## 8 References

ntwal, V. and Kunreuther, H (2000). "A CAT Bond Premium Puzzle?" *Journal of vchology and Financial Markets,* 1: 76-91.

mmins, J. D., Doherty, M., and Lo, A. (2002). "Can Insurers Pay for the 'Big ıe?' Measuring the Capacity of an Insurance Market to Respond to Catastrophic sses." *Journal of Banking and Finance,* 26: 557-583.

urance Services Office (1999). *Financing Catastrophe Risk: Capital Market Solutions* w York, N.Y.: Insurance Services Office.

y, A.D. (1952). "Safety-First and the Holding of Assets," *Econometrica*, 20: 431-9.

ndard & Poors (2000). *Sector Report: Securitization,* June.

ne, J. (1973). "A theory of capacity and the insurance of catastrophe risks: Part I d Part II," *Journal of Risk and Insurance* 40: 231-243 (Part I) and 40: 339-355 (Part

iss Re (2003). *Insurance-linked Securities* (New York: Swiss Re Capital Markets rporation).

iss Re (2004). *Insurance-linked securities quarterly* (New York: Swiss Re Capital ırkets Corporation) January.

S. General Accounting Office (2003). *Catastrophe Insurance Risks. Status of orts to Securitize Natural Catastrophe and Terrorism Risk.* GAO-03-1033. ıshington, D.C.: September 24.

# Chapter 10 – Extending Catastrophe Modeling To Terrorism

Major Contributors:
Howard Kunreuther
Erwann Michel-Kerjan
Beverly Porter

## 10.1 Introduction

Since the idea for this book was first conceived, the insurance industry and world were rocked by the events of September 11, 2001. While previous chapters have focused on the risk associated with natural disasters, at the core of this book is a more general problem: how to assess and manage risk associated with extreme events. This final chapter examines the unique challenges of extending catastrophe modeling to these types of risks by focusing on terrorism as well as the new challenges faced by the U.S for providing terrorism risk coverage after 9/11.

Section 10.2 discusses the impact of the 9/11 attacks on the insurance industry and the uncertainty regarding future terrorist activities. After discussing the nature of terrorism coverage in Section 10.3 and the differences between terrorism and natural disaster risk in Section 10.4, Section 10.5 turns to the passage of the U.S. Terrorism Risk Insurance Act of 2002 (TRIA). Section 10.6 discusses recent developments in terrorism modeling that can aid insurers and reinsurers in assessing insurance premiums and coverage limits, including a discussion of how models are used to establish insurance rates nationwide. Section 10.7 analyzes why the current demand for terrorism coverage has been at a low level since TRIA was passed. The chapter concludes with directions for future research for dealing with terrorism and other extreme events.

## 8 References

ntwal, V. and Kunreuther, H (2000). "A CAT Bond Premium Puzzle?" *Journal of vchology and Financial Markets,* 1: 76-91.

mmins, J. D., Doherty, M., and Lo, A. (2002). "Can Insurers Pay for the 'Big ıe?' Measuring the Capacity of an Insurance Market to Respond to Catastrophic sses." *Journal of Banking and Finance,* 26: 557-583.

ırance Services Office (1999). *Financing Catastrophe Risk: Capital Market Solutions* w York, N.Y.: Insurance Services Office.

y, A.D. (1952). "Safety-First and the Holding of Assets," *Econometrica*, 20: 431-9.

ndard & Poors (2000). *Sector Report: Securitization,* June.

ne, J. (1973). "A theory of capacity and the insurance of catastrophe risks: Part I l Part II," *Journal of Risk and Insurance* 40: 231-243 (Part I) and 40: 339-355 (Part

iss Re (2003). *Insurance-linked Securities* (New York: Swiss Re Capital Markets rporation).

iss Re (2004). *Insurance-linked securities quarterly* (New York: Swiss Re Capital ırkets Corporation) January.

S. General Accounting Office (2003). *Catastrophe Insurance Risks. Status of orts to Securitize Natural Catastrophe and Terrorism Risk.* GAO-03-1033. ıshington, D.C.: September 24.

# Chapter 10 – Extending Catastrophe Modeling To Terrorism

Major Contributors:
Howard Kunreuther
Erwann Michel-Kerjan
Beverly Porter

## 10.1 Introduction

Since the idea for this book was first conceived, the insurance industry and world were rocked by the events of September 11, 2001. While previous chapters have focused on the risk associated with natural disasters, at the core of this book is a more general problem: how to assess and manage risk associated with extreme events. This final chapter examines the unique challenges of extending catastrophe modeling to these types of risks by focusing on terrorism as well as the new challenges faced by the U.S for providing terrorism risk coverage after 9/11.

Section 10.2 discusses the impact of the 9/11 attacks on the insurance industry and the uncertainty regarding future terrorist activities. After discussing the nature of terrorism coverage in Section 10.3 and the differences between terrorism and natural disaster risk in Section 10.4, Section 10.5 turns to the passage of the U.S. Terrorism Risk Insurance Act of 2002 (TRIA). Section 10.6 discusses recent developments in terrorism modeling that can aid insurers and reinsurers in assessing insurance premiums and coverage limits, including a discussion of how models are used to establish insurance rates nationwide. Section 10.7 analyzes why the current demand for terrorism coverage has been at a low level since TRIA was passed. The chapter concludes with directions for future research for dealing with terrorism and other extreme events.

## 10.2 September 11, 2001: Impacts on Terrorism Insurance

Prior to the 9/11 attacks, terrorism coverage in the United States was included in most standard commercial policy packages without considering the risk associated with these events. The private insurance market had functioned effectively in the U.S. because losses from terrorism had historically been small and, to a large degree, uncorrelated. Attacks of a domestic origin were isolated and carried out by groups or individuals with disparate agendas.

None of these events created major economic disruption nor produced many casualties. The 1993 bombing of the World Trade Center (WTC) killed 6 people and caused $725 million of insured damages (Swiss Re, 2002). The Oklahoma City bombing of 1995, which killed 168 people, had been the most damaging terrorist attack on domestic soil, but the largest losses were to federal property and employees that were covered by the government. As a result, insurers and reinsurers did not have to pay close attention to their potential losses from terrorism in the United States prior to 9/11.

The terrorist attacks that day on the World Trade Center resulted in the death of nearly 3,000 people and inflicted damage estimated at nearly $80 billion. Approximately 40% of this amount was insured, resulting in the most costly event in the history of insurance (Lehman, 2004). The insurance industry was now confronted with an entirely new loss dimension. Reinsurers, who were liable for the lion's share of the claims, were for the most part unwilling to renew coverage and the few who did charged extremely high rates for very limited protection. Insurers unable to obtain reinsurance, or to raise sufficient capital either internally or from the capital markets, began to offer policies that explicitly excluded terrorism coverage.

The lack of available terrorism coverage had an immediate impact by delaying or preventing certain projects from going forward. For example, the U.S. General Accounting Office (GAO) noted a construction project that could not be started because the firms could not find affordable terrorism coverage (U.S. GAO, 2002). Several years after the event, the larger question being debated is whether terrorism is an insurable risk. That is, can insurers offer coverage at an affordable premium to potential insureds? If so, how does one go about determining how much to charge? Can one estimate the chances of another terrorist event occurring and the severity of insured losses?

