INSURING AGAINST AL-QAEDA

By Dr. Gordon Woo

Risk Management Solutions Ltd.
(Gordon.Woo@rms.com)

National Bureau of Economic Research Meeting, 2003

ABSTRACT

The broad spectrum of domestic terrorism in the USA has traditionally been underwritten as an insurance risk without the need for elaborate risk management tools. The disparate aims, origins, and domiciles of the various US terrorist groups provide an intrinsic degree of portfolio diversification, and risk accumulations are bounded by the limited damage objectives and capabilities of disaffected US citizens. By comparison with the sizeable database of domestic terrorist acts, the record of foreign attacks is barren: until 9/11, the US mainland had not been attacked since the British burned the White House in 1812. Against a background of al-Qaeda threats to 'destroy' America, insurers are obliged by the Terrorism Risk Insurance Act of 2002 to offer insurance coverage against foreign attacks. This paper outlines steps by which this coverage may be managed in a risk-informed manner, using knowledge of al-Qaeda modus operandi, expressed in a logical form suitable for decision-making on pricing and accumulating terrorism risk.

PRINCIPLES GOVERNING THE AL-QAEDA THREAT

Most scientists are surprised that the theory of fractals, which is a universal descriptor of the natural world, emerged from the dedication of a pacifist mathematician, Lewis Fry Richardson, to comprehend the outbreak of wars. Richardson showed that some degree of quantitative synthesis is achievable for human conflicts. This synthesis can never extend to predicting when wars occur, but it does provide insight into the risk of war breaking out. Similarly with low-intensity conflicts, nobody can predict the timing of the next major terrorist attack by al-Qaeda, but insight into the risk of an attack may be gained from comprehending and analyzing the principles that govern the al-Qaeda threat.

The principles expounded here were jointly elicited from two foremost international experts on terrorism: Rohan Gunaratna, author of 'Inside al-Qaeda' (2002), and Magnus Ranstorp, author of the book 'In the Service of al-Qaeda' (2003). Both of these experts have spent many years immersed in the study of this terrorist network and affiliated Islamic militant groups, and have direct access to their training manuals and tapes, as well as to a number of the terrorists themselves. Both are at the Centre for the Study for the Study of Terrorism and Political Violence at St. Andrews University. As Ranstorp (1997) demonstrated in his painstaking analysis of the tangled web of Middle Eastern

politics underlying the Lebanese hostage crisis in the 1980's, an assessment of a terrorist threat can only be superficial if the complex political background is not comprehended.

Following the Path of Least Resistance

With natural hazards, an understanding of the underlying principles governing these phenomena is essential if modeling is to progress beyond the level of statistical data analysis. Historical disaster catalogs are a valuable resource for flood hazard assessment, but this should be guided by basic hydrological principles, which find elegant mathematical expression in optimality criteria. *Following the path of least resistance* is one such principle, which is applicable also to al-Qaeda. Avoiding strength, and attacking weakness is a fundamental precept for asymmetric warfare, expounded by the master strategist Sun Tzu in the Art of War: *'Now an army may be likened to water, for just as flowing water avoids the heights and hastens to the lowlands, so an army avoids strength and strikes weakness'*.

In hydrology, the principle of minimum energy expenditure governs the pattern of river drainage networks. In a similar way to the flow of water, the flow of al-Qaeda terrorism activity is towards weapon modes and targets, against which the technical, logistical and security barriers to mission success are least. Since 9/11, the counter-terrorism environment for the development of new weapons and planning complex strategic operations has become oppressive for al-Qaeda. Increasingly, like a scavenging bear in the wild, it is becoming obliged to take targets of opportunity. Accordingly, it may look towards off-the-shelf, ready-to-use weapons, (such as SAM or Stinger missiles, hijacked aircraft, and propane tankers), or improvised conventional explosive devices, which do not involve intricate and potentially failure-prone technological development. The Mombasa attacks on November 28, 2002 were a stark restatement of this principle.

