

# **THE VIABILITY OF TERRORISM RISK MODELING: A FIVE-YEAR RETROSPECTIVE**

*Dr. Gordon Woo*

*Risk Management Solutions,  
Peninsular House, 30 Monument Street,  
London EC3R 8NB, U.K.*

World Jurist Association  
Conference on Terrorism and the Rule of Law  
Edinburgh, May 22 - 24 , 2006

## CONTENTS

|  |    |
|--|----|
| INTRODUCTION                                 | 2  |
| TERRORIST TARGETING                          | 4  |
| TERRORIST WEAPONRY                           | 5  |
| LAW ENFORCEMENT MITIGATION OF TERRORISM RISK | 6  |
| THE FREQUENCY ISSUE                          | 7  |
| ANALYSIS OF TERRORIST NETWORKS               | 9  |
| TERRORISM BEYOND 2007                        | 11 |

## INTRODUCTION

The five-year anniversary of 9/11 marks a milestone in terrorism insurance risk assessment. As a form of political violence, terrorism has existed as long as the insurance industry, but its catastrophic multi-billion dollar insurance loss potential was demonstrated for the first time on 9/11. If this cataclysm were just an isolated aberration, akin to a freak meteorite strike, then insurers could gradually adjust back to an earlier perception of world order. Sadly, this is not the case: terrorism is now a global catastrophe insurance risk, and it is here to stay for the medium term, at least. In the words of the head of counter-terrorism at the Metropolitan Police, Peter Clarke, spoken after the 2005 London bombings, *'The belief that the threat posed by Al Qaeda may be over in a decade is hopelessly optimistic, fifty years is a more realistic time scale for continuing Al Qaeda activity'*.

Fifty years is an order of magnitude longer a time horizon than the interim Terrorism Risk Insurance Act (TRIA), which has been drafted and renewed with a specified short-term sunset. Of all the complex issues that have been raised in the deliberations over TRIA, one which falls squarely within the domain of the catastrophe risk analyst is the capability of insurance risk modeling agencies to quantify terrorism risk in a meaningful way, with bounded uncertainty, to facilitate prudent insurance underwriting and risk management.

The widespread reluctance of insurers to provide cover against deliberate acts of terror is driven by a range of factors, not least actuarial misgivings over the possibility of quantifying terrorism risk reliably. Consequently, the capital allocation requirements for terrorism risk underwriting may be a serious concern to insurers and rating agencies alike. The viability of terrorism insurance risk modeling is a necessary, but not sufficient, condition for terrorism insurance to be commercially viable. As the menacing hazard events of 2005 have indicated, the solvency of an insurer may be threatened in other ways, for example by a natural hazard event of gargantuan proportions, or indeed by a global influenza pandemic. However, with these perils, there is no underlying malicious intent to cause catastrophic loss, which is the distinctive feature of terrorism. Modeling terrorist behavior in a robust quantitative manner is the key challenge for catastrophe risk analysts.

In the immediate aftermath of 9/11, the shock of the horrific event was deepened for insurers by the stark realization that no capability for quantitative terrorism risk modeling existed. Compiling statistics of terrorism crimes is one thing, constructing a catastrophe model of terrorism is another. Driven by the expectations and needs of the insurance industry, construction work on terrorism models began with an insurance loss assessment for 9/11. Maps of collateral damage around the World Trade Center were superposed on insurance exposure to provide estimates of loss for multiple lines of business. The staggering scale and surprise of the overall claims resulted in the largest catastrophe loss in insurance history, and underlined the urgency of developing software tools to improve terrorism insurance risk management.

As with natural catastrophes<sup>1</sup>, a deterministic Probable Maximum Loss (PML) approach can be adopted in establishing estimates of insurance loss within the spatial footprint of a variety of plausible terrorist attack scenarios, ranging from aircraft impacts, to bombs, sabotage, and the use of weapons of mass destruction. Understanding and limiting the portfolio loss potential from an individual urban terrorist attack were the essential prioritized risk management tasks in the months after 9/11. A feature common to every catastrophe peril is a long tail of the loss distribution: whatever rare PML scenario is considered, it could be worse, indeed much worse. Hurricane Katrina tragically reminded optimistic catastrophe insurers that Murphy's Law has not been repealed for determinists. Accordingly, a probabilistic framework is an intrinsic requirement for all catastrophe models, whether natural or man-made.

