

Wharton Risk Management & Decision Processes Center



Assessing and Managing Extreme Events

April 28, 2003

Report on a Roundtable held by the Wharton Risk Management and Decision Processes Center, Philadelphia, in conjunction with the Earth Institute at Columbia University. The center is co-chaired by Paul Kleindorfer and Howard Kunreuther.

EXECUTIVE SUMMARY

Among extreme events that threaten lives and infrastructure, terrorist attacks present one of the biggest challenges for government and business, particularly for the insurance industry. So little is known about the potential nature, location, frequency and impact of events, such as the attacks of Sept. 11, 2001. Both insurers and reinsurers have thus great difficulty in quantitatively assessing and managing terrorism risk to determine what type of coverage they can provide and the premiums they should charge. The Terrorism Risk Insurance Act (TRIA) of 2002, which establishes a partnership between private insurance and federal government to share insured losses in case of terrorist attacks, is itself a source of uncertainty as it is scheduled to expire at the end of 2004 with a possible one-year extension.

This was the backdrop to a Roundtable on “Assessing and Managing Extreme Events” held on April 28, 2003 at the Wharton School, University of Pennsylvania. The federal government must also rely on information from intelligence sources about the motivations, resources and organizational structures of those who carry out terrorist attacks to estimate future risks. Private companies who are modeling this risk are also hampered by the same lack of data. This is in stark contrast to natural hazards, such as hurricanes or earthquakes, are whose location, timing and effect is more predictable because of their history and because they lack a human motivational element that selectively chooses targets

Notwithstanding the difficulties of modeling terrorist attacks, insurers, reinsurers and modeling firms have been extending their expertise in catastrophe modeling derived from natural hazards to provide simulation tools to evaluate a range of scenarios of future terrorist attacks, incorporating hundreds of thousands of potential targets into their models. But there are significant uncertainties in such modeling, and many questions as to the use of such models in providing an adequate basis for exposure management and pricing of insurance and reinsurance contracts to cover terrorist events.

Added to the difficulties on the risk quantification side are demand issues. Today most businesses have elected not to take out insurance against a terrorist attack, either due to its high cost or because they believe they do not need coverage. The reinsurance industry, which effectively withdrew from accepting terrorism risk after the losses it suffered from the September 11th attacks, is now beginning to resume coverage – but at high prices. There is also a concern that uniformity of reinsurance products may reduce competition and innovation in the industry.

The Roundtable addressed these issues, with a focus on the significant uncertainties and current practices of the insurance and reinsurance industry in modeling, pricing and spreading terrorism risk. Representatives attended the Roundtable from the insurance and reinsurance companies, industry, risk modeling firms and the academic community. A list of participants with their e-mail addresses can be found at the end of this report.

REPORT:

A. Challenges facing insurers and brokers in managing extreme events

The opening session of the Roundtable focused on why insurers are reluctant to underwrite risks following catastrophes such as a terrorist attack, on the challenges faced by brokers in creating appropriate incentives for providing reinsurance protection to insurers, and on what role the public sector can play in encouraging businesses to purchase insurance and invest in protective measures.

One of the purposes in holding this Roundtable, Howard Kunreuther stated, is to understand the lack of interest by business and government in taking terrorism seriously today. Managers need to reconsider their position that “I’m not thinking about this risk; I’m not putting my money into protecting my organization against something I don’t think is going to happen.”

The magnitude of the Sept. 11 attacks requires new thinking about managing risk, said Paul Kleindorfer. “We feel that we have to expand our horizons, and to bring together representatives of academia, government and industry. It is really important to try to understand some of the tremendous challenges we face.”

Insurers reassessed their risks following the attacks of Sept. 11, Hurricanes Andrew in 1992 and the Northridge earthquake in 1994. Each of these events produced losses that had not been contemplated by insurers and reinsurers, resulting in a drastic reduction in capital and a realization that the premiums charged did not fully reflect the magnitude of the losses. A new appreciation by insurers of these risks led them to charge higher prices for coverage or, in the case of terrorism, to limit the number of policies that they wrote immediately after September 11th 2001.

During the first year after the terrorist attacks there was considerable demand by many businesses for protection against these events but little coverage available. This led Congress to pass the Terrorism Risk Insurance Act (TRIA) in November 2002. Insurers are now required to offer insurance against terrorism as a separate endorsement to an existing commercial policy. Firms can voluntarily purchase this coverage. Each insurer is financially responsible for a certain portion of the loss as a function of its total premiums written on its other commercial insurance. Now that terrorist coverage is available, the demand for such protection has been noticeably lacking either because businesses feel that a future terrorist attack will not happen to them and/or because they perceive the premium to be too high. However, some Boards of Directors are insisting that the firms they represent buy this insurance despite the high prices so as to avoid a worst-case scenario.