There is continued financial support from international Muslim communities to buy weapons, but skills to develop new weapons are becoming more scarce, given the security crackdown on al-Qaeda. In general, the more complex the weapon, the more terrorists there are with knowledge which may be compromised. For example, dozens of al-Qaeda operatives would need to be involved in the assembly of a nuclear detonation device. Given the vital role of trust in forging relationships in Islamic culture (Rosen, 2002), missions which have high manpower demands will tend to take more time to prepare, especially when key nodes of the al-Qaeda network are being removed by counter-intelligence.

Name Recognition of Targets

In the aftermath of 9/11, Osama bin Laden rejoiced that 'America had been struck by Allah in its vital organs'. Others in the Islamic world, and in continents beyond, recognized the targets, and chanted 'Osama'. Name recognition is a key factor in targeting for several reasons. If a strike against America is to be inspirational, the target

should be recognizable in the Middle East to the faithful, whose knowledge of America would be gained mainly from television and the newspapers, rather than through tourism. Secondly, a US target of opportunity may serendipitously appear on the Middle Eastern broadcast or print media, and may be picked for an al-Qaeda operation. Thirdly, those who present themselves for martyrdom operations are not indifferent to the style of their certain deaths: it would be futile to die in a foreign land striking a nameless target in the middle of nowhere.

Adaptive Learning from Past Experience

Al-Qaeda seeks to maximize success and minimize failure in launching its attacks, because these are designed to inspire the global Islamic Jihad. Like a neural network, al-Qaeda is known to be highly adaptive in learning from past successes and failures of their own as well as other terrorist groups. Thus practical lessons in suicide bombing were learned from the Tamil Tigers (LTTE) in Sri Lanka. Methods which have been successful in the past will tend to be replicated; attacks which have failed will tend to be discarded. Taking the example of improvised explosive bombs, the simple truck bomb recipe of fertilizer mixed with fuel oil, which the IRA mastered to great effect, is one which is used by Islamic militants, as effectively demonstrated in the Bali night-club attack of October 2002.

From adaptive learning studies in biology (Bonabeau et al., 1999), a mathematical expression for the relative likelihood of attack mode J is given below in terms of the number of previous attacks N_A of a general attack mode A. If the index k is unity, and the constant c is zero, then this relative likelihood is just the observed relative frequency. However, a higher value of the index would accentuate the continued usage of past successful attack modes, and recognize the phenomenon of copycat attacks.

$$\frac{\{c + N_J\}^k}{\sum_A \{c + N_A\}^k}$$

Clearly, because counter-intelligence forces are themselves adaptive, it is not enough just to repeat a past operation; there must be variety in these operations. In this regard, Ashby's Law of Requisite Variety, a basic law of cybernetics, is relevant. This states that, in order for one system to control another, the controlling system must contain at least as much variety as the system being controlled. For counter-intelligence forces to exert a measure of control over al-Qaeda, there must be a response for every terrorist action. It is in the interests of al-Qaeda to increase the entropy of the process by which its operations are undertaken, so that these are obscured from surveillance by their dynamical complexity. One way of boosting entropy is to increase the possible range of alternative operatives and targets for a mission. As a supply chain process, this is far from efficient, but then al-Qaeda is not short of funds, despite counter-terrorism efforts to impose a financial squeeze. With sufficient money available to sustain its operations, al-Qaeda maximizes its operational throughput subject to a loose financial cost.

PRINCIPLES GOVERNING THE COUNTER-TERRORISM RESPONSE

Interdicting Planned Attacks

It is known that four out of five IRA planned attacks were thwarted by MI5. Infiltration of the IRA by intelligence agents, and the use of republican informers, established this high interdiction rate. Such human intelligence is harder to gather for al-Qaeda operations, because agents encounter higher trust barriers, which take longer to surmount. But valuable human intelligence is being gained from operatives in captivity, as well as from seized computers and documentation. To supplement human intelligence, much effort is being directed towards the acquisition of intelligence from remote electronic sources.

