RMS WHITE PAPER

# A TERRORISM RISK ANALYST'S PERSPECTIVE ON TRIA

Submitted to Congress, 2005

*Gordon Woo, RMS catastrophe risk expert, wrote this paper for DRI, an organization of defense attorneys and in-house counsel, as part of a DRI submission to the U.S. Congress in 2005.*

## INTRODUCTION

A notable factor unsettling the terrorism insurance market is the ambiguity in quantifying terrorism risk. The less confidence there is in the process of risk evaluation, the harder the task of prudent risk management, and the more hesitant insurers will be to risk capital in providing terrorism cover. Compared with the technically more mature disciplines of seismology and meteorology, quantitative terrorism risk assessment is a nascent branch of risk analysis, essentially originating in the aftermath of September 11, 2001.

Partly because of their relative novelty, and partly because of the narrow circle of specialists in this field, the principles of terrorism risk assessment are not widely appreciated. At a qualitative non-mathematical level, these principles are elucidated in this paper, which aims to inform a general readership of the level of understanding attained after three years, and to review the future prospects for raising market confidence in terrorism risk modeling. In the short-term, government support is very effective at bolstering a fragile and nervous terrorism insurance market. In the medium-term, the growing maturity of terrorism risk assessment may eventually foster a greater degree of commercial market independence.

## TERRORISM: A CATASTROPHE RISK

As often happens in insurance risk assessment, impetus to model terrorism risk in a quantitative manner emerged spontaneously from the ashes of a major catastrophe. Terrorism had been an insured risk long before 9/11, but never before had terrorism been perceived by political risk underwriters, nor been priced by actuaries, as a genuine catastrophe risk. The severity of financial blow that a terrorist organization can strike depends on three crucial factors: intent, capability, and opportunity. Until Al Qaeda, never before had there existed a terrorist organization that possessed the ruthless ideological intent to cause maximum loss, the trained personnel and logistical capability to launch spectacular suicide attacks against western interests, and the patience in undertaking surveillance to identify and exploit defensive weakness.

A stark comparison may be made with the Irish Republican Army (IRA), in their longstanding terrorist campaign against British rule in Ulster. Through such atrocities as the bombings in the city of London, the IRA had shown the capability to exploit opportunities to launch massive attacks on the British mainland, but, needing to assuage the conscience of catholic supporters, it lacked the intent to maximize casualties, preferring to moderate human loss through the issue of vague telephone warnings.

9/11 was a singular irreversible moment in the annals of terrorism: the evil genie of terrorism catastrophe revealed itself, never again for its existence to be dismissed as some fantastic fable from the Arabian Nights. Never more can terrorism loss on such a calamitous scale be dismissed as speculative scare mongering, a blind extrapolation of a statistical curve into uncharted territory. Terrorists learn adaptively from collective international experience, and 9/11 has left an indelible mark on the historical consciousness and heritage of future generations of terrorists. As with all catastrophes, natural or man-made, once one extreme loss record has been broken, the specter of another such event casts a perpetual risk shadow over the insurance market. Terrorism history cannot be rewritten to eradicate the bitter memory of a tragic accomplishment of Islamist terror over western intelligence and a costly failure of the insurance industry to monitor and control its geographical risk accumulations.

As with the devastation wrought previously by Hurricane Andrew in 1992 and the Northridge Earthquake in 1994, the destruction of the World Trade Center raised the question of the commercial insurability of a catastrophe risk such as terrorism, without some form of government subsidy. With respect to hurricanes and earthquakes, the global reinsurance market responded positively to the 1992 and 1994 disasters by making capital available for underwriting these risks, capable though they are of causing massive insurance losses. To a minor extent, the issuance of hurricane and earthquake catastrophe bonds has supplemented the coverage. In contrast, since 9/11, there has been a reluctance to commit capital for underwriting U.S. terrorism risk, and no U.S. terrorism catastrophe bonds have yet been issued. In this nervous and hesitant underwriting environment, TRIA has been effective in spreading terrorism cover, the dearth of which might have been detrimental to the national economy.

