Guiding Resource Allocations Based on Terrorism Risk

Henry H. Willis
hwillis@rand.org

Follow this and additional works at: http://research.create.usc.edu/published_papers

Recommended Citation
http://research.create.usc.edu/published_papers/28

This Article is brought to you for free and open access by CREATE Research Archive. It has been accepted for inclusion in Published Articles & Papers by an authorized administrator of CREATE Research Archive. For more information, please contact gribben@usc.edu.
Guiding Resource Allocations Based on Terrorism Risk

Henry H. Willis*

Establishing tolerable levels of risk is one of the most contentious and important risk management decisions. With every regulatory or funding decision for a risk management program, society decides whether or not risk is tolerable. The Urban Area Security Initiative (UASI) is a Department of Homeland Security (DHS) grant program designed to enhance security and overall preparedness to prevent, respond to, and recover from acts of terrorism by providing financial assistance for planning, equipment, training, and exercise needs of large urban areas. After briefly reviewing definitions of terrorism risk and rationales for risk-based resource allocation, this article compares estimates of terrorism risk in urban areas that received UASI funding in 2004 to other federal risk management decisions. This comparison suggests that UASI allocations are generally consistent with other federal risk management decisions. However, terrorism risk in several cities that received funding is below levels that are often tolerated in other risk management contexts. There are several reasons why the conclusions about terrorism risk being de minimis in specific cities should be challenged. Some of these surround the means used to estimate terrorism risk for this study. Others involve the comparison that is made to other risk management decisions. However, many of the observations reported are valid even if reported terrorism risk estimates are several orders of magnitude too low. Discussion of resource allocation should be extended to address risk tolerance and include explicit comparisons, like those presented here, to other risk management decisions.

KEY WORDS: Homeland security; resource allocation; risk tolerance; terrorism

1. INTRODUCTION

The Urban Area Security Initiative (UASI) is a Department of Homeland Security (DHS) grant program designed to enhance security and overall preparedness to prevent, respond to, and recover from acts of terrorism by providing financial assistance to address planning, equipment, training, and exercise needs of large urban areas (DHS, 2004). In fiscal year 2004, UASI provided $675 million to 50 urban areas perceived to be at highest risk from terrorist attacks. These funds were allocated using a formula that accounted for several indicators of the terrorism risk to which each urban area might be exposed. Though precise details of the formula are not publicly available, allocation was reportedly based upon a formula that accounts for credible threat, presence of critical infrastructure, vulnerability, population, population density, law enforcement investigative and enforcement activity, and the existence of formal mutual aid agreements (DHS, 2004; U.S. Congress, 2004). As risk management at DHS continues to evolve, urban areas included in this program and approaches to resource allocation have as well. In fiscal year 2006, the UASI grant program adopted a regional risk and needs-based approach for allocating $765 million and reduced the number of urban areas eligible for new funding to 35, allowing 11 other urban areas that received funding in 2005 to apply for sustained funding for 2006 (DHS, 2006a).

Despite these efforts to allocate homeland security resources based on the relative risks to which each urban area is exposed, the Department of Homeland

* RAND Corporation, 201 North Craig Street, Suite 102, Pittsburgh, PA 15213, USA; hwillis@rand.org.
Security has frequently been criticized for inadequately calculating risk, and therefore for failing to distribute resources in proportion to urban areas’ shares of total terrorism risk (U.S. Congress, 2004). Criticism of resource allocation policies at DHS raises at least three questions:

1. Should resources be allocated based on risk, risk reduction, or some other basis?
2. How can terrorism risk be estimated?
3. What are tolerable levels of terrorism risk?

After briefly reviewing definitions of terrorism risk, rationales for risk-based resource allocation, and literature on risk tolerance (Section 2), this article presents estimates of terrorism risk for urban areas that received UASI funding in 2004 (Section 3) and demonstrates an approach for inferring levels of risk tolerance by comparing them to other federal risk management decisions (Section 4). This comparison suggests that UASI allocations are generally consistent with other federal risk management decisions. However, terrorism risk in several cities that received funding is below levels that are often tolerated in other risk management contexts. Conclusions drawn from this work are presented in Section 5 along with implications these findings have for homeland security policy.

