

THE EVOLUTION OF TERRORISM RISK MODELING

*Written by Dr. Gordon Woo
for the Journal of Reinsurance*

*Risk Management Solutions Ltd.
10 Eastcheap, London EC3M 1AJ, England*

April 22nd, 2003

1. ROOTS OF TERRORISM MODELING

As with natural perils, the insurance of international terrorism risks has a long history, pre-dating any attempt at formal risk analysis. In the absence of computational tools, risk management has traditionally relied upon the experience and judgement of specialist political risk underwriters, who have often proven effective and skilful in circumstances where mainstream underwriters have declined to offer terrorism coverage. For certain individual terrorism risks, specialist underwriters might seek the advice of law enforcement or military personnel, proficient at surveying site security. For a regional portfolio, premiums might be set higher for locations historically attacked or threatened by terrorists, and maximum aggregate loss exposure would be carefully monitored and capped, but the overall risk assessment procedure would remain essentially qualitative.

To anticipate rare acts of terrorism, beyond the experience of even the most seasoned underwriter, the judgement of external terrorism experts might be invoked. Terrorism risk management would still be largely qualitative, with underwriting being supported by the greater knowledge and perception of terrorism experts as to the intent and capability of the terrorists. For organizations, such as the IRA, whose acts of terror were politically restrained, this qualitative risk management approach might suffice, but for Al Qaeda, whose threats of violence acknowledge no such political or moral restraint, a more formal analytical methodology is demanded. This methodology has evolved rapidly since 9/11, in response to US insurance industry concerns about the viability of terrorism underwriting, and subsequently the passage of TRIA, the Terrorism Risk Insurance Act.

TRIA applies to foreign terrorism, of which there was little before 9/11, but does not cover domestic terrorism. However, the insurance loss burden from US domestic terrorism has been sufficiently low as to be effectively absorbed within the losses from criminal acts of violence and vandalism, which many home-grown terrorist acts resemble. Attacks on vivisection laboratories, mink farms, hamburger restaurants, ski resorts, sports utility vehicles etc. might be committed under the banner of the Animal or Earth Liberation Front, but nonetheless are crimes by another name. Right-wing militias have hatched more grandiose attack plans by which to rein back perceived government erosion of individual freedom, but such anti-government sentiment diminished after the Oklahoma bombing. Furthermore, left-wing terrorism has never recovered its motivation

or state support since the fall of the Berlin wall. As a result, US domestic terrorism may still be treated as a residual background loss burden, geographically distributed broadly across the USA. But whereas US domestic terrorism risk can be managed conveniently at an aggregate loss level, the much more severe threat from Al Qaeda and associated Islamic militants requires scenario-specific modeling.

1.1 Deterministic Scenario Loss Modeling

Coincident with the shock of the 9/11 Al Qaeda attack itself was the shock realization that an enormous aggregate insurance exposure, across many lines of business, was concentrated around a single location. Whatever the terrorist threat may be, insurers need to understand and control their exposure accumulations. Accordingly, GIS software tools are being licensed which allow insurers to map their exposures, and to evaluate loss potential within designated spatial footprints. These losses may vary significantly from one footprint to another, so worthwhile insight is gained by compiling a loss-footprint table. Ranking these losses by severity leads inexorably to the critical actuarial issue of estimating probable maximum loss.

In earthquake insurance, a deterministic approach may be taken to estimate Probable Maximum Loss (PML) using the following three-step procedure: identify the fault posing the greatest threat to the portfolio; assign the maximum credible earthquake to the fault; calculate the portfolio loss assuming this sized event occurs on this fault. For terrorism insurance, this kind of deterministic PML approach may also be attempted, assuming that a maximum credible size of weapon is deployed at the spot where it would cause the worst portfolio loss. This deterministic approach largely removes the human behavioral component from PML estimation, since it assumes pessimistically that the terrorist will have the upper hand in his conflict with counter-terrorism forces, and be allowed the weapon and target of his choosing.