The challenge of thwarting an attack by al-Qaeda has analogies with hunting down a swarm of submarines. In anti-submarine warfare, a key defensive tool is signal processing to extract the submarine signal from the background noise of the sea. In the context of al-Qaeda, the problem is to search for anomalies in the vast global electronic transaction space covering finance, credit cards, education, travel, immigration, transportation, housing and medicine. But just as submarines strive to minimize their acoustic signature, so terrorists will try to minimize their transaction space signature. However, through meticulous searching for electronic traces of terrorist activity, augmented by human intelligence and covert surveillance, the dots of a planned attack may be joined up; the conspirators identified and tracked; and the attack pre-empted. Since 9/11, the interdiction rate has been substantial, if perhaps not at the level achieved for planned IRA attacks.

Destabilizing the al-Qaeda Network

The quantitative tools for modeling social networks, developed by mathematically oriented sociologists, help to understand network destabilization. Three principal indicators of destabilization have been listed by Carley et al. (2002). These are: [a] the rate of information flow through the network is seriously reduced; [b] the network takes much longer to make decisions; [c] the network is a less effective organization, and its accuracy at doing tasks or interpreting information is impaired. Because of the paramount importance of secrecy for terrorists, and the time it takes in Islamic society to forge relations of trust between individuals, the al-Qaeda network has always been designed to operate slowly and patiently at low efficiency. Referring to the September 11 hijackings, Osama bin Laden noted that ‘those who were trained to fly didn’t know the others. One group of people didn’t know the other group’. The sparse links between the nineteen hijackers have been charted by Krebs (2002). This trade-off between efficiency and secrecy is potentially significant for prolonging the duration of attack preparation. But as Freedman (2002) has cogently remarked after the fall of the Taliban regime, terrorists need time more than space, and al-Qaeda is both patient and diligent.

By the standards of successful business corporations, al-Qaeda has thus always tended to operate at the margins of destabilization. But how can the al-Qaeda network be destabilized down to a level of ineffectiveness? Many resistance and terrorist groups are organized as distributed decentralized networks. The fracturing decentralization of the global al-Qaeda network makes it harder to destabilize severely than a conventional hierarchical network, which may be highly vulnerable to the loss of its main leadership. Social networks are dynamic: their structures adapt as nodes are removed or isolated. Counter-terrorism forces will strive to remove key nodes. This strategy would aim to set back plans for further terrorist attacks, but it may well result in new emergent leaders. The best efforts of intelligence officers are beset by the Law of Unintended Consequences. The removal of key nodes may lead to the emergence of even more radical and ruthless terrorist leaders than before, as happened with Hamas, in the aftermath of Israeli action against its main leadership. The course of the Hamas suicide bombing campaign of 2002 charts the difficulty in suppressing a terrorist network.

Issues of network destabilization of large, multi-nodal and adaptive systems are complex, but may be addressed through a Monte Carlo simulation process. Key nodes of the al-Qaeda network are being removed by counter-terrorism forces, but they are also being gradually replaced. In the context of winning the war against terrorism, the prospect of continual and sustained network repair may seem a negative long-term outlook, but from the risk assessment standpoint, node removal increases the preparation time for an attack, and hence decreases their frequency of occurrence.

A STOCHASTIC TERRORISM MODEL

State Space Model

The term *macroterrorism* has been coined to describe an act of terrorism, (which may be a multiple strike at several locations), which causes more than $1 billion of economic loss, or 500 deaths. Minor (micro) terrorist acts, such as house bombing or kidnapping, may well occur haphazardly, but the occurrence of 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. More objectively, following an act of macroterrorism, security and border controls are inevitably strengthened, and extra government funding released for improving protective measures. Furthermore, civil liberties may be curtailed as suspects are detained without trial. But the harshness of the security regime imposed after a successful strike is eroded by the political activism of human rights groups such as Amnesty International, which do not accept the orthodox definition of terrorism. Attackers may prudently, if cynically, take advantage of democratic sensibilities and decide to delay further action until security is relaxed; circumstances which would give a later attack a higher chance of success. In practice, color-coded alert levels serve more as a guide for civic preparedness than as a threat indicator.

