Towards a Unified Homeland Security Strategy: An Asset Vulnerability Model

Richard White

ABSTRACT

The 2013 National Infrastructure Protection Plan represents the latest attempt to rectify a faltering program that has suffered from the absence of a viable risk measure. This article introduces an Asset Vulnerability Model (AVM) to overcome recognized challenges and provide strategic direction in the form of (1) baseline analysis, (2) cost-benefit analysis, and (3) decision support tools. AVM is predicated on Θ, an attacker's probability of failure based on research in game theory. The Θ risk formulation provides a unifying structure within the Department of Homeland Security by combining elements from the Risk Management Framework and National Preparedness System. But critical infrastructure is not the only means of domestic catastrophic attack. Thus this article also proposes a policy framework supported by game theory to extend AVM protection to chemical, biological, radiological, and nuclear stockpiles. In this manner, AVM may account for protective investments and lead the nation towards a unified homeland security strategy.

INTRODUCTION

The attacks of September 11, 2001, exposed the vulnerability of critical infrastructure to precipitating domestic catastrophic attack through asymmetric means. In the intervening decade, the Department of Homeland Security (DHS) has struggled to develop a coherent infrastructure protection program. Various reviews reveal a program that is fragmented, uncoordinated, and adrift. The central difficulty has been in developing a risk assessment formulation to adequately inform strategic investment decisions. Without an appropriate measure, DHS is unable to (1) assess current protective status, (2) evaluate future protective improvement measures, or (3) justify national investments.

This paper examines current DHS infrastructure protection programs and the underlying challenges to developing an adequate risk assessment formulation. It then addresses these challenges before introducing an Asset Vulnerability Model (AVM) to overcome them and help provide strategic direction. It draws on insight from earlier research in game theory suggesting a coordinated defense for both critical infrastructure and domestic stockpiles of chemical, biological, radiological, and nuclear (CBRN) agents. It concludes by proposing a policy framework supporting interagency coordination protecting both sets of assets under a unified homeland security strategy.

CRITICAL INFRASTRUCTURE PROTECTION

On September 11, 2001, elements of the aviation infrastructure were exploited to attack the World Trade Center and the Pentagon representing seats of US economic and military power (The White House 2003, 8).[1] Nearly 3,000 people were killed and $41.5 billion suffered in damages.[2] 9/11 was a "wake-up call" to the catastrophic potential of critical infrastructure (The White House 2003, 5).[3] As a result, the 2002 Homeland Security Act made critical infrastructure protection a core mission of the newly created Department of Homeland Security.[4] Today, the 2013 *National Infrastructure Protection Plan* (NIPP) guides this mission. At the heart of the plan is the Risk Management Framework (RMF), a five-step process for identifying, prioritizing, applying, and evaluating infrastructure protection improvement measures.[5] A 2010 review by the National Research Council (NRC) 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 need of major revision."[6] Various other reviews support the NRC's findings.

Starting with Step Two, "Identify Infrastructure," the DHS Inspector General (IG) concluded that the National Asset Database 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 assets in question included 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 database were many other items from banking and finance and food and agriculture sectors.[7]

In Step Three, "Assess and Analyze Risks", the Government Accountability Office (GAO) found that less than 11 percent of DHS' assessments were conducted on high-priority assets. According to the 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 assets. Because of discrepancies between lists, GAO acknowledged another 129 assessments might also have been done on high priority assets.[8] GAO acknowledged that DHS had little control over industry participation in the voluntary program, but also noted that DHS (1) had not developed institutional performance goals to measure owner/operator participation, nor (2) positioned itself to assess why some high-priority asset owners and operators declined to participate.[9]

Moreover, the Homeland Security Grant Program (HSGP) raised a furor in 2006 when Wyoming received $28.34 per capita compared to $4.10 and $3.73 per capita for New York and California respectively. After the 9/11 Commission weighed in on the issue, and spurred by Congressional legislation, DHS undertook to develop a more risk-based approach for determining HSGP allocations. Accordingly, the 2007 HSGP grant guidance announced the adoption of the risk formula R=T*V*C where T is the likelihood of an attack occurring, V is the vulnerability to an attack, and C is the potential consequences of an attack. In applying the formula, however, DHS was unable to differentiate vulnerability across areas and states, and consequently assigned it a constant value of one.[10] In effect, DHS treated all assets as equally vulnerable to make resource decisions about reducing vulnerability.

In Step Four, "Implement Risk Management Activities," a 2011 Congressional Research Service (CRS) report indicated a lack of coordination between the RMF working "inside the perimeter" of critical infrastructure, and the National Preparedness System working "outside the perimeter" of critical infrastructure. According to the CRS 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.[11]

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.

