the results from analyzing seven different investment strategies designated as 1) Least Cost (LC), 2) Least Protected (LP), 3) Region Protection (RP), 4) Sector Protection (SP), 5) Highest DTheta (HD), 6) Highest Consequence (HC), and 7) Random Protection (RAN). Appendix C described installation and configuration of the AVM investment strategy simulation for researchers who wish to independently perform the same experiments. This appendix will describe how analysis was conducted on simulation results to support the findings in section 4.4.3 and facilitate further independent research.
D.2. Independent Simulation Results

As described in section Appendix C, AVM investment strategy simulation produces a
slew of result and data sensitivity files that must be reduced by Model Assessment Program
(MAP) and Data Sensitivity Analysis (DSA) modules. It further describes how the reduced data
sets may then be imported into corresponding MAP and DSA spreadsheets for independent
analysis of each simulated investment strategy. The combined results are represented as shown
in figures 4-15 through 4-18 charting 1) the number of successful attacks across varying
probabilities of attack for all investment strategies, 2) the amount of damages across varying
probabilities of attack for all investment strategies, 3) the average expenditures across varying
probabilities of attack for all investment strategies, and 4) the amount of protection purchased
across varying probabilities of attack for all investment strategies. The problem with these
representations is they cannot provide meaningful comparison because of data variances between
simulations. Fortunately it is possible to normalize these variances to accommodate meaningful
comparison between investment strategy simulations by using DSA collected data. As shown in
figures D-1 through D-3, DSA collects execution data related to 1) the average amount of
protection purchased, 2) the average number of attacks, and 3) the average damage value. Since
damages will be the determining value in comparing investment strategies, this will be the focus
of attention for subsequent analysis. The DSA data in figure D-3 shows a variance of 0.00137
and 0.00207 in damage calculations across the investment strategy simulations. These variances
must be normalized in order to make an accurate comparison of simulation results produced by
MAP. This is done in a third spreadsheet designated Analysis.xlsx.
D.3. Combined Simulation Results

Analysis of combined simulation results is conducted in the Analysis.xlsx spreadsheet. The Analysis.xlsx spreadsheet copies data from both the MAP and DSA spreadsheets and combines them in a single tab for the given simulations AVM12, AVM13, and AVM14. Combined analysis begins by calculating the percentage difference in damage calculations across the different simulations as shown in figure D-4. This is done by selecting one set of data as the
baseline and calculating the percentage difference of all other data with respect to the baseline data.

![AVM14 DSA Data Variances](image)

Figure D-4: Percent Variation in Damages Across Simulations.

The percentage differences between data variances become the adjustment factors for normalizing data across simulations. Figure D-4 displays data variances after being normalized.

![AVM14 DSA Adjusted Damages](image)

Figure D-5: Normalized Damages Across Simulations.
Figure D-5 demonstrates how the normalization factors can remove variances across simulations. The same normalization now needs to be applied to the MAP results. The adjusted results data is depicted in figure D-6.

The adjusted damages in figure D-6 now provides an equal basis for comparing different investment strategies as shown in figure D-7.
Figure D-7 includes the baseline data together with the adjusted data to demonstrate the comparison differences. Before normalization, the HD strategy seemingly incurred more damages than HC. After normalization, the relationships were completely reversed, demonstrating the importance of comparing equalized data to obtain true results.

D.4. Summary

AVM supports simulation and analysis of various risk reduction investment strategies to protect CI and WMD. The simulation programs described in Appendix C will produce results and that may be analyzed independently using the MAP spreadsheet. But in order to make an accurate comparison across investment strategies it is necessary to normalize data variations capture in the DSA spreadsheet. Comparative analysis across simulations is facilitated by the Analysis.xlsx spreadsheet. This spreadsheet uses DSA variance data to normalize MAP results to facilitate meaningful comparison across strategy simulations. Only after variance data has been taken into account may observations and conclusions be drawn from the results.
Bibliography


The Three Mile Island accident was a core meltdown in Unit 2 of the Three Mile Island Nuclear Generating Station in Dauphin County, Pennsylvania near Harrisburg, United States in 1979. The accident resulted in the release of approximately 2.5 million curies of radioactive gases, and approximately 15 curies of iodine-131. There was an evacuation of 140,000 pregnant women and pre-school age children from the area. In the end, the reactor was brought under control, although full details of the accident were not discovered until much later, following extensive investigations by both a presidential commission and the NRC. The Kemeny Commission Report concluded that "there will either be no case of cancer or the number of cases will be so small that it will never be possible to detect them. The same conclusion applies to the other possible health effects". Several epidemiological studies in the years since the accident have supported the conclusion that radiation released from the accident had no perceptible effect on cancer incidence in residents near the plant, though these findings are contested by one team of researchers. Cleanup started in August 1979 and officially ended in December 1993, with a total cleanup cost of about $1B. The accident crystallized anti-nuclear safety concerns among activists and the general public, resulted in new regulations for the nuclear industry, and has been cited as a contributor to the decline of new reactor construction that was already underway in the 1970s (Wikipedia).

