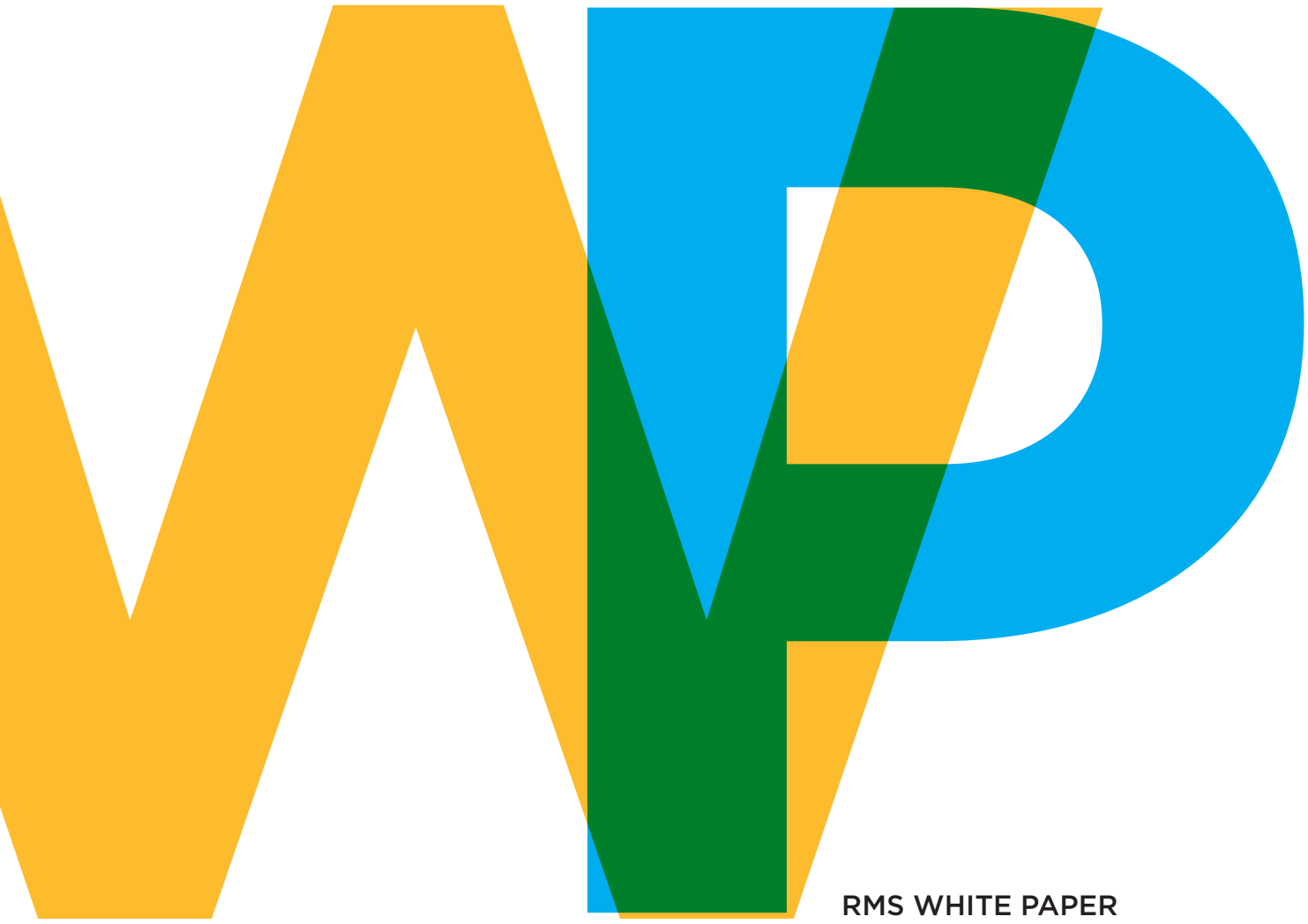

RMS WHITE PAPER

QUANTIFYING U.S. TERRORISM RISK

Using terrorism risk modeling to assess the costs and benefits of a TRIA renewal

RMS™

EXECUTIVE SUMMARY

The threat of a large-scale terrorist attack in the U.S. is still high and will remain so for the foreseeable future. In the decade after 9/11, 30 major plots in the United States led to terrorism court convictions. Demand for terrorism insurance is robust; take-up rate is over 60% nationwide.

The Terrorism Risk and Insurance Act (TRIA), a federal insurance backstop providing $100 billion of coverage in the event of a large-scale terrorist attack, expires at the end of 2014. In order to assess the costs and benefits of a renewal, policymakers must gauge the risk of terrorism quantitatively.

