Terrorism Threats and the Insurance Market

Testimony by

Peter Ulrich

Senior Vice President, Model Management

Risk Management Solutions, Inc.

Tuesday, July 25th at 10am

to

The Intelligence, Information Sharing, and Terrorism Risk Assessment Subcommittee of
The Committee on Homeland Security and
The Oversight and Investigations Subcommittee of
The Committee on Financial Services of The House of Representatives

1. Background

Risk Management Solutions, Inc.

Founded at Stanford University in 1988, RMS is the world's leading provider of products and services for the quantification and management of catastrophe risks. RMS grew rapidly in the 1990s, offering technology and services for the management of insurance catastrophe risk associated with natural perils such as earthquakes, hurricanes, and windstorms, as well as products for weather derivatives and enterprise risk management for the P&C insurance industry. Today, RMS is also the leader in risk modeling for man-made disasters associated with acts of terrorism by analyzing the impact of weapons of mass destruction on property and people for many sectors of the insurance industry.

Terrorism Modeling at RMS

RMS developed the first commercially available model of terrorism risk in the U.S. in 2002, a model that was widely acclaimed as ground-breaking. RMS has undertaken a review and updating exercise for the model each year. RMS maintains a team of advisors which includes some of the world's leading authorities on terrorism threat, asymetrical warfare techniques, and security and intelligence issues. RMS was a co-founder with RAND of the RAND Center for Terrorism Risk Management Policy (CTRMP), a policy research think-tank to explore terrorism issues in government and private sector interraction.

The RMS® U.S. Terrorism Risk Model provides a comprehensive analysis of terrorism risk in the U.S., quantifying risk from both foreign and domestic terrorist organizations. It supports multi-line risk analysis for both certified and non-certified events causing property loss, business interruption, workers compensation claims, and losses to Life & Health lines.

The model quantifies the impact of a representative suite of potential terrorist attacks, ranging from various conventional weapons historically used by terrorists including chemical, biological, radiological, and nuclear (CBRN) weapons, also known as "weapons of mass destruction." Attacks are simulated using sophisticated models that analyze the impact of these weapons on property and people. Casualty estimates produced by the model can assist with risk assessment of other insurance lines including life, personal accident, and accidental death and dismemberment.

Attacks are modeled at potential terrorist targets across the U.S., implementing techniques for target prioritization that replicate the processes of target selection known to be employed by terrorist organizations. The numbers and types of attacks incorporated into the model include the potential for multiple synchronized attacks, a signature of Al Qaeda and its associated organizations around the globe.

RMS does **not** attempt to predict the time and place of the next terrorist attack. Our focus is on modeling the ***likelihood*** of an attack occurring at a given target, using a specific weapon, and then determining the ***consequences*** of such an attack.

Terrorism is a rapidly changing risk. RMS regularly assesses and reviews the risk environment, producing a periodic Terrorism Risk Briefing for clients and parameterizes the probabilistic model through the provision of Risk Outlooks. Clients are able to use alternative Risk Outlooks to

perform sensitivity analyses against U.S. exposures and test risk management decisions under different assumptions for potential future developments.

Applications of the RMS Terrorism Model

Well over 100 insurers, reinsurers and brokers in the Property Casualty and Life & Health industries are now actively using the RMS Terrorism Model to manage risk. These companies are using the model to:

- Idenitify and quantify multi-line exposure concentrations
- Quantify the greatest potential losses to portfolios under a management selected benchmark attack scenario
- Generate aggregate exceedance probability (AEP) loss distributions by line of business and in total
- Analyze key drivers of loss by account, location, target type, and city
- Quantify the risk of fire-following terrorist attacks for policies ***without*** terrorism coverage
- Evaluate alternative treaty reinsurance or securitization structures for risk transfer
- Analyze the impact of TRIA under various insurance take-up rates
- Examine the impact of exclusions (e.g. CBRN) on re/insurance offerings
- Pricing re/insurance policies
- Design and implement underwriting guidelines to diversify portfolio risk

There are also a number of corporations and entities outside the insurance industry using the RMS Terrorism Model. For instance the Congressional Budget Office used the model to measure the risk transfer effectiveness of TRIA and evaluate different government/insurer sharing options for the Terrorism Risk Insurance Extension Act.