> A central question that may be asked is what has been the rate of return, as defined by identifiable and empirical risk reductions, on this $12 billion investment? It does not appear, however, that there is an established methodology to engage in such analyses, nor are the data sets necessary for such analyses well-developed.[12]

Indeed, the National Research Council

> [D]id 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.[13]

Developing an appropriate risk measure is essential to guiding homeland security strategy, without which it is impossible to (1) assess current status, (2) evaluate future measures, or (3) justify national investments. Furthermore, it is a requirement under the 1993 Government Performance and Results Act. That the 2014 DHS budget justification to Congress does not include such measures for infrastructure protection indicates this is still a pertinent issue.[14] The state of affairs is of such a concern that in February 2013 the Obama Administration issued Presidential Policy Directive 21 calling for a review and analysis of current efforts to advance "a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."[15]

RISK ASSESSMENT CHALLENGES

Among its conclusions, the National Research Council found that the DHS Risk Management Framework "is sound and in accord with accepted practice in the risk analysis field."[16] 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."[17] Where the NRC took exception was with the DHS risk assessment formulation R=f(T,V,C).[18]

Risk assessment "pertains to the quantification or measurement of identified risk and probabilistic assessment that certain risks will manifest themselves."[19] By one estimate, there are more than 250 proposed risk assessment methodologies for critical infrastructure alone.[20] Ted Lewis wrote the textbook on risk analysis for critical infrastructure protection.[21] Lewis applies a threat-driven approach to risk assessment. Threat-driven methodologies begin with a predefined set of initiating events. A 2001 study indicated that 80 percent of risk assessment models are of the event- or threat-driven variety.[22] Threat-driven approaches are supported by decades of experience in safety and reliability engineering using logic trees, influence diagrams, causal loop diagrams, and other methods to model human-initiated events.[23] According to McGill, "threat-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 ultimately fail to consider emerging or unrecognized threats devised by an innovative adversary...."[24] 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.[25] The National Research Council concurs 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."[26]

Altogether the 2010 National Research Council report cited ten challenges to developing a risk formulation adequate for guiding strategic investment decisions.[27] In addition to the difficulty of making reliable threat predictions, the NRC cautioned against risk formulations that were either too simple or too complex. The problem with developing high fidelity risk 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 NRC, is to develop risk models that are "documented, transparent, and repeatable."[28] For the purpose of guiding strategic decisions, the risk formulation must also be comprehensive in scope. According to the NRC report, "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."[29] In other words, the risk

formulation should address all phases of disaster, currently identified in the FEMA Integrated Emergency Management System as prevent, protect, mitigate, respond, and recover.[30] Similarly, the risk formulation needs to capture the broader effects of a disaster beyond the immediate damage. "DHS's consequence analyses tend to limit themselves to death, physical damage, first-order economic effects, and in some cases, injuries and illness."[31] Ultimately, the effectiveness of any risk formulation is judged by its usefulness to decision makers in managing resources. According to the National Research Council, the attributes of a good risk analysis include 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.[32]

The preceding summary does not address all the challenges identified by the National Research Council, but provides sufficient criteria for making a cursory evaluation of some current risk models. A 2006 survey identified thirty critical infrastructure models specializing in interdependency analysis.[33] A separate survey in 2012 identified twenty-one critical infrastructure risk models for informing strategic decisions.[34] Together, the two surveys identified forty-one distinct models. McGill's Critical Asset and Portfolio Risk Analysis (CAPRA) was also added, making a total of forty-two models (See Table 1). The limited information available was sufficient to examine only the twenty-two models identified in bold text in Table 1. Of the twenty-two models examined, twelve used a threat-driven approach, seven were described as "complicated," fourteen did not address "resiliency", and two did not capture the broader impacts of a disaster. None of the models appeared to satisfy the NRC challenges.

Table 1: Critical Infrastructure Risk Assessment Models

1. AIMS	22. IIM
2. Athena	23. KM&V
3. BIRR	24. MDM
4. BMI	25. MIN
5. CAPRA	26. MUNICIPAL
6. CARVER2™	27. N-ABLE
7. CIMS	28. NEMO
8. CIP	29. Net-Centric GIS
9. CIPDSS	30. NEXUS-FF
10. CIPMA	31. NGtools
11. CISIA	32. NSRAM
12. CommAspen	33. PFNAM
13. COUNTERACT	34. RAMCAP-Plus
14. DECRIS	35. RMCIS
15. DEW	36. RMF (DHS)
16. EMCAs	37. RVA
17. EURACOM	38. SRAM
18. FAIT	39. TRAGIS
19. FINSIM	40. TRANSIMS
20. Fort Future	41. UIS
21. IEISS	42. WISE