Spectacular as were the 9/11 losses to the WTC and the Pentagon, do they represent a worst-case scenario? If some predictions concerning a possible chemical or biological attack become a reality, the answer is probably "no." Since March 2003, the U.S. government has issued clear warnings that additional terrorist attacks are likely, and indeed several have occurred including the deadly explosion at a nightclub in Bali that killed close



to 200 people in October 2002 and the large-scale attacks on trains in Madrid, Spain on March 11, 2004 that killed more than 200 people and injured more than 1,500 others (Kunreuther and Michel-Kerjan, in press).

## 10.3 The Nature of Terrorism Coverage

Another key question triggered by the events of 9/11 is the appropriate role of the private and public sectors in reducing losses and offering insurance protection against the impacts of terrorism (Kunreuther, Michel-Kerjan, and Porter, 2003). In Congressional testimony five months after the 9/11 attacks, Richard J. Hillman of the U.S. General Accounting Office indicated "both insurers and reinsurers have determined that terrorism is not an insurable risk at this time" (U.S. General Accounting Office, 2002).

The following scenario (with fictitious names) illustrates the challenges confronting private industrial companies in obtaining terrorism coverage prior to the passage of the Terrorism Risk Insurance Act (TRIA) in November 2002[1]:

> Over the past 10 years, the AllRisk (AR) Insurance Company has provided $500 million in coverage to Big Business (BB) Inc. against risks to its building, including those due to terrorism at a total premium of $13 million. AR covers $100 million itself and has purchased an excess-of-loss reinsurance contract from Reinsurance Enterprise (RE) to cover the remaining $400 million. Given the events of 9/11, RE has decided that terrorism will no longer be included in its coverage because of the uncertainties associated with the risk. BB needs terrorism coverage since the bank that holds its mortgage requires this as a condition for the loan. AR must decide whether or not to continue providing BB with the same type of insurance as it has had previously and, if so, how much coverage it is willing to offer and at what price.

This scenario raises the following questions regarding terrorism coverage:

- What factors determine whether the risk is insurable?
- How much capital will AR require in order to provide protection against terrorism?

[1] This scenario and the analysis of insurability issues associated with terrorism insurance are

### 10.3.1 Insurability Issues

As discussed in Chapter 2, insurers would be willing to provide insurance coverage if two conditions are met. First, they must be able to identify and quantify, or estimate at least partially, the risk (e.g., probability of an event occurring and the associated losses). Second, they must be able to set premiums for different classes of customers so the risk of insolvency is deemed acceptable.

In quantifying the risk from terrorist attacks, insurers can utilize an exceedance probability (EP) curve. However, it is considerably harder to construct an EP curve for terrorist activities than it is for natural disasters due to the difficulty in determining the likelihood of a terrorist attack. A potential target that may appear to have a high likelihood of attack, such as a trophy building, may also have a high level of protection and security which makes it less likely to be chosen by terrorists (Woo, 2002). So rather than trying to construct an EP curve, insurers normally turn to a scenario-based approach, by considering a range of terrorist-related events and estimating the likelihood of their occurrence and the resulting losses. Section 10.6 illustrates how catastrophe modeling can be utilized for constructing such scenarios.

### 10.3.2 Expanding Capacity Through Catastrophe Bonds

For insurers to provide their clients with the level of coverage offered prior to 9/11, they need to find new sources of capital. If the cost of this capital is high, the insurance premium will be prohibitively expensive and demand for coverage will dry up. To illustrate this point, it is useful to consider the scenario involving the AR Insurance Company providing terrorism coverage to BB Inc.

Now that RE has decided to eliminate terrorism coverage in its reinsurance treaties, AR has to determine how much protection it can offer BB and what price to charge for this coverage. The first concern of the underwriters at AR is to keep the firm's chance of insolvency below an acceptable risk level; profit maximization is of secondary interest. For AR to offer BB $500 million in coverage, it now has to raise an additional $400 million in capital.

One possibility would be for an investment bank to issue AR a $400 million catastrophe bond to cover the losses from a potential terrorist attack. As discussed in Chapter 7, a catastrophe bond requires the investor to provide upfront money that will be used by AR if a prespecified event, such as a terrorist attack, occurs. In exchange for a higher return than normal, the investor faces the possibility of losing either some or the entire principal invested in the catastrophe bond.

The amount paid out to AR depends on the design of the catastrophe bond. If investors are concerned with the ambiguity associated with terrorism risk, they will require a much larger than average return on their investment in



order to compensate them for the possibility of losing their principal. To determine the costs to AR of a cat bond one needs to specify the annual return on investment (ROI) required by investors of a catastrophe bond and compare it with the normal annual return on AR investments, which for illustrative purposes will be assumed to be 8%. The annual cost, C, to AR of obtaining $400 million through issuing a catastrophe bond would then be:

$$C = (ROI - 0.08)\$400$$

Suppose AR believes that the expected annual loss for providing $500 million of coverage is $1 million. Assuming a loading factor of $\lambda_{AR} = 0.5$, AR would have to charge an annual premium (in millions) of P = ($1 + C) (1.5). Table 10.1 shows how C and P are affected by different required ROIs of investors.

*Table 10.1.* Changes in return on investment (ROI) on catastrophe bond cost (C) and insurance premiums (P) (in millions)

| ROI | Catastrophe Bond Cost (C) | Premium (P) |
|---|---|---|
| 10% | $8 | $13.5 |
| 12% | $16 | $25.5 |
| 14% | $24 | $37.5 |
| 16% | $32 | $49.5 |
| 18% | $40 | $61.5 |
| 20% | $48 | $73.5 |

In the above example, it should be noted that the high premium is principally due to the cost (C) of borrowing money from the bond investors. During the fall of 2001, it was not unusual for an ROI to be as high as 20% on capital provided to insurers and reinsurers. The ROI has since declined, but even if it were only 12%, insurers would have to charge $25.5 million to BB for $500 million in terrorism coverage. This is almost twice the $13 million that BB was paying prior to 9/11.

### 10.3.3 Potential Role of Catastrophe Bonds

It is interesting to speculate as to why with the exception of a few issuances a market for catastrophe bonds to cover losses from terrorist attacks has not emerged since 9/11. Consider the case where an investment banker was issuing a one-year catastrophe bond for covering terrorism losses. Let $p$ represent a conservative estimate of the probability of a terrorist attack during a given year that would destroy BB's building, in which case the investor would lose the principal invested in a cat bond. If the normal annual rate of

return is 8%, a risk neutral investor who committed $Y to a catastrophe bond would require a ROI such that:

$$(1-p)(ROI)Y - pY = 0.08Y$$

Let $p_i$ be the annual probability of a terrorist attack where an investor is indifferent between receiving an annual ROI = $i$ % on a catastrophe bond knowing it would lose its entire investment should the attack occur. Substituting $i$ for ROI and $p_i$ for $p$ in the above equation and rearranging terms, $p_i$ becomes:

$$p_i = \frac{(i-0.08)}{(1+i)}$$

Thus, if $i$ = 10%= 0.10, then $p_{0.10}$ = 0.02/1.10 = 0.018 or 1.8%. If a risk neutral investor believes the annual probability of a terrorist attack is less than .018, an ROI of 10% would be an attractive investment. If $i$ = 20%= 0.20, then $p_{0.20}$ = 0.12/1.20 = 0.10 or 10%. This implies that if $p < .10$, a risk neutral investor would invest in a catastrophe bond if it returned 20% in the case of no terrorist attack. These indifference probabilities would be slightly lower if the investor were risk averse. Yet it is still hard to comprehend why the investment community has not viewed catastrophe bonds as a viable option for dealing with terrorism, particularly if the bond comprised only a small portion of the investor's portfolio.

