WORKING
PAPER

Guiding Resource Allocations Based on Terrorism Risk

HENRY H. WILLIS

WR-371-CTRMP

March 2006

CENTER FOR TERRORISM RISK
MANAGEMENT POLICY

Abstract

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 rationales for risk-based resource allocation and challenges in estimating terrorism risk, this paper 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 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.

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 2006).

Despite these efforts to allocate homeland security resources based on the relative risks to which each urban area is exposed, the Department of Homeland 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 rationales for risk-based resource allocation and challenges in estimating terrorism risk, this paper compares estimates of terrorism risk for urban areas that received UASI funding in 2004 to other federal risk management decisions. This comparison suggests that terrorism risk in several cities is below levels that are often tolerated in other risk management contexts.

Risk Assessment Versus Resource Allocation

Ultimately, efficient allocation of homeland security resources should be based upon assessment of the cost-effectiveness of alternative risk reduction opportunities. But, this requires being able to calculate the effectiveness of different types and amounts of investment. As a hypothetical example, even if terrorism risks were greater in New York City than in Des Moines, Iowa, allocating resources according to proportion of risk may not be optimal if available countermeasures are more cost effective in Des Moines. For example, terrorists could respond strategically to countermeasures in New York City and target less protected areas, or the marginal effectiveness of resources spent in New York City may decrease with continuing investment.[1] 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.

There are several other reasons why it is still important for decisionmakers 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 counter terrorism 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.

Estimating Terrorism Risk

Terrorism risk assessment for informing resource allocation has suffered from several problems. For instance, currently, there is no shared and precise definition of terrorism risk, so stakeholders in allocation debates are often referring to different concepts of risk. Even if a precise definition were widely used, there are no standard methods for estimating and monitoring changes in the level and nature of terrorism risks. Instead, various indicators of risk have been used (for instance in the UASI formula), or proposed (e.g., Canada, 2003), which are presumed to correspond in some way with true terrorism risk.

Moreover, terrorism risk changes over time as terrorist motives, capabilities, and targeting change and adapt to risk mitigation efforts. These facts defy the efficacy of any simplistic model that attempts to enumerate a single index as a measure of risk. Measuring terrorism risk must always reflect uncertainties in estimates of the relative risks faced by different cities.

Willis et al. (2005) defined terrorism risk as a function of threat, vulnerability and consequences. As discussed in Section 2, these definitions are similar to others proposed in risk literature and to language more recently used by Secretary Michael Chertoff (DHS 2005). Willis et al (2005) also demonstrated how this framework could be used to develop a single measure of risk that accounts for uncertainties in risk measurement. They then proposed and demonstrated a framework for evaluating terrorism risk estimates to understand resulting errors given uncertainties in their measurement.

Risk Tolerance and Risk Management

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. If risks are deemed too large,

---

[1] For discussions of how terrorist strategy affects resource allocation decisionmaking see Woo 2002a, Woo 2002b, and Lakdawalla and

regulations are established and resources allocated. If risks are tolerated, activities remain unregulated and resources are often directed elsewhere.

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. Government provides a mechanism for the collective decisions to balance these factors and determine tolerable levels of risk (Derby and Keeney 1981). 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.

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' 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 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*.

Overview of Report

The remainder of this report is organized as follows. Section 2 reviews Willis et al's (2005) definitions of terrorism risk and the factors that comprise it. Section 3 provides an estimate of terrorism risk building on methods of Willis et al. 2005 and compares these estimates to UASI allocations and other proxies for terrorism risk. In Section 4, lifetime and maximum exposed individual estimates are derived from the Willis et al. estimates and use Travis et al.'s risk management framework to compare terrorism risks to carcinogenic risks managed by the federal government to identify potentially *de minimis* and *de manifestis* terrorism risks. Finally, since terrorism risks are clearly different than carcinogenic risks, factors that might affect the conclusions from Section 4 are discussed along with implications these findings have for homeland security policy.