SHAPING AN ADEQUATE RISK FORMULATION

Obviously, an adequate risk formulation for guiding strategic decisions needs to overcome the previous challenges. The foremost challenge is overcoming the inherent problems to the threat-driven approach. Adopting an asset-driven approach may do this. An asset-driven approach estimates the consequences and probability of adversary success for an exhaustive set of plausible initiating events without regard to their probability of occurrence, and then overlays their likeliness of occurrence if such information is available.[35] The main criticism of the asset-driven approach is that it is an "impact analysis" not a "risk analysis."[36] Without a firm probability occurrence, the asset-driven approach is deemed less efficient at allocating resources where they're most needed; i.e., the assets most likely to be attacked. Again, the dearth of attack data renders robust statistical analysis problematic. 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 is in localizing their effects. Thus, for example, while earthquakes are a national phenomenon, California justifiably bears the cost of more stringent seismic standards compared to Connecticut. Localization can be similarly applied to critical infrastructure without the benefit of statistical analysis. Homeland Security Presidential Directive 7 does this by specifying protection for critical infrastructure "whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to the use of a weapon of mass destruction… [or] have a debilitating effect on security and economic well-being."[37] Of the sixteen infrastructure sectors currently categorized by the federal government, the nine listed in Table 2 could be targeted to precipitate mass or debilitating effects.

Table 2: Critical Infrastructure Threats

1. Chemical Plants
2. Dams
3. Energy
4. Financial Services
5. Food & Agriculture
6. Information Networks
7. Nuclear Reactors, Materials, & Waste
8. Transportation Systems
9. Water & Wastewater Systems

Not included in the list in Table 2 are commercial facilities, communications, critical manufacturing, defense industrial base, emergency services, government facilities, and healthcare and public health. 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 did not 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 precipitate mass effects. Similar arguments may be made for the remaining sectors.

Insofar as developing an adequate risk formulation is concerned, it is also important to choose the right metric. An appropriate metric must answer three questions: (1) What is the risk to? (2) What is the risk from? and (3) How much risk is acceptable?[38] To answer these questions, it is necessary to turn to earlier work in game theory.

Game theory is the study of multi-agent decision problems. Most of the current research and applications are conducted by micro-economists, though game theory has also been successfully applied to areas as diverse as computer science and evolutionary biology.[39] 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.[40] In 1988, Todd Sandler and Harvey Lapan used game theory to examine the strategic relationship between terrorists' choice of targets and the 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 and Lapan's findings were dependent on a particular value representing the terrorist's probability of attack failure, which they designated as θ.[41] Sandler and Lapan's research suggest a metric based on θ as it answers the three questions: (1) What is the risk to? The risk is to critical infrastructure assets; (2) What is the risk from? The risk is from an attacker; (3) How much risk is acceptable? Targets are optimally protected when they are equally protected.

AN ASSET VULNERABILITY MODEL

An Asset Vulnerability Model is now introduced to work with the DHS Risk Management Framework and (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. 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 comprised of three elements: (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. Theta is calculated in an asset-based risk formula addressing the five phases of emergency management. A separate Θ is calculated for every critical infrastructure asset as listed in Table 2 that may be exploited or destroyed to create mass or debilitating effects. The proposed risk formulation for Θ is as follows:

$$\Theta = P(dis)*P(def)*P(den)*P(dim)*\%dam) \quad (1.0)$$

where

$$P(dis) = \text{Probability an attack can be detected/disrupted} \quad (1.1)$$

$$P(def) = \text{Probability an attack can be defeated} \quad (1.2)$$

$$P(den) = \text{Probability a worst case disaster can be averted} \quad (1.3)$$

$$P(dim) = \text{Probability 100\% of the survivors can be saved} \quad (1.4)$$

$$\%(dam) = \text{\% decrease in economic output * \% increase in mortality rate} \quad (1.5)$$

P(dis) corresponds to the "prevent" phase of emergency management and is calculated from known intelligence data by dividing the number of thwarted attacks by the number of planned and executed attacks. This estimation for stopping an attack is fundamentally different from trying to predict the start of one, making acceptable use of what limited historical data available. P(def) corresponds to the "protect" phase of emergency management. P(def) is derived from the Protective Measure Index (PMI) assessed by security surveys and vulnerability assessments currently conducted by DHS. PMI are assessed at Argonne National Laboratory from data collected by a cadre of DHS Protective Security Advisors, helping maintain consistency of results.[42] P(den) corresponds to the "mitigate" phase of emergency management and examines failure modes and redundancy designed to prevent an asset's incapacitation or subversion. As part of its PMI calculation, Argonne National Laboratory also produces a Resiliency Index that may be used in this estimation.[43] P(dim) corresponds to the "response" phase of emergency management. P(dim) is calculated based on the capacity of first responders to rescue and treat survivors within seventy-two-hours of a catastrophe. A default value may be calculated from historical data for similar size incidents independent of cause. The %(dam) parameter simultaneously represents the "recovery" phase of emergency management and the magnitude component of the risk assessment formula. It taps existing national economic and mortality data capturing the broader impacts for incidents of both mass destruction and disruption.