In a recent paper, Bantwal and Kunreuther (2000) specified a set of factors that might account for the relatively thin market in catastrophe bonds in the context of natural hazard risks. They point out that spreads in this market are too high to be explained by standard financial theory, suggesting that they are not just a consequence of investor unfamiliarity with a new asset, but signal some deeper issues that need to be resolved before the catastrophe bond market can fully develop. In particular, the authors suggest that ambiguity aversion, myopic loss aversion, and fixed costs of education might explain the reluctance of institutional investors to enter this market.

Four additional factors may help explain the lack of interest in catastrophe bonds covering terrorism risk. There may be a moral hazard problem associated with issuing such bonds if terrorist groups are connected with financial institutions having an interest in the U.S. In addition, investment managers may fear the repercussions on their reputation of losing money by investing in an unusual and newly developed asset. Unlike investments in traditional high yield debt, money invested in a terrorist catastrophe bond can disappear almost instantly and with little warning. Those



marketing these new financial instruments may be concerned that if they suffer a large loss on the catastrophe bond, they will receive a lower annual bonus from their firm and have a harder time generating business in the future. The short-term incentives facing investment managers differ from the long-term incentives facing their employers.

A third reason why there has been no market for these catastrophe bonds is the reluctance of reinsurers to provide protection against this risk following the 9/11 attacks. When investors learned that the reinsurance industry required high premiums to provide protection against terrorism, they were only willing to provide funds to cover losses from this risk if they received a sufficiently high interest rate.

Finally, most investors and rating agencies consider terrorism models to be too new and untested to price a catastrophe bond. Reinsurers view terrorism models as not very reliable in predicting the frequency of terrorist attacks, although they provide useful information on the potential severity of the attacks under a wide range of scenarios. Furthermore, one of the major rating firms noted that the estimates derived from the models developed by AIR Worldwide, EQECAT and Risk Management Solutions could vary by 200% or more. Without the acceptance of these models by major rating agencies, the development of a large market for terrorist catastrophe bonds is unlikely (U.S. General Accounting Office, 2003).

## 10.4 Comparison of Terrorism Risk with Natural Disaster Risk

Although both terrorist activities and natural disasters have the potential to create catastrophic losses, there are some significant differences between these two risks. Two features of terrorism – information sharing and dynamic uncertainty – make it difficult for the private sector to provide insurance protection without some type of partnership with the public sector.

The sharing of information on the terrorism risk is clearly different than the sharing of information regarding natural hazard risk. In the latter case, new scientific studies normally are common knowledge so that insurers, individuals or businesses at risk, as well as public sector agencies, all have access to these findings. With respect to terrorism, information on possible attacks or current threats is kept secret by government agencies for national security reasons. One justification for government intervention in insurance markets relates to the asymmetry of information between buyers and sellers and the problems this may cause, such as adverse selection. In the case of terrorism, there is symmetry of non-information on the risk between those insured and insurers where government is the most informed party.

A principal terrorist goal is to destabilize a region or country by attacking certain targets that disrupt normal activities and create fear. Since

terrorists will adapt their strategy as a function of available resources and their knowledge of the vulnerability of the entity they are attacking, the nature of the risk changes over time, leading to *dynamic uncertainty* (Michel-Kerjan, 2003b). This feature, which translates into considerable ambiguity of risk, reflects an important difference from estimating natural hazards risks. Damage due to a future large-scale earthquake in Los Angeles can be reduced through adoption of mitigation measures; however, it is currently not possible to influence the occurrence of the earthquake itself. On the other hand, the likelihood of specific terrorist attacks will change over time as a function of the constellation of protective measures adopted by those at risk and actions taken by the government to enhance general security.

These characteristics of terrorism, along with the difficulty for insurers in finding new capital for covering this risk, raise the question as to how the government and the insurance industry can work together in providing protection and reducing future losses from these risks. The need for public-private partnerships was actually recognized in November 2002 when the Terrorism Risk Insurance Act of 2002 (TRIA) was passed.

## 10.5 Terrorism Risk Insurance Act of 2002

In the aftermath of the 9/11 attacks, many insurers warned that another event of comparable magnitude could do irreparable damage to the industry. By early 2002, 45 states permitted insurance companies to exclude terrorism from their policies, except for workers' compensation insurance policies that cover occupational injuries without regard to the peril that caused the injury. On the one-year anniversary of the 9/11 attacks, the U.S. remained largely uncovered (Hale, 2002). The President and the U.S. Congress viewed such a situation as unsustainable. If the country suffered future attacks, it would inflict severe financial consequences on affected businesses deprived of coverage. As a result, the U.S. Congress passed the Terrorism Risk Insurance Act of 2002 (TRIA).

### 10.5.1 Public-Private Risk Sharing under TRIA

While the passage of TRIA may have been welcome news for the business community, it was a mixed blessing for insurers who were obligated to offer coverage against terrorism to all their clients. The commercial establishments have the choice of either purchasing this coverage or declining it. Insured losses from property and contents damage and business interruption are covered under TRIA under the following conditions: 1) if the event is certified by the U.S. Treasury Secretary as an "act of terrorism" carried out by foreign persons or interests and 2) results in aggregate losses greater than $5 million.



Under TRIA's three-year term (ending December 31, 2005), there is a specific risk-sharing arrangement between the federal government and insurers[2] that operates in the following manner. First, the federal government is responsible for paying 90% of each insurer's primary property-casualty losses during a given year above the applicable insurer deductible (ID), up to a maximum of $100 billion. The insurer's deductible is determined as a percentage of the insurer's direct commercial property and casualty earned premiums for the preceding year. This percentage varies over the three-year operation of TRIA as follows: 7% in 2003, 10% in 2004, and 15% in 2005. The federal government does not receive any premium for providing this coverage.

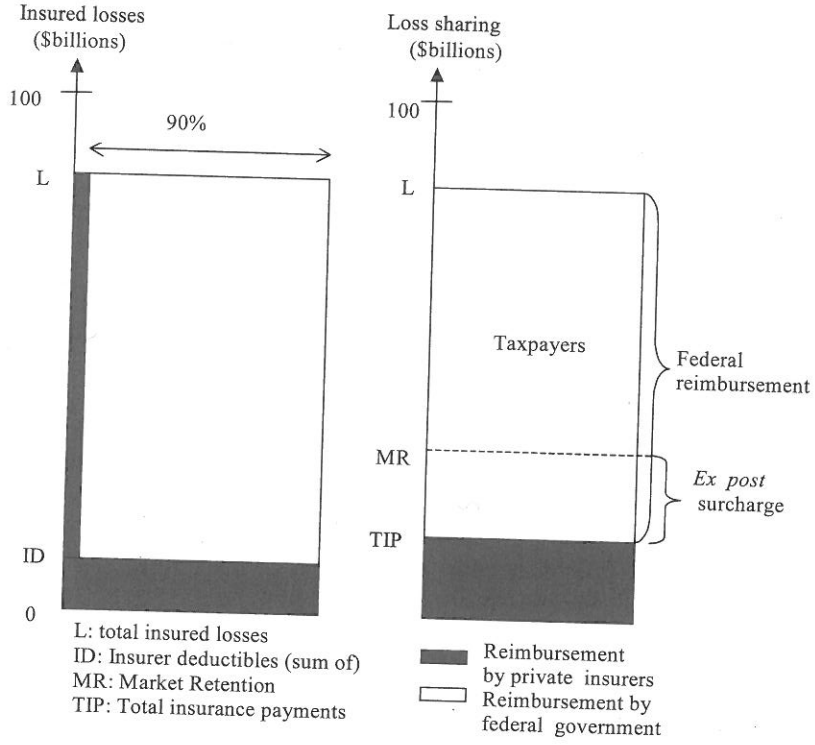


*Figure 10.1.* Loss sharing under TRIA.