This conservative assumption reduces PML estimation to a series of problems in the domain of the engineering, physical, chemical and biological sciences: evaluating the blast effect of a bomb detonation; the extent of fire from a fuel tanker explosion; the radiation fall-out from a radiological dispersal device; the spread of contagion from a smallpox outbreak etc.. These problems may still be technically complex and challenging, but at least the core mathematical models for blast analysis; conflagration; atmospheric dispersion, pollution transport, epidemiology etc. are well established. The models are founded on standard scientific principles, and the model results have some validation against observational or surrogate data. But, as with the vulnerability of individual buildings against earthquake or windstorm loading, lack of detailed information about a building's protection against a terrorist attack limits the resolution of site-specific loss estimation. Another limiting factor for workers' compensation and other casualty risks is the temporal variation in the size of population within the area under terrorist attack. Generic assumptions may be made for this, as for supply chain bottlenecks which may indirectly affect business interruption.

The uncertainty in scenario loss modeling is one reason why, as with natural hazards, a deterministic terrorism PML approach can only be partially satisfactory. Another cogent reason is that the probability of extreme loss is not addressed. Detonation of a nuclear device, or the sabotage of a nuclear plant, might lead to massive losses, but these hypothetical contingencies should not dominate terrorism PML evaluation, since these are very unlikely, even if conceivable, scenarios. PML is best inferred from the tail of a loss exceedance probability distribution, which can only be constructed through a probabilistic terrorism risk model. Assignment of probabilities to the terrorist attack scenarios is a task which has an intrinsic human behavioral dimension, and so requires a new set of mathematical modeling tools, and makes greater recourse to the elicitation of expert judgement than for natural hazards.

1.2 The Use of Expert Judgement

Prior to the Earth Science revolution of plate tectonics in the 1960's, earthquake risk assessment was predominantly judgement-based. There were historical catalogs on past earthquakes, but no adequate theory by which seismic phenomena might be properly understood. Even into the 1980's, professional seismologists, who monitored earthquakes, were sceptical of the objectivity of practical engineering seismic hazard analysis. But with the increasing power of computation and theoretical developments, earthquake modeling has become more quantitative, and less subjective. In principle, not just terrorism or earthquakes but any technical risk issue may be resolved simplistically just by direct interrogation of experts. One might ask US space-flight engineers the probability of a shuttle disaster, or UK railway workers the probability of a rail crash. Answers can be readily obtained through such direct use of expert judgement, but we have known since at least the Challenger disaster of 1986, that this is not a very reliable approach: an underlying structural event model is needed. It is hard to avoid a fair measure of expert judgement in terrorism risk assessment, but minimizing subjectivity is key to the scientific evolution of terrorism risk modeling.

Where expert judgement is elicited, the most informed terrorism experts should be sought: those in the prime of their careers, engrossed regularly in advising and receiving intelligence from governments and leading news agencies. Since Al Qaeda operates in almost a hundred countries across the globe, the use of international experts is crucial. These experts should have active contact with terrorists and a current appreciation of their modus operandi. Because each expert is privy to his own sources of intelligence often gained verbally from debriefings, and has his own security clearances, there is no common database of information upon which all experts can form their judgements. If there were a common literature, as in the sciences, relevant publications could be distributed to all experts, whose opinions might then be elicited on an individual basis. But the world of intelligence is opposite to that of science: the most crucial information is often the most confidential. Accordingly, expert judgement is well elicited through decision conferences, at which intelligence and other confidential information can be pooled and opinions shared.

2. QUANTITATIVE TOOLS FOR TERRORISM RISK MODELING

The most rigorous attitude to any risk model development spurns the excessive use of expert judgement, and terrorism risk is no exception. The use of expert judgement can be minimized through exploring and developing mathematical models and simulations of the underlying causative processes, which can then be parametrized from observational data. In the following sections, a review is given of mathematical concepts which have already found their way into advanced terrorism risk modeling, and an outline is given of additional ideas which currently are being researched.