Cost-benefit analysis finds the optimum combination of security improvement measures proposed for each asset. Cost-benefit analysis is conducted using ΔΘ and D(ΔΘ) for each improvement measure. Delta theta is the estimated increase in Θ for the proposed improvement measure. Delta theta is provided in component form as P(Δdis), P(Δdef), P(Δden), and P(Δdim). The magnitude component, %(dam) remains unchanged as it represents the worst-case disaster if an asset is compromised. An associated cost component is provided for each ΔΘ in the form of D(Δdis),

D(Δdef), D(Δden), and D(Δdim). Each proposed improvement measure has an associated set of paired ΔΘ and D(ΔΘ) data tuples. P(Δdef) and P(Δden) are directly related to assets, whereas P(Δdis) and P(Δdim) represent national and regional improvement measures that are proportionally assigned to affected assets. The given ΔΘ and D(ΔΘ) values are discrete, representing specific capabilities for purchase. The choice of whether or not to buy them is also discrete; there are no fractional solutions. The data sets associated with each improvement are also independent. This stipulation eliminates dependency analysis. Estimating ΔΘ will be difficult enough using either expert elicitation or computer modeling. Consistency will be key, suggesting that ΔΘ should be estimated by a central source, perhaps at Argonne National Laboratory using techniques already developed for the Protective Measure Index and Resilience Index. Cost-benefit analysis calculates the combined ΔΘ and D(ΔΘ) for each asset according to the formulations shown in 2.0 and 3.0. A proportional value is then derived by dividing ΔΘ by D(ΔΘ). The cost-benefit analysis program selects the combination of measures producing the highest proportional value for the given asset.

$$\Delta\Theta = P(\Delta dis)*P(\Delta def)*P(\Delta den)*P(\Delta dim)*\%(dam) \quad (2.0)$$

$$D(\Delta\Theta) = D(\Delta dis)+D(\Delta def)+D(\Delta den)+D(\Delta dim) \quad (3.0)$$

Decision support tools graphically portray the results of baseline and cost-benefit analyses and facilitate various views to present the information in a manner most meaningful to a decision maker. Figure 1.1 portrays the unfiltered results from baseline analysis using simulated data. Real data was unavailable as it is protected under the 2002 Homeland Security Act from disclosure even under the Freedom of Information Act. Alternative views of the data may be selected. For example, Figure 1.2 shows the baseline data sorted by Θ, identifying the most protected to the least protected assets. Figure 1.3 sorts baseline data by asset type, depicting the relative protection of assets within the same sector. Figure 1.4 indicates relative protection of assets within a given geographic region. Other views may also be generated as desired. Similarly, the results from cost-benefit analysis can be graphically portrayed to assist decision makers with allocating resources. For example, Figure 2.1 shows assets ordered by largest to smallest improvement gains, facilitating the purchase of the highest protection within a fixed budget. Figure 2.2 shows assets ordered by improvement cost, facilitating the purchase of the most protection measures within a fixed budget. If the decision maker wishes to concentrate on protecting a particular sector, then improvements can be sorted by asset type as in Figure 2.3. If the decision maker wishes to concentrate on protecting a particular region, then improvements can be sorted by asset location as in Figure 2.4. The significance of these tools is that they provide a snapshot of the current homeland security profile and can inform resource allocation decisions based on any number of different investment strategies.

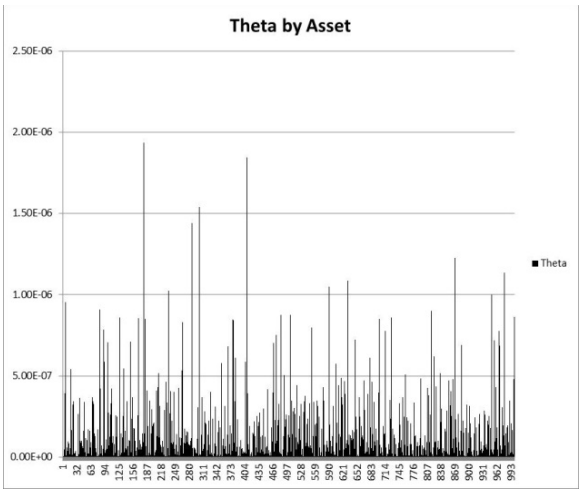

Figure 1.1: Unfiltered AVM Baseline Analysis Depicting Current Homeland Security Risk Profile

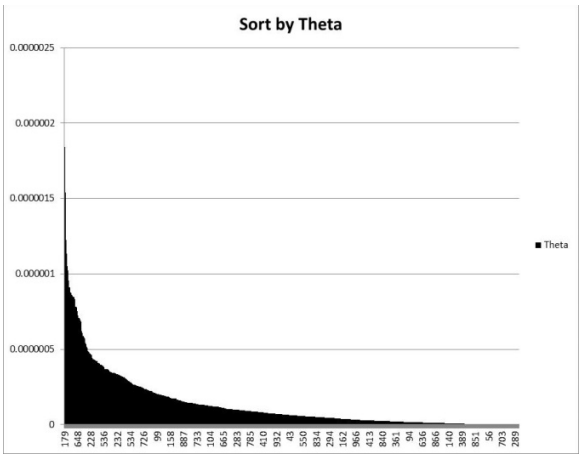

Figure 1.2: Baseline AVM Data Sorted by Theta Identifying Assets from Least to Most Vulnerable