Terrorism Risk Management Differs from Natural Catastrophe Risk Management

While the management of natural catastrophe perils focuses heavily on probabilistic output, the dynamic nature of terrorism risk requires an approach that focuses on exposure management, scenario modeling and probabilistic loss modeling. This three-pronged approach is used to analyze terrorism risk from a number of angles, allowing risk managers to triangulate on the risk.

The first step in managing terrorism risk is exposure management. Insurers need to identify, understand and control their exposure accumulations across multiple lines of business, especially in urban areas. For example, depending on the size of the company, they may set a guideline that limits the amount of multi-line exposure in any 400 meter radius to $500 million. By limiting business in over-exposed areas or flagging possible non-renewal accounts, companies are able to maintain acceptable levels of risk.

A deterministic approach is then used to quantify loss due to potential attack scenarios. Typically, companies select a benchmark event in order to manage losses to an acceptable loss threshold. A major conventional attack, such as a 2-ton or 5-ton truck bomb, is typically selected given this type of attack mode is relatively likely to occur and will produce a significant amount

of loss. Thus, a company may set a guideline such as the modeled losses from a 2-ton bomb anywhere in the U.S. can not cause multi-line losses to their portfolio of more than $100 million.

While these first 2 methods can help control a companies absolute exposure to terrorism risk, one also needs to factor in the relative likelihood of an attack mode and target location. This is accomplished through use of the probabilistic model. With this step the insurer manages their terrorism risk around probabilistic loss levels such as annual average loss or return period losses (250yr, 500 yr, 1,000 yr)

2. Risk modeling for terrorism insurance

The RMS model of terrorism risk is based on open source material. It relies on the following sources of information:

- Statistical catalogs of terrorism events and open source event reports
- Academic literature on the study of the motivation and modus operandi of terrorism threat groups
- Analysis of the costs and logistics involved in mounting terrorist attacks and theoretical analysis of the potential for carrying out attacks not seen historically
- Expert opinion interpreting latest trends

Wherever possible, RMS models are empirical and derived from objective and quantitative data.

The model represents the motivation of the terrorist threat groups, as interpreted by some of the leading academic experts on terrorism and political violence. It mathematically represents the intent and 'utility' to the terrorist group of carrying out different types of attacks on different targets. It incorporates this within a game theory framework of how actions by the security services, and improving the defenses for different types of targets, will affect the tactical decisions by terrorist groups on the attack modes they choose and the targets they prioritize.

The RMS model draws on a catalog of historical terrorism events. This catalog now includes over 24,000 events, of which 1,000 are 'macro' (i.e. car bombs or worse) terrorist attacks carried out worldwide since September 2001. Statistical analysis of this attack catalog information yields valuable insights into general attack patterns and targeting preferences that can be incorporated in the modeling. For example, the catalog shows that almost half (around 45%) of all jihadists macro attacks occur in the economic or political capital city, and two thirds occur in a major top 5 city of any particular country. This demonstrates the prioritization of major cities for large scale attacks by jihadists, which corroborates their publicized intent to maximize destruction and economic damage. Mapping this kind of prioritization onto the United States, shows risk being concentrated in major cities like New York, Washington, Chicago, Los Angeles, and other cities, far more than if the risk analysis had used only their population statistics as the metric.

Other important information about the likelihood of different attack modes being used in a strike against the U.S. can be gleaned from an analysis of recent attacks in other countries. For example the relative likelihood of vehicle bombs of different yield can be seen in the statistical distribution of different bomb sizes that have been perpetrated or attempted in countries with similar security environments to the U.S. This is supplemented with additional analysis of the relative difficulties ('logistical burden') of putting together attacks of different levels of skill, explosive material, manpower and other equipment.

Where factual data is not easily available, for example to assess the likelihood of an attack types that has never been carried out before – and the obvious example being attacks involving chemical, biological, radiological or nuclear (CBRN) weaponry – then we have to use supposition, informed by additional analysis, background material, expert opinion and other open source material. An example is a survey RMS commissioned for our last parameterization of the terrorism model, reviewing material on jihadist websites referring to CBRN attacks, as input into our estimates of jihadist intent and capability to carry out CBRN attacks within the U.S.

To assess the frequency of terrorist attacks being experienced in the U.S. we calibrate a model of the number of attacks that are likely to be attempted per year, and the number of attempted attacks that are likely to be interdicted. We monitor this component data (attempted attack frequency and interdiction rate) for all relevant countries and also attempt to quantify uncertainty on these parameters. We use expert opinion and trend analysis to estimate this frequency for the next twelve months and for longer periods, such as the average over the next five years.