Within a few months of 9/11, efforts to build such a probabilistic framework began, and sustained progress has been made since then. The principles of probabilistic terrorism risk assessment are now established, and the five years since 9/11 have provided an observational basis for model parameterization and validation. This retrospective review of progress focuses on the biggest challenge, namely behavioral modeling of the terrorist threat itself: the modus operandi of targeting and weaponry, and the frequency of attacks. Much less contentious has been the technical capability of engineering analysts to assess damage potential: e.g. evaluating the physical consequences of a bomb blast or aircraft impact; the spread of an arson fire; and the atmospheric dispersion of a toxic or radioactive plume.

The key to behavioral threat modeling is an appreciation of the strategic nature of the conflict between terrorists and the forces of counter-terrorism. In countries with experienced professional law enforcement and security services of high integrity, the wanton criminal actions of terrorists are severely constrained by counter-terrorism vigilance. In failed states, terrorists can run riot, but not in western democracies. Acknowledging the diverse range of political applications of game theory, it is fitting that the 2005 Nobel Prize in economics should have been awarded jointly to Robert Aumann and Thomas Schelling, *'for having advanced our understanding of conflict and cooperation through game theory analysis.'*

The two pillars of game theory that support its applicability are the assumed intelligence and rationality of the protagonists. Sceptics of terrorism risk modeling might doubt whether either holds for Jihadis. But there is little to be gained from underestimating an adversary, especially one intent on martyrdom. It was the French philosopher of the Enlightenment, Blaise Pascal, who argued that it might be considered irrational not to risk one's finite life for the infinite reward of heaven. Three centuries later, Pascal's wager is taken up regularly by Islamist suicide bombers. In the words of the brother of a Palestinian suicide bomber who had studied enough mathematics to understand Pascal, *'If you want to compare it to the life of Paradise, you will find that all of this life is like a small moment. You know, in mathematics, any number compared with infinity is zero'.*

---

<sup>1</sup> Woo G., *The Mathematics of Natural Catastrophes*, Imperial College Press, 1999.

Not only are terrorists rational in the sense of Pascal's wager, they are also intelligent. Abdel Bari Atwan, editor of an influential Arabic language newspaper, Al Quds Al Arabi, that receives communications from Al Qaeda, has written<sup>2</sup>, '*The West should never underestimate the intellectual prowess or scope of the Al Qaeda leadership, which is extremely learned, well read and well informed.*' Atwan reports that the chief strategist of Al Qaeda, Dr. Ayman Al Zawahiri, is an admirer of the epic book on world history, 'The Rise and Fall of the Great Powers', written by the Yale professor, Paul Kennedy. This intriguing indirect link between long-term Islamist political strategy and his Ivy League alma mater must seem ironical to President Bush, whose terms in the White House have been dominated by the war on terrorism.

## TERRORIST TARGETING

In his book, 'Knights Under the Prophet's Banner', published in London in 2001, Osama bin Laden's deputy, Dr. Ayman Al Zawahiri, proclaimed that '*Al Qaeda wins over the Umma when we choose a target it favors*'. The Umma is the global community of Muslims, and is the public for whom the brutal theater of Islamist terrorism is enacted to inspire the global Jihad through graphic television images, video and internet. Just as Irish republicans rejoiced heartlessly at hearing of the cruel IRA murder of the Queen's cousin, Lord Mountbatten, in 1979<sup>3</sup>, so many Muslims around the world rejoiced over the surprise attack on the World Trade Center in 2001.

There is a common misperception that the over-riding objective of terrorism is to terrorize its victims, and that the victims' own views as to targeting are therefore important and worthy. On this basis, credence has been given to the so-called heartland theory: the notion that a terrorist attack in the middle of nowhere, on an unknown target, is likely to be perpetrated, because of the implied message that nobody is safe from a terrorist attack. As Al Zawahiri has made clear, far more important is the Umma's collective idea of targeting – striking at places with international name recognition, with some familiarity to ordinary Muslims. Accordingly, since 9/11, the world has witnessed major attacks in Bali, Mombasa, Istanbul, Riyadh, Casablanca, Madrid and London, places named in tourist guides for world travelers. As revealed in opinion polls taken after the London bombings, a significant percentage of British Muslims condoned this act of terrorism on British soil. How can the Umma's pride and gratification in Islamist capability to strike at the heart of London compare with a strike in the open countryside?