“Transfer of low-frequency, high-impact risk is a difficult sell,” said Jim Ament of State Farm. “The fact that the risk is unlikely to occur, even if it does have the potential for devastating consequences, results in a reluctance on the part of potential risk transferors to incur the cost associated with the risk transfer... The challenge is to help stakeholders understand the nature of low-frequency, high-impact events and appreciate the means available to mitigate or transfer those risks.”

In encouraging adequate levels of insurance coverage and protection against terrorism, Ament in his remarks urged government to avoid mandating and instead focus on measures such as the development and implementation of safer building design and construction. He further noted that government involvement in the insurance market should be limited to providing financing for risk transfer in the most infrequent but extreme events.

In New York City, perceived as a prime target for any future terrorist attack, only one in three or four businesses is initially placing orders for terrorist insurance, John DeMartini, of Towers Perrin Reinsurance told participants. Of those, only about half are actually buying it; the rest decline “when they see the bill.” In attempting to quantify exposure, brokers, insurers and reinsurers need high-quality information on the property and the individuals at risk. That includes the street address, construction codes, occupancy, height, age of building and the value of it and its contents. Such information is generally available because it has been compiled as part of natural catastrophe modeling.

Data to facilitate workers’ compensation coverage is less complete although many companies have significantly improved their information, DeMartini noted. In this case the required data include the number of employees and payroll by street address, whether or not they are engaged in hazardous work, and details on the buildings in which they work.

Some insurers are willing to pay a very high price for reinsurance coverage due to the uncertainty of future losses they may experience. One graphic example provided by DeMartini was that of an insurer who paid a reinsurer \$900,000 for \$9 million of coverage with a 25% rebate if there were no claims during the year. This rate is out of all proportion to the perceived probability of a terrorist attack occurring, which is more likely to be of the order of 0.5% or less, DeMartini indicated.

B. Risk Management Strategies for Terrorism and Other Extreme Events

The Roundtable then turned to ways of improving cooperation and sharing information between the private and public sectors on the front lines of the fight against terrorism such as government and airlines. A key issue raised by participants was how trust can be created between insurance and reinsurance companies so that valuable information will be shared while at the same time respecting privacy rights.

To illustrate the tension between security needs and the sharing of data, one can turn to the airlines. In seeking to reduce risk in the air transportation sector, every individual entering or transiting through the United States will be subject to scrutiny using the Commercial Airline Passenger Prescreening System (CAPPS II). This is equivalent to a risk assessment of every person at a port of entry, Geoff Shaw of Lockheed Martin told the conference.

The system will seek to authenticate travelers’ identity, but it won’t try to acquire personal data such as social security or passport numbers or credit information. Information gathered through the program can help government and industry manage their terrorism risk in ways that go beyond the enhancement of physical security measures, Shaw told Roundtable participants. The challenge is “how to utilize this information in ways that allow industry to better manage its risk,” he said. He praised cooperation between the public and private sectors in this regard.

Improvements in risk management at a range of facilities require a series of technological and organizational enhancements that are aided by policy and intelligence initiatives, noted Tom Gallagher of Wachovia Securities. An airport, for example, should seek to control access by passengers, employees, cargo, baggage, service vehicles and equipment, and to continuously monitor them. Those objectives can be achieved by using a range of technologies including low-ambiguity biometric technology (i.e., fingerprinting, palm, iris, retinal, facial and voice recognition) for passengers and employees for passengers and employees, ID tags on mobile equipment, baggage and cargo, and software supervision of all sensor devices including those that scan hand baggage, tickets and boarding passes. These measures

are equally applicable to ports, borders, and large installations such as financial institutions, nuclear power plants and telecommunications centers.

The drive to protect critical infrastructure should identify and catalog all crucial public utilities, food and agriculture facilities, as well as vital centers of industry, transportation, banking and finance, Gallagher told Roundtable participants. The defense of cyberspace is also a significant concern. The cost of defending these facilities is likely to be met by the private sector, since federal government funding will be limited to first-response services such as firefighters. The public and private sectors must also defend against low-probability, high-impact catastrophic threats. Initiatives include improved detector technology, the tracking of hazardous materials, and the development of antidotes in the event of chemical or biological attack.

C. Challenges Facing Reinsurers:

This session focused on how the reinsurance market is responding to the need for additional coverage, how it can estimate the losses stemming from extreme events such as a terrorist attack, and how much insurers and reinsurers will raise their premiums to deal with greater risks than they had previously anticipated. A natural question posed was whether the premiums charged will be affordable for clients wanting terrorism coverage.

The reinsurance community was responsible for approximately three-quarters of the \$40 billion loss stemming from the Sept. 11 attacks. After the effective withdrawal of reinsurance in the immediate aftermath of these events, some reinsurers have now begun to provide coverage but at very high rates. Yet there is still some demand by insurers for protection.