Efforts have been made (e.g. Enders et al., 1990) to use econometric tools to analyze statistically, through auto-regression, the time series of terrorist attacks, such as hijackings, taking account of the inhibiting effect of interventions designed to deter such attacks. With al-Qaeda, the time series is too short to permit such statistical analysis, and a simulation approach is required. A natural basis for such a simulation is a state-space approach, in which events drive the stochastic process. From a modern physics perspective, the passage of time is measured as intervals between events, rather than having intrinsic significance. This modern view happens to accord with the traditional perspective of Islamic culture, where the sense of cosmic time order is less linear and progressive than in Western society (Rosen, 2000). Rather as the Koran does not follow a chronological sequence, so the progress of a terrorist campaign by Islamic militants may ebb and flow, backwards and forwards, up and down, according to the evolving pattern of attack and defense.

The simplest representation of such a campaign is a two-state Markov process. In the first state, security is comparatively relaxed or fatigued, and conducive to a terrorist attack. In the second state, security is comparatively strict and alert, and not conducive to a terrorist attack. (It is known that Osama bin Laden has expected very high reliability levels for martyrdom operations). As a didactic illustration, consider the binary situation where attacks only take place during the relaxed or fatigued security state. If the rate of macroterror attacks in this first state is U, and the erosion rate of security in the second state is V, then, assuming a macroterror attack causes a state transition from 1 to 2, the limiting proportion of time spent in state 1 is V/(U+V), and the limiting frequency of macroterror attacks is UV/(U+V). The effect of maintaining security measures is to keep V low, and hence suppress the limiting frequency of macroterror attacks.

Constraints on The Annual Number of Successful Spectacular Attacks

In a reference to the IRA, although it would apply also to Islamic militants, Margaret Thatcher observed that terrorists thrive on the 'oxygen of publicity'. In the days before television, terrorists might signal their presence repeatedly via an intensive bombing campaign: the IRA exploded 127 devices in Britain during the late 1930's. In contrast, IRA political frustration with the Ulster peace process was vented in 1996 by a showpiece bomb blast at Canary Wharf, London's WTC, followed four months later by a truck bomb which destroyed a shopping mall in Manchester. Publicity and fear go together. The absolute number of spectacular attacks within a year, i.e. the rhythm of terror, is determined as much by publicity goals and the political anniversary calendar as by the size of the terrorist ranks. As exemplified by the IRA campaign, well-publicized occasional moderate bomb damage suffices to perpetuate a reign of fear, and concentrate the minds of politicians on the terrorist's own political agenda.

In the modern era of instant global news communication and video replay, it only requires a few major successful attacks for a terrorist's message to be firmly retained by the public. It is extremely rare for a terrorist organization to launch more than two

successful spectacular (non-synchronous) attacks against one country within 12 months. Hezbollah succeeded in bombing both the US embassy and the US marine barracks in Beirut in 1983; the Tamil Tigers (LTTE) bombed both Colombo airport and a Sri Lankan warship in 2001; and the IRA exploded large truck bombs in London and Manchester in 1996.

The probability distribution for the annual number of successful spectacular attacks, which may be determined through a Monte Carlo simulation of possible realizations of a terrorist campaign over a year, is distinctly non-Poissonian. In a simulation which recognizes the inhibiting effect of counter-terrorist interventions following any successful spectacular attack, the probability of three or more (non-synchronous) successful spectacular attacks within a year is sharply curtailed at a small fraction of a per-cent.

But just as the purpose and advantage of three or more successul spectacular terrorist attacks in a year may be questioned, the political incentive to achieve such attacks from time to time is undeniable. For an active terrorist group, a hiatus of four years between major spectacular attacks is long by historical reckoning.

The Selection of Targets

The distributed spatial intelligence of trans-continental terrorist networks allows attacks to be made across the globe, by operatives of many nationalities, at locations which may be far distant from any cell. From the bombing of the Khobar Towers in Saudi Arabia in 1996, to the Nairobi and Dar-es-Salaam US embassy bombings in 1998, to the bombing of the U.S.S. Cole in 2000, the WTC disaster of 2001, and the ramming of the French tanker Limburg in 2002, al-Qaeda have developed a swarm-like campaign of pulsing attacks from different nodes of its global network. As illustrated tragically by the Bali night-club bomb on the second aniversary of the U.S.S. Cole attack, the dependence of target location on vulnerability introduces a nonlinear feedback in risk computation.