2. ESTIMATING AND MANAGING TERRORISM RISK

The use of terrorism risk assessment to inform homeland security resource allocation has been limited until recently. Common definitions are not used, so stakeholders in allocation debates are often referring to different concepts of risk. Even if a precise definition were widely used, methods for estimating and monitoring changes in the level and nature of terrorism risks are still nascent. Instead, various indicators of risk, which are presumed to correspond in some way with true terrorism risk, have been used (for instance, in the original UASI formula), or proposed (e.g., Canada, 2003).

Willis et al. (2005) defined terrorism risk as a function of threat, vulnerability, and consequences. These definitions, which are reviewed below, are similar to others proposed in risk literature (Ayyub, 2005; Haimes, 2004; von Winterfeldt & Rosoff, 2005) and to language more recently used by Secretary Michael Chertoff (DHS, 2005) and included in the National Infrastructure Protection Plan (DHS, 2006b).

2.1. Threat

A person or organization represents a terrorist threat when they have the intent and capability to impose damage to a target. Threat only exists when intent and capability are manifested together in a person or organization. When the scope of threat is defined in terms of a specific set of targets, a specific set of attack types, and a specific time period, probability can be used as a measure of the likelihood that an attack will occur. Thus, a measure of threat is defined as:

\[
\text{Measure (Threat)}: \text{The probability that a specific target is attacked in a specific way during a specified time period, or}
\]

\[
\text{Threat} = p(\text{attack occurs}).
\]

Since this measure for threat is uncertain, one should keep in mind that it can also be represented by a probability distribution, not a point estimate.

2.2. Vulnerability

A precise definition of vulnerability captures information about the infrastructure. Paraphrasing Haimes, vulnerability is the manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can result in damage if attacked by an adversary (Haimes, 2004, p. 699). Referring again to the domain of engineering risk analysis, where threat can be thought of as being a load or force acting on a system, vulnerability can be considered the capacity of a system to respond to terrorist threats (Pate-Cornell, 2005). To use this definition for measurement, a specific threat and type of consequence must be identified. Probability can be used as a measure of the likelihood that vulnerability will lead to damage when attacks occur.

\[
\text{Measure (Vulnerability)}: \text{The probability that damages (where damages may involve fatalities, injuries, property damage, or other consequences) occur, given a specific attack type, at a specific time, on a given target, or}
\]

\[
\text{Vulnerability} = p(\text{attack results in damage|attack occurs}).
\]

\footnote{Most of this italicized phrase is verbatim from this source, but the definition has been changed slightly so as not to imply that an attacker needs to knowingly exploit a vulnerability—that is, a target can be vulnerable without the vulnerability being recognized by an attacker.}
2.3. Consequences

“Consequence” is the magnitude and type of damage resulting from successful terrorist attacks. To define a measure of consequence, specificity is again required. In this case, specificity necessarily involves treatment of two important considerations: how consequences are measured and how uncertainty is addressed. Consequences can be expressed in terms of fatalities, injuries, economic losses, or other types of damage. Formally,

**Measure (Consequence):** The expected magnitude of damage (e.g., deaths, injuries, or property damage), given a specific attack type, at a specific time, that results in damage to a specific target or,

\[
\text{Consequence} = E[\text{damage} | \text{attack occurs and results in damage}].
\]

Haimes (2004) notes that risk assessment of rare and extreme events requires special consideration of worst-case outcomes, and that the expected value often misrepresents true risk. Conversely, estimates of the worst-case outcomes, captured in the tail of the distribution of consequences, will be very dependent upon assumptions when considering events like terrorism where there is large uncertainty about events and limited historical information. For this reason, and to simplify, continued discussion of consequences will consider the expected value of the distribution of damage.

2.4. Risk as a Function of Threat, Vulnerability, and Consequences

Terrorism risk represents the expected consequences of attacks taking into account the likelihood that attacks occur (i.e., threat) and that they are successful if attempted (i.e., vulnerability). In probabilistic terms, risk from an attack of a certain type is the unconditional expected value of damages of a certain type. For a specific threat, target, and type of consequence, risk can be measured as:

**Measure (Terrorism Risk):** The expected consequence of an existent threat, which for a given target, attack mode, target vulnerability, and damage type, can be expressed as

\[
\text{Risk} = p(\text{attack occurs}) \times p(\text{attack results in damage | attack occurs}) \times E[\text{damage | attack occurs and results in damage}]
\]

\[
= \text{Threat} \times \text{Vulnerability} \times \text{Consequence}.
\]

**Fig. 1.** Risk is the intersection of threat, vulnerability, and consequences.

Conceptually, risk can be considered as the intersection of events where threat, vulnerability, and consequences all are present. As shown in Fig. 1, this can be represented as a Venn diagram where each of the circles represent the probability sets where threat, vulnerability, or consequences are present and risk is the black area where all three intersect.