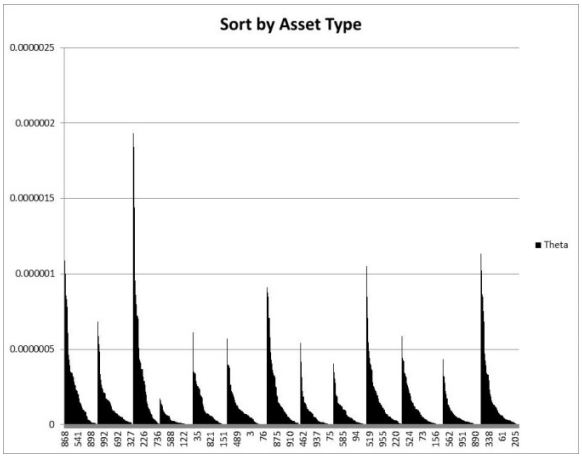

Figure 1.3: Baseline AVM Data Sorted by Asset Type Identifying Vulnerabilities by Infrastructure Sector

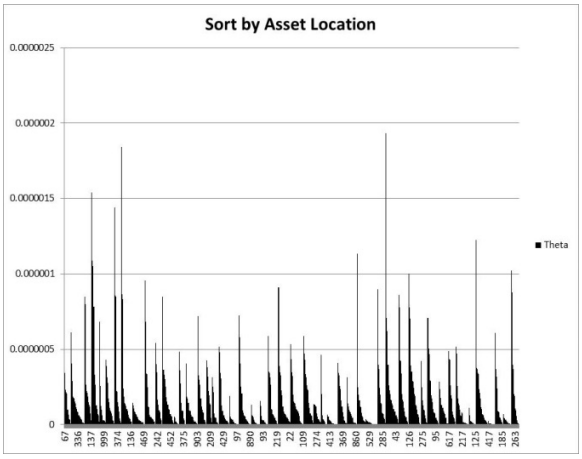

Figure 1.4: Baseline AVM Data Sorted by Asset Location Identifying Vulnerabilities by Region

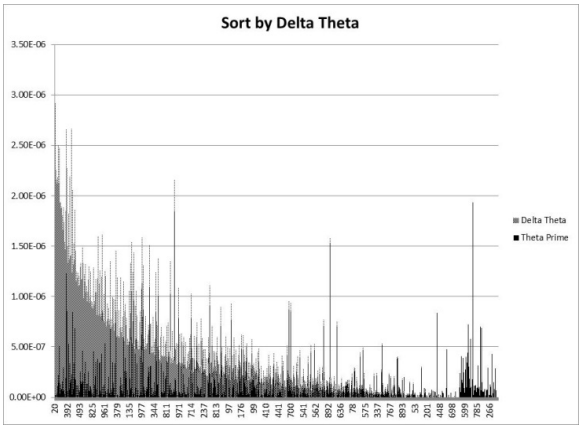

Figure 2.1: AVM Cost-Benefit Analysis Identifying Improvements in Order of Benefit (largest to smallest)

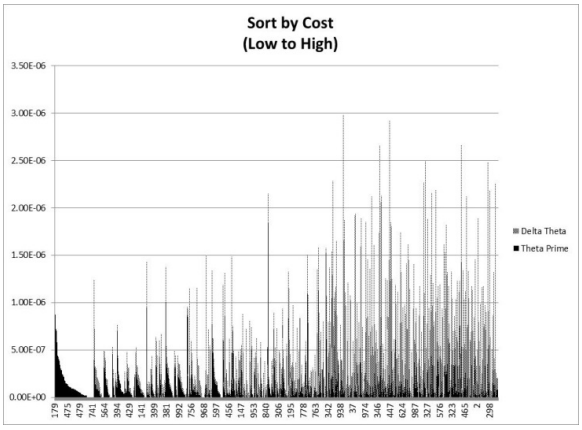

Figure 2.2: AVM Cost-Benefit Analysis Identifying Improvements by Cost (smallest to largest)