3. The use of intelligence information in risk modeling

Using classified information in models would limit insurers ability to model and manage risk

RMS has not had access to classified intelligence information in the building of the model, nor sought to attain clearance in order to incorporate it.

Intelligence information could be made available for use in insurance risk models in one of two ways: either by declassifying information so that insurers could use it, or by requiring users of models that incorporate classified information to have security clearance to run the model or to analyze output.

The second option presumably would enable more information to be used, but if insurance companies were required to have employees with security clearance on staff in order to model their terrorism risk, then we could see this being a major obstacle to insurers using classified modeling in the management of terrorism risk.

A better option would be to explore certain data that could be declassified for insurers to have access to.

Risk information is less time sensitive than intelligence information

Terrorism risk analysis is fundamentally different from intelligence operations. Most intelligence information is geared to anticipating and preventing the next terrorist attack. Insurance companies by contrast are assessing the overall landscape or pattern of risk: the frequency and severity of likely losses that may occur, for example which cities and which parts of cities and types of insured asset, are more at risk than others. They also have a very different timescale over which they are interested. Intelligence information is often time-sensitive. Insurance companies are managing insurance policies of a year or more duration, so are assessing a gradual shaping of a portfolio over a period of one or more years. Insurance pricing cycles last several years: insurance risk management is about managing levels of loss and balancing capital across this multi-year cycle.

RMS updates its model once a year, and issues interim 'Briefings' to its clients, alerting them to emerging trends, every three to four months. Insurance clients are reluctant to change their modeled view of risk more often than this.

A lot of the information needed for terrorism modeling becomes public over time

Most of the important information about terrorism activity becomes open source after some time. Actual attacks are known, and salient facts about the target and operational methods used are usually part of public briefings. When alleged attacks are interdicted, RMS tracks indictment papers from arraignment and other public statements, which often detail the evidence for the targets and modus operandi suspected. The fact that there is usually a considerable time delay between an arrest being made and a charge or public disclosure of the suspected plot is not usually an issue for the modeling. RMS accumulates such material for an annual review and updating of its model.

4. Adding intelligence information to risk modeling

As a risk partner with the government, the insurance industry should be fully informed

Insurers' uncertainty about terrorism risk includes concerns about information asymmetry. Classified information is today an "unknown unknown". Declassifying certain information may improve insurer's confidence that they have access to the relevant information about their risk and increase the willingness of the insurance industry to be a risk partner with the government in sharing terrorism risk, for the good of all U.S. industry and commerce.

Insurers do not need real time information

Insurers are not like the security services – they have less need for real-time information. This is due to the fact that even if they knew of a definite, imminent attack, their ability to minimize the risk to their existing portfolio from the attack would be very restricted. They would be unable to cancel insurance policies or to change policy terms. Insurers would perhaps be able to protect their own balance sheets by purchasing reinsurance, but this has the potential to create information asymmetries if their reinsurer was not privvy to the same information.

Real time information provision would need careful management to avoid commercially disadvantageous information asymmetry

Real-time information might potentially be useful for underwriting new policies. For example, if the intelligence services disclosed information that a certain building might be the target of an attack, an insurer being asked to insure that building might chose not to offer coverage, or offer coverage at a very different price than they would have absent the intelligence. A process of disclosing information to the insurer about an imminent attack would presumably have to include a wider process of informing the building owner or other potential purchaser of insurance to avoid commercially disadvantageous information asymmetry.

5. Useful information if classified information was available

Classified information that is not currently available to the insurance industry that might be useful for risk modeling would include the following:

Information on interdicted attacks

The number of attempted attacks or the number of suspected attacks that intelligence services have identified over the past five years that have not been made public – i.e. where suspects have not been arrested or indicted or for other reasons no information has been made public. The stage that the plot had reached and an objective assessment of the degree of confidence with which these attacks are suspected would be helpful. This currently unavailable information would enable insurance companies to make a better assessment of the number of terrorist attack attempts per year, which combined with an assessment of the likely rates of attempted attacks succeeding, provides the likely average annual frequency of experiencing successful terrorist attacks: a key metric for managing the risk.