Within the US, disrupted plots have revealed plans to attack the Liberty tower in Los Angeles, financial targets in New York and Washington, transport infrastructure, energy facilities etc.. Even without a survey of global Muslim opinion, all of these targets might readily be counted among those favored by the Umma for a strike against US economic and political power.

---

<sup>2</sup> Atwan A.B. *The Secret History of Al Qa'ida*, Saqi books, 2006

<sup>3</sup> Rees P. *Dining with Terrorists*, Macmillan 2005.

It is known from computers seized from arrested terrorists that meticulous surveillance and reconnaissance is carried out on targets to identify weaknesses in security. Given two targets of equal attractiveness, terrorists will tend to attack that which is less secure. The substitution of targets according to security is a game-theoretic concept, and has been validated repeatedly since 9/11. For example, the British consulate in Istanbul was chosen as a target in November 2003, after surveillance of the relocated US embassy showed it was much too hard to attack. On an individual scale, a Chechen 'black widow', whose husband had been killed by Russian forces, substituted another restaurant in Moscow for MacDonaldis, when uniformed guards were seen outside the US hamburger restaurant. Target substitution operates on all levels, and even has an international dimension. When Jemaah Islamiyah operatives found the US embassy in Manila too difficult to strike effectively, attention was switched from the Philippines to Singapore.

## TERRORIST WEAPONRY

In 1746, the French savant, Pierre de Maupertuis, was the first to explain that, in producing its effects, Nature acts always according to the simplest paths. In parallel with natural hazards, a guiding principle for all successful guerilla and terrorist organizations is following the path of least resistance in their modus operandi. This principle, which was expounded by Sun Tzu several thousand years ago in 'The Art of War', applies as much to the choice of terrorist weaponry as to targeting.

Reflecting de Maupertuis' principle, the simplest reliable and effective weapon of terrorist choice has been the improvised explosive device. IED's have proliferated in variety, disguise and impact, most notably in Iraq, which has become a crucible of terrorism. The use of ready-to-use military weapons, such as surface-to-air missiles and mortars, has also been a logistically efficient terrorist choice since 9/11. Also favored is the exploitation of western transportation, such as aircraft, HAZMAT and gas tankers, that can be turned by terrorists into deadly weapons. However, as yet, the procurement or manufacture of technically sophisticated weapons of mass destruction remain a far more elusive objective. In the 2006 Old Bailey trial of Abu Hamza, video recordings of the radical London imam were shown in which he is heard saying, '*You can't do it with a nuclear weapon, you have to do it with a kitchen knife. You can't do it by chemical weapons, you have to do it by mice poison.*'

The decentralization of the global Jihadi movement encourages grass-roots CBRN (Chemical-Biological-Radiological-Nuclear) weapons initiatives. Jihadi web-site chatter indicates a growing interest in disseminating information on CBRN weapons. However, with less direction and coordination from the Al Qaeda leadership, the most spectacular attacks are harder to organize, and hence are less likely. Furthermore, counter-terrorism pressure makes it more difficult for sophisticated weapons to be developed. However, more moderate attacks might be anticipated, with improvised weapons, such as poisons. Evidence of attempts to make lethal plant poisons, including a recipe for ricin, was found in the London apartment of Algerian refugees, who had links with the Finsbury Park

mosque, where Abu Hamza was the imam. The home production of lethal poisons might result in a modest number of casualties, but not on the devastating scale of an anthrax or smallpox attack. Fortunately, these biological weapons are very hard to acquire and weaponize effectively. Plague exists naturally in the wild, and is more readily acquired. However, it has limited lethality, and the public health counter-measures available would tend to discourage terrorists from attempting to spread this disease.

A weapon which is less deadly, but potentially highly disruptive economically and socially is the radiological dispersal device, or 'dirty bomb'. Simple radiological dispersal devices are comparatively easy to produce from readily available radiation sources, but sophisticated, more effective, weapons involving nuclear fuel rods are much less plausible, given the difficulty of acquiring the fuel rods. Even such an ambitious radiological dispersal device would pale in its potential harmful consequences compared with a nuclear detonation bomb. Thankfully, it is extremely difficult to acquire nuclear weapons or significant quantities of fissile material. Despite the logistical and financial resources of a nation state, Saddam Hussein failed to acquire any Iraqi nuclear capability. Thomas Schelling, the 2005 Economics Nobel Laureate, noted in his book 'Choice and Consequence' that, *'It appears to require a group of significant size, high professional quality, and excellent organization and discipline, to convert unauthorized or illicitly obtained materials into a useable nuclear weapon.'* Ever since the Cold War, western intelligence officials have been vigilant to deny nuclear capability to those with malicious and hostile intent. Such continued vigilance is vital for the maintenance of western homeland security.