Like primary insurers, the reinsurers are reacting to the random nature of the terrorist threat, and pricing their coverage accordingly. "A big part of the availability and price of terrorism coverage is a function of the inability to understand the risk," said DeMartini. "They don't know when, where or how the next terrorist attack will occur and how much damage it will do."

Reinsurers are also challenged by the lack of consensus on the magnitude of risk posed by terrorism, and by their lack of protection from TRIA said Carl Hedde of American Re. But there is an opportunity for reinsurers to aid insurers who are concerned about the likelihood of having to dig into their own pockets to cover the losses from a terrorist attack for which they are responsible.

Joan Lamm-Tennant of General CologneRe also highlighted the danger of all reinsurers imitating each other by offering the same coverage against terrorism at the same rates because there is reluctance by any of them to innovate when there is considerable ambiguity associated with the risk. In such a situation where competition is effectively stifled, there is a danger that all will fail to accept the risk that insurers need to transfer, she said.

Looking to possible future risks, David Durbin of Swiss Re outlined the new threat scenarios under consideration by his company. They include terrorism on nuclear plants; blowing up the Channel Tunnel between England and France; massive telecommunications failure and viruses infecting cyberspace. Other possible threats include a falling asteroid, a tsunami, a dam failure, and a major systemic failure of financial institutions, Durbin said. The challenge facing reinsurers is whether to provide protection against these low probability but high consequence events and if so what premiums to charge.

D. The role of modeling in managing terrorism and other extreme events

In seeking to reduce the uncertainty of the terrorist threat, the Roundtable turned to a panel of experts to discuss how to develop meaningful scenarios for estimating the probability and consequences of such attacks. Representatives of three leading modeling firms – Applied Insurance Research (AIR), EQECAT and Risk Management Solutions (RMS) addressed this question and also focused on the quality and reliability of the information used in their models, whether their models can be quickly adjusted to allow for new information, and how their models influence the insurance and reinsurance markets.

Jack Seaquist of AIR noted that his firm's model incorporated more than 300,000 U.S. landmarks including corporate headquarters, industrial and energy installations, transportation facilities, sports arenas and government buildings. The model contains a Group Threat Index (GTI) for known terrorist organizations which incorporates information on the target type, the weapon type and the likely location of an attack. The index is based on knowledge of a terrorist group's objectives, means of attack, and history. The biggest variations in pricing are directly related to urban density and the concentration of targets.

The aspect of a terrorist attack which is most certain and easiest to quantify is what the damage would be in certain scenarios added Karen Clark of AIR. The location of future attacks is much harder to predict. The most uncertain aspect of any given scenario is its frequency of occurrence.

EQECAT's model incorporates a "severity assessment" that includes a database of probable target sites, a simulation of the "footprint" of a CBRN attack, and a vulnerability assessment in which the intensity of the hazard is converted into property damage and injury rates, and into financial loss pointed out Jim Johnson of EQECAT. The model also includes a "frequency assessment" which ranks targets and modes of attack such as industrial chemicals, bombs and other possible weapons such as aircraft and nuclear plant sabotage.

Modelers and insurers should consider different scenarios for future attack, Johnson noted. They might include, for example, another hit on New York City as an act of defiance despite all the new security measures, or on sites in the heartland of America, commonly supposed to be a much lower risk than big cities, in a gesture that would seek to show that "nowhere is safe". He also warned that some current security enhancements might be off the mark. "We are probably focusing on all the wrong targets," he said. "The surprise will be multi-mode attacks, not just bomb blasts. And if there is another airliner attack it's not likely to be a passenger jet, it's more likely to be a plane filled with explosives."

The effectiveness of a terrorist organization in carrying out attacks depends on the connectivity of different parts of the organization, Gordon Woo of RMS told the conference. Computer simulations of the terrorist network assess the likelihood of different scales of attack in conjunction with techniques such as Bayesian belief networks for modeling causal structure. For example, discovery of the agent ricin, used recently in the U.K., provides evidence for the importance of training in biological weapons as a component for updating the probability of a biological attack. The key to developing a meaningful estimate of both the likelihood and consequences of future events is to understand how the terrorist mind operates. Hence the importance of developing game theory where both the terrorists and the defenders against attacks take into account what the other side is likely to do.

Participants in the Roundtable also discussed whether its democratic tradition and legal foundations no

longer restrain the United States response to terrorism. Woo quoted law professor Alan M. Dershowitz, who declared that “The United States would be incapable of mounting an unlimited war against terrorism because we are constrained by our Constitution, our commitment to the rule of law, and our heritage of fairness, humaneness, and proportionality.”