Identification of changing trends

Where intelligence identifies something that changes the picture of risk, or indicates a new trend in the modus operandi, or targeting patterns of threat groups, it would be useful for the insurance industry to factor this into their risk analysis as early as possible, particularly given the long reaction time required for the insurance industry to reshape its portfolio or change its risk transfer arrangements. An example would be a shift in terrorist groups to go after economic targets as opposed to focusing on high-casualty outcomes, or the employment of a new method of attack.

Capability assessments

The potential for terrorist threat groups to carry out attacks more severe or more sophisticated than others have done historically is an area of expert opinion. This includes the use of very large yield conventional bombs and also the use of chemical, biological, radiological or nuclear weapons (CBRN). Assessments of these using only open source material would not be able to factor in additional circumstantial data, such as known quantities of explosives or other materiel that are missing, or a known missing nuclear weapon from a military arsenal.

Intelligence assessment of the likelihood of an attack using these types of agents using classified sources are likely to be better than those using only open source.

Quantification of other inputs on terrorism risk

Other inputs into the modeling of terrorism risk could also be improved with access to briefings or assessments by those with access to classified information. These would include information such as:

- Assessments of the number of suspected jihadist sympathizers – and their geographical concentrations, to assist with determining the probabilistic distribution of number of active jihadist terrorist operatives, and numbers of attacks that could potentially be attempted

- Intelligence views on the quantitative effectiveness of border security (i.e. the likelihood of a terrorist operative or cargo passing undetected through the current measures in place), including ports and airports.

- Security ratings of individual cities or individual targets

- Internal assessments of weakspots in defenses, high risk areas or problems in security that could cause specific vulnerabilities that may take some time to fix.

Information provision does not need to be highly specific

These information inputs listed here show that significant improvements to the confidence and ability of the insurance industry to model and manage terrorism risk could be achieved without providing highly specific information. For example, it would not be necessary for the data on attempted attacks to contain information on all the operational details known to the intelligence services – it would be sufficient to provide aggregate numbers or summary information about the type and scale of plot suspected and some classification of stage and confidence. Assessments of trends would not need to identify sources of the data that suggested the new assessment. Assessments of numbers of jihadist sympathizers would not need to identify individuals or disclose names or other details.

The insurance industry would benefit from aggregate information that plugged the gaps in the information they currently have access to. The insurance industry is at present unsure what it is that they do not know. They would benefit from a snapshot of the information that at present they do not know.

6. Comparison of Uncertainty in Natural Castrophe Models to Terrorism Models

Frequency Control

Einstein remarked that Nature is subtle, but not malicious. There is no universal definition of terrorism, but all such acts are recognized as being malicious. Does this imply necessarily that the uncertainty in risk assessment for terrorism is far greater than that for natural catastrophes? The answer to this question depends on the political regime against which acts of terrorism are perpetrated. The destructive forces of Nature are beyond human control. But through strengthening counter-terrorism legislation and empowering the intelligence and law enforcement services, there is much that democracies can do to control terrorism, albeit at an increasing cost to civil liberties.

Last year, the Greek alphabet had to be used to name the latter Atlantic tropical storms. Meteorologically, it is possible for both the Latin and Greek alphabets to be exhausted: fifty tropical storms in one hurricane season is a possibility. However, given the post-9/11 diligence of the NSA, CIA, FBI and their intelligence counterparts across the world, it isn't possible for fifty major attacks against the US homeland to be planned without anyone being arrested - one successful terrorist attack alone would be considered an intelligence failure. Thanks to the vigilant security services, the uncertainty in the frequency of successful terrorist attacks is smaller

than the uncertainty in the frequency of land-falling Atlantic hurricanes. Considering future terrorist activity, it isn't a matter of if but when; with hurricanes, it isn't a matter of when, but how many.

Hazard Concentration

Earthquakes can occur anywhere in the U.S., but earthquake hazard is concentrated around active geological faults. Similarly, a terrorist attack can occur anywhere, but terrorism hazard is tightly concentrated within the principal populous urban centers with international name recognition. Since 9/11, Islamist attacks have followed Dr. Ayman Al-Zawahiri's injunction that Al Qaeda should choose targets that the worldwide Muslim community approves. Enormous accumulations of risk in New York and other major cities limit industry capacity to provide terrorism coverage. The accumulation problem would be less acute if there were more uncertainty over terrorist targeting.