There are two advantages of using this formulation of terrorism risk. First, it provides an approach for comparing and aggregating terrorism risk. With this definition, it is possible to compare risks of a specific type across diverse targets such as airports and electrical substations. For example, the injury risk from an explosives attack could be expressed for each as the expected annual injuries resulting from such attacks against each target and then the two could be compared.

Second, this definition of risk provides a clear mapping between risk and approaches to managing or reducing risk. Intelligence and active defense involving “taking the fight to the enemy” represent an approach to risk management that focuses specifically on threats. Managing risk through vulnerability requires increasing surveillance and detection, hardening targets, or other capabilities that might reduce the success of attempted attacks. Finally, managing risk through consequences can be done through increasing preparedness and response that reduces the effects of damage through mitigation or compensation.

2.5. Risk Assessment Versus Resource Allocation

Ultimately, efficient allocation of homeland security resources would distribute resources where
they can most reduce risks, not where risks are the greatest. But this requires being able to calculate the effectiveness of different types and amounts of investment. Currently, neither the methods nor the data are available to answer questions about the effectiveness of available risk reduction alternatives or determine reasonable minimum standards for community preparedness.

Until these questions are answered, allocating homeland security resources based on risk is the next best approach since areas at higher risk are likely to have more and larger opportunities for risk reduction than areas at lower risk. That is, resources would be allocated roughly proportionally to the distribution of risk across areas receiving funding.

Aside from allocating resources, there are several other reasons why it is still important for decision-makers to understand the levels and distribution of terrorism risk. First, because assessing risk and risk reduction is a critical first step in assessing cost effectiveness of counterterrorism efforts, methods developed to support terrorism risk assessment will also support analysis of resource allocation. Further, even when large risks are not mitigated by current efforts, identifying them could help direct intelligence gathering, research, and future counterterrorism efforts. Finally, following changes in the levels and patterns of terrorism risk over time provides insights into the effectiveness of current homeland security risk management efforts and the emergence of new risks.

2.6. Risk Tolerance and Risk Management

Establishing tolerable levels of risk is one of the most contentious and important risk management decisions. Risks may be tolerated simply because they are small compared to benefits obtained through the risky activity. Alternatively, they may be tolerated because the available countermeasures could lead to equal or greater risks themselves (Wildavsky, 1979). Acceptable risk is defined by individuals’ and society’s risk tolerance for specific hazards.

Variation of risk tolerance by hazard is well recognized. Starr (1969) demonstrated that individuals accept up to three orders of magnitude greater risk for voluntary activities than involuntary activities because of the perceived benefits associated with the voluntary activities. Slovic et al. (1979) further revealed how factors such as immediacy, control, and knowledge also affect perception of risk and acceptability.

Clearly, answering the question of “How safe is safe enough?” depends on many social, political, and ethical factors in addition to risk magnitude. Fischhoff et al. (1981) frame acceptable-risk problems as decisions that require choices among risk management options that have different desirability. Fischhoff et al. (1981) further identify three approaches that can be used to analyze acceptable-risk problems: formal analysis (like risk and cost-benefit assessment), bootstrapping (i.e., iterative learning contributing to an agreed upon risk level), and professional judgment elicited from technical experts, decisionmakers, and/or citizen stakeholders. Often, analysis of risk tolerance relies several of these approaches at once.

The foundation of bootstrapping methods is that government provides a mechanism for the collective decisions to balance consequences of competing risk management options and determine tolerable levels of risk (Derby & Keeney, 1981). With every regulatory or funding decision for a risk management program, society decides whether or not risk is tolerable. If risks are deemed too large, regulations are established and resources allocated. If risks are tolerated, activities remain unregulated and resources are directed elsewhere.