E. Next steps:

In discussing future research that the Wharton and Columbia team should undertake in conjunction with Sponsors, Roundtable participants made the following points:

- undertake case studies of management of extreme events
- consider the use of game strategy in the fight against terrorism. This could include bluffing, i.e. the fictitious implementation of anti-terrorist measures to make terrorist organizations believe defenses are stronger than they really are;
- urge anti-terrorist planning in business and industry take place at the highest corporate levels.
- recognize that government mandation of anti-terrorist measures won't work in the long run although it can be useful in the short run.

The group agreed on the challenges associated with the impact of the Terrorism Risk Insurance Act (TRIA) of 2002 on insurer behavior and demand for coverage by firms at risk. In particular, the group felt that it would be important to undertake studies now on what type of program would be most appropriate for replacing TRIA if it is not extended for another year at the end of 2004. The following issues were discussed in this regard:

- Under TRIA insurers are obliged to offer coverage against certified acts of terrorism to their clients but most of them currently refuse to purchase coverage. We need to understand what factors influence their decisions not to protect themselves.
- Differences in risk perception among different firms faced with a terrorist risk. In particular one should understand how trophy targets view the risk relative to other firms. Do those firms who feel they are most vulnerable, purchase more terrorist insurance? What price do they pay for coverage?
- What are the decision processes utilized by insurers in determining how much coverage to offer and what prices to charge? Similarly what decision processes do firms use in determining whether or not to buy protection?
- What is the effectiveness of different strategies regarding risk assessment, information sharing and public-private initiatives associated with the security of critical infrastructure?
- What are the other national public-private partnerships established post 9/11 by foreign countries to cover against terrorism?
- Insurers are also challenged by the uncertain future of TRIA and therefore need to develop a long-term strategy for risk transfer as a function of different scenarios regarding the government role in providing protection against terrorism and other extreme events.

Two studies were proposed at the Roundtable for address the above questions and issues.

Understanding Firm Behavior There is an opportunity for the Wharton/Columbia team to study factors influencing buyers of terrorist coverage that will be undertaken in the near future by the U.S. Treasury Department. Such a study complements one that is currently underway on understanding insurer behavior. These studies should provide data for formulating a program that could replace TRIA. One could contrast the perception of risk by different firms with the risk assessments undertaken by AIR, EQECAT and RMS, using their terrorism models.

Airport Security A study could focus on an airport or a group of airports (possibly some hubs) for a case study to determine the types of protective measures that could be undertaken and their impact on the pricing and availability of insurance. Such a project would be of interest to Lockheed Martin and LexisNexis as part of the Radiant Trust project as well as insurers and reinsurers concerned with providing coverage to the airlines against losses from terrorism. It would be a case study for providing recommendations for a post-TRIA type program.

These studies would serve as points for interaction with Roundtable Sponsors over the coming months. The findings would be presented at the next Roundtable. The date of this meeting will be determined in consultation with Sponsors of the *Managing Extreme Events* project.

.....

Roundtable Participants

Name	Organization	Email
Elizabeth M. Abrams	Wharton School, Univ. of Penn	abramsme@wharton.upenn.edu
James Ament	State Farm Fire & Casualty Co.	james.ament.aamm@statefarm.com
Karen Clark	Applied Insurance Research, Inc.	kclark@air-worldwide.com
John DeMartini	Towers Perrin Reinsurance	demartj@towers.com
Neil A. Doherty	Wharton School, University of Pennsylvania	doherty@wharton.upenn.edu
David Durbin	Swiss Reinsurance Company	David_Durbin@swissre.com
Tom Gallagher	Wachovia Securities	tom.gallagher@wachovia.com
Geoffrey Heal	Columbia University	gmh1@columbia.edu
Carl G. Hedde	American Re-Insurance Company	chedde@amre.com
Ken Jenkins	American Re-Insurance Company	kjenkins@amre.com
Jim Johnson	EQE International, Inc.	jjjohnson@absconsulting.com
William Keogh	Risk Management Solutions	william.keogh@rms.com
Paul Kleindorfer	Wharton Risk Management and Decision Processes Center	kleindorfer@wharton.upenn.edu
Howard Kunreuther	Wharton Risk Management and Decision Processes Center	kunreuth@wharton.upenn.edu
Dennis Kuzak	EQE International, Inc.	dek@eqe.com
Joan Lamm-Tennant	GeneralCologne Re Capital Consultants	jlammten@gcr.com
Don Mango	American Re-Insurance Company	dmango@amre.com
Erwann Michel-Kerjan	Wharton Risk Management & Decision Processes Center	erwannmk@wharton.upenn.edu
Alex Muermann	Wharton School, Univ. of Penn	muermann@wharton.upenn.edu
Jack Seaquist	Air Worldwide Corporation	jseaquist@air-worldwide.com
Geoff Shaw	Lockheed Martin ISR	geoffshaw@attbi.com
Yuichi Takeda	Tokio Marine Management, Inc	yuichi.takeda@tokiom.com
Gordon Woo	Risk Management Solutions	gordon.woo@riskinc.com