## LAW ENFORCEMENT MITIGATION OF TERRORISM RISK

Earthquakes and hurricanes will tend to inflict most damage on the weakest structures. This is a simple consequence of the Laws of Physics, not of any malicious intent. Powerful as mankind is in subjugating the wildness of Nature, there is no human control over the occurrence of earthquakes and hurricanes. The loss consequences of these events can be mitigated through reducing engineering vulnerability, but the causative hazard itself cannot. The number of hurricanes forming during an Atlantic hurricane season is utterly beyond the influence of nations, except indirectly through carbon emissions and their impact on global warming.

Malicious intent, by contrast, lies at the root of terrorism. However, terrorism is a man-made hazard, and is therefore subject to the control of state law enforcement and security services. In a democracy, counter-terrorism action should be commensurate with the threat. Repressive measures that sweep aside basic human rights may be the first response of a dictator, but not of an elected president or prime minister. Even so, lethal terrorist attacks such as on 9/11/2001 in the US, and 7/7/2005 in the UK, call for stricter legislation. The Patriot Act arose from the debris of the World Trade Center. Out of the horror of the London transport bombings came new British criminal offences of acts preparatory to terrorism, and incitement to terrorism. In September 2005, the director-general of the UK security service, MI5, Eliza Manningham-Buller, delivered a keynote

speech in the Hague, in which she urged, *'There needs to be a debate on whether some erosion of what we all value may be necessary to improve the chances of our citizens not being blown apart'*.

Periods of quiescence may cause libertarians to question the need for some of the more draconian legislation; conversely, further atrocities may compel the introduction of yet tougher counter-terrorism legislation. The balance between liberty and safety will be adjusted by governments according to their intelligence-led threat perception, and in line with public opinion. In terrorism court cases, it is the function of the judiciary to uphold the fundamental principles of justice and human rights which are valued by all western democracies.

Faced with the landfall of Hurricane Jeanne, the fourth to impact on Florida in 2004, there was nothing that the state governor, Jeb Bush, nor his brother, the President, could do to prevent its arrival. But after any major terrorist attack, the level of counter-terrorism response can be ratcheted up to face the manifest threat. The capability of nations to respond forcefully to acts of terror serves as a control mechanism to mitigate the risk. Whatever the armed capability of a terrorist organization, the counter-terrorism forces of a western democracy are much greater. Terrorism warfare is asymmetric. Accordingly, within a western democracy as opposed to a failed state, it is very hard for terrorist organizations to perpetrate major attacks on a regular basis. Seasoned political risk underwriters with memories of the sporadic IRA campaign in Britain may sense that this is the case, but a more formal quantitative risk analysis of the frequency of major terrorist attacks has been developed to justify this premise.

## THE FREQUENCY ISSUE

Macro-terror attacks are acts of terrorism, such as perpetrated on 9/11, that aim to cause substantial societal loss. In contrast with the lesser micro-terror attacks, that aim to terrorize but have limited potential for inflicting casualties and property damage, macro-terror attacks require significant logistical resources, and considerable time for planning and preparation. Al Qaeda is noted for meticulous detail over attack planning, which involves reconnaissance, surveillance and rehearsal. Most notably, Al Qaeda has developed a long-term strategy<sup>4</sup>, and is very patient in planning its military campaign. There are no specific prescribed time deadlines, so there is no need to rush missions if extra risks are incurred. The patience of militant Islamists may be understood from the structure of the Koran itself, which has no linear sense of time, unlike the Bible.

Breaking a silence of more than a year, an audio tape from Osama bin Laden was aired on Al-Jazeera on January 19th, 2006. The taped message carried the explicit threat: *'The new operation of Al-Qaeda has not happened not because we could not penetrate the security measures. It is being prepared and you'll see it in your homeland very soon.'* Ever since 9/11, the intention of Jihadis to plan and prepare further strikes against the US has never been in doubt. Indeed, about a dozen have been interdicted. Past counter-

---

<sup>4</sup> Atwan A.B. *The Secret History of al-Qa'ida*, Saqi books, 2006

terrorism experience indicates that 75% to 90% of planned terrorist attacks eventually are interdicted in countries, such as the US and Western Europe, with strict security regimes and good state control over law and order.