Even so, government decisions vary widely about which risks will be reduced and how much will be spent to do so. Viscusi (1995) and Tengs et al. (1995) demonstrated the value of life that can be inferred from government risk management decisions is very inconsistent. From one decision to the next, the value of life may differ by several orders of magnitude.

Comparing terrorism risk to other risks that our society decides to manage or not could provide benchmarks for what terrorism risks should be tolerated and why. For example, Travis et al. (1987) used this approach to establish levels of acceptable risk for cancer risk management. By reviewing 132 federal regulatory decisions, Travis et al. determined that tolerated risk varied by levels of population risk (cancers/year) and maximum individual risk (marginal increase in lifetime probability of cancer). Along these two factors, Travis et al. found that some risks were low enough on both factors to never be regulated, i.e., de minimis risk, and some risks were high enough to always be regulated, i.e., de manifestis risk.

In Travis’s analysis, when regulations were finalized the federal government decision was to manage risk. When regulations were not adopted, the federal government decision was not to manage risk. In the context of homeland security, the decision of whether or not to provide resources to urban areas is a comparable decision of whether or not to manage risk.
Until risk tolerance is established for terrorism, it will be difficult for homeland security policy to justify not providing resources to reduce specific terrorism risks. Travis et al.’s (1987) analysis provides a framework for also considering which terrorism risks are de minimis.

3. TERRORISM RISK ESTIMATES

Since September 11, 2001, the insurance industry has begun using risk modeling to better understand the magnitude and distribution of terrorism risk in the United States. Risk Management Solutions, Inc. (RMS) developed the Probabilistic Terrorism Model to assess the risks of macroterrorism for this purpose. Like other models developed for this purpose, the RMS model reflects risk as a function of threat, vulnerability, and consequences and calculates the expected annual consequences (human and economic) from diverse terrorist threats. Since the model is designed to calculate insured losses, human consequences are accrued as losses from life and worker compensation lines of insurance. When using the model for assessing public policy, the underlying estimates of injuries and fatalities can either be disaggregated and used alongside property damage estimates or combined together with property damage estimates if the relative weights of fatalities, injuries, and property damage are appropriately elicited.

The methodology relies on models of specific threat scenarios and calculations of economic and human life consequences of each scenario. The RMS model calculates the threat of different types of attacks at different targets using expert judgment about target selection by terrorists, capabilities for different attack modes, overall likelihood of attack, and propensity to stage multiple coordinated attacks. More information on the RMS model is provided in Willis et al. (2005) and from the RMS website (http://www.rms.com).

Willis et al. (2005) used the RMS Terrorism Risk Model to calculate the expected annual fatalities for each of the urban areas that received funding through the UASI grant program. This was done by summing the expected annual fatalities for each of the attack-mode target pairs modeled for an urban area.

The definitions of urban areas were provided in the Fiscal Year 2004 Urban Areas Security Initiative Grant Program: Program Guidelines and Application Kit (DHS, 2004). Though 50 urban areas were allocated UASI funding, several of these were analyzed as larger urban areas because of how the RMS model is configured. Specifically, Los Angeles, Long Beach, Santa Ana, Anaheim, Minneapolis, and St. Paul received separate allocations but were modeled as the three regions of Los Angeles–Long Beach, Orange County, and Minneapolis–St. Paul, respectively. As a result, the analysis to follow covers 47 urban areas instead of 50. These risk estimates were converted to risk-shares by calculating each urban area’s proportion of the total expected annual fatalities calculated for all urban areas.

3.1. Comparing Allocations and Risk Estimates

Fig. 2 compares the Willis et al. (2005) estimates of urban area risk-shares to two commonly used indicators: population and density-weighted population. Density-weighted population is simply the product of a region’s population and population density. Data for population and population density were taken from the 2000 decennial census (http://www.census.gov). For comparison, the shares of DHS FY2004 UASI allocations are also included in this figure, along with a vertical line representing equal shares across all funded urban areas. All data are plotted as each urban area’s share or proportion for each of these metrics.

---

2 Founded at Stanford University in 1988, RMS is a provider of products and services to the insurance and reinsurance industries for the quantification and management of catastrophe risks. RMS is also one of the founding sponsors of the RAND Center for Terrorism Risk Management Policy, which supported this study.

RMS defines macroterrorism as attacks capable of causing (1) economic losses in excess of $1 billion, or (2) more than 100 fatalities and/or 500 injuries, or (3) massively symbolic damage.