2.1 Model for the Occurrence of Terrorist Attacks

Randomness plays a significant part in any human conflict. This is reflected in Bismarck's perceptive comment that when you draw the sword, you roll the dice. But there are causal factors as well, which shape the conflict landscape, including the temporal pattern of successful attacks. In constructing a stochastic model of terrorist attacks, these non-random factors need to be taken into account through invoking an appropriate methodological paradigm, such as cybernetics. Magnus Ranstorp, director of the renowned Center for the Study of Terrorism and Political Violence at St. Andrews University, 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. In particular, the time development of the Al Qaeda conflict is a stochastic process which may be described by a controlled Markov chain model.

At any moment in time, the predator (i.e. Al Qaeda) is in some specific state of attack preparedness, whilst the prey (i.e. USA) is in some corresponding state of defense preparedness. In a democracy, there are rigorous checks and balances imposed on the law enforcement and security services. Accordingly, the counter-terrorism response has to be commensurate with the terrorism threat: draconian measures (e.g. detention without trial) are only tolerable when the threat level is high. Democracies are prevented constitutionally from mounting an unlimited war on terrorism.

A Markov chain is defined by the series of states that Al Qaeda occupies, and makes transitions to and from. This is a controlled Markov chain because, whatever state Al Qaeda occupies, the police and security forces counter the prevailing threat with actions which aim to control terrorism. These actions are commensurate with the threat, and hence are a function of the Al Qaeda state. Because of these controlling counter-actions, the process of attack occurrence is not Poissonian, as is generally assumed for natural hazards. In mathematical terms, these counter-actions are termed the *Markov feedback policy*. The Markovian concept of a system state is well suited to the fluctuating dynamics of the terrorism conflict, with the need for periodic updating of the threat situation. System states are distinguished from one another in respect of significant differences in the terrorists' organization, attack capability, and modus operandi. In some substantive degree, the threat parameters vary from one state to another. In increasing

threat order, the alternative states of the terrorist network range from destabilization, to facility at launching conventional attacks, to capability of attempting attacks using weapons of mass destruction.

The term *macroterrorism* has been coined to describe a spectacular act of terrorism, (which may be a multiple strike at several locations), which causes more than \$1 billion of loss, or 500 deaths. Minor ‘potboiler’ terrorist acts, such as house bombing, may occur haphazardly, but the occurrence of spectacular macroterrorism events does not satisfy the prerequisites of a Poisson process. Once a terrorist’s message has been delivered successfully across the media through a spectacular macroterrorism event, perhaps after a series of failures, a publicity reminder may not be needed for a while. On the counter-terrorism side, following an act of macroterrorism, security and border controls are inevitably strengthened, and extra government funding made available for improving protection. Civil liberties may be temporarily curtailed as suspects are detained without trial, and the human rights pleas of asylum seekers and refugees may be denied. Examples of more brutal terrorism suppression methods are to be found from previous conflicts. Scandalously, in response to an IRA bombing outrage at Enniskillen in 1987, the British security services even colluded in the murder of a Catholic human rights lawyer in an attempt to control support for republican violence.

2.2 Adaptive Learning of Attack Modes

‘Avoid strength, and attack weakness’, a saying of the legendary military strategist Sun Tzu, is a fundamental precept for the terrorist conduct of asymmetric warfare against a much more powerful adversary. For Al Qaeda, this may be expressed in the succinct language of physical science as: *follow the path of least resistance*. The notion that this principle may guide the probability distribution of certain human actions was originally developed by Zipf in his quantitative sociological studies, and may be considered in the context of attack mode preferences. One of the main signposts on the path of least resistance is adaptive learning. Al Qaeda is eager to learn from past terrorist experience – the successes and failures of attacks perpetrated by its own network, and by other terrorists around the world. Al Qaeda would tend to ‘copycat’ methods which either have proven to be successful, or are perceived to have the potential to be successful. If an attack mode has demonstrated effectiveness, or has the promise of being effective, it is likely to be an attack option. Statistical learning models may be more relevant than pure frequency models in quantifying attack mode likelihood.