This feedback may be recognized explicitly using the mathematical theory of conflict, i.e. game theory. The hijacking of a Singapore Airlines plane in March 1991 by Pakistani militants provided an early case study of the use of game theory in terrorism strategy. In the context of negotiations with terrorist kidnappers, the dominant strategy for a government is to execute a raid, provided that the public are led to believe that the terrorists started shooting first, so that the government is not blamed if hostages are killed. The violent resolution of the Moscow theatre Chechen hostage crisis of October 2002 might have been previsioned by a game theorist. Another issue of terrorist strategy of interest to a game theorist is target prioritization.

Consider the potential targets in the USA, and suppose that they have been ranked in discrete city tiers and type classes (skycrapers, bridges, nuclear plants etc.) by terrorism experts, according to their attractiveness (or utility). Symbolic and publicity value; name recognition in the Middle East; economic and human loss consequence would be factors

in gauging target utility. In order to express target prioritization in a quantitative way, the ranking by city and target type has to be converted into mathematical form. This interpolation is simply achieved by invoking Fechner's Law, which states that an arithmetic progression in human perceptions requires a geometrical progression in their stimuli. This implies a logarithmic formula for the utility of the C'th city tier, and for the T'th type class. This form of rank interpolation allows the logarithm of the utility to be written parametrically as:

$$Log\{U[C,T]\} = k_0 - k_1 C - k_2 T$$

In order to arrive at a target probability distribution, a mathematical expression needs to be obtained for the functional dependence of target probability on utility. For this, game theory is required. It is known that al-Qaeda is committed to achieving success, is watchful that missions are cost-effective, and is sensitive to target hardening. In order to ensure, as far as possible, that a strike will be successful, irrespective of defensive action by security forces, al-Qaeda will effectively seek to minimize the impact of target hardening. From knowledge of its modus operandi, this goal is attained by al-Qaeda by adopting a mixed strategy of randomizing its target selection, meticulously undertaking surveillance on targets and avoiding targets where the level of security is very uncertain; and switching targets if the original target has hardened. This might happen if the National Guard were deployed, or the police were working over-time; resources which are sparingly used, because they are expensive for civic authorities to procure.

For an attack using a specific weapon against a target in category [C,T] with defense D, let P_D be the probability that the defense is unable to prevent or stop the attack. As increasing defensive resources are applied to protect targets of high utility, the marginal improvement in security diminishes. This is reflected by a defense saturation condition, the power-law form of which is motivated by the fractal nature of defense-in-depth hierarchy (Paparone et al., 2002), as realized, for example, in multiple defence barrier models (Major, 2002):

$$\frac{\partial P_D}{\partial D} \propto -U[C,T]^{-\lambda} \qquad (\lambda > 0)$$

For a mixed attack strategy, designed so as not to be impaired by changes in defense strategy, game theory optimization analysis suggests that the probability of selecting a target $P(U[C,T])$ may be expressed as follows (Major, 2002):

$$1/P(U[C,T]) \propto -U[C,T]\frac{\partial P_D}{\partial D} \propto U[C,T]^{1-\lambda}$$

Combining formulae, the following result is obtained:

$$Log\{P(U[C,T])\} = a - (\lambda - 1).k_1 C - (\lambda - 1).k_2 T$$

Substituting b_1 for $(\lambda - 1).k_1$, and b_2 for $(\lambda - 1).k_2$,

$$Log\{P(U[C,T])\} = a - b_1 C - b_2 T$$

From this equation, one can see that the relative likelihood of targets being selected depends simply on the two parameters b_1 and b_2. The form of this equation is reminiscent of the elegantly simple Gutenberg-Richter relation in seismology, which is the cornerstone of seismic hazard analysis. As with the Gutenberg-Richter relation, the parsimony of the equation, which has just two parameters to determine, compensates for the approximate nature of the model. The notation, b_1 and b_2, is chosen to echo the Gutenberg-Richter b-value. As with the seismological b-value, the parameters b_1 and b_2 may be estimated from empirical data, supplemented by expert judgement, where data are sparse. Note that the game theory impact is to shift the target probability distribution away from the targets of highest utility, which are likely to be well defended. This is in keeping with intelligence warnings of possible attacks against relatively soft US targets: apartments, shopping malls, railroads etc..