End Notes

1 In October 2011, US military operations in Afghanistan surpassed 104 months, longer than the US involvement in Vietnam, formerly the longest conflict in US history.
2 Denial of habeas corpus to Guantanamo prisoners, kidnapping terror suspects, warrantless wiretaps, water boarding, airport scanners, and capture/kill lists have all pressed the bounds of Constitutional authority. While past presidents have suspended US civil liberties in times of crisis or war (Adams – Alien and Sedition Acts, Lincoln – Suspension of Habeas Corpus, Roosevelt – Japanese American Internment), judicial precedent threatens to embed current measures in customary law.
4 Direct 9/11 costs include $34B in insured losses for buildings and infrastructure, plus $576M for rebuilding the Pentagon, and $7B for official victim compensation. Indirect losses due to the downturn in world markets may place the total cost of 9/11 near $300B.
5 On the morning of December 7, 1941, a strike force of the Imperial Japanese Navy struck the US naval base at Pearl Harbor Hawaii. The base was attacked by 353 Japanese fighters, bombers and torpedo planes in two waves, launched from six aircraft carriers. Four US Navy battleships were sunk, 188 aircraft destroyed, 2,402 Americans killed, and 1,282 wounded.
6 Khalid Sheikh Mohammed, the architect of 9/11, estimated the total cost of the operation at less than $400,000.
7 The classification and number of critical infrastructures has evolved over presidential administrations. The original concept can be traced to PPD-63 in the Clinton Administration. The Bush Administration reiterated the original concept in HSPD-7, then expanded the number of CI sectors to 18 in the 2009 National Infrastructure Protection Plan. In February 2013, the Obama Administration issued PPD-13 reducing the number of CI sectors to 16.
8 The Year 2000 problem (also known as the Y2K problem, the Millennium bug, the Y2K bug, or simply Y2K) was a problem for both digital (computer-related) and non-digital documentation and data storage devices stemming from the practice of abbreviating a four-digit year to two digits. In computer programs, the practice of representing the year with two digits becomes problematic with logical errors arising upon "rollover" from x99 to x00. This caused some date-related processing to operate incorrectly for dates and times on and after January 1, 2000 and on other critical dates which were billed "event horizons". Without corrective action, long-working systems would break down when the "...97, 98, 99, 00..." ascending numbering assumption suddenly became invalid. Companies and organizations worldwide checked, fixed, and upgraded their computer systems. The number of computer failures that occurred when the clocks rolled over into 2000 in spite of remedial work is not known; among other reasons is the reticence of organizations to report problems. There is evidence of at least one date-related banking failure due to Y2K. There were plenty of other Y2K problems, but the fact that none caused major incidents is seen by some as vindication of the Y2K preparation. However, some questioned whether the relative absence of computer failures was the result of the preparation undertaken or whether the significance of the problem had been overstated (Wikipedia).
9 The Three Mile Island accident was a core meltdown in Unit 2 of the Three Mile Island Nuclear Generating Station in Dauphin County, Pennsylvania near Harrisburg, United States in 1979. The accident resulted in the release of approximately 2.5 million curies of radioactive gases, and approximately 15 curies of iodine-131. There was an evacuation of 140,000 pregnant women and pre-school age children from the area. In the end, the reactor was brought under control, although full details of the accident were not discovered until much later, following extensive investigations by both a presidential commission and the NRC. The Kemeny Commission Report concluded that "there will either be no case of cancer or the number of cases will be so small that it will never be possible to detect them. The same conclusion applies to the other possible health effects". Several epidemiological studies in the years since the accident have supported the conclusion that radiation released from the accident had no perceptible effect on cancer incidence in residents near the plant, though these findings are contested by one team of researchers. Cleanup started in August 1979 and officially ended in December 1993, with a total cleanup cost of about $1B. The accident crystallized anti-nuclear safety concerns among activists and the general public, resulted in new regulations for the nuclear industry, and has been cited as a contributor to the decline of new reactor construction that was already underway in the 1970s (Wikipedia).
On 26 April 1986, the Chernobyl Nuclear Power Plant in Ukraine exploded and caught fire, releasing large quantities of radioactive contamination into the atmosphere and spreading it over much of the Western Soviet Union and Europe. It is considered the worst nuclear power plant accident in history, rivaled only by the Fukushima Daiichi nuclear disaster in March 2011. The battle to contain the contamination and avert a greater catastrophe ultimately involved over 500,000 workers and cost an estimated 18 billion rubles, crippling the Soviet economy. From 1986 to 2000, 350,400 people were evacuated and resettled from the most severely contaminated areas of Belarus, Russia, and Ukraine. According to official post-Soviet data, about 60% of the fallout landed in Belarus. The accident raised concerns about the safety of the Soviet nuclear power industry, as well as nuclear power in general, slowing its expansion for a number of years and forcing the Soviet government to become less secretive about its procedures. The government cover-up of the Chernobyl disaster was a "catalyst" for glasnost, which "paved the way for reforms leading to the Soviet collapse." Russia, Ukraine, and Belarus have been burdened with the continuing and substantial decontamination and health care costs of the Chernobyl accident. Thirty one deaths are directly attributed to the accident, all among the reactor staff and emergency workers. A UN report places the total confirmed deaths from radiation at 64 as of 2008. The World Health Organization suggests it could reach 4,000 civilian deaths, a figure which does not include military clean-up worker casualties. A 2006 report predicted 30,000 to 60,000 cancer deaths as a result of Chernobyl fallout. A Greenpeace report puts this figure at 200,000 or more. A Russian publication, Chernobyl, concludes that 985,000 premature cancer deaths occurred worldwide between 1986 and 2004 as a result of radioactive contamination from Chernobyl (Wikipedia).