The much shorter historical record of terrorism, compared with hurricane and earthquake occurrence, is commonly cited as a factor influencing the cautious state of the U.S. terrorism insurance market. Risk analysts can be relied upon nowadays to quantify, with a moderate but acceptable level of confidence, the rarity of extreme natural peril events, even exotic risks such as a massive meteorite strike, a gigantic landslide-driven tsunami, or cataclysmic volcanic eruption, all of which have the potential to devastate multiple cities. But the principles of terrorism risk quantification remain relatively unfamiliar, and unease over the brief track record of terrorism risk assessment lies at the heart of the debate over the commercial insurability of terrorism.

In the weeks after the terrorist attacks on 9/11, risk analysts set about mapping the impact and debris damage around the World Trade Center, and gauging the loss across all lines of insurance coverage. Towards the end of 2001, attention could be turned from mapping terrorism loss towards the ambitious challenge of modeling terrorism risk. In the three years that have passed since then, progress has been driven not just by insurance risk managers, but also by the pressing need for finite Homeland Security resources to be allocated efficiently, in a risk-informed manner, to maximize public protection. Likewise, risk assessment is needed for a cost-benefit review by the Office of Management and Budget of proposals for terrorism regulations.

## UNDERSTANDING TERRORIST BEHAVIOR

Skepticism over terrorism modeling has stemmed from a commonly held prejudice that, in contrast with natural perils, violent human behavior is beyond quantitative analysis. Remarkably, it was the founder of numerical weather forecasting, the English scientist, Lewis Fry Richardson, who also pioneered the modeling of human conflict, through his peace studies on the statistics of deadly quarrels. Furthermore, it was Richardson's innovative analysis of the frontier dependence of conflicts that led to the discovery of universal power-law (fractal) phenomena that pervade the environmental sciences, and characterize the severity of natural catastrophes.

To the general public, terrorists may appear to be dysfunctional people, whose criminal behavior defies rational comprehension, let alone quantitative risk modeling. However, to a dispassionate mathematician, trained in the search for order and structure, another perception emerges. Guided by their own radical Islamist political agenda, terrorists are driven to maximize the likelihood that their Islamist objectives are attained, even at the expense of their own lives and those of fellow Muslims. Like all ruthless political propagandists, terrorists use violence for effect, preferring to speak with actions rather than words. Verbal explanations may appear later on Islamist websites, but the attacks speak for themselves in their targeting, timing, and choice of weaponry.

Looking back over history, successful counter-terrorism campaigns have "out-thought" rather than "out-fought" the terrorists. As Dr. George Habash, co-founder of the Popular Front for the Liberation of Palestine, once remarked, "Terrorism is a thinking man's game." The global war on terrorism is waged not only by land, sea, and air, but also across one of the most complex of terrains: the human brain. Given the overwhelming superiority of the military assets of nation states, the brain is the most potent weapon in the terrorist arsenal.

Just three days after the fall of the twin towers of the World Trade Center, a cognitive neuroscience paper was published which sheds light on the decision-making process in the current war on terrorism. This is an asymmetric war, in that, according to a standard definition, the instigator, Al Qaeda, has a disproportionate advantage gained by exploiting dissimilar values, strategies, and capabilities, and capitalizing on perceived weaknesses. One such dissimilarity is the degree to which decisions can be made in a ruthless, cold and calculating manner, void of moral judgment and human compassion.

Consider the following classic moral dilemma: A runaway railway carriage is bearing down on five people, who will be crushed to death unless you find some means to change the carriage's course. You can choose to turn a switch that diverts the carriage onto another track, where a worker is carrying out repairs. If you do, the worker is likely to be killed, but five lives will have been saved. What should one do? Now consider the following variation of this moral dilemma: You are standing at a point overlooking the tracks, between the railway carriage and the five people. Near you is a stranger; should he be pushed onto the track and struck by the train, the five people further down the track would be saved. What should one do in this case?