CBRN Severity

The biggest source of volatility in terrorism risk assessment is not attack frequency, but the severity of extreme CBRN attacks. The size of the greatest Californian earthquake is limited by the length of the San Andreas Fault. If this maximum earthquake were to occur, the insurance loss would be massive, but the burden of loss could be withstood by the insurance industry worldwide. By contrast, there are realistic CBRN scenarios that are so catastrophic as to ruin utterly the capital base of the global P&C insurance industry. The variability in loss potential from an extreme CBRN attack is far greater than that from a Magnitude 8 earthquake. However, this does not hold for the variability in loss potential from a conventional terrorist attack.

7. The Insurability of Terrorism Risk

RMS is a co-founder with RAND of the RAND Center for Terrorism Risk Management Policy (CTRMP), a policy research think-tank to explore terrorism issues in government and private sector interraction. Through our work with RAND and other clients, RMS analysis has been used and cited in many of the studies published in the debate over TRIA, including:

- 'Cost Estimate for H.R. 4634; Terrorism Insurance Backstop Extension Act of 2004'; Congressional Budget Office, U.S. Department of the Treasury; November 2004.
- 'Issues and Options for Government Intervention in the Market for Terrorism Insurance'; RAND Center for Terrorism Risk Management Policy, Sept 2004.
- 'TRIA and Beyond'; Wharton Risk Management and Decision Processes Center, August, 2005.

In addition, RMS has published an independent, objective study on the government's role in terrorism insurance entitled "A Risk-Based Rationale for Extending the Terrorism Risk Insurance Act". This study can be downloaded in its entirety at http://www.rms.com/Terrorism/Publications/. The executive summary of the document is included below.

Executive Summary: "A Risk-Based Rationale for Extending the Terrorism Risk Insurance Act"

RMS models terrorism risk and assists insurance clients with terrorism risk management. This report provides insights from the modeling of terrorism risk to the debate around the renewal of the Terrorism Risk Insurance Act (TRIA).

The U.S. continues to be the target of political violence from Islamic militant threat groups worldwide, and anti-American sentiment shows no sign of abating. The U.S. has become more secure and improvements in counter-terrorism measures are making it harder for terrorists to succeed in perpetrating large scale attacks. However, the chance of a major terrorist attack in the homeland U.S. still remains. There is a chance that a future terrorist attack could cause catastrophic losses on a scale that far exceeds any losses previously faced by the insurance industry and possibly beyond the resources of the insurance industry to pay.

Terrorism is a unique peril and poses complex risk management issues for insurers. Terrorism risk management challenges include:

1. Terrorism can potentially cause much greater insured loss than from natural catastrophe perils such as earthquakes, hurricanes and floods, and claims could potentially exceed the total capital of the P&C insurance industry
2. Diversification of the risk is problematic – terrorism risk is highest in the places where there is the greatest demand for terrorism insurance and highest concentrations of value
3. State regulations severely limit insurers ability to price and control their exposure
4. Fully pricing for the uncertainties associated with terrorism risk could make insurance prohibitively costly
5. Government is an active player in shaping the risk which insurers cover

A major benefit of having TRIA in place is it has allowed key sectors of the economy to return to "business as usual". TRIA has succeeded in leading to the creation of a relatively stable, viable market for terrorism insurance allowing commercial businesses, real estate owners and construction companies located in areas of perceived high risk to obtain coverage from terrorist attack. Further, TRIA has allowed three years of experience to be gained, to test out market appetites and to explore potential opportunities.

While some view TRIA as a government subsidy, the insurance industry assumes the first dollar loss, and in over 90% of attacks, the industry pays the majority of the loss. The insurance industry bears over 80% of the overall terrorism risk, measured in annual expected loss. TRIA protects the insurance industry only in the case of extreme losses that could force them out of business. It provides the insurance industry with solvency, not subsidy. Without TRIA, many insurance companies will take the same decision as they did in 2002 and quit the market.

The Treasury has proposed a number of modifications to the structure of TRIA in considering its extension, mainly to leave a greater share of terrorism risk to the insurance industry. These include raising the threshold of 'certified' events; raising insurance company retentions; changing the Federal Government co-payment share, and reducing the number of lines covered by TRIA. While revising the TRIA structure may be sensible, the Federal Government should closely analyze the impact of retention increases and co-payment adjustments as these changes could threaten the solvency of some insurers and defeat TRIA's original objective.

An extension of TRIA is needed because the chance of ruinous losses will otherwise force a large majority of insurers to quit the terrorism market. There are many variants in how the Federal Government could participate in a terrorism insurance market. The most practical in the current legislative timescale is to renew TRIA.