In order to estimate the frequency of successful attacks, the following question then has to be addressed: how many attacks can be planned for execution within the US in a single year? Insurers might worry that the number of planned macro-terror attacks in the US could escalate significantly above recent experience. After all, the logistics of attack planning would seem to present no fundamental obstacle to the supply of multiple conventional macro-attacks with the requisite funding, materiel, and personnel. The scheduling of macro-attacks within a pipeline production process might suggest some degree of organizational time ordering, but it is difficult to argue a reasonable limit to macro-attack capacity from supply chain management principles. Indeed, the unrelenting daily bombings in lawless chaotic Iraq appear to bear this out.

However, during the previous dictatorial regime of Saddam Hussein, strict law and order were maintained via a dense network of secret agents and informers, and any acts of terrorism against the Ba'hist regime, or assassination attempts on the president, were viciously and ruthlessly put down. Quite apart from any attack pipeline restrictions, aggressive counter-terrorism action imposes a fundamental security constraint on the planning of multiple terrorist attacks in the same country within a period of a year.

In the game of checkers, having many pieces on the board carries the risk that a sizeable connected group might be swept away in a single adversarial move. Similarly, in the asymmetric war game of terrorism, having too many active terrorist operatives in the same field induces a degree of congestion in the space of terrorist operations, and carries a heightened risk of 'dots being joined' by security services. Terrorists will be concerned over the disruptive effect of counter-terrorism network surveillance in a small inter-connected world. This anxiety promotes caution, and a restriction of the number of attacks, and the multiplicity of synchronous attacks, that can be prudently planned within the same theater of operation, during a particular time interval.

An illustration of this concern is given by 9/11 itself. At one early stage of planning, the plot was even grander and more ambitious than it turned out, with other planes involved. As shown by the arrest of Zacharias Moussaoui, the so-called twentieth hijacker, who was detained prior to 9/11, the bigger the plot, the bigger the risk of it potentially ending in failure, due to the Jihadi identity of one or more operatives being compromised and secrets divulged. Richard Reid, the shoe-bomber, who was named as an accomplice by Moussaoui, himself might also have been detained before 9/11, and might have put at risk the eventual success of the entire 9/11 mission. Suppose the pack of terrorist cards had been stacked too high by al-Qaeda in 2001, perhaps being twice or even three times as ambitious. It might have all collapsed under the scrutiny of the FBI and CIA, who would then have had a much simpler task of joining the dots.

Another example is given by the 7/7 bombing of London in 2005. The cell ringleader, Mohammed Siddique Khan, was known by the British security service, MI5, to have

been in communication with an Al Qaeda operative involved in another plot. But there were insufficient terrorist connections for him to have been put under surveillance. He was still designated as a so-called 'clean skin', without significant terrorist associations. Had there been more connections, the dots might have been joined, Khan might have been arrested, and the 7/7 London bombing averted.

A third example is given by the foiled Jemaah Islamiyah (JI) plot to explode six large truck bombs around Singapore shortly after 9/11. Outside the Middle East, this is the most audacious and ambitious terrorist plot conceived after 9/11. This plot involved three JI cells in laying the groundwork for the attacks. In this case, a tip from the public drew attention to a Singaporean of Pakistani origin. The security services started to monitor his close associates, one of whom was seeking to buy a large amount of ammonium nitrate, another had family links with Islamist extremism. Gradually the whole plot unraveled with many arrests. Large complex plots involving many terrorists are highly vulnerable to being wound up through diligent counter-terrorism surveillance. The metaphor of a thread unraveling a sweater has been used by security officials to illustrate this process.

## ANALYSIS OF TERRORIST NETWORKS

Suppose there are a number of operatives actively involved in planning and preparing attacks. Any communication between two operatives, whether via a meeting, letter, phone, email, or internet, and however clandestine, carries a finite risk of interception by security services. Surveillance technology is increasingly sophisticated, intrusive and pervasive: Ramsi bin al-Shibh, a top Al Qaeda leader, was tracked down in Karachi after an Al-Jazeera interview, through electronic recognition of his telephone voice print<sup>5</sup>.