In the first formulation of the dilemma, most people might be prepared, reluctantly, to divert the carriage. An aviation parallel can be drawn with the firm policy, now resolutely adopted by U.S. and European governments, to shoot down hijacked aircraft; the cold reckoning being that casualties among innocent street bystanders from falling debris should be much fewer than among those trapped in an impacted high-rise building.

By contrast, in the second formulation of the dilemma, almost all people would baulk at pushing a stranger into harm's way, even though more lives would be saved. The human decision-making process in coping with these two dilemmas has been elucidated by a brain imaging experiment conducted at Princeton University, and reported in the neuroscience paper referenced previously. The contrasting decision response to the second dilemma is observable through the activation of brain areas associated with emotion rather than pure rationality.

Throughout the history of human warfare, battle-hardened generals have ordered their soldiers into harm's way, even into suicidal situations, for the greater military good. For Al Qaeda, martyrdom missions are the standard means of prosecuting the Jihad. There are no moral constraints on Al Qaeda attacks—no concern for the lives of the operatives, nor for the number of their victims, some of whom may well be Muslims. The robotic calculated rationality of Al Qaeda decision-making allows attack decisions to be optimized, like moves on a chessboard, without the emotional interference of moral concerns over human welfare. Consider a variation of the second railway carriage dilemma, where you are standing next to a stranger, and the vital objective is to halt the train. An Al Qaeda operative would have no compunction in either pushing the stranger onto the track, or jumping onto the track–or both. Exchanging a railway for an aviation metaphor, this is essentially the shocking behavioral paradigm of 9/11.

## THE PRINCIPLE OF TARGET SUBSTITUTION

The thinking man's handbook of terrorist strategy is Sun Tzu's military masterpiece, *The Art of War*, which emphasizes the utility of a fundamental law of Nature: following the path of least resistance. The fact that water follows the path of least resistance is enshrined in Newton's laws of motion. Two millennia earlier, Sun Tzu wrote that: "Now an army may be likened to water, for just as water avoids heights and hastens to the lowlands, so an army avoids strength and attacks weakness." According to this principle, terrorists will choose softer targets, if the harder targets offer too little prospect of success: suicide alone does not make a militant a martyr. Civilians would be safe if terrorists strove for a tough macho image, and struck only at hard military targets, even if the chances of success were slim. Alas for insurers, the rules of asymmetric warfare are different.

[1] Greene J.D., Sommerville R.B., Nystrom L.E., Darley J.M., Cohen J.D. (September 14, 2001) An fMRI Investigation of Emotional Engagement in Moral Judgment, Science, 2105-2109.

Our understanding of terrorist behavior is constantly being put to the test. In particular, terrorists operate in a global laboratory for checking the least-resistance principle. The massive $1.2 billion spent on counter-terrorism protection at the Athens Olympic Games illustrates the universal deterrent value of high security. Globally, the type of attacks that do occur, or are aborted or interdicted, provide observational evidence of the terrorists' modus operandi in target selection.

Sheikh Yassin, the founder and spiritual leader of Hamas, once declared that when all doors are sealed, Allah opens a gate. For a militant fundamentalist to believe in the providence of Allah does not imply naively that he would blindly turn up at a target, and just hope for the best—*Insh'Allah* or God-willing. Those whose image of a terrorist is a stereotype of crazed religious fanaticism should have been astonished by the mass of technical data found in July 2004 in the possession of a Pakistani computer engineer, Muhammad Naeem Noor Khan.

On computer storage were meticulous details of sophisticated patient Al Qaeda surveillance of some iconic financial targets in New York and Washington. Not only were geographical and temporal variations of security noted, but potential engineering and architectural weaknesses of potential targets were also documented, so that their vulnerability to bombing might be discerned. Indeed, the professional manner with which these targets had been selected, and their engineering and security vulnerability evaluated, mirrors remarkably closely the game-theoretic procedure by which terrorism insurance risk analysts assemble and prioritize their own lists of attractive targets.