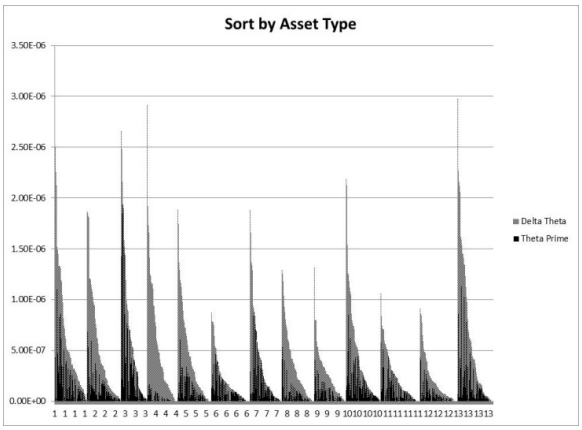

Figure 2.3: AVM Cost-Benefit Analysis Identifying Improvements by Asset Type

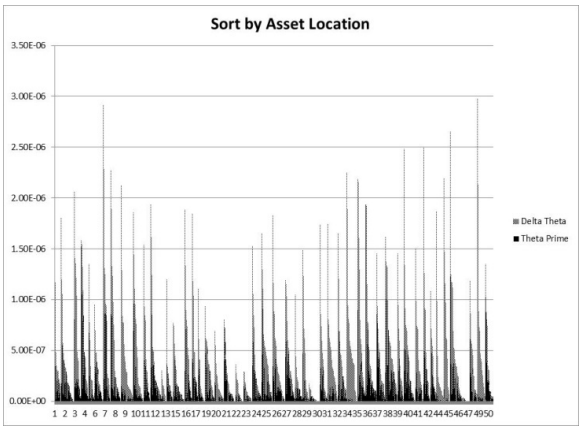

Figure 2.4: AVM Cost-Benefit Analysis Identifying Improvements by Region

AVM addresses many of the challenges to developing an adequate risk formulation for critical infrastructure. AVM avoids the problem of reliable threat estimation by adopting an asset-based vulnerability approach to risk management. Yet AVM is a comprehensive formulation addressing the five phases of emergency management: prevent, protect, mitigate, respond, and recover. All probability components in the AVM risk formulation, P(dis), P(def), P(den), and P(dim) make use of available empirical data facilitating documentation, transparency, and repeatability. The consequence component, %(dam), incorporates national economic and health data that capture the broader effects of both disruptive and destructive attacks. And AVM provides cost-benefit analysis and graphical presentation of the results in multiple formats supporting flexible decision strategies at all levels of management.

Working within the Risk Management Framework, AVM provides direction and coordination to help overcome current operational shortfalls. Beginning with Step Two of the framework, "Identify Infrastructure," AVM can help differentiate what infrastructure is critical from what is not. For example, shopping malls, race tracks, theme parks, and other questionable assets currently tracked by DHS would not be evaluated under AVM as they are inert, and by themselves could not be subverted or employed to create mass or debilitating effects. AVM baseline analysis conducted in Step Three, "Assess an Analyze Risks," provides a current risk profile of critical assets using the same capabilities and processes currently employed at DHS. By addressing risk components both "inside" and "outside" the perimeter of critical infrastructure, AVM provides a coordinating mechanism between the Risk Management Framework and National Preparedness System. Of course, there remains the question of voluntary versus mandatory data collection on the part of private industry. Most sectors identified in Table 2 are already federally regulated. It would not require much regulatory change to institute mandatory data collection from these sectors.[44] AVM cost-benefit analysis evaluates proposed improvement measures and identifies those providing the largest protective gain for the least cost. Thus AVM compares protective measures across all five phases of emergency management to determine the best investment option. AVM decision support tools present results in a flexible format that assists decision makers in recommending and justifying resource allocations in Step Four, "Implement Risk Management Activities." Through iterative application within the Risk Management Framework, AVM can measure and track investments and improvements over time.

POLICY EXTENSION

As has been demonstrated, AVM can help unify and guide strategic investment decisions for protecting critical infrastructure. Critical infrastructure, though, is only half the problem. Weapons of mass destruction in the form of chemical, biological, radiological, and nuclear agents also present the opportunity for asymmetric attack. Referring back to Sandler and Lapan's findings in game theory (a coordinated defense is more efficient than an uncoordinated one) suggests that AVM should be extended to encompass both critical infrastructure and CBRN stockpiles. This will require interagency coordination between DHS, the Department of Defense, and the Department of Energy. Strategy coordination between executive departments is conducted at the highest level in the National Security Council.[45] Strategy formulation is shaped by National Security Strategy (NSS), which serves as a coordinating framework for federal agencies to prioritize resources and schedule activities to work towards common national goals.[46]

Current National Security Strategy reiterates the definition of homeland security promulgated in the 2010 *Quadrennial Homeland Security Review* as "a concerted national effort to ensure a homeland that is safe, secure, and resilient against terrorism and other and other hazards where American interests, aspirations, and way of life can thrive."[47] This definition places terrorism at the forefront of homeland security concerns. Such a suggestion belies the historical significance of 9/11. The United States had suffered terrorist attacks long before 9/11, but it wasn't until those attacks that homeland security became a national priority. What was unique about 9/11 that prompted the largest re-organization of US government since World War II and made homeland security part of the national lexicon? According to the 9/11 Commission, it was the "surpassing disproportion" of the attack. On September 11, 2001, nineteen men inflicted as much damage on the United States as the Imperial Japanese Navy on December 7, 1941.[48] 9/11 made manifest the unprecedented threat of domestic catastrophic attack accomplished through asymmetric means by small groups or individuals acting on their own behalf. The problem is not terrorism. Terrorism is defined as "any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments."[49] Terrorism is a motive. Certainly it played a role in the 9/11 attacks, but who is to say it is the only motive that could precipitate another such attack?