3 Two other firms, Equecat and AIR Worldwide, have independently developed terrorism risk models.

4 As with any model, the estimates from the RMS model are dependent upon the model’s underlying assumptions. For example, because the RMS model was designed to be used by the insurance industry it assesses only the direct damage of attacks and not consequences that result from interdependencies among economic systems and infrastructures. More generally, the model provides a structure for specifying beliefs about factors that determine levels of risk. In this article, I use these terrorism risk estimates as a point of departure for considering risk tolerance with respect to terrorism, realizing that conclusions drawn should be subject to analysis using other models of terrorism risk.

5 As an example of calculating density-weighted population, based on the 2000 decennial census, the population of the Pittsburgh Metropolitan Statistical Area is approximately 2.4 million and the population density is approximately 510 people/mile². Thus, the density-weighted population for this urban area is 2.4 million × 510, or approximately 1.2 billion people²/mile².
Shares of total population across the UASI-funded urban areas are presented in Fig. 2 as filled triangles. The size of city shares of risk using this measure ranges from a high of 0.078 of total risk (Los Angeles–Long Beach, CA) to a low of 0.004 (New Haven–Meriden, CT), with 14 metropolitan areas having shares greater than the equal-share line.

Density-weighted population shares (filled diamonds in Fig. 2) run from a high of 0.378 (New York) to 0.0003 (Las Vegas), thus resulting in a much larger spread of estimated shares of total risk than derived by the population estimator. Moreover, using density-weighted population, just eight cities are found to have more than the equal-share allocation of terrorism risk.

The Willis et al. (2006) estimates of city risk-shares are displayed in Fig. 2 as open squares. Immediately apparent is that risk is very concentrated and most of these estimates of city risk-shares are several orders of magnitude lower than the population or density-weighted population estimates. Six cities (New York, Chicago, Washington, San Francisco, Los Angeles, and Boston) hold more than 90% of the total terrorism risk-shares for these estimates. The risk-shares range from a low of $4.16 \times 10^{-7}$ (Baton Rouge) to 0.627 (New York), with just six cities having shares greater than the equal share. Interestingly, these risk estimates suggest that 23 (Minneapolis through Baton Rouge in Fig. 2) of the urban areas account for less than 0.005% of the total calculated risk. If, for instance, the $795$ million FY04 UASI funds had been distributed in proportion to these risk estimates, these cities would have received less than $3.4$ million in total or on average only $147,000$ each.

Finally, Fig. 2 shows how the FY2004 UASI allocations (open circles) compare with risk estimates. Shares of UASI funding closely track urban area’s shares of population. On average, city population shares differ from grant allocation shares by just 0.006, with the maximum discrepancy of 0.020 occurring for Jersey City.

If one believes the underlying assumptions of the RMS Terrorism Risk Model, then the distribution of resources does not match the distribution of terrorism risk. In particular, high-risk urban areas appear to be underemphasized in the resource allocations. This might be acceptable for many reasons. The
cost effectiveness of available risk reduction opportunities may be better in lower risk cities. Urban areas may not be able to effectively use more money than they were allocated in a given year. Finally, the UASI grants are just one grant program and DHS uses other grants and other risk management approaches to reduce terrorism risk. Assessing the adequacy of funding for high-risk cities requires consideration of all resources and risk management efforts implemented.

4. COMPARING TERRORISM RISK TO OTHER RISK MANAGEMENT DECISIONS

As previously mentioned, Travis et al. (1987) reviewed 132 regulatory decisions for cancer risk management. Each case provided an estimate of individual risk (measured as the marginal increased lifetime risk of death) and population risk based on the exposure (measured as expected fatalities per year). Each case also provided a record of whether a decision was made to regulate the exposure or not. One novel finding of this analysis was that risks can be divided in terms of individual and population risk into sensible categories that are meaningful benchmarks for risk management decisions.

This observation yields three revealed regions of federal risk management decisions. Travis found that risks that affect many people (i.e., high population risks) or certain people severely (i.e., high individual risks) are always regulated. Risks that affect few people and present only modest individual risk are never regulated. Travis used these categories to establish de manifestis and de minimis levels of risk. Between these regions was an area where risks were sometimes managed, but not always. In this region, cost effectiveness explained federal risk management decisions. The three risk management regions that Travis identified are presented and labeled in Fig. 3.