If government assets are perceived to be targeted, the government has a duty to provide protection, commensurate with the level of the threat. Sites differ in their intrinsic protectability: governments will aim to remove the "low-hanging fruit" which lies easily within the terrorist grasp. In the 1990s, many embassies fell within this category. But soon after the 1998 bombings of the U.S. embassies in Kenya and Tanzania, the White House feared political recriminations from another embassy loss, and assumed the task of enhancing embassy security. Following security assessments by "red teams" of special forces personnel acting as terrorists, scores of embassies were hardened. Others that were too vulnerable were closed and more securely relocated.

Several hundred million dollars have been allocated to the embassy hardening program, with the result that, since 1998, terrorists have largely failed in their attempts at attacking U.S. embassies. In November 2003, during President Bush's visit to Britain, the British consulate in Istanbul was bombed, together with the local headquarters of the British-based bank HSBC. It is actually known that terrorist reconnaissance of the U.S. embassy was also undertaken, but no attack plan emerged because of the high security at the relocated embassy stronghold.

This example illustrates a dilemma: a terrorist thwarted from attacking a military or diplomatic target, because of effective protection, may substitute another more vulnerable target. This may be another embassy, or any of a large number of soft civilian targets of opportunity, e.g. rail commuters, hotel guests, or night-clubbers. Explicit admission of a soft target strategy has come directly from the interrogation of Khalid Sheikh Mohammed, the former Al Qaeda chief of military operations.

Al Qaeda target substitution is a veiled warning contained within the unclassified testimony of the director of Central Intelligence, George Tenet, in February, 2001: "As security is increased around government and military facilities, terrorists are seeking out softer targets that provide opportunities for mass casualties." At the start of 2004, Robert Hutchings, the chairman of the National Intelligence Committee concurred: "Soft targets are a prime focus of active Al Qaeda planning. These targets are seen to be easier to hit than other high-priority targets, such as U.S. government buildings, and major infrastructure targets, which have higher security postures." As landmark "postcard" targets are ever better protected, so there will be a corresponding descent towards soft targets. Such downwards escalation is familiar from crime statistics. A potential soft target that has the three "V" attributes of being plainly Visible, Valuable, and Vulnerable may fulfill the role of a lightning rod, in respect of drawing the attention of watchful terrorists. Public transport infrastructure may have all these attributes.

On March 11, 2004, a few days before the Spanish election, Islamist militants bombed Madrid. The attack was not aimed at any hardened political target, but rather was directed against the soft Madrid commuter rail network. Whatever the causal effect on the electorate, victory for the anti-war party was an outcome that Al Qaeda could celebrate and claim to have influenced, and Osama bin Laden could use as a pretext for straining yet further U.S.-European relations. The attack decision-making was entirely rational: why chance an attack against a well-protected government building or politician, if an easier and more reliable attack against a soft target can achieve the desired political objective?

The targeting of weak points in public transport infrastructure may become more widespread in future, as stricter counter-terrorism measures are adopted over time by security managers of commercial property. Provided that underwriters are diligent in ensuring high security standards at properties that are insured, the terrorism risk burden should gradually be deflected from the commercial to the public sector, with a corresponding decrease in insurance risk.

## TERRORIST TARGET SELECTION AND GAME THEORY

In order to quantify terrorist target selection, it is natural to use the mathematical theory of conflict, game theory, which is designed to help understand the adversarial interaction of opposing decision-makers. The 2001 Oscar-winning movie, "A Beautiful Mind" has served to popularize and celebrate this branch of applied mathematics. The two fundamental principles underlying game theory are that the protagonists are rational and intelligent in strategic reasoning. If the idea of rational and intelligent individuals dueling with each other may appear abstract, recall the dastardly post-9/11 kidnapping in Pakistan of the Wall Street Journalist, Daniel Pearl, by the Al Qaeda operative Omar Saeed Sheikh. Dan was the son of Professor Judea Pearl, an eminent probabilistic decision theorist; Sheikh was a British school chess champion, and former mathematics student at the London School of Economics. Like the computer engineer, Muhammad Naeem Noor Khan, his ethnic background and veneer of academic respectability allowed him to travel freely between Britain and the Al Qaeda strongholds in Pakistan and Afghanistan.