The current preoccupation with terrorism distracts attention from the real threat discerned by the 9/11 Commission: domestic catastrophic attack precipitated by subverting critical infrastructure or employing weapons of mass destruction. To effectively coordinate interagency efforts towards this problem, a new definition of homeland security should be considered. An alternative definition might be "to safeguard the United States 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 catastrophic attack 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." This statement offers a concise strategy specifying "ends," "ways," and "means." Together with the new definition, they can help direct interagency efforts towards a unified homeland security strategy.

FUTURE RESEARCH

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

First, a definitive taxonomy must be developed to help identify those things that can create a domestic catastrophic attack. DHS previously developed taxonomy for its National Asset Database.[50] Perhaps it can be adopted for this application. CARVER+Shock analysis has also been employed and may be sufficiently useful.[51] 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."[52] For reasons stated earlier, 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.

Understandably, the National Research Council places a premium on verifying and validating model results.[53] Again, the availability of historical data is problematic. In this regard, the NRC suggests one possible method recommended by the JASON scientific advisor group to "address smaller, well-defined, testable pieces of the larger problem."[54] How this might be accomplished is also an area for research.

A glaring omission from this proposal is how to treat natural disasters? Disaster response became a homeland security mission when FEMA was folded into DHS. The prevailing logic was that many of the same response and recovery capabilities for natural disasters were applicable to manmade catastrophes.[55] This rationale is supported by early work done at the Disaster Research Center (DRC) examining the demands a crisis imposes upon a social system and concluded that different agents may precipitate similar responses.[56] However, accounting for disasters in the same risk formulas for catastrophic attack presents a challenge in skewing the results because they have comparatively higher rates of probability and predictability. The problem is how to incorporate natural disasters into the analysis so they don't distract from the root problem of catastrophic attack. The National Research Council recommends keeping them separate.[57]

Finally, while AVM provides the means for developing coherent strategy, the next logical step is to explore among the alternatives. What investment strategy affords the greatest protection? Should DHS allocate funds towards (1) protective improvement measures based on least cost, (2) assets that are least protected, (3) regional improvements, (4) sector improvements, (5) improvements that provide the greatest protective gain, (6) assets with the highest consequences, or (7) some other strategy? Research has just begun to examine these strategies using AVM, and the preliminary results look interesting.

CONCLUSION

This paper has examined current problems and underlying challenges to developing strategic direction for protecting critical infrastructure. It introduced an Asset Vulnerability Model to overcome these challenges and provide a coordinating framework facilitating strategic direction. Then, informed by insights from game theory, it proposed a policy framework that would extend AVM protection to encompass both critical infrastructure and domestic CBRN stockpiles. In this manner, AVM can account for investment of scarce national resources and lead the nation towards a unified homeland security strategy.

ABOUT THE AUTHOR

Richard White *has a PhD in Security Engineering from the University of Colorado at Colorado Springs. He has taught various courses in homeland security since 2003, and directed homeland security exercises for United States Northern Command. He has a Bachelor's Degree in History and Master's Degree in Computer Science. He has published textbooks on military strategy, homeland security, and homeland defense. Richard may be contacted at rwhite2@uccs.edu.*

NOTES

1. The White House, *Homeland Security Presidential Directive/HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection* (Washington, DC: Government Printing Office, 2003), 8.

2. Dick K. Nanto, *9/11 Terrorism: Global Economic Costs* (Washington, DC: Congressional Research Service, 2004), 2.

3. The White House, *HSPD-7,* 5.

4. Homeland Security Act of 2002, Pub. L. No. 107-296, 107th Cong. (2002).

5. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2013), 15-20.

6. National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, DC: The National Academies Press, 2010), 11.

7. John Moteff, *Critical Infrastructure: The National Asset Database* (Washington, DC: Congressional Research Service, 2007), 1-7.

8. Government Accountability Office, *Critical Infrastructure Protection: DHS could Better Manage Security Surveys and Vulnerability Assessments* (Washington, DC: United States Government Accountability Office, 2012), Summary.

9. Ibid., 14.

10. Todd Masse, Siobhan O'Neil, and John Rollins, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress* (Washington, DC: Congressional Research Service, 2007), 2-7.

11. John Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (Washington, DC: Congressional Research Service, 2011), 29.

12. Masse, O'Neil, and Rollins, *Assessment Methodology,* 14.

13. National Research Council of the National Academies, *Approach to Risk Analysis,* 2-3.

14. Department of Homeland Security, *Budget-in-Brief* (Washington, DC: Department of Homeland Security, 2014), 160-163.

15. The White House, *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (PPD 21) (Washington, DC: Government Printing Office, 2013).