Fig. 3 also plots the Willis et al. (2005) estimates of terrorism fatality risk for urban areas that received UASI funding in FY2004 into the Travis et al. (1987) regions of de manifestis and de minimis risk. The Willis et al. (2005) estimates provide the expected annual fatalities in each urban area, or the population risk for each area. Individual risk estimates were derived from these estimates by assuming an average lifetime of 70 years and an exposed population equal to the population within the urban areas. Using these assumptions, individual risk was calculated as,

$$\text{Individual Risk} = \frac{\text{Population Risk} \times \text{Average Lifetime}}{\text{Population Exposed}}.$$  

For example, the RMS estimate for expected annual fatalities in New York is 304. On the log scale in Fig. 3, this is plotted at the point 2.48. Assuming an exposed population of 9.3 million and an average lifetime of 70 years, the expected annual fatalities estimate corresponds to an estimated individual lifetime risk of 0.0029, or −2.64 when plotted on a log scale.

Fig. 3 supports three observations. First, only one urban area (New York) falls squarely within the de manifestis risk region. Second, estimates of terrorism risk for many cities appear to fall in the area of de minimis risk. Allocating resources for counterterrorism and preparedness in these cities may be directed toward risks that would otherwise be tolerated. Third, many of the classifications of city risk as de minimis appear to be valid even with several orders of magnitude of error in the risk estimates. For example, in the case of Memphis, this conclusion holds with errors over three orders of magnitude. Thus, these conclusions are fully defensible even with significant errors in risk estimates or unique characteristics of terrorism risk (discussed below) that may affect risk management decisions.

The derivations required to plot terrorism risk in Fig. 3 incorporate several assumptions. First, individuals are assumed to spend their entire lives in a single urban area. In reality, people move quite often, so this assumption provides for a maximum exposure for a lifetime in each urban area. Second, population is assumed constant over an individual’s lifetime. Population growth rates are such that this assumption is a reasonable first-order approximation. Third, population density is assumed uniform across the urban area and this may or may not be the case. Finally, important dependencies that may exist between individual risk and population risk as a result of terrorist motivations and goals are not captured in this simple derivation. While these last two assumptions may not correspond to reality, they are reasonable considering the robustness of the conclusions to several orders of magnitude of error in risk estimates.

It is also interesting to observe how DHS decisions to drop certain urban areas from the UASI grants program after 2005 correspond with these
Fig. 3. Willis et al. (2005) estimates of terrorism risk in FY04 UASI-funded urban areas compared to Travis et al. (1987) areas of de manifestis and de minimis risk. Urban areas that are designated to receive only sustained UASI funding in fiscal year 2006 are indicated with a “◊” and labeled using underlined italics. Urban areas that received funding in fiscal year 2004, but not fiscal year 2005, are indicated using italics. Honolulu, Jacksonville, Omaha, and Toledo received UASI funding in 2005, but not in 2004, thus were not in the Willis et al. (2005) data set and are not plotted.

regions, particularly the region of de minimis risk. Nine of the 12 urban areas that received funding in FY2004 but will not receive funding in FY2006 fall within the de minimis risk region.6 This includes five of the eight urban areas plotted in Fig. 3 that have been identified by DHS as only being eligible for sustained funding in FY2006, and no funding thereafter.7 Thus, while the funding provided by DHS is not fully consistent with the Travis’s region of de minimis risk, recent decisions to drop urban areas from the UASI program are more consistent with this framework.

4.1. Why Terrorism Risk Management Is Different

There are several reasons why the conclusions about specific cities’ terrorism risk being de minimis should be challenged. Some of these surround the means used to estimate terrorism risk for this study. Others involve the comparison that is made to cancer risk management.