The TRIA renewal dialogue must include an objective quantification of the economic cost of terrorism, its impact on the insurance industry, and the cost of federal involvement in any insurance solution. Given the advances in risk modeling over the past decade and the recently increased transparency into U.S. counter-terrorism operations, such quantification is now possible, with an ever-increasing degree of certainty surrounding the results. Policymakers should make use of these tools to best estimate the costs and benefits of any terrorism legislation.

RMS' industry-leading terrorism model simulates over 90,000 large-scale terrorist attacks across 9,800 global targets using 35 different attack types. The attacks range from 600-pound car bombs to 10-ton truck bombs as well as chemical, biological, nuclear, and radiological attacks. Based on analyses using high-definition industry-wide exposure, the model results point to several key findings:

- The financial impacts of terrorist attacks are comparable with severe winter storms and convective storms including tornado, hail, and wind, at return periods commonly used in the reinsurance industry (100, 250, and 500-year return periods). At longer return periods, they are comparable with hurricanes and earthquakes.
- According to the RMS terrorism model, more than 75% of the nation's expected annual loss from terrorist attacks is concentrated around high profile targets in five urban areas where building value and population density is highest: New York, Chicago, Washington D.C., Los Angeles, and San Francisco.
- Damage from attacks involving chemical, biological, nuclear, and radiological weapons is harder to estimate and far more severe than attacks involving conventional explosives. Several simulated attacks in RMS' event catalog cause insured losses that approach the surplus level of the entire U.S. insurance industry.

The concentration of loss from a terrorist attack makes it extremely difficult to insure. The September 11, 2001 attacks caused insured losses exceeding $40 billion, most of which occurred at the World Trade Center—an area of approximately 16 acres. This can be contrasted to Hurricane Katrina's damage footprint, which spanned large swaths of Mississippi, Louisiana, and Florida. Insurance companies must geographically diversify their risk in order to manage the volatility of their losses; writing terrorism coverage makes this obligation difficult to achieve.

Terrorism risk can be successfully modeled as a control process, whereby terrorists' actions are constrained by counter-terrorism operations. The recent revelations of Edward Snowden have revealed the pervasiveness of these operations. Just as flood insurance covers the breach of flood barriers, terrorism insurance covers the breach of the U.S. countersecurity infrastructure.

INTRODUCTION

It has been eleven years since the Terrorism Risk and Insurance Act (TRIA) was signed into law, following the September 11, 2001 attacks and an insurance industry loss of over $40 billion dollars. The legislation, which addressed the significant disruption in the property insurance market, created a $100 billion federal backstop in exchange for insurance companies offering terrorism coverage with every commercial policy. Since 2002 it has been renewed twice, with each renewal narrowing coverage by raising deductibles, increasing minimum losses, and reducing the pro-rata government share of losses (currently 85% of the $100 billion layer; see Figure 1).

The current TRIA legislation will expire at the end of 2014. In 2013, sponsoring members from both parties have proposed a renewal three times in Congress. But opposition has emerged from groups at both ends of the ideological spectrum. Discussions on modifications to the bill to reduce its cost are well underway.

TRIA (TRIPRA) PROGRAM HIGHLIGHTS	
LEGISLATION	Terrorism Risk Insurance Program Reauthorization Act of 2007
COVERAGE	$100 Billion, covers foreign and domestic acts of terrorism
PARTICIPATION	85% (federal), 15% (insurer)
INSURER DEDUCTIBLE	20% direct earned premiums, prior year
EXPIRATION DATE	December 31, 2014
MINIMUM LOSS FOR CERTIFICATION	$5 Million
MIMINUM LOSS FOR INDEMNIFICATION	$100 Million

Figure 1: TRIA program summary

This paper examines the quantitative dimensions of insurable loss from terrorist attacks in the United States and discusses the process of modeling terrorist risk. The basis for the quantitative analysis presented in the following pages is the RMS® Probabilistic Terrorism Model, developed in 2002 and continually updated to reflect the latest view of terrorism risk. The model covers 35 types of attacks, ranging from conventional explosives to chemical, biological, nuclear, and radiological attacks. It utilizes high-resolution property and human exposure throughout the United States in order to estimate losses from these attacks.

The losses presented in this paper, consistent with how catastrophe risk is managed by insurance carriers, are calculated on the basis of "exceedance probability" for a given time period. For example, a 100-year return period loss of $100 million indicates that there is a 1% annual chance of a loss equal to or exceeding $100 million.