Second, if the insurance industry suffers losses that require the government to cover part of the claims payments, then these outlays shall be partially recouped *ex post* through a mandatory policy surcharge. This

[2] Reinsurers are not part of TRIA but can provide coverage to insurers against their losses from terrorist attacks.

surcharge is applied on all property and casualty insurance policies whether or not the insured has purchased terrorism coverage, with a maximum of 3% of the premium charged under a policy. The federal government will pay for insured losses above a specific insurance marketplace retention amount (MR), as depicted in Figure 10.1. That amount evolves as follows: $10 billion in 2003, $12.5 billion for 2004, and $15 billion for 2005.

### 10.5.2 Challenge for Insurers and Firms: Quantifying the Residual Risk

Under TRIA, insurers were given 90 days after the legislation was enacted on November 26, 2002 to develop and disclose to policyholders new premiums and coverage terms. Many insurance companies found themselves in the situation of having to set a price for a risk they would rather not write. Although their exposure to terrorism risk is much reduced through the public-private partnership created by TRIA, it is still significant. Over the course of these 90 days, insurance companies followed a variety of strategies. Some determined that their exposures were not in high-risk locations and chose to leave existing premiums unchanged. Others with portfolio concentrations in major metropolitan areas deemed at high risk, such as New York, Washington, D.C., Chicago, and San Francisco, set very high premiums. In this situation, many businesses chose not to insure (Hsu, 2003; Treaster, 2003).

At the same time, many insurers and reinsurers have taken advantage of newly available tools designed to help them estimate their potential losses and therefore make rational and informed pricing decisions. Catastrophe modelers, leveraging their considerable experience and expertise in modeling natural hazard events, released the first generation of models to provide insurers with estimates of loss across multiple lines from terrorist attacks. The value of such models is in their ability to reduce uncertainty in risk estimates. One effect of that reduced uncertainty should be a lowering of premiums for terrorism insurance.

## 10.6 Catastrophe Models for Terrorism Risk

Insurance markets function best when losses are relatively small, random and uncorrelated, and when there is an abundance of historical loss data to which statistical techniques can be applied to predict future losses. As has been discussed throughout this book, when it comes to natural catastrophes, losses can be of catastrophic proportion and are often highly correlated. Furthermore, because such events occur infrequently, loss data are relatively scarce, making reliance on traditional actuarial techniques dubious at best.

As limited as the data is for nature catastrophes, there is much less information available on terrorist attacks for risk estimation purposes. To the



extent that historical data do exist and are available from such sources as the Federal Bureau of Investigation (FBI), the U.S. Department of State, the Center for Defense and International Security Studies (CDISS), and the Central Intelligence Agency (CIA), they may not be representative of current threats.

To explore the alternative approaches that modelers have used to overcome the challenges of quantifying terrorism risk, it is useful to begin with the simple modeling framework introduced in Chapter 2 and reproduced here as Figure 10.2.

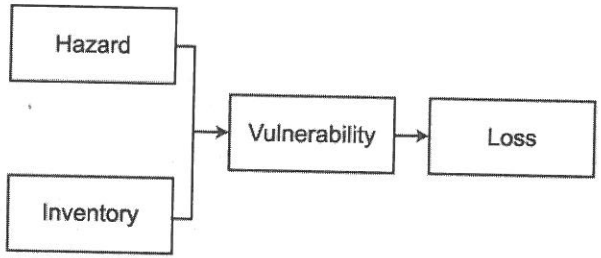


*Figure 10.2.* Catastrophe model components.

### 10.6.1 Terrorism Hazard

A terrorism model must first address three basic issues regarding the hazard itself: frequency of occurrence, the most likely locations of future terrorist attacks, and their severity in terms of insured loss. In undertaking this analysis, the different potential targets plus the interdependencies among networks and systems must be taken into account (Pate-Cornell and Guikema, 2002). For example, the loss of electric power or contamination of the water supply could create long-term business interruption risks and require residents in the affected areas to relocate.

The management of international terrorism risks has traditionally relied upon the experience and judgment of a specialist underwriter. For certain individual risks, recourse might be made on the advice of security professionals. For a portfolio, maximum loss would be carefully capped, but the overall risk assessment procedure would remain essentially qualitative and subjective. The most basic terrorism risk model is thus one encoded within the working experience of an underwriter and dependent on his personal expert judgment.

To cover rare catastrophic acts of terrorism, beyond the experience of even the most seasoned underwriter, the judgment of external terrorism experts might be invoked. Terrorism risk management would still be judgment-based, but the underwriter would be supported by the greater knowledge of terrorism experts. Recognizing that experts' risk estimates are

based on their own set of assumptions and may reflect a set of biases, the challenge is to evaluate these figures carefully in modeling terrorism risk. Terrorism models incorporate the judgment of teams of experts familiar both with available data and current trends. These experts have operational experience in counterterrorism at the highest national and international levels, with many specializing in terrorism threat assessment. Because each expert is privy to his own sources of intelligence and has his own security clearances, there is no common database of information upon which all experts can form their judgments. In fact, much of the crucial information is confidential.

*Determining Likelihood of Attacks*

To elicit expert opinion on the likelihood of attacks, several different approaches have been utilized. Some modeling firms employ the Delphi Method; others convene a conference of experts to capture and statistically combine various opinions into a useful and cohesive form that can be used to generate probabilities. For complex problems not governed by scientific laws, the judgment and intuition of experts in their field is not only an appropriate ingredient in any model, but a critical one.

The Delphi Method is a well-known and accepted approach developed by the RAND Corporation at the start of the Cold War. Among its first applications was the forecasting of inter-continental warfare and technological change. The Delphi Method comprises a series of repeated interrogations, usually administered by questionnaire, where the responses are anonymous. Direct interaction between the participants is precluded to eliminate the natural bias of following the leader. After an initial round of interrogation, individuals are encouraged to reconsider and, when appropriate, to change their views in light of the replies of all the others that are shared with everyone in the group (Adler and Ziglio, 1996). While the methodology is highly structured, the final estimates by each participant still only represent opinions, informed by other members of the group.

Experts are asked to weigh in on several aspects of event frequency and intensity: the number of attacks per year, the type of target, the attack mode or weapon type, and finally the specific target of each potential attack. Each of these issues depends in part on the nature of the terrorist organization originating the attack. Critical to the results is the team's operational understanding of the likely terrorist actions in the context of the current state of security countermeasures. Targets and attack methods that were once undefended may now be more vigorously protected by federal homeland security, state and local policy, and private security resources.

An alternative to the Delphi Method is using a conference of experts where participants can exchange views. The agenda is usually topics, such as the kind of weapons a specific terrorist group is more likely to use or what areas/countries are more susceptible to attack. When some experts are unable



to attend the conference, their judgment can be elicited separately and fed back to others using the Delphi Method.