The Fukushima Daiichi Nuclear Power Plant suffered major damage from a 9.0 earthquake and subsequent tsunami that hit Japan on March 11, 2011. The incident permanently damaged some reactors making it technically impossible to restart the reactors, and the other reactors politically impossible to reopen. The earthquake and tsunami disabled the reactor cooling systems, leading to releases of radioactivity and triggering a 30 km evacuation zone surrounding the plant.

Some might reasonably argue that CI policy traces roots to the Federal Civil Defense Act of 1950 which addressed localized emergency protective and response measures in the event of an attack. Civil Defense authorities were transferred to the Federal Emergency Management Agency when it was created in 1978. Following Hurricane Andrew in 1993, FEMA was re-organized to more specifically focus on natural disasters, and in 1994 the Federal Civil Defense Act of 1950 was repealed.

A Markov chain, named for Andrey Markov, is a mathematical system that undergoes transitions from one state to another, between a finite or countable number of possible states. It is a random process characterized as memoryless: the next state depends only on the current state and not on the sequence of events that preceded it. This specific kind of "memorylessness" is called the Markov Property (Wikipedia).

The Poisson Distribution is a discrete probability distribution that expresses the probability of a given number of events occurring in a fixed interval of time and/or space if these events occur with a known average rate and independently of the time since the last event (Wikipedia).

A feedback policy is a maximizing function for a Markov chain. The point of this statement is that stochastic processes can reveal behavioral influences separate from deterministic processes, such as earthquakes.

The Bojinka plot was a planned large-scale Islamist terrorist attack by Ramzi Yousef and Khalid Shaikh Mohammed to blow up 12 airliners and their approximately 4,000 passengers as they flew from Asia to the United States. Khalid Shaikh Mohammed evolved this plot into the 9–11 airliner attacks (Wikipedia).

A feedback policy is a maximizing function for a Markov chain. The point of this statement is that stochastic processes can reveal behavioral influences separate from deterministic processes, such as earthquakes.

The 7 July 2005 London bombings (often referred to as 7/7) were a series of coordinated suicide attacks in the United Kingdom, targeting civilians using London's public transport system during the morning rush hour. On the morning of Thursday, 7 July 2005, four terrorists detonated four bombs, three in quick succession aboard London Underground trains across the city and, later, a fourth on a double-decker bus in Tavistock Square. Fifty-two people, as well as the four bombers, were killed in the attacks, and over 700 more were injured.

On June 6, 2013, news reports disclosed the existence PRISM, a clandestine national security electronic surveillance program operated by the National Security Agency since 2007. Operating under the authorization of the Foreign Intelligence Surveillance Court, PRISM analyzed massive amounts of communications traffic collected from major commercial providers including Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, AOL, Skype, and Apple. The unprecedented scale of the surveillance may be gauged by the fact that Verizon was ordered to turn over to the NSA logs tracking all of its customers' telephone calls on an ongoing daily basis (Wikipedia).