2. Terrorism Risk and Its Components

Differing notions of terrorism risk frequently fuel disagreements about the relative risks to which different regions or cities are exposed. Some arguments implicitly link risk to terrorism threats. If, for example, one city were known through gathered intelligence or past history to be the preferred target for terrorists, this view would support a claim that this city has a high level of terrorism risk. Alternatively, others argue that risk is more closely associated with infrastructure vulnerabilities within a region because these represent logical targets for terrorism. Thus, for example, even if we do not know of a threat to a nuclear power plant, reason and prudence argue that we should include that facility in considering a region's risk. Finally, discussions of risk occasionally emphasize the possible consequences of terrorist attacks in evaluating risk. Thus, if two cities have similar chemical storage facilities, but one has the facility located close to its

population center, a persuasive argument can be made that the first city's chemical facility presents a greater risk than the second's.

Clearly, strong arguments can be made that threats, vulnerabilities, and consequences play a significant part in the overall risk to which a city is exposed. Willis et al (2005) proposed definitions for threat, vulnerability, consequences, and risks and the measures that can be used to assess and track each. These definitions are reviewed below in context of other proposed definitions.

Threat

A person or organization represents a terrorist threat when they have the intent and capability to impose damage to a target. Note that neither intentions without capabilities nor capabilities without intentions pose a threat. Threat only exists when both are manifested together in a person or organization. Allocating homeland security resources to protect critical infrastructure or cities requires measuring the threats posed to specific targets or from specific types of attack. 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:

> **Measure (Threat):** *The probability that a specific target is attacked in a specific way during a specified time period, or*
>
> $$Threat = P(attack\ occurs)$$

This measure of terrorist threat emphasizes a specific type of attack on specific targets. Radiological attack represents a different threat to a specific target than nuclear attack. Attacks on stadiums represent different threats than attacks on skyscrapers. A complete description of the threats to which a target is exposed would require consideration of every mode of attack separately. In practice, however, it may suffice to focus on a limited number of attack types that are representative of chemical, biological, radiological, nuclear (CBRN) and explosive attack modes. Similarly, it may suffice to focus on a limited number of target types or groups of targets in a region.

This measure of threat is specified in terms of attack types and targets. The intelligence community more customarily considers threat in terms of groups of attackers given its interest in identifying and stopping those who might pose a threat. An attack-type perspective is more useful for the task of resource allocation because the decision context is most concerned with what targets are threatened as compared with by whom and why.

Finally, 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. These definitions are consistent with methods and terminology proposed though applications of engineering risk analysis to terrorism risk assessment (Ayyub 2005, Pate-Cornell 2005, von Winterfeldt and Rosoff 2005).

Vulnerability

Clearly, not all threats of the same type are equally important. Furthermore, the threat of terrorism is dynamic in that it adapts to current conditions that affect the likelihood of attack success. For example, even if a typical hotel and fortified military base have equal probability of being subjected to a car bomb attack, the attack would be more likely to achieve the aim of causing significant damage at the less secure hotel. Therefore, a precise definition of vulnerability that captures information about the infrastructure is also needed.

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).[2] 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 must be identified. Probability can be used as a measure of the likelihood that vulnerability will lead to damage when attacks occur.

---

[2] Yacov Y. Haimes, *Risk Modeling, Assessment, and Management,* Second Edition, John Wiley, 2004, p. 699. 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.

Measure (Vulnerability): *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*

$$\text{Vulnerability} = P(\text{attack results in damage} \mid \text{attack occurs})$$

In other words, a target's vulnerability can be articulated as the probability that an attack of a given type will be successful once it has been launched and, as articulated, measures vulnerability to specific types of damages only (i.e., there would be separate vulnerability assessments for deaths, injuries, and property damage).