Evidence for a logarithmic terrorist target prioritization formula comes from data on IRA attacks during the Troubles from 1969 to the ceasefire in 1994. With London being the central hub of military, government, financial and tourist activity, it is not surprising that the great majority of IRA attacks on the mainland were focused on London. However, England's second and third cities, Birmingham and Manchester, each were bombed a similar number of times. By contrast, England's lesser cities were only seldom bombed. The city target prioritization is representable by a logarithmic formula with London alone in class 1; Birmingham and Manchester in Class 2; the next six largest English cities in Class 3 etc..

The catalog of IRA killings in Northern Ireland during the Troubles from 1969 to the ceasefire in 1994 provides an example of the logarithmic prioritization of target types. For Ulster terrorism, there were three distinct IRA target classes: military personnel; police and prison officers; and loyalist civilians. The prime IRA targets were military. However, target substitution took place as the wearing of body armor made military targets increasingly hard for the IRA to attack. As shown in the plot below (Figure 1), the relative numbers of killings follows a logarithmic trend.

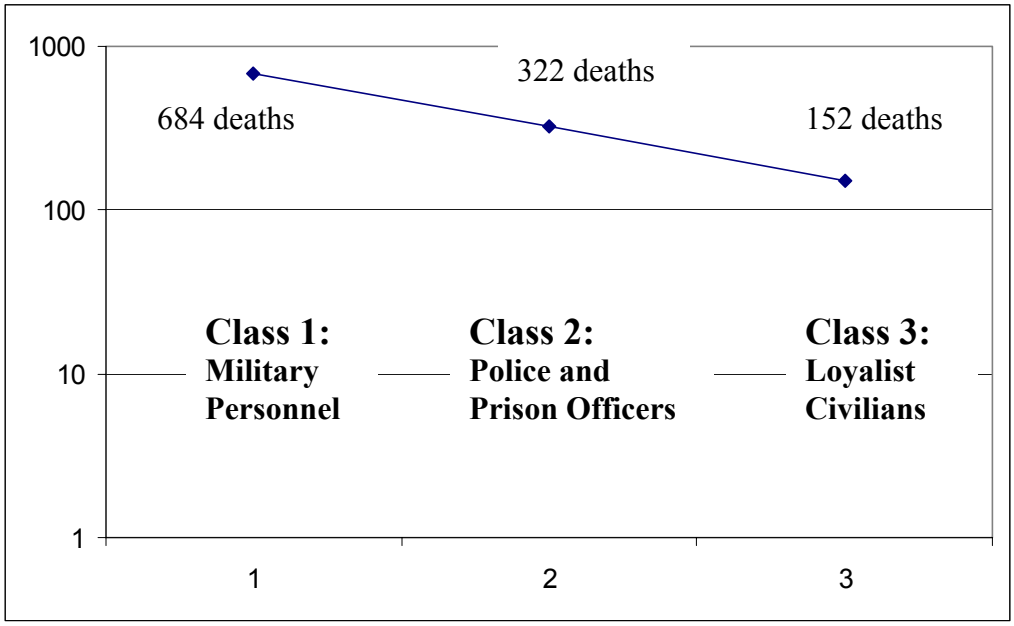

Figure 1: IRA Killings in Northern Ireland during the Troubles: 1969 - 1993

The Loss Severity Distribution

Before war was declared on terrorism, al-Qaeda could afford to take time, and devote resources, to plan meticulous attacks against targets which gained legitimacy through being emblematic of US economic, political and military power: the greater the loss, the more attractive to al-Qaeda. With this positive feedback, the loss severity distribution prior to September 11 would have been skewed towards heavy economic losses; a risk characteristic consistent of course with the WTC attack. Since its setbacks in Afghanistan, al-Qaeda has been more opportunistic in its global operations. The IRA campaign provides illustrations of the effectiveness of heightening security, and cutting off supplies of armaments, in reducing the options for terrorist action.