INSURING TERRORISM REMAINS A CHALLENGE

Unlike natural catastrophes, which can cause damages over thousands of square miles, the damage footprint of a terrorist attack can be measured in square yards. Most of the damage incurred by the 9/11 attacks occurred on a building site of only sixteen acres. Compare this to Hurricane Katrina, where damage was so widespread that every county in Mississippi and Louisiana, along with 22 in Alabama and 11 in Florida, were declared federal disaster areas.

The spatially concentrated nature of a terrorist event makes it difficult to insure against. Successful insurance underwriting requires adequate spreading of risk, across industries, lines of coverage, and most importantly, geographies. Since insured value is most highly concentrated in densely populated urban areas—the very places terrorists seek to target—avoiding the excessive concentration of risk is a rigorous task. This underwriting challenge, coupled with the steadily declining rates for terrorism insurance over the past ten years, contribute to insurance companies' reluctance to devote their capital to covering terrorism risk.

In extending $100 billion of protection under TRIA, the federal government required insurance companies to offer terrorism insurance as part of all commercial property policies. This condition, known as the "Make Available Provision," has guaranteed the availability of terrorism coverage to insurance buyers in urban areas over the past eleven years. In the absence of this provision with TRIA's expiration, market capacity for terrorism coverage would be limited. Evan Greenberg, the CEO of ACE Ltd, a prominent property & casualty carrier, recently offered this blunt assessment: "If TRIA does not renew … I wouldn't make [terrorism coverage] available, and nor would any other company that I know of. How much money does my company gain from writing terrorism insurance? It's a rounding error."

Underwriters of terrorism insurance also face challenges with the inherent uncertainty of terrorism events and the loss associated with them. As data for terrorist attack loss is very limited, particularly compared to natural catastrophe data, insurers face difficulties in appropriately pricing their risk and must load factors for this uncertainty into their charged rates. In the RMS probabilistic model, the measure of uncertainty for terrorism risk modeling (known as the coefficient of variation) is almost six times higher than the expected average annual loss itself.

TERRORISM RISK IS COMPARABLE WITH THAT OF NATURAL CATASTROPHES

In order to gauge the financial risk of terrorism, it is useful to look to weather-related and other natural catastrophes as a point of reference. TRIA, like many federal insurance programs, was created to fulfill a demand that the private market could not fully provide. The bill was signed shortly after Fitch downgraded more than $4 billion in commercial mortgage securities due to the inability to procure terrorism insurance.

Based on more than 90,000 simulated terrorist events using the RMS Probabilistic Terrorism Model, the financial impact of terrorist attacks at return periods commonly used in the reinsurance industry (1-in-100, 250, and 500 years) can be comparable with severe winter storms and convective storms (including tornado, hail, and wind). At longer return periods, financial impacts can be comparable with earthquakes and hurricanes (Figure 2)

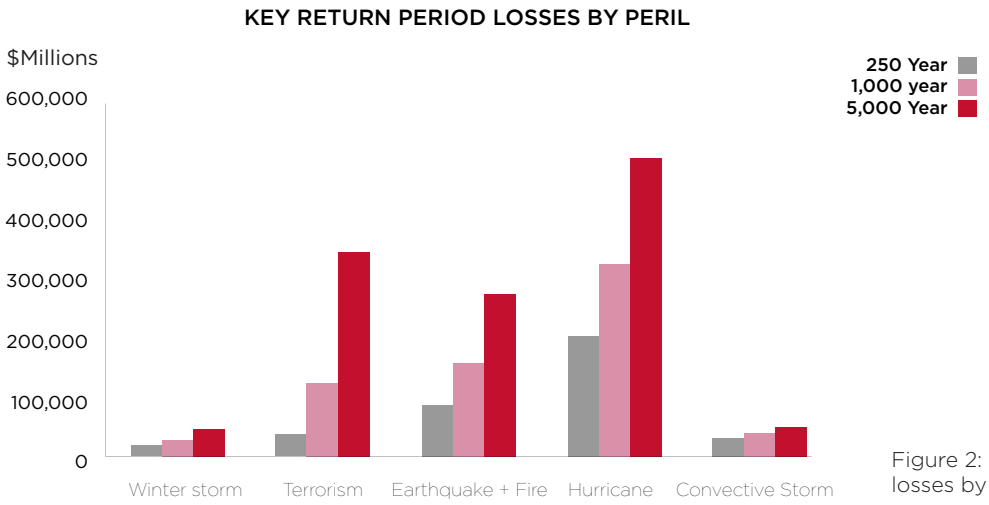

Figure 2: Key catastrophe return period losses by peril

Comparing terrorism with natural catastrophe perils for a given level of risk, however, does not fully illustrate the differences between the two with respect to rare events with extremely high severity—in statistical terms, "tail risk." Many natural catastrophes occur with relatively high frequency, the range of possible damages are better understood, and insurance companies can more accurately underwrite their loss potential. Successful large-scale terrorist attacks, however, are events that may only occur once a generation, or less. The most severe types of attacks, which involve nuclear detonation or the use of biological warfare agents, may cause hundreds of billions of dollars of damage. However, the frequency associated with these events in the modeling of terrorist risk is extremely low.