Note that for the measure specified above, magnitude of the damage is not part of the definition of vulnerability. This measure assumes a simplified representation of vulnerability in which there is either a successful attack with damage or no success and therefore no damage. As a result, "success" is defined in terms of whether or not damage, having a distribution of magnitude, is inflicted by the attack. Consequence measurement is discussed below. A more general model (used in many military analyses) is that there are a range of damage levels, each associated with its own probability. This is simply a more discrete representation of damage and defense mechanisms.

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. 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,*

$$\text{Consequence} = E[\text{damage} \mid \text{attack occurs and results in damage}]$$

Consequences can be expressed in terms of fatalities, injuries, economic losses, or other types of damage. Other aspects of consequences can also be considered using the approach outlined here

and this definition. For example, the damage or destruction of critical infrastructures that could cause injury, loss of life, and economic damage outside the area of immediate attack are important. They may in fact dominate the results of an analysis if the impact on society as a whole is considered rather than solely the impact on the target and its occupants and owners.[3]

Consequences are determined by many uncertain factors, such as wind speed or relative humidity (which could be important factors in a chemical or biological attack, for example). These uncertainties can be addressed by considering a full distribution for potential consequences or specific points along this distribution. Haimes (2004) notes that risk assessment of rare and extreme events requires special consideration 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.

Risk as a Function of Threat, Vulnerability, and Consequences

Risk is the anticipated consequences over a period of time to a defined set of targets, resulting from a defined set of threats, and considering the vulnerabilities of the specific targets. 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
>
> *Risk* = P(attack occurs)
>
> * P(attack results in damage| attack occurs)
>
> * *E[damage | attack occurs and results in damage]*
>
> = Threat * Vulnerability * Consequence

---

[3] See Rinaldi, Peerenboom and Kelly for a comprehensive discussion of these topics.

In other words, 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. Conceptually, risk can be considered of the intersection of events where threat, vulnerability and consequences all are present. As shown in Figure 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.

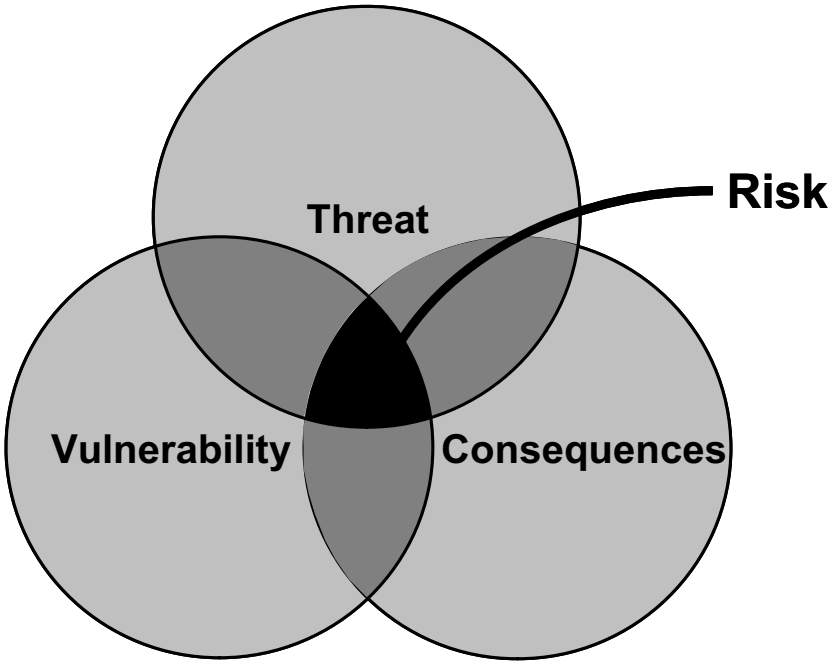

Figure 1 Risk is the intersection of threat, vulnerability, and consequences.

There are two advantages to 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. Estimating overall terrorism risk requires further analysis that considers all threat types and targets. If risks were independent, expected damages of a specific type could be

aggregated by summing across threat types and target types[4]. However, dependencies likely exist between risks. For instance, a successful nuclear attack in a city could dramatically change the expected risks for targets in the damage footprint of the explosion.