The lack of historical data makes the use of experts the only way for modelers to determine the likelihood of new attacks. However, experts have their own limitations in forecasting future behavior, as each of them has specialized knowledge. Some are much more focused on a given terrorist group and disregard dangers from others. Others are specialized on a given type of weapon or on a very specific kind of biological or chemical agent. In other words, each expert can be accurate within his or her small window of expertise, but the whole group of experts can be wrong about the reality of the global threats -- a kind of illusory expertise (Linstone and Turoff, 1975).

Another pitfall is the possible optimism/pessimism bias of experts. For instance, if a terrorist attack recently occurred, a natural trend would be to overestimate the likelihood of new attacks in the short run. Conversely, if a governmental agency arrested leaders of a terrorist group, a natural bias could be to concentrate only on that group and overlook other terrorists, resulting in misconceptions of the likelihood of other attacks.

*Identifying Likely Targets and Attack Modes*

Obviously target types vary depending on the nature and goals of the individual terrorist groups or organizations, not only because of differences in the resources at this group's disposal, but because of its different political agenda.

Once the target types are identified, databases of individual potential targets are developed. In the case of terrorism, targets within the U.S. might include high profile skyscrapers, government buildings, airports, chemical plants, nuclear power plants, dams, major tunnels and bridges, large sports stadiums, major corporate headquarters, and marine terminals. Trophy targets normally represent a higher value to the terrorists due to the publicity associated with them, and they therefore have a higher probability of attack, other things being equal. Target databases can comprise tens of thousands or even hundreds of thousands of structures.

In the simulations developed by modelers, the terrorist group receives value or utility from the damage inflicted on its adversaries. The expected loss is determined by the probability of success in carrying out the attack and the economic and psychological value of the target. In turn, the probability of success is determined not only by the amount of resources the terrorist group allocates to the attack, but also by the resources its opponent allocates to detecting terrorist activity and defending the target. Both parties are constrained by the funds and people-power at their disposal and the "model" becomes one of strategic decisions as to how to deploy those resources, i.e. which targets to attack and with what weapons, and which to defend. Game theory can thus be used to analyze likely targets and attack modes.

The severity of the attack is a function of the weapon type. Modeled weapon types include so-called conventional weapons, such as package, car and truck bombs, as well as aviation crash. In light of Al Qaeda's clearly expressed interest in acquiring and deploying weapons of mass destruction, models also account for the possibility of non-conventional weapon attacks including chemical, biological, radiological, and nuclear (CBRN) weapons (Central Intelligence Agency, 2003).

### 10.6.2 Inventory

The 9/11 attacks revealed that not only are the terrorist targets themselves at risk, but so are the surrounding buildings. Nevertheless, the effects of terrorist attacks with conventional weapons are likely to be highly localized compared to natural disasters such as hurricanes and earthquakes. The resulting damage depends on such things as the kind of explosive material used, the amount of material, and the density and verticality of the surrounding buildings. For non-conventional weapons, the spatial extent of damage depends on the delivery mechanism and on external factors such as wind speed and wind direction.

Terrorism models can estimate total losses as well as aggregate insured or insurable losses for individual buildings, insurance company portfolios, and/or the entire insurance industry. While the large losses resulting from natural catastrophes have historically been to property, terrorist attacks can affect multiple insurance lines that include life, liability, workers' compensation, accident, and health, as was the case on 9/11. They can also result in severe stress on the psyche of a nation under siege.

The databases that are utilized in natural catastrophe models are also relevant for terrorism models. Modelers have developed industry databases of employees by building occupancy and construction type at the ZIP code level. These can be supplemented with state payroll and benefit information, generally available to insurance companies, to create an inventory at risk. Since 9/11, modelers are emphasizing to insurers the importance of gathering detailed data on the buildings they insure and the employees who work in them (Insurance Accounting, 2003).

### 10.6.3 Vulnerability

Research on the impact of explosives on structures has been ongoing since the 1950s. The Department of Defense and the Department of State have examined blast loading in the course of developing anti-terrorism designs for U.S. embassies. In addition, research activity has surged since the bombing of the Alfred P. Murrah Federal Office Building in Oklahoma City (1995) and the U.S. military housing facilities in Dhahran, Saudi Arabia (1996) (Olatidoye et al., 1998).



Modelers have developed damage functions that incorporate historical data from actual events combined with the results of experimental and analytical studies of how different building types respond to such attacks. In the case of a terrorist attack using conventional and nuclear weapons, buildings sustain damage as a result of a variety of assaults on their structural integrity and their non-structural components. In the case of non-conventional weapons, the structure of the building is likely to be unaffected, but the resulting contamination may render it unusable for long periods and result in extensive cleanup costs. In either case, the damage functions determine loss to building, contents, and loss of use.

*Conventional Weapons*

In terrorism modeling, damage is a function of the attack type and building type. The type of attack, whether package, car or truck bomb, can be expressed as a TNT-equivalent. The size of this charge can be thought of as the intensity of the event. Damage to the target building results from the shock wave, the subsequent pressure wave, and fire.

The target building may sustain total damage from the point of view of insured loss even if it remains standing. If the building collapses, however, it would increase the number of fatalities. Furthermore, different modes of collapse, such as an overturn versus a pancake collapse, will affect the degree of damage to surrounding buildings and thus the total area affected by the event. The buildings surrounding the target building are also likely to be damaged by the resulting shock and pressure waves and/or by falling or flying debris.

*Non-conventional Weapons*

The effects of nuclear weapons on both structures and populations have been the subject of extensive research for decades (Glasstone and Dolan, 1977). Chemical, biological and radiological (CBR) attacks are more problematical and only a few accidental releases of chemical agents, such as the one that occurred at the Union Carbide chemical plant in Bhopal, India (1984) have been analyzed. Other events include the 1995 sarin attack in the Tokyo subway and the more recent distribution of anthrax through the mail in autumn 2001 in the U.S. (U.S. Department of State, 2003). These examples provide data for empirical analysis and research. Fortunately, those attacks have been extremely rare so there is limited historical data.

Some modelers have developed relationships between the use of non-conventional weapons and potential damage; others employ models developed for various government agencies that follow what is known as a source/transport/effects approach. The "source" refers to how a hazard agent originates, including the type, yield, effectiveness, and other properties of the agent. Various attack types are simulated, including chemical agents such as

sarin, VX, tabun, biological agents such as anthrax and smallpox. Nuclear and radiological agents such as cesium, cobalt and plutonium are also simulated (Central Intelligence Agency, 2003).

"Transport" refers to the means by which the agent disperses or moves from the source to the people or facilities presumed to be the targets. A full range of mechanisms is considered ranging from mail-borne dispersal to wide area dissemination via aerosol spraying and conventional bomb blast. "Effects" refers to the physical, performance, and psychological impact of the attack on humans as well as on the environment. While even a small suitcase nuclear device can cause extensive physical damage to buildings over a relatively large geographical area, the primary effects of other non-conventional weapons is contamination, which may render the structures unusable for long periods of time as discussed. In fact, in some cases, the most cost-effective way of dealing with badly contaminated buildings may be demolition under very cautious and well-defined procedures.

### 10.6.4 Workers' Compensation Loss

In addition to property damage, terrorism models estimate fatalities under both workers' compensation and life insurance policies, as well as losses from injuries arising from personal accident and other casualty lines. The number of injuries and fatalities, as well as the severity of injuries, is a function of the nature of damage sustained by the structural and non-structural components of buildings and their contents. Figure 10.3 illustrates the process for computing workers' compensation loss.