In comparing the risk of terrorism to that of natural catastrophes, RMS used its industry exposure databases, which estimate population and property exposure at high resolutions. The estimated loss includes damage to buildings and their contents, business interruption (downtime), and workers compensation, whose benefits vary by state. The following additional assumptions are made:

- The loss is from the "ground up," meaning no insurance policy terms are considered
- Workers compensation losses assume that terrorist attacks occur during peak occupancy hours, but earthquakes and other natural catastrophes occur at a random time during the day or night
- Loss amplification, the surge in raw material demand that can result in higher reconstruction costs, is not considered
- Take-up rate for terrorism insurance is not considered in the underlying loss exposure

Finally, the modeled losses are based on "aggregate" exceedance probability, which takes into account the probability of aggregate losses incurred in any year, not just a single event, exceeding a certain loss threshold.

TERRORISTS ARE RATIONAL ACTORS WHOSE TARGETING STRATEGIES ARE GUIDED BY THE PRINCIPLES OF "ATTACK LEVERAGE," AND WHOSE ACTIONS ARE CONSTRAINED BY SOCIAL NETWORKS AND SUPPRESSIVE COUNTER-TERRORISM.

For any insurance risk with catastrophe loss potential, statistical analysis of past claims experience alone cannot adequately model and quantify claims from future events. This is as true for terrorism as it is for earthquakes, hurricanes, and floods. Beyond a statistical analysis of past events, structured catastrophe risk modeling of future events is required. For natural hazards, structure is provided by the laws of nature, as embodied in the sciences of seismology, meteorology, and hydrology. For terrorism, structure is provided by the established principles of asymmetric warfare and the laws of social networks.

As stressed by Dr. George Habash, the founder of the Popular Front for the Liberation of Palestine, "terrorism is a thinking man's game." In asymmetric warfare against powerful nation states with proficient counter-terrorism forces, terrorists can only hope to coerce government policy through being smart and cunning about their acts of political violence. Accordingly, terrorists of concern to the U.S. homeland adopt the modus operandi of following the path of least resistance. This optimal principle, expounded by the master of military strategy, Sun Tzu, also underpins the universal laws of nature governing natural hazards. Much as tornadoes and hurricanes follow the path of least resistance by moving in the direction of low pressure, terrorists follow the path of least resistance by selecting weapons that are most accessible, cost-effective, and deadly.

This guiding principle helps explain terrorists' weapon selection preference, with improvised explosive devices being especially popular. The development of advanced technology weapons is beset with problems of reliability, particularly since most terrorists lack safe havens for weapons laboratories. Terrorists aspire to achieve substantial attack leverage—a high ratio of loss to input force—to maximize operational efficiency. Meticulous attention is thus given to the placement of vehicle bombs to cause the maximal structural damage. But even small bombs may have devastating consequences if detonated on a plane or in crowded city centers.

Many audacious terrorist plots may be imagined, but the actual scale of any real terrorist plot is fundamentally restricted by the laws of social networks. Every person has a family, friends, or acquaintances. This is true for terrorists as much as for anyone else. A terrorist plot can be compromised through information leakage. Mass surveillance of communication links, and the intrusion of intelligence moles, all serve to elevate the likelihood of plot interdiction with plot size. The RMS terrorism model measures plot interdiction likelihood as a function of the number of operatives involved. This method is corroborated by Osama bin Laden's injunction, issued from his Abottabad hideout, that plots against the U.S. homeland should not involve more than 10 operatives. The slim chance that large, spectacular terrorist plots will not be foiled substantially diminishes the prospect of catastrophic insurance losses. Lone wolf attacks are the most likely to evade interdiction. After this, plots involving two terrorists may have a reasonable chance of succeeding, especially, as in Boston, when the operatives are brothers, with just one family as a potential leakage source.