16. National Research Council of the National Academies, *Approach to Risk Analysis*, 11.

17. Masse, O'Neil, and Rollins, *Assessment Methodology,* 16.

18. National Research Council of the National Academies, *Approach to Risk Analysis*, 58-70.

19. Masse, O'Neil, and Rollins, *Assessment Methodology*, 16.

20. Ted G. Lewis, Rudolph P. Darken, Thomas Mackin, and Donald Dudenhoeffer, "Model-based Risk Analysis for Critical Infrastructures," in Francesco Flammini, *Critical Infrastructure Security: Assessment, Prevention, Detection, Response* (Ashurst, Southampton, UK: WIT Press, 2012), 4.

21. Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: John Wiley & Sons, Inc., 2006).

22. William L. McGill, "Critical Asset and Portfolio Risk Analysis for Homeland Security" (PhD diss., University of Maryland, 2008), 15.

23. Barry Charles Ezell, Stven P. Bennett, Detlof von Winterfeldt, John Sokolowski, and Andrew J. Collins, "Probabilistic Risk Analysis and Terrorism Risk," *Risk Analysis* 30, no. 4 (2010): 575-589.

24. McGill, "Critical Asset and Portfolio Risk Analysis," 16.

25. Masse, O'Neil, and Rollins, *Assessment Methodology*, 16.

26. National Research Council of the National Academies, *Approach to Risk Analysis*, 45, 47.

27. Ibid., 51.

28. Ibid., 64-65.

29. Ibid., 62.

30. Michael K. Lindell, Carla S. Prater, Ronald W. Perry, and William C. Nicholson, *Fundamentals of Emergency Management* (Washington, DC: FEMA, 2006), 23-26.

31. National Research Council of the National Academies, *Approach to Risk Analysis*, 51.

32. Ibid., 68-70.

33. P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research* (Idaho National Laboratory, 2006).

34. Georgios Giannopoulos, Roberto Filippini, and Muriel Schimmer. *Risk Assessment Methodologies for Critical Infrastructure Protection Part I: A State of the Art* (European Commission Joint Research Centre, Institute for the Protection and Security of the Citizen, 2012).

35. McGill, "Critical Asset and Portfolio Risk Analysis," 15.

36. Giannopoulos, Filippini, and Schimmer, *Risk Assessment Methodologies,* 3.

37. The White House, *HSPD-7.*

38. Masse, O'Neil, and Rollins, *Assessment Methodology*, 17-18.

39. Ezell, et al., "Probabilistic Risk Analysis," 586.

40. Gordon Woo, "The Evolution of Terrorism Risk Modeling" *Journal of Reinsurance* (April 22, 2003), 7, https://support.rms.com/Publications/EvolutionTerRiskMod_Woo_JournalRe.pdf.

41. Todd Sandler and Harvey Lapan, "The Calculus of Dissent: An Analysis of Terrorists' Choice of Targets," *Syntese* no. 76 (Kluwer Academic Publishers, 1988), 249-254, http://link.springer.com/article/10.1007/BF00869591#page-1.

42. Government Accountability Office, *Critical Infrastructure Protection,* 9.

43. Giannopoulos, Filippini, and Schimmer, *Risk Assessment Methodologies,* 11.

44. Ted G. Lewis and Rudy Darken. "Potholes and Detours in the Road to Critical Infrastructure Protection Policy," *Homeland Security Affairs* 1, no. 2 (August 2005): 7, http://www.hsaj.org/?article=1.2.1.

45. Alan G. Whittaker, Shannon A. Brown, Frederick C. Smith, and Elizabeth McKune, *The National Security Policy Process: The National Security Council and Interagency System* (Washington, D.C.: Industrial College of the Armed Forces, National Defense University, 2011) 5.

46. Catherine Dale, *National Security Strategy: Legislative Mandates, Execution to Date, and Considerations for Congress* (Washington, DC: Congressional Research Service, 2008), 2.

47. The White House, *National Security Strategy* (Washington, DC: Government Printing Office, 2010), 15.

48. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: US Government Printing Office, 2004), 339-340.

49. Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: Department of Homeland Security, 2002), 2.

50. Moteff, *The National Asset Database,* 9.

51. Food and Drug Administration, *Vulnerability Assessments of Food Systems: Final Summary Report* (Washington, DC: Food and Drug Administration, 2012).

52. Clive Williams, "Prospects for Macroterrorism," working paper presented at Pugwash Workshop on East Asian Security, Beijing, China, March 7-9, 2002, 9.

53. National Research Council of the National Academies, *Approach to Risk Analysis*, 12.

54. Ibid., 48.

55. Office of Homeland Security, *National Strategy,* 41.

56. Lindell, et al., *Fundamentals of Emergency Management,* 24-25.

57. National Research Council of the National Academies, *Approach to Risk Analysis*, 9.