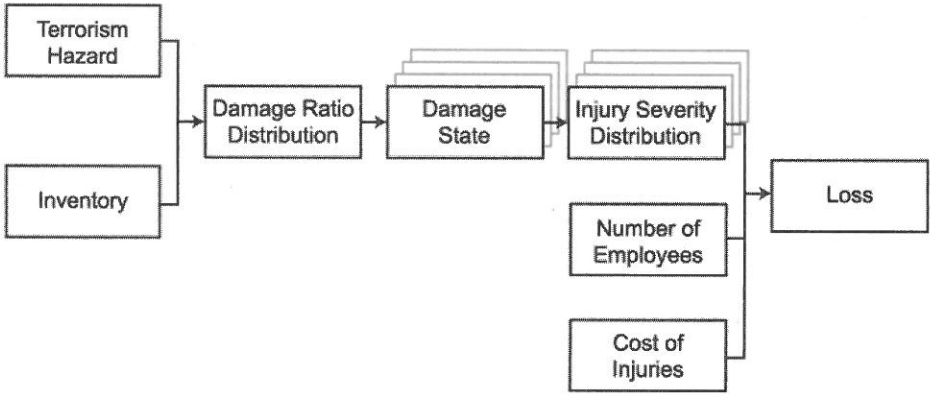


*Figure 10.3.* Modeling workers' compensation loss.

In estimating workers' compensation loss, models account for variability in damage to individual buildings so that one can estimate the extent of injuries and fatalities. For each level of severity, a mean damage ratio is calculated along with a probability distribution of damage. Because



different structural types will experience different degrees of damage, the damage functions vary according to construction materials and occupancy. A distribution of damage for each structure type is mapped to different damage states. These may be, for example, slight, moderate, extensive and complete, as shown in Figure 10.4 for a specific building.

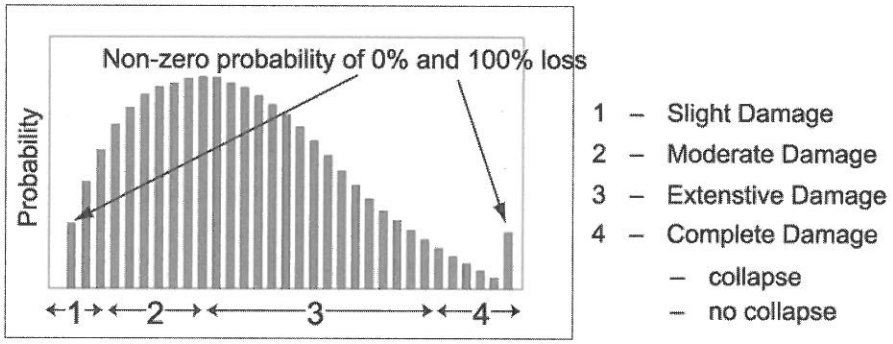


*Figure 10.4.* Building damage distribution mapped to different damage states.

At the level of complete damage, the building may or may not have collapsed. Complete damage means that the building is not recoverable. Collapse will typically result in more severe injuries and larger numbers of fatalities than if the building is still standing. Estimates of workers' compensation (and other casualty lines) loss are based not only upon the number of people injured, but also on the severity of the injuries, such as minor, moderate, life threatening and fatality. Distributions of injury severity are then developed for each damage state for each building and occupancy type.

By combining information on the number of employees in each damaged building and the cost of injuries, the model generates the total loss distribution for a particular structure. Losses are calculated based on the number of employees in each injury severity level and on the cost of the injury as shown in Figure 10.5. To calculate losses arising from life insurance and personal accident claims, potential losses are calculated for both residential and commercial buildings. These calculations use assumptions about the distribution of the population between these two types of structures at the time of the attack.

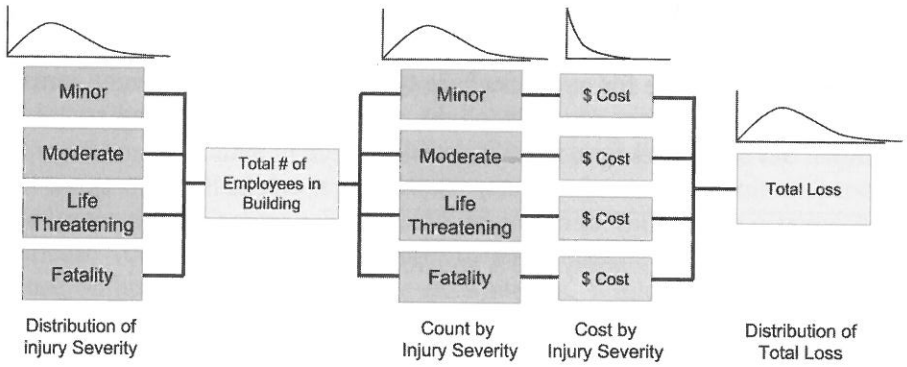


*Figure 10.5.* Calculation of workers' compensation loss for an individual building.

### 10.6.5 The ISO Advisory Loss Costs

Loss estimates generated by terrorism models are of interest to all parties. The insureds would like a better understanding of their exposure to potential terrorist attacks in order to determine whether to purchase coverage. Insurers can use model output to develop their pricing, reinsurance needs, and fashion policy conditions such as deductibles, exclusions, and coverage limits. Model output is also of interest to policy makers. In New York City for example, modeled loss estimates have been used to support a request for a larger share of federal funding for homeland security.

Since these terrorism models have been applied to thousands of potential targets, they can provide a picture of the relative risk by state, city, ZIP code and even by individual location. The Insurance Services Office (ISO) used the estimates provided by one of its subsidiaries, AIR Worldwide, to file commercial property advisory average loss costs with the insurance commissioner for each state at the end of 2002.[3] ISO defined three tiers for the country, with certain areas within Washington, DC, New York, Chicago and San Francisco in the highest tier, with assigned loss costs of approximately $0.10 per $100 of property value. A second tier consisted of Boston, Houston, Los Angeles, Philadelphia and Seattle as well as other portions of the highest rated cities; the rest of the country fell into the third tier.

In pre-filing discussions with regulators, ISO's advisory loss costs were challenged by some regulators who felt that such premiums would

[3]A *loss cost* is defined by ISO as that portion of a rate that does not include provision for expenses (other than loss adjustment expenses) or profit. It may be used by ISO companies as a starting point to set insurance rates, after reflection of company-specific expenses and profit. Once an ISO advisory loss cost has been approved by a state, an ISO participating insurance company can usually adopt it without having to undertake its own often lengthy and expensive rate filing process.



lead businesses to relocate to other areas (Hsu, 2003). Negotiations ensued and compromises were made. ISO filed loss costs for first-tier cities based on zip code level model results, which differentiated between the higher risk of downtown city centers and the lower risk of properties on the outskirts. But nowhere did the filed loss costs exceed $0.03 per $100 of property value.[4] Thus, while the new official advisory average loss costs no longer adequately reflected the risk in the eyes of the modelers, they became more palatable to other stakeholders. The Departments of Insurance in all 50 states eventually approved these ISO advisory loss costs that covered the years 2003, 2004, and 2005.

## 10.7 Low Insurance Demand for Terrorism Coverage

When Congress passed the Terrorist Risk Insurance Act (TRIA) in November 2002, the expectation was that it would ease insurers' concerns about suffering large losses from another extreme attack and then enable buyers at risk to purchase coverage at reasonable prices. However, the demand for coverage has been much lower than anticipated even though insurance is now available nationwide under the TRIA requirement (Hsu, 2003; Treaster, 2003).