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.

3. Terrorism Risk Estimates

Willis et al. (2005) used a terrorism risk model developed by Risk Management Solutions, Inc. (RMS) as the basis for estimates of expected annual fatalities from terrorist attacks (i.e., terrorism risk). 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.

The RMS Terrorism Risk Model was developed as a tool for the insurance and reinsurance industries to assess risks of macroterrorism[5]. To reflect risk as a function of threat, vulnerability, and consequences, the RMS model calculates the expected annual consequences (human and economic) from diverse terrorist threats. 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

---

[4] Damage of different types (i.e., casualties versus economic damages) should be treated using approaches of multiobjective decision making, not simple aggregation.

[5] 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.

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). Two other firms, Equecat and AIR Worldwide, have independently developed similar terrorism risk models to support the insurance and reinsurance industries.

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.

Comparing Allocations and Risk Estimates

Figure 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[6]. 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.

---

[6] 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/mile^2. Thus, the density-weighted population for this urban area is 2.4 million X 510, or approximately 1.2 billion people^2/mile^2.

Shares of total population across the UASI-funded urban areas are presented in Figure 2 as filled circles. 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 Figure 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. (2005) estimates of city risk-shares are displayed in Figure 2 as filled 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 0.000000416, (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 Figure 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 thousand each.

Finally, Figure 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. As stated previously, this might be acceptable because of other issues, including the cost effectiveness of available risk reduction opportunities.