The risk estimates used are derived from a single model. By using a single model, this analysis is subject to all of the limitations and assumptions of the

---

6 Albany, Baton Rouge, Buffalo, Fresno, Louisville, New Haven, Phoenix, Richmond, Sacramento.
7 Baton Rouge, Buffalo, Louisville, Phoenix, Sacramento.
model. For example, as discussed in descriptions of the RMS Terrorism Risk Model (Willis et al., 2005; RMS, 2004), the RMS analysis may not capture the interdependencies between attack modes or targets. This could lead to an underestimation of risk. Similarly, the RMS model incorporates expert elicitation of the potential frequency of attacks and likelihood of attacks occurring in different cities, by different attack modes, and against different target types. Using different models or different parameterizations of the RMS model would yield different results. The Willis et al. (2005) estimates did consider several perspectives on terrorism threat. Fatality risk estimates did not vary by several orders of magnitude, as would be required to change the conclusions drawn in this study. A sensible step for further research would be to incorporate analysis with different models to see whether and how the conclusions drawn would change.

This analysis is based on expected annual consequences. Haimes (2004) highlights how expected value decision making is misleading for rare and extreme events. Risk management based on expected annual consequences may be irrelevant considering the potential consequences of a nuclear detonation in an otherwise low-risk urban area. However, risks such as this might be better dealt with using countermeasures other than those funded through the UASI grant program, such as counterproliferation. While it is important to consider uncertainty in these estimates and how they may differ, particularly for the extreme tails on risk estimates, conclusions drawn in this study are robust for several orders of magnitude of error in stated risk estimates.

Preparedness efforts funded through the UASI grant program may be dual use. While this analysis has only attempted to estimate terrorism risk, preparedness resources may also reduce risk from common hazards (e.g., fires) or natural disasters (e.g., floods, hurricanes, or earthquakes). The regions of de manifistis and de minimis risk defined by Travis et al. (1987) reveal levels at which risk regulation should or should not be used. Plotting terrorism risk estimates in these same regions allows consideration of whether or not resources should be used to reduce the risks based on levels of expected fatalities to the exposed populations. Including other hazards in the urban area risk estimates would effectively raise the individual and population risks plotted in Fig. 3. However, once again, the conclusions drawn in this article are robust to several orders of magnitude error in terrorism risk estimates.

Finally, cancer risk management is different from terrorism risk in several ways. First, cancer risk is typically only discussed in terms of fatalities or quality of life. In contrast, terrorism risk has many other dimensions, including economic losses, psychological impacts, and national security impacts, to name a few. Second, terrorism risk differs from cancer risk in important ways that would affect risk perceptions. Some cancer risks may be perceived as being voluntary, controllable, killing one person at a time, and familiar. Terrorism risks, however, may be perceived as involuntary, uncontrollable, catastrophic, and new. Cancer risks may be associated with activities that afford benefits to the exposed individuals. Terrorism risks are probably less associated with beneficial activity. All of these factors may increase the concern over terrorism risks compared to cancer risks of equivalent magnitude in terms of expected fatalities. Extending the Travis et al. (1987) analysis to consider risk management of technological risks, natural hazard risks, and other activities and hazards managed by the federal government would provide a better basis for comparisons discussed here.

5. CONCLUSIONS

This article has demonstrated how comparison of terrorism risks to other risk management decisions could provide benchmarks for which risks to manage or not. While the conclusions are subject to the limitations discussed above, they are robust to uncertainty in terrorism risk estimates and the demonstrated analysis is readily extensible. As federal management of homeland security resources continues to evolve, this analysis supports three conclusions.

First, as this article demonstrates, quantitative risk modeling can contribute to policy discussions of terrorism risk management. Since any model is limited by its inherent structure and assumptions, more complete analysis can be done by integrating results from multiple models.

Second, the modeling used in this article only addresses direct consequences in terms of fatalities. Modeling could be readily extended to direct economic losses. Incorporating indirect effects and other types of consequences would require either improving the models discussed here or linking these results to those from other models. Extending the analysis of risk tolerance to consequences other than human or economic will be difficult, however, until regulatory
impact assessments include more explicit and consistent treatment of other types of consequences.

Finally, discussion of resource allocation should be extended to address risk tolerance and include explicit comparisons, like those presented here, to other risk management decisions.

ACKNOWLEDGMENTS

I would like to thank several colleagues for providing critical review and inspiring debate during various stages of this work. These include Paul Davis, Bruce Don, Paul Dreyer, Baruch Fischhoff, Yacov Haimes, Scott Hickey, Terrence Kelly, Tom LaTourrette, Granger Morgan, Jamison Medby, Andrew Morral, and Jack Riley. While this work has benefited tremendously from these interactions, the work represents the views of the author alone, and does not represent those of any other person or institution.

REFERENCES