The Provisional Irish Republican Army (IRA) is a paramilitary organization whose aim was to remove Northern Ireland from the United Kingdom and bring about a socialist republic within a united Ireland by force of arms and political persuasion. The IRA's initial strategy was to use force to cause the collapse of the Northern Ireland administration and to inflict enough casualties on the British forces that the British government would be forced by
public opinion to withdraw from the region. From 1971–1994, the IRA launched a sustained offensive armed campaign that mainly targeted the British Army, the Royal Ulster Constabulary (RUC), the Ulster Defence Regiment (UDR), and economic targets in Northern Ireland. The first half of the 1970s was the most intense period of the IRA campaign. On 28 July 2005, the IRA Army Council announced an end to its armed campaign, stating that it would work to achieve its aims using “purely political and democratic programs through exclusively peaceful means (Wikipedia).

20 The Armed Islamic Group (GIA from French Groupe Islamique Armé) is an Islamist organization that wants to overthrow the Algerian government and replace it with an Islamic state. The GIA adopted violent tactics in 1992 after the military government voided the victory of the Islamic Salvation Front, the largest Islamic opposition party, in the first round of legislative elections held in December 1991. The group uses assassinations and bombings, including car bombs, and it is known to favor kidnapping victims and raping them. The GIA is considered a terrorist organization by the governments of Algeria, France and the United States (Wikipedia).

21 A comprehensive review of DHS infrastructure protection efforts conducted by the Congressional Research Service in 2011 reported “DHS’s Annual Performance Report matches specific program with specific metrics. However, as with the budget justifications, reporting and the metrics identified in the Annual Performance Reports have varied over the years. DHS’s FY2008-FY2010 Annual Performance Report identified three performance metrics which it measures progress of the Infrastructure Protection Program (apparently referring to the non-cyber and non-communications related activities of the Infrastructure Protection and Information Security Program in the budget). These were: the percentage of critical infrastructure and key resource sector specific protection implementation actions on track (apparently referring to actions identified in the individual Sector Specific Plans); the percent of high-priority critical infrastructure and key resources where a vulnerability assessment has been conducted and enhancements(s) have been implemented; and percent of inspected high-risk chemical facilities in compliance with risk based performance standards”

22 According to the Commerce Department Bureau of Economic Analysis, GDP dropped from 6.43% in 2000 to 3.38% in 2001. A similar drop was registered in personal income rates for which data is available back to 1958. In both cases, they were the largest drop in economic growth until the global economic crisis of 2008. See www.bea.gov.

23 According to data from the Centers for Disease Control and Prevention National Center for Health Statistics, the homicide rate jumped from 5.9 deaths per 100,000 to 7.1 from 2000 and 2001. The rate dropped to 6.1 in 2002, continuing a decreasing trend in murder rates from their peak of 9.9 in 1991. The nearly 3,000 people killed by 9/11 registered a significant spike in this trend. See www.cdc.gov/nchs/hdi.htm.

24 Infrastructure data collected by DHS is protected under the 2002 Homeland Security Act from disclosure even under the Freedom of Information Action.

25 On February 26, 1993, a huge bomb went off beneath the two towers of the World Trade Center. Ramzi Yousef, the Sunni extremist who planted the bomb, said later that he had hoped to kill 250,000 people. He and his accomplices were successfully captured by the FBI, and later prosecuted and sent to prison. The 9/11 Commission Report cites the 1993 bombing as signaling a new terrorist challenge, one whose rage and malice had no limit. The 9/11 Commission also implicates the superb investigative and prosecutorial effort in creating a false sense that the law enforcement system was well-equipped to cope with terrorism.

26 In 1983, a Hezbollah suicide bomber drove a truck bomb into the Marine barracks in Beirut, killing 241 US Marines. The Marines had been sent to Lebanon on a peace keeping mission during the Lebanese civil war. As a result of the attack, President Reagan withdrew the Marines from Lebanon; a reversal routinely cited by jihadists as evidence of US weakness according to the 9/11 Commission.


28 In October 2008, the Troubled Asset Relief Program (TARP) dispensed $418 billion to prevent collapse of the US banking system and avoid economic depression.

29 All AVM program inputs, including probabilities, are specified as integer values to facilitate processing with batch file variables.

30 AVM simulation batch files were named according to a convention that 1) identifies the simulation type (i.e., LC, LP, R44, etc.), 2) by the number of assets (i.e., 100), and 3) the number of simulations (i.e., 100).