In striving to maximize loss impact subject to counter-terrorism security constraints, terrorists predominantly choose iconic targets with name recognition in populous urban centers. As a result, the threat level declines precipitously outside New York, Washington D.C., and a handful of other major American cities. The concentration of force at key target points is a strategic military principle, implying that terrorism risk is not geographically diversifiable across America. Hurricane insurance is required all along the East Coast, in suburban and rural areas as well as in cities. But unlike hurricanes, terrorists intentionally focus on striking cities, particularly centers of financial and political power. The lack of geographical diversification inherently limits the insurance market capacity for covering terrorism risk in the central business districts of Manhattan and other main metropolitan areas with high population and insured value (Figure 3).

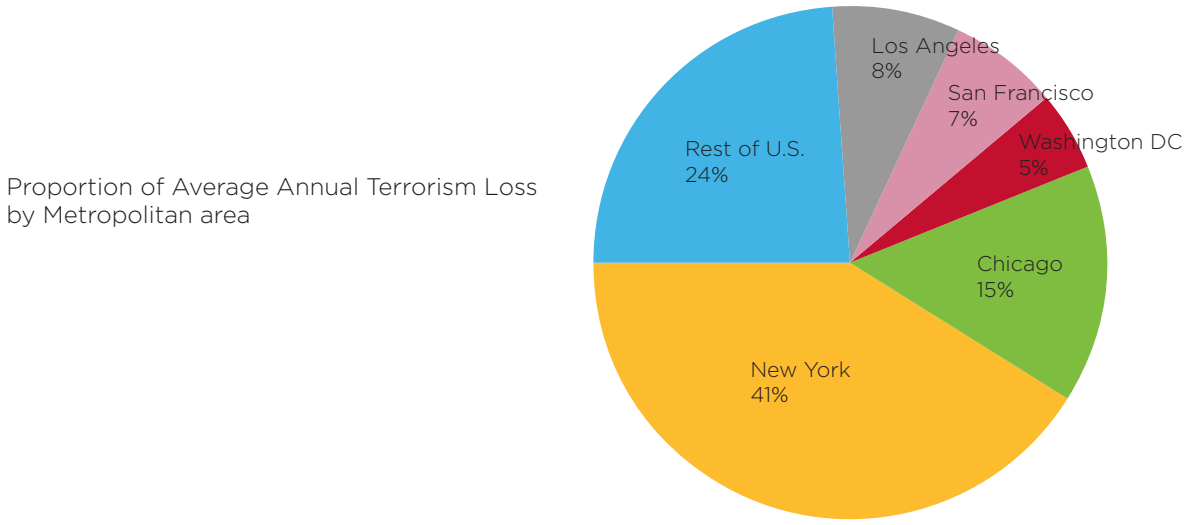

Figure 3: Proportion of average annual terrorism loss by U.S. metropolitan area

Even though the probability of a terrorist attack drops sharply as attack severity increases, insurers are well aware that the infliction of massive loss on the U.S. homeland is an abiding objective of Islamist militants. The possibility of a devastating attack using weapons of mass destruction still remains; this scenario could plausibly produce an insurance loss higher than what the Property and Casualty insurance industry could commercially sustain. Massive losses can also be caused by natural hazards, but no catastrophic terrorism loss could occur without a gross failure of counter-terrorism, for which the U.S. government would bear responsibility.

Given the proficiency of counter-terrorism action, including widespread surveillance, the annual frequency of any kind of significant terrorism loss is low. RMS evaluates this frequency objectively using data on terrorism court convictions as an open source baseline for enumerating plots, and keeping count of the occasional plots evading interdiction. A counterfactual analysis of plots in the decade after 9/11, accounting for the dependence of interdiction rate on operative count and the chance of technical failure, shows that the counterfactual frequency, after allowing for near misses, aligns closely with the RMS modeled frequency. Contrary to popular perception, the annual frequency of terrorist attacks against the U.S. homeland is quite narrowly bounded, being tightly constrained by intelligence and law enforcement vigilance. While it is impossible to stop successive natural catastrophes from striking the U.S. in one year (as occurred in 2004 when four hurricanes hit Florida), successive terrorist strikes in the U.S. at different times would be countered with an extremely vigorous counter-terrorism response.

Since 2002, RMS has reiterated to insurers that, in contrast with the randomness that characterizes natural hazard occurrence, terrorism is a "control process" that constrains the volatility in loss outcome. An important aspect of this control process is the suppressive security and law enforcement response to any terrorist success. This has been clearly demonstrated in the countries of the western alliance since 9/11. For example, after the London bombings of July 7, 2005, Prime Minister Blair instigated new draconian counter-terrorism legislation that has effectively curbed the spread of radicalization. The increasing evidence base for terrorism threat model parameters, such as post-strike risk mitigation, has greatly reduced terrorism risk modeling ambiguity.