### 10.7.1 Empirical Evidence

The Council of Insurance Agents and Brokers (CIAB) undertook the first national survey on the level of demand for terrorism coverage at the beginning of 2003 (CIAB, 2003a). At the time, almost half of its members that handle the largest accounts (customers who pay more than $100,000 annually in commission and fees to the broker) indicated that less than 1 in 5 of their customers had purchased terrorism insurance. The low demand was even more pronounced for smaller companies (less than $25,000 in commission and fees to the broker). Only 65% of the brokers indicated that less than 1 in 5 customers were purchasing insurance against terrorism.

According to another national survey by the CIAB undertaken during the spring of 2003, 72% of the brokers indicated that most of their commercial customers were still not purchasing terrorism insurance coverage even in locations like New York City (CIAB, 2003b). A survey by Marsh Inc. of 2400 of its policyholders revealed that 29.3% of them had purchased terrorism insurance in 2003 (Marsh, 2004). If this level of demand continues, a severe terrorist attack will likely have a more devastating effect on business continuity today than after 9/11.

Although TRIA limits the potential losses to the insurance industry, some insurers are still concerned about the impact of a large terrorist attack on

[4]The second tier (third tier) settled at $0.018 ($0.001) per $100 of property value.

the solvency of their firms and their ability to pay. Some businesses are concerned not only with acts of terrorism certified by the federal government, but also by the prospect of "domestic terrorism", such as an attack similar to the Oklahoma City bombings in 1995, which would not be covered by TRIA. The market for domestic terrorism is still mixed with some insurers offering coverage (sometimes at no cost if the risk is perceived to be low) while others simply excluding it (CIAB, 2003a). In the latter case, businesses may prefer not to buy any terrorism coverage than partial protection.

### 10.7.2 Heuristics and Biases

Since most businesses have little or no information on terrorism risk and no new attack since 9/11 has occurred on U.S. soil at the time this book goes to press, firms may perceive the chances of another event to be extremely low. This behavior has been well documented for natural hazards where many individuals buy insurance after a disaster occurs and cancel their policies several years later if they have not suffered a loss It is hard to convince them that the best return on an insurance policy is no return at all. In other words, there is a tendency for most people to view insurance as an investment rather than as a form of protection (Kunreuther, 2002).

A few years after 9/11, concern with damage from terrorism appears to have taken a back seat. In 2003, most firms believed that if a terrorist attack occurred, it would not affect them, whereas in the first few months after 9/11, they had the opposite belief. The aforementioned CIAB study indicated that more than 90% of the brokers said that their customers eschew terrorism insurance because they think they don't need it (CIAB, 2003b). These firms consider insurance, even at relatively low premiums, to be a bad investment. The expectation that government may financially aid affected businesses whether or not they are covered by insurance, as illustrated by the airline industry following 9/11, may also contribute to limited interest in spending money on coverage.

There seems to be a large difference in the perception of the seriousness of the terrorist threat by those who are potential buyers of insurance and those who are supplying coverage. In these circumstances, TRIA will not solve the problem. To create a market for terrorism insurance, both buyers and sellers need to do a more systematic analysis of the relationship between the price of protection and the implied risk. There is no guarantee that firms will be willing to pay more for coverage or that insurers will greatly reduce their premiums. But there is a much better chance that a larger market for terrorism coverage will emerge than if the status quo is maintained (Kunreuther and Michel-Kerjan, in press).

The U.S. Treasury Department is required by Congress to undertake studies of the supply and demand for terrorism coverage so that more informed decisions on the renewal of TRIA in 2005 may be made. Those



studies, launched in December 2003, should contribute to better understanding the current level of demand for terrorism insurance, as well as to suggest possible improvements in the partnership to create a more stable insurance market should another attack occur.

## 10.8 Future Research Directions

This concluding section suggests future research for dealing with terrorism and other extreme events, such as natural disasters, by focusing on three areas: vulnerability analyses, risk perception and interdependencies.

### 10.8.1 Vulnerability Analyses

Risk assessment needs to be supplemented by vulnerability analyses that characterize the forms of physical, social, political, economic, cultural, and psychological harms to which individuals and modern societies are susceptible. Modeling events with considerable uncertainty and ambiguity creates discomfort in undertaking risk assessments. Constructing scenarios that may lead to the occurrence of specific events is a useful first step.

A meaningful example of work in this regard is a study undertaken over 25 years ago by Warner North and his colleagues on estimating the likelihood of microbial contamination of Mars from the first Viking mission, where a landing on the planet was planned on July 4, 1976. They first constructed a series of scenarios characterizing how microbes could contaminate Martian soil based on the possible location of microbes on the spacecraft and Martian environmental conditions. They then assigned probabilities of contamination to each of these scenarios and undertook extensive sensitivity analyses to determine how changes in the inputs to these scenarios would lead to changes in these probabilities. On the basis of these analyses, they determined that the probability of contamination was more than one order of magnitude below the predetermined acceptable level of risk of 1 in 10,000. Scientists who had initially expressed concern about the risk of contamination agreed that the mission should proceed without the need for further steps to reduce the microbial burden on the Viking. The Viking successfully landed on Mars in the summer of 1976.

### 10.8.2 Risk Perception

The terrorist attacks of 9/11 have raised the question as to what should be done to mitigate the consequences of future catastrophes and aid the recovery process should another disaster occur. In order to develop a strategy, incorporating the growing knowledge of how individuals process information on extreme events and then make choices regarding mitigation is necessary.

As illustrated by the examples of Hurricane Andrew and the Northridge earthquake, people are not very concerned about the possibility of catastrophe events before they occur. They want to take protective action only after the event and this concern dissipates over time. To reduce the consequences of natural disasters, safer structures can be built and/or people can move out of harm's way. To mitigate the consequences of chemical accidents, the inventory level and/or production of specific toxins can be reduced to lower the risk of another mishap occurring.

Taking steps to reduce the risk of future terrorist activities is more difficult than for natural disasters or industrial accidents. Considerable uncertainty exists with respect to who the perpetrators are, their motivations, the nature of their next attack and where it will be delivered. Terrorist groups can attack anything, anywhere, at any time, and not everything can be protected. Additionally, there are challenges associated with allocating resources for dealing with terrorism risk. The government may be tempted to invest huge sums of money in protection to provide reassurance for its citizens (i.e., reassuring expenditures). Educating the public on the current likelihood of attacks might reduce such costs. On the other hand, actions taken by government services to curb terrorism might not be publicly revealed to protect national security.

### 10.8.3 Interdependencies

The antecedents to catastrophes can be quite distinct and distant from the actual disaster, as in the case of the 9/11 attacks, when security failures at Boston's Logan airport led to crashes at the World Trace Center (WTC), Pentagon, and rural Pennsylvania. The same was true in the case of recent power failures in the northeastern US and Canada, where the initiating event occurred in Ohio but the worst consequences were felt hundreds of miles away.

Future research should address the appropriate strategies for dealing with situations where there are interdependencies between agents (persons, organizations, countries). In these situations, there may be a need for the public sector to take the leading role with respect to providing protective measures because the private sector may have few economic incentives to take these steps on their own. Kunreuther and Heal (2003) have addressed this issue by asking the following question: What economic incentives do residents, firms or governments have for undertaking protection if they know that others are not taking these measures and that their failure to do so could cause damage to them?