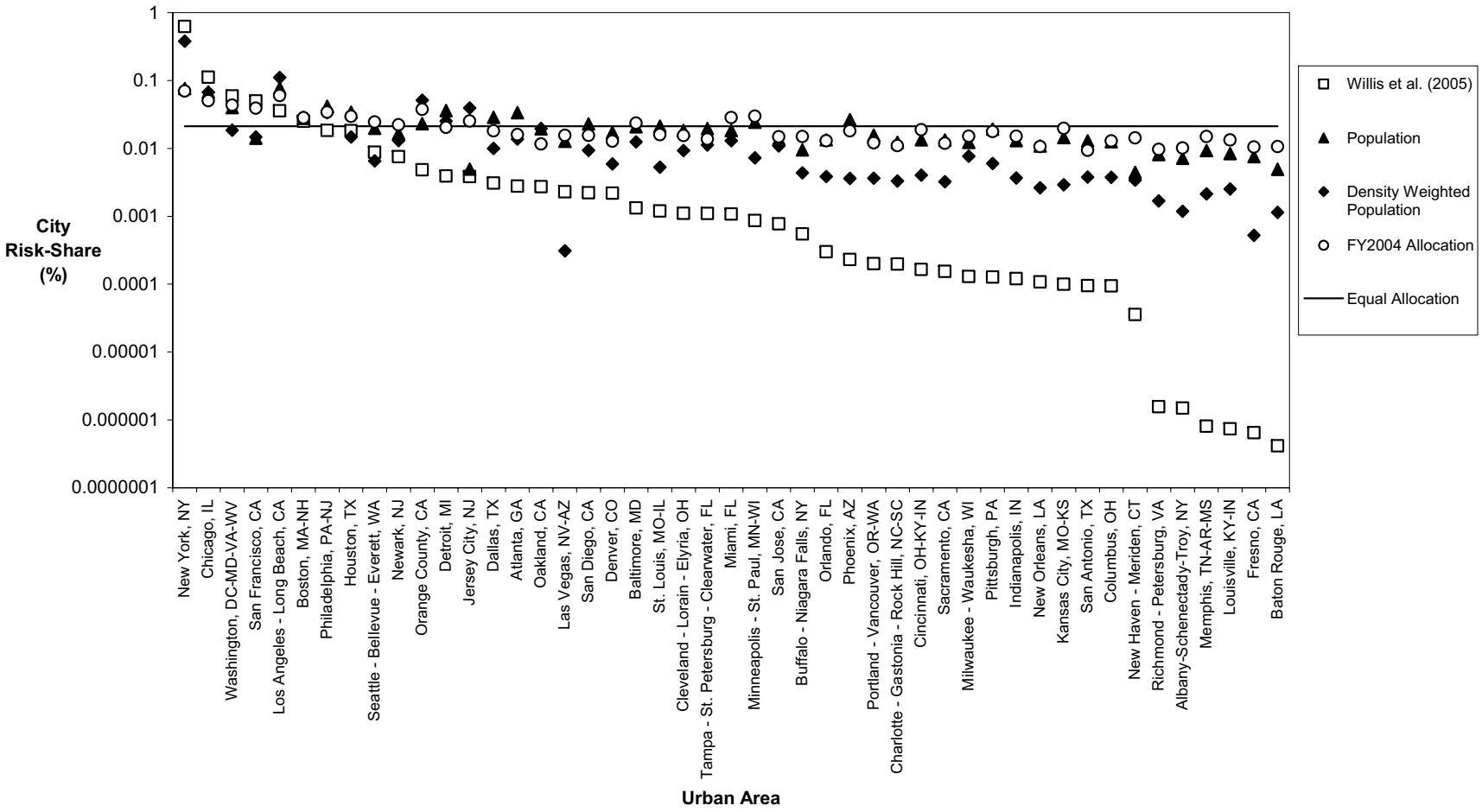

Figure 2 City shares of estimated total risk based on urban area population, density-weighted population, FY2004 UASI allocations, and expected annual fatalities, calculated by the RMS Terrorism Risk Model published in Willis et al (2005), with a horizontal line indicating equal risk across cities

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. The 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.

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.

Figure 3 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 Figure 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.

Figure 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 towards 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 my affect risk management decisions.

The derivations required to plot terrorism risk in Figure 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 and 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, as mentioned previously.

It is also interesting to observe how DHS decisions to drop certain urban areas from the UASI grants program after 2005 correspond with these regions, particularly the region of de minimis risk. Nine of the twelve urban areas that received funding in FY2004 but will not receive funding in FY2006 fall within the de minimis risk region[7]. This includes five of the eight urban areas plotted in Figure 3 that have been identified by DHS as only being eligible for sustained funding in FY2006, and no funding thereafter[8]. Thus, while the funding provided by DHS is not fully consistent with the Travis' region of de minimis risk, recent decisions to drop urban areas from the UASI program are more consistent with this framework.

---

[7] Albany, Baton Rouge, Buffalo, Fresno, Louisville, New Haven, Phoenix, Richmond, Sacramento