In the years since 9/11, the western alliance has shown that terrorism is controlled through effective, professional and well-resourced counter-terrorism action. Only a handful of major terrorist plots in western alliance countries have not been interdicted in the past decade. Before the Boston Marathon attack on April 15, only three major plotters were not foiled in the United States: the aircraft shoe bomber, Richard Reid, in December 2001; the aircraft underpants bomber, Umar Farouk Abdulmutallab, in December 2009; and the Times Square vehicle bomber, Faisal Shahzad, in May 2010. In the U.K., non-interdicted plots include the London transport bombings of July 7, 2005 and July 21, 2005, and an attempted vehicle bombing of a nightclub in the London theater district in June 2007.

THE RISK OF TERRORISM CAN BE SUCCESSFULLY MODELED AS A MAN-MADE CATASTROPHE. CARRIERS WRITING TERRORISM COVER ARE INSURING AGAINST THE FAILURE OF A GOVERNMENT'S COUNTER-TERRORISM OPERATIONS.

Terrorism loss only occurs when a terrorist plot evades interdiction. Terrorism insurance in the countries of the western alliance is thus essentially insurance against the failure of counter-terrorism. The frequency of such failures is low because of concerted suppressive western government counter-terrorism measures, which are stepped up even further after any successful act of terrorism.

This does not hold true for other countries where counter-terrorism forces are weak and corrupt, such as Pakistan. In countries with ineffective counter-terrorism forces, terrorists can attack more or less at will, without constraint. In the midst of this lawlessness, terrorism insurance risk cannot be modeled, except for a few specific properties with guaranteed high levels of site security, often involving military protection.

The following section addresses some commonly held views about U.S. terrorism risk modeling, which tend to presume a lack of Western counter-terrorism capability to control terrorist action against the U.S. homeland. This presumption may be attributable to a dearth of public information about counter-terrorism activities. Counter-terrorism officials are duty-bound to "serve in silence." The whistle-blowing revelations of Edward Snowden have broken this code of silence, and by so doing have alerted the general public to the widespread and intensive surveillance undertaken to protect them from terrorist attack. Widespread public concern over this surveillance has provoked the NSA to publicly declare the importance of such surveillance in terrorist plot interdiction.

[1] It is impossible to model human behavior.

RMS models terrorism as a control process by which terrorist operations are countered by security and intelligence services. This involves modeling terrorist activity at a strategic, but not tactical, level. At a strategic level, terrorists seek to maximize loss subject to security constraints. This strategy is well validated by experience since 9/11. It is also a conservative premise, given that a sub-optimal strategy would result in smaller loss outcomes.

Dealing with terrorist operations at a tactical level is a task for government officials, not risk modeling agencies. RMS does not predict the time or location of any type of catastrophe, natural or man-made, and does not track individual terrorist movements. The essence of a control process is that counter-terrorism forces are responsible for tracking tactical behavioral changes made by terrorists. Since 9/11, such tracking has been undertaken very capably.

[2] Terrorism risk cannot be modeled without access to classified information.

RMS has access to the intelligence community, and indeed, since 9/11, has sponsored a number of major closed high-level international terrorism and intelligence conferences in both London and Washington, D.C. However, RMS does not have access to classified information. Such access is essential for predicting and preventing terrorist attacks. But this is not a risk analyst's job. This is the responsibility of state and federal law enforcement agencies. For terrorism, as with natural hazards, a catastrophe insurance risk analyst's task is to assess the likelihood of an event occurring, not to predict (nor prevent) an attack.

[3] Expenditure on counter-terrorism resources may decrease in the future.

A key aspect of Western counter-terrorism control is the adaptive flexible response to changes in the threat level. When evidence of an elevated terrorist threat appears, resources are made available to counter the threat. Security is the top priority for every government in the western alliance. This was reiterated by Secretary of State John Kerry after the Nairobi mall attack of September 21, 2013.

[4] Terrorism risk cannot be modeled and therefore priced with anything close to the same degree of precision as traditional natural disaster risk.

Through vigorous counter-terrorism response, the annual volatility in terrorism losses involving conventional weapons is actually lower than for natural hazards. In contrast to natural catastrophes, for which probability of multiple severe events occurring in a single year is highly uncertain, the possibility of a wave of successful terrorist attacks against the U.S. homeland in a single year is extremely remote because of the prompt and vigorous counter-terrorism response that would inevitably follow any single successful attack. This has been manifest all across the Western alliance since 9/11.