In applying game theory to terrorism, it is important to leave behind popular notions of rationality, and to return to the formal mathematical definition of rational behavior, namely that actions are taken in accordance with a specific preference relation. There is no requirement that a terrorist's preference relation should involve economic advantage or financial gain. Much of the purpose of terrorism is psychological: inspiring the global Jihad; whipping up malicious joy at seeing the U.S. suffering loss; and terrorizing the general public. Nor is it necessary that a terrorist's preference relation conform to those of society at large. Game theory is not restricted to any one cultural or religious perspective. For the devout, martyrdom is a rational choice: everyone has to die sooner or later, and bounteous eternal benefits are promised to the faithful who choose to die on the Path of God.

## MODELING TERRORIST ATTACK FREQUENCY

Otto von Bismarck, the nineteenth century founder of the German empire commented that, "When you draw the sword, you roll the dice." In his pioneering peace studies, Lewis Fry Richardson showed statistically that randomness plays a significant part in any human conflict. But, as with earthquakes, there are causal non-random factors as well. These shape the conflict landscape, and influence the temporal pattern of successful attacks. In constructing a stochastic model of the recurrence of terrorist attacks over time, these non-random factors need to be taken into account through invoking an appropriate conceptual paradigm: cybernetics, which is the science of control.

Magnus Ranstorp, a leading scholar of militant Islam, has referred to Al Qaeda operatives as parasites on globalization. In common with other prey-predator situations, the conflict between the forces of terrorism and counter-terrorism may be represented using the principles of cybernetics. At any moment in time, the predator (i.e. Al Qaeda) is in some specific state of attack preparedness, whilst the prey (i.e. U.S.) is in some corresponding state of defense preparedness. In a democracy, the counter-terrorism response has to be commensurate with the terrorism threat: draconian measures are only tolerable when the threat level is high. In the U.S., concern over state infringement of individual liberty exceeds even worry over terrorism. Democracies are prevented constitutionally from mounting an unlimited war on terrorism.

Whereas minor terrorist acts, such as individual kidnapping and shooting, may occur more or less haphazardly, the occurrence of "spectacular" macroterror attacks does not satisfy the prerequisites of a random (so-called Poisson) process, because of these controlling counter-actions. Following a spectacular macroterror attack, security and border controls are inevitably strengthened, and extra government funding made available for improving protection. As with the Patriot Act introduced soon after 9/11, new tougher counter-terrorist legislation may be enacted.

After a major U.S. land-falling hurricane or earthquake, the government is utterly powerless to prevent the occurrence of another of these natural perils. Long ago, scientific attempts were made to seed storms and lubricate faults to try to prevent windstorm and earthquake disasters, but these proved unsuccessful. As is evident from 2004, in a given hurricane season, there may be four or even more land-falling hurricanes. However, after any major terrorist attack, the government does have the power (and indeed the democratic mandate) to suppress the likelihood of a further attack through additional security measures. Thus, there is only an exceedingly slight chance of three or more major attacks at separate times during a year.

Major terrorist attacks take months or years for Al Qaeda to organize, and are apt to be discovered, so the policy is always to have a number in the planning pipeline. Increasingly, more detailed knowledge is being acquired about the cell and network structure of Islamist militants, adding insight for mathematical models of the capability of Al Qaeda to plan and launch coordinated damaging attacks. Used in conjunction with an analysis of counter-terrorism interdiction rates, these new models should impose ever tighter constraints on the rate of occurrence of successful attacks, and so reduce the ambiguity in terrorism risk assessment.