[8] Baton Rouge, Buffalo, Louisville, Phoenix, Sacramento

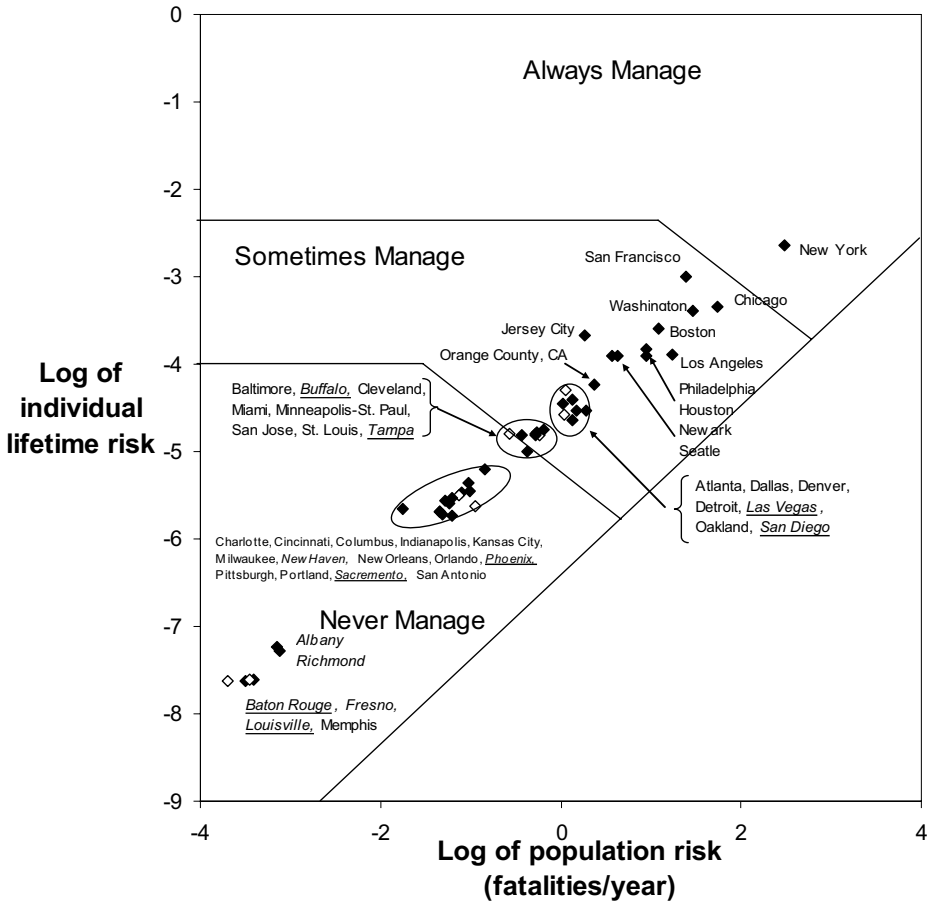

Figure 3 Willis et al. (2005) estimates of terrorism risk in FY04 UASI-funded urban areas compared to Travis et al. (1987) areas of *de manifestis* and *de minimis* risk. Urban areas that are designated to receive only sustained UASI funding in fiscal year 2006 are indicated with a "◊" and labeled using *underlined italics*. Urban areas that received funding in fiscal year 2004, but not fiscal year 2005, are indicated using *italics*. Honolulu, Jacksonville, Omaha, Toledo received UASI funding in 2005, but not in 2004, thus were not in the Willis et al. (2005) dataset and are not plotted.

5. 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 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 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 decisionmaking 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 counter proliferation. 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 manifestis and deminimis risk defined by Travis et al. (1987)

reveal levels of risk which 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 Figure 3. However, once again the conclusions drawn in this paper 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.

6. Conclusions

This paper 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 extendable. As federal management of homeland security resources continues to evolve, this analysis supports three conclusions.

First, terrorism risks that receive risk management resources would benefit from using quantitative risk modeling. As discussed above, any model is limited by its inherent structure and assumptions, so better analysis can be done by integrating results from multiple models.

Interpretation of this analysis also demonstrates the importance of transparency to quantitative analysis. Efforts to use quantitative modeling should include plans to subject tools and results to independent review.

Second, the modeling used in this report only addresses direct consequences in terms of fatalities and economic losses. Risk modeling should be extended to incorporate indirect effects and other types of consequences. This can be done either by improving the models discussed here or linking these results to those from other models.

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, Jamieson 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

B. A. Ayyub (2005). *Risk Analysis for Critical Infrastructure and Key and Key Asset Protection.* Symposium on Terrorism Risk Analysis, University of Southern California, January 13-14, 2005. Available at: http://www.usc.edu/dept/create/events/2004_11_18/Risk_Analysis_for_Critical_Infrastructure_and_Key_Asset_Protection.pdf.

B. Canada (2003). *State Homeland Security Grant Program: Hypothetical Distribution Patterns of a Risk-Based Formula*. October 8, 2003, Government and Finance Division, Congressional Research Service, Library of Congress, Washington, DC.

Derby, S. L., R. L. Keeney (1981). Risk Analysis: Understanding "How Safe is Safe Enough?," *Risk Analysis*, Vol 1, No 3, 217 – 224.