Given the al-Qaeda prioritization of targets and weapons, a probability distribution for the severity of losses can be computed once an assessment of the consequences of an attack is made. For this purpose, standard engineering tools are available for analysing the spatial footprints of arson attacks, bomb blasts, the dispersion of toxic aerosols, etc.. By overlaying these impact footprints on high-resolution maps of insured commercial and residential property, estimates are made of property damage, casualties, and the scale of business interruption.

TERRORISM INSURANCE

Implications of Government Self-protection

In their insightful economic analysis of self-protection against the terrorism threat, Lakdawalla and Zanjani (2002) point out that investments in self-protection may have negative external effects. As an illustration, businesses may relocate their offices away from major city centers, thus reducing local economic activity. Lakdawalla and Zanjani remark that government subsidies for terrorism insurance may act to discourage self-protection, and hence limit the societal impact of such negative externalities. Ironically, it is the US government itself which is most self-protective, and is responsible for the hardening of many of the prime targets most attractive to al-Qaeda, because they symbolize US political and military domination. As US embassies, consulates, and military bases abroad become ever more difficult to strike, Islamic militancy against US foreign policy is being directed more at the softer targets encompassing US business interests. Within the US homeland itself, target substitution is also occurring: government self-protection is transferring an additional risk burden to the softer commercial sector, and hence indirectly to insurers.

Without necessarily offering 'honey-pot' targets of opportunity, or 'briar-patch' targets of deception which invite terrorist attack, government decisions on protection levels might prudently consider the implications for target substitution, in particular the impact on those for whom protection is either technically unfeasible or unaffordable. If an aircraft were to be brought down by a shoulder-launched missile, it would be better if it crashed around an airport, where there are emergency services at hand, than in an urban area, where the risk of ground casualties would be far greater. This may sound like thinking that no government could act upon, but it is being taken seriously for airports with flight paths over metropolitan centers.

Interdependence of Risk Pricing

The passage of the Terrorism Risk Insurance Act of 2002 has been celebrated by advocates for the commercial real estate industry. Instead of remaining partially uninsured or self-insured, commercial real estate owners can insure against al-Qaeda. The stochastic model sketched above provides a quantitative basis for pricing this cover. The legislation is intended to secure adequate levels of terrorism insurance at affordable rates and reasonable terms. But, from an insurer's perspective, what is an appropriate rate? This rate has a component associated with the attack likelihood for a target of a particular type in a specified location, and a site-dependent component which is adjusted according to the dual standards of local security and vulnerability. These local factors affect the chance that any attack would be successful, and the size of the consequential loss.

Measures to increase security and reduce vulnerability are potentially expensive. But these costs may be defrayed if terrorism underwriters allow an insurance premium reduction in respect of such measures. However, such a reduction may be predicated on the actions of other agents. As Kunreuther and Heal (2002) have demonstrated through a game theory analysis, the interdependence of security may have a major influence on decision-making on protective measures. Attacks by al-Qaeda differ from common acts of criminality, such as burglary, in that they are occasional events of potentially extreme violence, focused on carefully identified and surveillanced targets. Accordingly, there exist some interesting examples of Nash equilibria.

If collateral damage would result from an attack on a neighbor, then it would be mutually beneficial if the neighbor increased security. Thus lax security against the packing of an apartment with explosive (and possibly toxic) weapons, or the parking of bomb-laden trucks, might jeopardize multiple apartment buildings in a block. If no other apartment manager takes protective action, then there may be little incentive for a lone individual manager to take action. Conversely, if every other apartment manager does take protective action, there may be a strong incentive to follow suit.

Because of target substitution by terrorists, increased neighborhood security can also have a deleterious effect. Consider the predicament of a commercial property situated in the vicinity, but outside blast range, of a recognized trophy landmark building. Because of its attractiveness as a target, the trophy building should have expensive security. Under these circumstances, protective measures would be warranted for the commercial property, lest it be taken as a target of opportunity by terrorists thwarted by the high security at their primary trophy target. The IRA campaign provides a salutary instance of a target of opportunity: a man observed accidentally, and shot dead on the spur of the moment, by a terrorist who had planned to kill somebody else.