To illustrate this point, suppose Airline A is considering whether to institute a sophisticated passenger security system knowing that passengers who transfer from other airlines may not have gone through a similar screening procedure and could cause damage to its airplane. If there is no



screening process for passengers who transfer from one airline to another and there is a relatively high probability that these dangerous passengers could get on board Airline A due to the failure of other airlines to adopt screening systems, then Airline A will also not want to invest in such a system. The interdependent risks across firms may lead all of them to decide not to invest in protection.

The 9/11 events and the anthrax attacks during the fall of 2001 also demonstrated a new kind of vulnerability. Terrorists can use the capacity of a country's critical infrastructures to have an immediate large-scale impact on the nation by reversing the diffusion capacity of the networks and turn them against the target population so that every aircraft and every piece of mail now becomes a potential weapon (Michel-Kerjan, 2003a). During the anthrax episode, the attackers used the U.S. Postal Service to spread threats throughout the country and abroad. The entire network was potentially at risk as any envelope could have been considered to be contaminated by anthrax (Boin, Lagadec, Michel-Kerjan and Overdijk, 2003).

The emerging vulnerabilities in critical infrastructures raise challenging questions related to strategies for mitigation given the large operating networks associated with the water supply, electricity, transportation networks, telecommunications, banking and finance, energy, emergency, and defense services. The social and economic continuity of a nation's activities critically depend on their operation (OECD, 2003; Michel-Kerjan, 2003a; White House, 2003).

Future research should examine the nature of these interdependencies as well as the appropriate role of regulations, standards, third party inspections, and insurance to encourage individuals and firms to take protective actions. Without some type of coordinating mechanism, or economic incentives such as a fine, subsidy or tax, it may be difficult to convince any individual group to invest in mitigation because they know others may contaminate them.

To better understand these interdependencies at a managerial level, it would be meaningful to organize international strategic debriefings much more systematically after an extreme event or a large-scale threat occurred with senior-executives who were in charge and with academic experts. Every threat offers an opportunity to learn and be collectively prepared (Lagadec and Michel-Kerjan, 2004).

While launching such initiatives requires expertise and commitment by the top-management of organizations, it would help to learn more about these emerging risks and to examine more adequate global security strategies given limited resources. By developing trusted public-private partnerships to deal with interdependencies associated with extreme events substantial benefits can be provided to the affected individuals and firms as well as improving the social welfare.

## 10.9 References


Adler, M. and Ziglio, E. (eds) (1996). *Gazing Into the Oracle: The Delphi Method and Its Application to Social Policy and Public Health*, London, Kingsley Publishers.

Bantwal, Vivek and Kunreuther, Howard (2000). "A Cat Bond Premium Puzzle?" *Journal of Psychology and Financial Markets*, 1: 76-91.

Boin, A., Lagadec, P., Michel-Kerjan, E., and Overdijk, W. (2003). "Critical Infrastructures under Threat: Learning from the Anthrax Scare" *Journal of Contingencies and Crisis Management,* 11 (3): 99-105.

Central Intelligence Agency (2003). "Terrorist CBRN: Materials and Effects (U)", CIA: Directorate of Intelligence, May 2003, CTC 2003-40058.

Council of Insurance Agents and Brokers (2003a). "Many Commercial Interests Are Not Buying Terrorism Insurance, New CIAB Survey Show" News Release, March 24.

Council of Insurance Agents and Brokers (2003b). "Commercial Market Index Survey" News Release, July 22.

Glasstone, S. and Dolan, P. J. (eds.) (1977). *The Effects of Nuclear Weapons*, Third Edition, 1977, Prepared and published by the United States Department of Defense and the United States Department of Energy.

Hale, D. (2002). "America Uncovered" *Financial Times*, September 12.

Hsu, S. (2003). "D.C. Disputes Insurance Study Raising Rates For Terrorism" *Washington Post*, January 7, page A01.

Insurance Accounting (2003). "Knowledge a Key for Terror Risk Pricing", January 27, 2003, Thomson Media.

Kunreuther, H. and Michel-Kerjan, E. (in press). "Policy Watch: Challenges for Terrorism Risk Coverage in the U.S." *Journal of Economic Perspectives.*

Kunreuther, H. and Heal, G. (2003). "Interdependent Security" *Journal of Risk and Uncertainty,* 26(2/3): 231-249.

Kunreuther, H. (2002). "The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage" *Risk Analysis*, 22: 427-437.

Kunreuther, H., Michel-Kerjan, E. and Porter, B. (2003). "Assessing, Managing and Financing Extreme Events: Dealing with Terrorism", *Working Paper 10179*, National Bureau of Economic Research, Cambridge, MA.

Lagadec, P. and Michel-Kerjan, E. (2004). "A Framework for Senior Executives To Meet the Challenge of Interdependent Critical Networks Under Threat: The Paris Initiative, 'Anthrax and Beyond'." Working Paper, WP #2004.28, Center for Risk Management and Decision Processes, The Wharton School, Philadelphia.





Lehmann, Raymond. (2004). "Twin Towers Insured Loss Estimate Drops to Between $30 and $35 Billion", Bestwire, May 10.

Linstone, H. and Turoff, M. (1975). *The Delphi Method. Techniques and Applications.* Addison-Wesly Publishing Company.

Major, J. (2002). "Advanced Techniques for Modeling Terrorism Risk" Journal *of Risk Finance,* 4 (1): 15-24.

Marsh Inc. (2004). "Marketwatch: Property Terrorism Insurance," April 2004.

Michel-Kerjan, E. (2003a). "New Vulnerabilities in Critical Infrastructures: A U.S. Perspective" *Journal of Contingencies and Crisis Management,* 11 (3): 132-140.

Michel-Kerjan, E. (2003b). "Large-scale Terrorism: Risk Sharing and Public Policy" *Revue d'Economie Politique*, 113 (5): 625-648.

Olatidoye, O., Sarathy, S., Jones, G., McIntyre, C., Milligan, L. (1998). "A Representative Survey of Blast Loading Models and Damage Assessment Methods for Buildings Subject to Explosive Blasts", Clark Atlantic University, Department of Defense High Performance Computing Program, CEWES MSRC/PET TR 98-36.

Organisation for Economic Co-operation and Development (2003). *Emerging Systemic Risks in the 21st Century: An Agenda for Action*. Paris: OECD.

Pate-Cornell, E. and Guikema, S. (2002) "Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures" *Military Operations Research*, 7: 5-20. December.

Swiss Re (2002). *Natural catastrophes and man-made disasters 2001: man-made losses take on a new dimension*, Sigma No1, Zurich: Swiss Re.

Treaster, J. (2003). "Insurance for Terrorism Still a Rarity" *New York Times*, March 8.

U.S. Department of State (2003). *Patterns of Global Terrorism 2002*. April 2003.

U.S. General Accounting Office (2003). *Catastrophe Insurance Risks. Status of Efforts to Securitize Natural Catastrophe and Terrorism Risk.* GAO-03-1033. Washington, D.C.: September 24.

U.S. General Accounting Office (2002). "Terrorism Insurance: Rising Uninsured Exposure to Attacks Heightens Potential Economic Vulnerabilities", Testimony of Richard J. Hillman Before the Subcommittee on Oversight and Investigations, Committee on Financial Services, House of Representatives. February 27.

White House (2003). *National Strategy for Physical Protection of Critical Infrastructures and Key Assets Washington*, DC, February 2003.

Woo, G. (2002). "Quantitative Terrorism Risk Assessment" *Journal of Risk Finance,* 4 (1): 7-14.