THE SEVERITY OF TERRORIST ATTACKS INVOLVING CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR AGENTS MAKES THEM UNINSURABLE BY PRIVATE MEANS ALONE.

Terrorism insurance contracts typically include coverage for conventional bomb attacks. However, "CBRN" attacks—those involving chemical, biological, radiological, and nuclear devices—are almost always excluded. This is due to the high uncertainty and extreme severity of these types of attacks, many of which would render insolvent any insurer faced with paying for them. A comparison of the modeled risk between conventional and CBRN attacks (Figure 4) helps illustrate the basis for the CBRN exclusion in most terrorism policies.

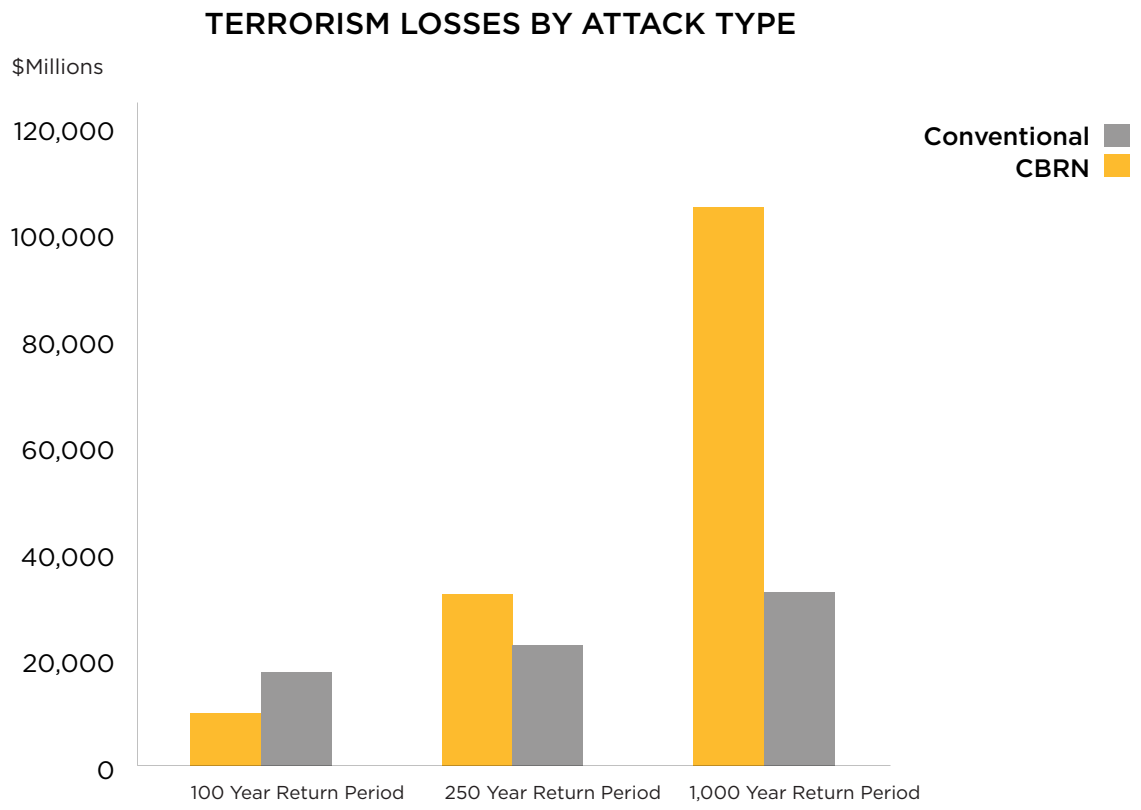

Figure 4: Terrorism losses by attack type

RMS utilizes a number of attack scenarios in calculating CBRN risk. For attacks involving the dispersal of a chemical or biological agent, the model simulates the aerosolization of contaminant in various quantities, in both indoor and outdoor locations, with different prevailing wind conditions. For nuclear attacks, both small tactical use devices (1 kiloton) and large battlefield or theatre weapons (5 kilotons) are simulated. The extreme damage caused by CBRN events is driven by several factors: first, casualty rates tend to be high, due to the toxicity of the attack agent. Second, windy conditions can significantly increase the size of an attack footprint by carrying a toxic contaminant downwind. Third, effective decontamination is time consuming, difficult, and expensive. Finally, the psychological fear of CBRN contamination can elevate the response to an attack: longer business downtimes, larger radii of restricted access, and more stringent decontamination guidelines. RMS' modeled view of a radiological device attack ("dirty bomb") assumes relatively few fatalities. However, business downtime due to evacuation and decontamination to rigorous EPA guidelines result in very costly attack scenarios.