The basic arsenal for terrorists contains a range of conventional weapons: improvised explosive and incendiary devices, and standard military weapons such as automatic rifles, grenades, mortars, and surface-to-air missiles. Sticking with off-the-shelf or tried-and-tested weapons might seem to be the easiest strategy, but further variety in attack modes is necessary from time to time as it keeps counter-terrorism forces guessing. This necessity leads to the invention of unconventional attack modes: industrial, infrastructure and agricultural sabotage, hijacked jets, helicopters and ships, bomb-laden boats and

planes, chemical-biological-radiological-nuclear (CBRN) weapons, cyberspace hacking, food and drink contamination etc..

The process of terrorist attack mode selection can be simulated as follows. At any given time, there is a small probability that a new terrorist attack mode will be chosen, and a complementary probability that one of the existing attack modes will be chosen. In keeping with the principle of adaptive (copycat) learning, the relative likelihood that a specific existing attack mode will be preferred may be assumed to be an increasing function of the amount of its previous usage. The more often an attack mode has been used, the more likely it is to be re-used in another terrorist operation. This usage growth pattern is common to a number of sociological contexts, where this type of stochastic growth modeling has proved instructive. An outcome of this simulation is insight into the empirical probability distribution of attack mode preferences: some of the key modes dominate the distribution, with a long tail of other ancillary attack modes.

2.3 The Selection of Targets

There is an earthquake engineering adage that an earthquake will expose the weakest link in a building. But if a number of structures are randomly distributed in a region, the pattern of seismicity does not alter so that the weakest structure is most likely to be shaken. Yet, with a terrorist threat to a number of prize targets, the most vulnerable may have the highest probability of being attacked. As with burglar alarms, self-protection has the externality of shifting risk to one's neighbors. This effect may be recognized explicitly using the mathematical theory of conflict, i.e. game theory, which is a collection of tools designed to help understand the interaction of decision-makers.

The two fundamental precepts underlying game theory are that the protagonists are rational and intelligent in strategic reasoning. These are justifiable for macroterrorism. As a weaker force confronting a nation state with far greater military and economic resources, a terrorist organization needs to have a smart strategy to survive and launch spectacular attacks: terrorists poor in strategic reasoning fade rapidly into oblivion. Indeed, Dr. George Habash, co-founder of the Popular Front for the Liberation of Palestine, referred to terrorism as a thinking man's game. Like Dr. Habash, Dr. Ayman Al-Zawahiri, the Al Qaeda chief strategist, was an eminent doctor before turning to terrorism, and noted for his brilliance.

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 USA suffering loss; and terrorising the general public. Nor is it necessary that a terrorist's preference relation conform with those of society at large. Game theory is not restricted to any one cultural or religious

perspective. In particular, we should not be surprised if a terrorist who prefers the company of ladies in Paradise to men on Earth takes action along the path to martyrdom. For the faithful, martyrdom is a rational choice: everyone has to die, so why not die on the path of God?

The test of any mathematical risk model is its explanatory and predictive capability. Game theory predicts that, as prime targets are hardened, rational terrorists will tend to substitute lesser softer targets. This prediction is essentially equivalent to the statement made by the CIA director, George Tenet, in his prophetic unclassified but unheeded testimony of February 7, 2001, (prior to 9/11): 'as security is increased around government and military facilities, terrorists are seeking out softer targets that provide opportunities for mass casualties.' In the language of terrorism experts, this is called target substitution. A year after the destruction of the World Trade Center, the Bali bombing provided another tragic confirmation of this game theory prediction. A bomb left at the US consulate perimeter fence was too distant at 100 meters to cause any damage, but a bomb-laden truck could park immediately outside a nightclub and kill hundreds. Explicit admission of this soft target strategy has since come from Khalid Sheikh Mohammed, the Al Qaeda chief of military operations, who was arrested in March 2003. Further validation of the terrorism target prioritization model is provided by analysis of the IRA campaign in Ulster and England, and the GIA campaign in France. The success of this game theory model illustrates the future potential for quantitative terrorism model development.