From the terrorists' organizational perspective, the network should be resilient against random links between operatives that might possibly be intercepted and decoded. Even though operatives may minimize communication, such links may arise because of the close-knit social networks of Islamist militants, centered on mosques, Islamic bookshops, gyms etc.. To maintain a stable environment for attack planning, terrorists will strive to ensure that network dots are hard to join, even if there happened to be some occasional intercepted links.

Intuitively, the larger the community of active operatives, the larger the number of random intercepted links that may arise between them, and the easier it becomes for counter-terrorism forces to join the dots. The organizational worry for terrorists is that if there is excessive planning activity for many attacks during a short period of time, there will be a greater likelihood of more random intercepted links, so making the security services' task of the joining of dots much easier. A major part of this audacious attack planning might then be wound up in a domino-style sequence, and prove ultimately to be counter-productive, and wasteful of terrorist resources. A smaller, less ambitious,

---

<sup>5</sup> Miles H., *Al-Jazeera*, Abacus books, 2005.

number of planned attacks would be less prone to network disruption, and hence make better sense overall.

It turns out that the number of operatives involved in planning and preparing attacks has a tipping point in respect of the ease with which the dots might be joined by counter-terrorism forces. The opportunity for surveillance experts to spot a community of terrorists increases nonlinearly with the number of operatives - above a critical number, the opportunity improves dramatically. This nonlinearity has been discovered recently through analytical studies of networks, using modern graph methods<sup>6</sup>. Below the tipping point, the pattern of terrorist links may not necessarily betray much of a signature to the counter-terrorism services. However, above the tipping point, a far more obvious signature may suddenly become apparent in the guise of a large connected network cluster of dots, which reveals the presence of a form of community.

The actual tipping point value is a decreasing function of the likelihood of random intercepted linkage. Even from open source information on terrorist networks<sup>7</sup>, it is apparent that, at any given time, a small proportion of terrorist network links have been identified. From the high interdiction rate of planned attacks achieved by counter-terrorism forces, the proportion of links discovered through surveillance must be yet larger. For a five man attack cell, which consequently has ten possible intra-cell links, on average, one link may be known in some form to the counter-terrorism forces. This corresponds to a value of the linkage likelihood of about 10%. If this were to be the case, the dots may still be hard to join, and the terrorist network would remain comparatively resilient. Tracking down just a couple cells is hard work for the counter-terrorism forces. However, the difficulty would be alleviated substantially if the number of operatives exceeded the tipping point of 50 that corresponds to a 10% chance of random intercepted linkage. The emergence of a coherent pattern would then identify a community of active terrorists.

Al Qaeda seems to be smart, patient and adaptive enough to acknowledge and respect this tipping point limit. According to the testimony of Mohammed Mansour Jabarah<sup>8</sup>, Osama bin Laden addressed the Al Farooq training camp in Afghanistan in May 2001, and said that there were *'50 men willing to bear their souls in their hands for the Jihad to attack America'*. Intuitively, he would have understood that launching a greater number of Jihadis in attack waves against the US in 2001 would have been rash and foolhardy. Indeed, the 9/11 operation was scaled back to the East coast from an original plan to attack skyscrapers on the West coast as well.

An annual limit of 50 operatives in one theater of operation equates to a maximum of about 10 separate planned attacks per year. Allowing for the interdiction rate, this limits the annual number of successful attacks to a few at most. The historical track record of Al Qaeda's operation in USA and Western Europe indicates an implicit awareness of the

---

<sup>6</sup> Derenyi I., Palla G., Vicsek T. Clique percolation in random networks, Phys. Rev. Lett., 94, 2005

<sup>7</sup> e.g. [www.tracking-the-threat.com](http://www.tracking-the-threat.com)

<sup>8</sup> Bell S., *The Martyr's Oath*, John Wiley & Sons, 2005

undue detection risks associated with having too many plots planned within the comparatively brief time scale of one year.

To date, the largest number of attacks planned within one year in one country is five. This record is held by the UK in 2005, one on July 7 was successful; one on July 21 was a technical failure; and three later attempts were interdicted. Since 9/11, the interdiction rate of planned macro-terror attacks on the US and Western Europe has been consistent with that achieved by counter-terrorism forces in other major terrorist campaigns against leading military nations, e.g. the IRA in the UK. Furthermore, the annual rate of attack planning has been running at a few attempts per country. The resultant outcome has been just a few sporadic successful Jihadi attacks, e.g. Madrid (March 11, 2004) and London (July 7, 2005).