## TERRORIST WEAPON SELECTION

Being comparatively easy and cheap to fabricate, the improvised explosive device (IED) has become the terrorist weapon of choice, elaborated in literally hundreds of innovative deadly guises in Iraq. Standard military weapons, such as rocket-propelled grenades and mortars, are also widely available to Islamist militants, as are Man-Portable Surface-to-Air (MANPAD) missiles. These are enough of an international threat to civil aviation for the installation of anti-missile systems on passenger jets to be considered. However, at a cost of $1 million per aircraft, such systems must be technically very reliable to be cost-effective.

Highly lethal though these conventional weapons are, they lack the geographical footprint of chemical-biological-radiological-nuclear (CBRN) weapons. One of the most vexed low-frequency but high-severity issues concerns terrorist access to weapons of mass destruction, especially nuclear weapons. Rogue states suspected of acquiring such weapons pose an international threat, not so much because of the potential for cross-border conflict, but because terrorists may eventually gain access to these weapons. D.H. Rumsfeld stoutly defended Washington's position that the United States could not wait for absolute proof before taking action against such states.

This position was endorsed and explained by the Brussels-based American writer, Robert Kagan, in his seminal book, *Paradise and Power*, which Henry Kissinger has compared with Huntingdon's *The Clash of Civilizations*. Kagan's book has become mandatory reading for European bureaucrats, and was influential in Downing Street in the run-up to the Iraq war. To contrast the attitudes of the U.S. (as the God Mars) and Europe (as the Goddess Venus), Kagan has used the rustic metaphor of the marauding bear in a forest: a hunter armed with a rifle ought not to risk being mauled in his tent by the bear, but be emboldened to take pre-emptive action.

The U.S. defense secretary preferred the more obscure technical dialect occasionally spoken by probabilistic risk analysts. "There are known knowns. There are things we know that we know. We also know there are known unknowns, that is to say there are things we now know we don't know. But there are also unknown unknowns–things we do not know we don't know."

In the context of a probabilistic terrorism model, one of the known knowns is Al Qaeda's implacable commitment to use nuclear weapons, if acquired. This much is clear from the chilling statement of the chief strategist, Dr. Ayman Al Zawahiri, urging militants "to inflict the maximum casualties on the opponent." More equivocal are the means by which terrorists might acquire nuclear materials. Here, there are both known unknowns as well as unknown unknowns. In the former category are Russian officials with some access to the Russian nuclear armory. Since the end of the Cold War, nuclear smuggling has been carried out by former Soviet bloc military and intelligence personnel, who may have past experience in transporting material from West to East, and have a financial incentive in reversing this traffic.

Among the unknown unknowns are the nuclear capabilities of rogue states, and their preparedness to transfer nuclear technology and materials to terrorists. These uncertainties have been used to justify pre-emptive military action, and would merit a non-zero probability assignment for the likelihood of a nuclear terrorist attack. This probability is undoubtedly a challenge to assess, but it may be estimated by a standard quantitative risk analysis technique, which is commonly used in safety risk assessments for critical industrial installations. This involves the decomposition of the attack scenario into all plausible ramifications, each of which carries a likelihood weighting. Collectively, these constitute an elaborate event-tree with multiple branches for alternative sources and trafficking routes of nuclear material.

## THE MULTIPLICITY OF A TERRORIST ATTACK

A hallmark of Al Qaeda military operations is the multi-pronged synchronous swarm attack. Apart from the global media publicity associated with their audacity and military precision, there are key strategic advantages of having many points of attack. First, the element of surprise with a novel style of attack is maximized if it is multiply deployed at the same time. Secondly, redundancy in the number of operations allows for success to be hailed even if there is partial failure, as with United flight 93 on 9/11, and several of the Madrid train bombs two and a half years later. The main disadvantages with high attack multiplicity are the increased logistical burden of attack preparation, and the heightened chance of the entire plan being compromised by an indiscretion or detention of one of the terrorists. The balance between operational redundancy and secrecy may be represented in a mathematical form suitable for terrorism risk analysis.