3. DEVELOPMENTS IN TERRORISM SIMULATION

The simplest approach to modeling a conflict is by considering the interplay between two opposing force blocks. This is the approach described above, with the terrorist organization opposing the counter-terrorism organization. But extra insight into the dynamics of a terrorist network can be gained by looking inside: analysing the social network of inter-connections between network nodes, which correspond to individual terrorists. The French magistrate, Jean-Louis Bruguière, has aptly likened Al Qaeda to a virus. In order to survive, a virus must mutate faster than its environment changes. Similarly, the Al Qaeda network has shown flexibility in adapting to survive counter-terrorism action. This adaptation process can be simulated by evolving the social network according to a set of basic rules.

Nodes communicate with one another to exchange information, financial and logistical resources, subject to the risk that any communication might be detected by security services. Local cells are autonomous to a substantial degree, and recruit attack team members and carry out target reconnaissance. Spectacular attacks are planned, but the larger and more ambitious that an attack becomes, the higher the chance of it being compromised by one of the attack team. If any node is removed from the network, there is a chance that any node connected to it might also be named and removed. Thus, the

more hierarchical the network, the greater the chance of destabilization through the arrest of senior leaders.

Through repeated computational network simulation following these rules, an ensemble of different network evolutions can be generated, the contrasting patterns of network structure can be studied, and the relative likelihood of different network configurations can be gauged. From analysis of these simulations, cell statistics and the network capability to launch major multiple attacks can be assessed probabilistically.

Such network analysis has to cope with the problem of missing data. As in the war on terrorism, massive amounts of uncertainty and dearth of data plague decision-makers on the military battlefield. Where should we attack? When should we attack? What weapons should we use? These are some of the critical questions facing military leaders. In this parallel warfare context, battle decisions might just be left to the judgement of generals, rather as terrorism insurance decisions might be left to the judgement of underwriters. Creditably, instead of an air of technical resignation pervading the Pentagon, massive investments of resources are being made to provide quantitative decision-support tools for the military. Sophisticated methods of combat modeling are being developed which incorporate all manner of extraneous factors that impact upon the decision-making processes of battlefield commanders. This wargaming has been substantially advanced through a variety of quantitative means: mathematical equations, also large-scale simulations, and distillations (i.e. relatively simple simulations that capture the salient features of the situation, without trying to model all the details). Similar bottom-up combat modeling initiatives are being explored for the war on terrorism. One of the purposes of the analysis is to identify emergent dynamic behavior, such as might arise if there were a concentration of terrorist resources in a particular threat mode, as defined by choice of weaponry, target and mode of attack delivery.

4. CONCLUSION

The terrorism threat from Islamic militants may well be the defining conflict of the 21st century. Already, wars in Afghanistan and Iraq have been waged by the USA in retaliatory response to this perceived threat. In his seminal treatise, 'Paradise and Power', Robert Kagan has elucidated starkly the different parts that America and Europe play in the new world order which is unfolding. Kagan explains this using a metaphor from the Wild West. In dealing with rogue muslim states, the world's superpower is prepared to play the role of the sheriff, even while weaker European nations play the role of saloon-keepers doing business as usual. The price of such Middle Eastern intervention by USA is likely to include increasing hostility amongst muslims around the world. Given that Islamic extremists form the apex of a pyramid of global muslim discontent, the need for US insurance against foreign terrorism seems assured for decades to come.

The maneuver warfare techniques used by the US military for decision-making, and successfully exercised in the Iraq war, are being made more elaborate, complex and

computationally intensive. Progress is being made to introduce these techniques into terrorism risk assessment. The insurance industry plays a key part in the war on terrorism, not least by devising risk-based methods to assist Homeland Security in the allocation of finite resources for civil protection, and the Office of Management and Budget in the cost-benefit analysis of federal security legislation. With such diverse and important commercial and government applications, the methods for quantifying terrorism risk will continue to evolve with increasing mathematical and computational sophistication, in the same way that the methods for quantifying windstorm and earthquake risk have systematically advanced over the past decade since the devastation caused by Hurricane Andrew and the Northridge earthquake.