## TERRORISM BEYOND 2007

At the end of the nineteenth century, Winston Churchill served as a young British army officer on the northwest frontier region, between Pakistan and Afghanistan. In his memoirs, he wrote, *'Except at harvest time, when self-preservation enjoins a temporary truce, the Pathan tribes are always engaged in private or public war. Every man is a warrior, a politician and a theologian.'* After Osama bin Laden, there will no shortage of replacement candidates to carry on the Holy War against western political interests. There is over a century of bitter historical experience testifying to the lawlessness and fierce independence of this tribal border region, which has never been subjugated in the past. Some terrorist havens can be disrupted, but not eradicated. Through the diligence of western counter-terrorism forces, the capability of Al Qaeda can be checked, but the threat of a catastrophic terrorist attack will persist in the future as a low probability scenario. With Muslim populations expanding in western countries, the virus of Islamist militancy may become endemic through constant mutation under counter-terrorism pressure.

Looking back over the period of terrorism model development since 9/11, progress in quantifying terrorism insurance risk has been rapid. The basic principles of terrorism risk modeling, founded on the game theory of conflict, are now understood. There remains of course a significant degree of uncertainty in parameterizing a terrorism risk model, but this is generally true of all low-probability, high-consequence catastrophe models. Acknowledging that behavioral sociological factors influence all large portfolio claims settlements, terrorism insurance risk modeling is intrinsically no less viable than other varieties of catastrophe modeling. The debate over the insurability of terrorism risk need not therefore linger over the technical hurdle of modeling capability, but should focus on the fundamental conundrum of managing the extreme risk of potential gigantic losses that threaten insolvency. Regardless of the odds offered, no risk-averse insurer would volunteer to bet the future of the company on the non-occurrence of a plausible catastrophic event.

Although a catastrophic bioterror smallpox attack could cause massive insurance loss, the scale of human disaster would be eclipsed by an influenza pandemic of 1918 proportions or worse. Experimental studies by leading international virologists in the best equipped laboratories attest to the enormous difficulty of producing a transmissible and lethal mutated H5N1 influenza virus. The possibility of a pandemic virus being fabricated in an improvised terrorist laboratory by rank-and-file biologists is therefore exceedingly remote, even if there were any terrorist motivation to try. However Nature's biological weapon, as security analysts have described the influenza pandemic, is a major concern for life and health insurers. In particular, it is virologically conceivable that an H5N1 mutation might occur that is both extremely lethal, and extremely infectious. If, as in 1918, adults or working age were preferentially to fall victim due to auto-immune response, the losses to the life and health industry would be absolutely catastrophic.

Sabotage of a nuclear installation is known to be a possible terrorist attack mode, although heightened security would be a major deterrent. Were any attack to be successful, it might cause a catastrophic release of radiation. But such a disastrous contingency could happen for many other reasons. As manifest at Three Mile Island and Chernobyl, basic human error is a more likely cause of a nuclear accident. For the US nuclear industry to stay in business, when the potential exists for massive liability claims following an operator error-induced core melt-down, there has to be a government backstop beyond the scope of the nuclear plant insurance pool. Indeed there is one: namely as legislated by the Price-Anderson Act.

As with nuclear plant human error, there are terrorism scenarios with loss consequences that are well beyond the capital base of the insurance industry, or the heartiest appetite of capital markets investors in risk-linked securities. Suppose the nightmare Armageddon scenario were to materialize, and there were a nuclear explosion in New York or Washington, To the extent that such an ultimate expression of political violence might well have depended on state assistance if not sponsorship, and would constitute, de facto, an act of war, (albeit undeclared), it is hard to imagine that the US government would not act as an insurer of last resort, and make an attempt to compensate the victims financially. Some form of permanent government backstop, akin to what is in place for nuclear industry, would seem to be unavoidable for terrorism insurance.

Given that the annual risk of a nuclear detonation in the US is only a few basis points, the value of a terrorism risk subsidy is modest compared with the military expenditure on the war on terror. As with TRIA, terrorism risk analysts can assist in assessing the cost implications of any backstop. Already, the bulk of the expected loss from US terrorist attacks is being borne by the insurance industry. This burden may be extended further, but not without eroding the global pool of voluntary terrorism risk insurers.