DHS (2004). *Fiscal Year 2004 Urban Areas Security Initiative Grant Program: Program Guidelines and Application Kit*. U.S. Department of Homeland Security, Washington, DC.

DHS (2005). *Remarks for Secretary Michael Chertoff U.S. Department of Homeland Security George Washington University Homeland Security Policy Institute.* George Washington University, Homeland Security Policy Institute, Washington, D.C., March 16, 2005. Available online at http://www.dhs.gov/dhspublic/display?theme=42&content=4392 as of March 12, 2006.

DHS (2006). *DHS Introduces Risk-based Formula for Urban Areas Security Initiative Grants*. U.S. Department of Homeland Security, Washington, DC. Available online at http://www.dhs.gov/dhspublic/display?content=5317 as of March 2, 2006.

Y. Y. Haimes (2004). *Risk Modeling, Assessment, and Management*. 2nd Edition, John Wiley & Sons, Inc., Hoboken, New Jersey.

Lakdawalla, D., G. Zanjani (2004). *Insurance, Self-Protection, and the Economics of Terrorism*. Manuscript, Rand Corporation, Santa Monica, CA.

M. E. Pate-Cornell (2005). *Risks of Terrorist Attack.* Symposium on Terrorism Risk Analysis, University of Southern California, January 13-14, 2005. Available at: http://www.usc.edu/dept/create/events/2005_02_01/Risks_of_Terrorist_Attacks_Probabilistic_Assessment_and_use_of_Intelligence_Information.pdf.

Rinaldi, S. M., J. P. Peerenboom and T. K. Kelly (2001). Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, *IEEE Control Systems Magazine*, December 2001, pp. 11 – 25.

RMS (2004). *Managing Terrorism Risk in 2004*. Risk Management Solutions, Newark, CA. Available at http://www.rms.com/publications/terrorism_risk_modeling.pdf.

C. Starr (1969). Social Benefit versus Technological Risk. *Science*. Vol. 165, pp. 1232 – 1238.

Slovic, P., B Fischhoff, S. Lichtenstein (1979). Rating the Risks, *Environment*, Vol. 21, No. 3, pp 14 – 20, 36 – 39.

Tengs, T. O., M. E. Adams, J. S. Pliskin, D. G. Safran, J. E. Siegel, M. C. Weinstein, J. D. Graham (1995). Five Hundred Life-Saving Interventions and Their Cost Effectiveness. *Risk Analysis*. Vol 15, No. 3, 369 – 390.

Travis, C. C., E. Crouch, R. Wilson, E Klema (1987). Cancer risk management: A review of 132 federal regulatory decisions. *Environmental Science and Technology*, Vol 21, No. 5, 415 – 420.

U.S. Congress (2004). *Homeland Security: The Balance Between Crisis and Consequence Management Through Training and Assistance*. Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives, 108th Congress, November 20, 2003.

von Winterfeldt, D., H. Rosoff (2005) *Using Project Risk Analysis to Counter Terrorism*. Symposium on Terrorism Risk Analysis, University of Southern California, January 13-14, 2005. Available at: http://www.usc.edu/dept/create/events/2005_01_31/Using_Project_Risk_Analysis_to_Counter_Terrorism.pdf.

A. Wildavsky (1979). No Risk is the Highest Risk of All. *American Scientist*. Vol 67, January – F ebruary, 32 – 37.

Willis, H. H., A. R. Morral, T. K. Kelly, J. Medby (2005) *Estimating Terrorism Risk*. MG-388-RC, RAND Corporation, Santa Monica, CA.

K. Viscusi (1995). *Fatal Tradeoffs: Public and Private Responsibilities for Risk*. Oxford University Press, New York, NY.

G. Woo (2002a). *Quantifying Insurance Terrorism Risk*. Manuscript, Risk Management Solutions, Newark, CA.

G. Woo (2002b). *Understanding Terrorism Risk*. Manuscript, Risk Management Solutions, Newark, CA.