Another possible defensive target configuration is one where a large number of similar properties are distributed across a city, and are sufficiently separated that damage to one would not affect another. There are again two clear Nash equilibria. If all but one of the properties are secure, the remaining property would be an obvious target if it were not also made secure. Al-Qaeda would be expected to be diligent and patient in seeking out the weak target for attack. Given the heightened chance of attack, the price of security should be worth paying. Conversely, if no other property is secure, the safety of the remaining unsecure property may rest purely on the protection afforded by the herd phenomenon: if a lion is intent on preying on one gazelle, it is best for the gazelles to stay together in a herd. There is safety in numbers. This seems to be the implicit safety policy adopted for a sizeable proportion of US buildings of low al-Qaeda target priority. Recognizing the contrasting types of equilibria, one may surmise the evolution of spatial patterns of distinct high-security and low-security areas, where the balance is tipped regionally between decisions for and against protection expenditure.

Terrorism Alternative Risk Transfer

Mortgage-backed securities have a latent exposure to terrorism risk, because a catastrophic attack might destroy, or render uninhabitable, a mortgaged building. Such securities are financial instruments which implicitly transfer terrorism risk. In the post-September 11 environment, such securities are being reviewed. Furthermore, given the scarcity of terrorism insurance cover, the possibility of the issuance of a specific terrorism catastrophe bond has been raised. Quantitative terrorism risk models may provide impetus for securitizing terrorism risk, or at least some parts of it. For example, one might conceive of a workers compensation terrorism catastrophe bond triggering well above the macroterrorism level, at 1000 employee fatalities. Depending on the territorial region and trigger threshold, this might be competitively priced. Another prospect would be a catastrophe bond to cover life insurers against massive losses following an attack using a weapon of mass destruction. Just as an earthquake catastrophe bond (Concentric Re) was issued to provide business interruption coverage in respect of a theme park, Tokyo Disney, so a terrorism catastrophe bond might be issued to provide coverage for loss of revenue for leading organizations in the tourism, entertainment and sports industries. Opportunities for diversification exist since terrorism exposure is spread across different continents – America, Europe or Australasia; and the risk may be property, casualty, aviation, shipping, business interruption, event cancellation etc.. Another opportunity which may develop is in the field of contingent finance. The economic fallout from another terrorism showpiece may leave some vulnerable corporations disappointed by the support from their bankers. A prior guarantee of finance is thus worth having, but at a price.

REFERENCES

Bonabeau E., Dorigo M., Theraulaz G. *Swarm intelligence: from natural to artificial systems.* Oxford University Press, 1999.

Carley K.H., Lee J-S, Krackhardt D. "Destabilizing networks". *Connections*, 24, pp.79-92, 2001.

Drake C.J.M. Terrorists' target selection. Macmillan Press, Basingstoke, 1998.

Enders W., Sandler T., Cauley J. "UN Conventions, technology and retaliation in the fight against terrorism: an econometric evaluation". *Terrorism and Political Violence*, pp.83-105, 1990.

Freedman L. "A new type of war". In: *Worlds in Collision* (K. Booth and T. Dunne Eds.) Palgrave Macmillan, New York, 2002.

Gunaratna R. *Inside Al-Qaeda*, Hurst, 2002.

Krebs. V.E. "Uncloaking terrorist networks". *First Monday*, issue7_4., 2002.

Kunreuther H., Heal G. "Interdependent security: the case of identical agents", NBER paper, 2002.

Lakdawalla D., Zanjani G. "Insurance, self-protection and the economics of terrorism" NBER working paper No. w9215, 2002.

Major J. "Advanced techniques for modeling terrorism risk". *Journal of Risk Finance*, Vol.4, (2002), pp.15-24.

Paparone C.R., Crupi J.A. "Janusian thinking and acting". *Military Review*, Jan.-Feb., 2002.

Ranstorp M. *Hizb'Allah in Lebanon*. Macmillan Press, London, 1997.

Ranstorp M. *In the Service of al-Qaeda.* 2003.

Rosen L. *The Justice of Islam*. Oxford University Press, 2000.