Though relatively rare, CBRN attacks, both attempted and successful, are not unprecedented. In the United States, a series of Anthrax-laden letters were mailed in 2001; Jose Padilla, a U.S. citizen turned jihadist, was detained in the Chicago in 2002 while plotting a dirty bomb attack in the United States. In 2006, Georgian security forces arrested a man trafficking bomb grade uranium; and in 2011 a group of suspects was arrested in Moldova after trying to sell enriched uranium. Most recently, the repeated use of Sarin agents in attacks against Syrian civilians has drawn international condemnation.

Critics of TRIA are quick to make three points: first, that TRIA's federal guarantee has been provided—and insurer money collected—for over 10 years without incident. Second, that U.S. insurance industry surplus has grown to approximately $600 billion as of this writing, more than double the surplus level at time of the September 11, 2001 attacks. Finally, from these two points they contend that the insurance industry is sufficiently capitalized to absorb the losses from a catastrophic terrorist incident without government assistance. With CBRN attacks, particularly those involving large quantities of weaponized toxins deployed in major cities, this is not the case. The RMS model simulates 47,000 attacks on U.S. targets using CBRN weapons; some of these events would result in insurance losses that approach the surplus level of the entire U.S. insurance industry.

EVENT DESCRIPTION	TOTAL LOSS ($BILLIONS)	PROPERTY DAMAGE LOSS ($BILLIONS)	WORKERS' COMP LOSS ($BILLIONS)	FATALITIES
Nuclear detonation - 5 kiloton yield, Chicago	**$530**	$323	$207	300,000
Nuclear detonation - 1 kiloton yield, Los Angeles	**$230**	$163	$67	110,000
Anthrax attack, 75 kg anthrax slurry, Philadelphia	**$216**	$125	$91	60,000
Nuclear power plant sabotage, Illinois	**$148**	$146	$2	Few
Dirty bomb, 15,000 curies cesium-137, New York	**$127**	$127	$0.1	Few
Anthrax attack, 1 kg anthrax slurry, Philadelphia	**$44**	$26	$18	10,000
Sarin gas attack, 1,000 kg release, New York	**$17**	$12	$5	2,000

Figure 5: Attacks simulated by the RMS Terrorism Model

THE THREAT OF A TERRORIST ATTACK IN THE UNITED STATES IS SUBSTANTIAL AND WILL REMAIN SO FOR THE FORESEEABLE FUTURE. TERRORISM'S COST MUST BE MEASURED QUANTITATIVELY.

Despite significant improvements in counter terrorism infrastructure, determined terrorist groups remain resilient and intent on attacking the United States. Since 2002, approximately 30 large-scale plots have been executed in the United States. While the lethality of these plots has been relatively low and many of the perpetrators were amateurs with more enthusiasm than skill, the considerable frequency of plots indicates that the terrorism threat has not subsided.

The situation remains perilous outside the U.S. as well. When TRIA was reauthorized in 2007 for seven years, it may have been hoped that, by the end of 2014, Afghanistan's transformation into a peaceful and stable country would be well underway. Ironically, the scheduled sunset of TRIA coincides precisely with the withdrawal of NATO combat troops, leaving security in the hands of the Afghan National Army, whose allegiance and funding are in doubt.

Mohammad Daud Yaar, the Afghan ambassador to London, recently alluded to game theory in his grim assessment of the situation in Kabul: with numerous Afghan factions (including the Taliban) all vying for power, the eventual outcome is unlikely to produce optimal stability. Instead of a harmonious coalition governing the country as originally envisioned by the U.S., the result will more likely involve pervasive low intensity conflicts between opposing regional groups, leading to chronic insurgency or even outright civil war. If stability in Afghanistan serves as any benchmark for the ambient terrorist threat to the U.S. homeland, terrorist risk will remain elevated for an extended period.

Studies of the federal government's involvement in lines of insurance including flood, crop, mortgage, health, and pension are periodically undertaken, and they nearly always involve quantitative assessments of the cost of risk, probability of loss, and economic viability of each program. Terrorism insurance should be no different. The TRIA renewal dialogue must include an objective quantification of the economic costs of terrorism, their impact on the insurance industry, and the cost of federal involvement in any insurance solution. Given the advances in risk modeling over the past decade and the recently increased transparency into US counter terrorism operations, modelers have an increasing ability to quantify this aspect of the risk substantially compared to a decade ago, although inherent uncertainties still remain. Policymakers should make use of these tools to best estimate the costs and benefits of any terrorism legislation.