## ESTIMATION OF PROPERTY LOSS

Contingent on a specific weapon being deployed against a target, the task of estimating the loss consequences is essentially reduced to an objective technical problem, of the type encountered routinely in loss estimation for natural hazards. There is uncertainty in the loss estimation, due to imprecision in the target vulnerability, but largely absent are the human behavioral factors that guide the terrorist threat assessment.

Sophisticated modern modeling software programs are available for simulating the dynamic effects of conventional explosive as well as nuclear blasts. Programs are capable also of tracking the atmospheric dispersion of toxic and radioactive aerosols, as well as the epidemiology of a contagious disease, such as smallpox. Validation of modeling software is provided by batteries of experimental and theoretical tests, as well as by actual observations of past historical incidents.

The density of urban areas introduces a further degree of geographical complexity in the resulting damage patterns, which are influenced by the dynamical interactions between neighboring properties. High concentrations of property within the damage shadow of a prime target can exacerbate the attack loss considerably, as shown horrifically on 9/11. High resolution property databases exist which allow such concentrations to be mapped and analyzed in detail for insurance loss potential.

Knowledge of loss potential is instructive for feeding back into terrorism risk mitigation. Given the more common threat from improvised explosive devices, one of the most cost-effective means of mitigating individual building risk is to thwart suicide bombing. Prevention of an unauthorized vehicle from a very close approach has been proven to mitigate potential loss significantly. As an example, in Jakarta, Indonesia, in August 2003, an 800lb bomb in a sports utility vehicle was detonated about 25 meters short of the entrance to the Marriott Hotel, as the vehicle negotiated the horseshoe driveway. Blast modeling suggests that the damage probably would have been one and a half times as costly if it had gone off at the entrance.

## CONCLUSION

As with all catastrophe risk modeling, progress in model development and user confidence depend to some degree on the future turn of actual events. All models are rooted in actual loss experience. Optimistically, a medium-term world future might be envisaged where the threat from Islamist militants had been so suppressed as to vitiate the need for U.S. government involvement in terrorism insurance. However, few terrorism experts would take such a positive perspective. Apart from the general political volatility of the Arab world, persistent unease among Muslim communities over the plight of the Palestinians, Chechens, and Kashmiris may further radicalize small groups of impressionable Muslim youths into joining the Jihad. As shown in past terrorist campaigns, it only requires a tiny minority of militants to maintain and carry out the threat of terrorist acts. Where such militants are born and raised in the West, and thus are entitled to the full legal and human rights accorded to citizens of democracies, the threat is harder to uncover and eradicate.

The insurance industry as a whole should be concerned with the level of the terrorist threat, not just over a short term horizon of the next few years, but as it evolves over several decades. A far-sighted insurance risk manager may endeavor to develop a terrorism book of business so that it should remain profitable over this extended medium-term period—even if a major loss were to be suffered. Over the next few decades, the demand for terrorism insurance is likely to be sustained by the tide of Islamic fundamentalism, which may ebb and flow, but even if at a low level, it may be swelled by the oratory of charismatic radical religious leaders—fundamentalists like Muqtada Sadr.

As time passes, the empirical terrorism database of successful, failed, aborted, and foiled attacks becomes statistically ever more substantial and robust. Progressively, the underlying causes and manifestations of terrorism are being understood better, and the complex web of Islamist terrorist networks is being tracked more closely. Furthermore, the paramount importance of security in risk control is becoming ever more evident. But even if an insurer has been meticulous over property security, and is satisfied that it can quantify its portfolio terrorism risk with a reasonable degree of confidence, the risk of extreme loss from spectacular multi-target attacks, even if very slight, may still be deemed commercially unacceptable, unless there is some explicit external government safety net. The risk-reward curve may otherwise be unattractive, especially allowing for adverse selection. The continued vigor of the U.S. terrorism insurance market may thus depend on cautious risk-averse insurers having this external support. As in Robert Kagan's metaphor of the camper in a forest with a prowling bear, sleeping at night is so much easier if someone else has already taken care of the most worrying risk.