

TERRORISM THREAT ASSESSMENT AND MANAGEMENT

Dr. Gordon Woo

Risk Management Solutions, London EC3R 8NB

Keynote Lecture given at the NATO Centre of Excellence: Defence against Terrorism

Ankara, Turkey, 25th May 2009

Course on: Efficient Crisis Management to Mitigate the Effects of Terrorist Activities

ABSTRACT

The dynamic adaptive nature of terrorism requires a systematic and methodical intelligent strategy for terrorism threat assessment and management. Unwitting weaknesses in approach and deficiencies in scope invite strategic surprise. Effective decision-making on managing terrorism risk benefits from insights available from quantitative thinking across the range of significant risk factors. This way of thinking about terrorism is presented in a manner accessible to military and security personnel, emphasizing key conceptual principles and ideas, whilst minimizing technical mathematical detail.

This review begins with an outline framework for terrorism risk modelling, developed from construction of a spectrum of future attack scenarios. Terrorist targeting, attack mode and multiplicity are analyzed, and the prioritization of targets for attack and defence is assessed according to criteria of societal criticality, attack vulnerability, and terrorist capability. The role of counter-terrorism forces in limiting the ambition and success of major plots is reasoned quantitatively, and evaluation procedures are suggested for comparing terrorist threats. Measures to mitigate and avoid terrorism risk are reviewed, with a focus on the need for a joined-up global approach, taking account of threat shifting at all geographical scales, and adopting a sensible risk-informed approach to counter-terrorism resource allocation.

1 TERRORISM THREAT ASSESSMENT

1a. Terrorism risk model

On 11 December 2007, two 800 kg vehicle bombs were exploded in Algiers by martyrs of the Salafist Group for Preaching and Combat (GSPC). One struck the Algerian Constitutional Court at approximately 9.30 am. Twenty minutes later, a similar bomb detonated at the UN offices, destroying the building and severely damaging surrounding structures. 17 UN personnel were killed and 40 injured. Amongst the victims was a UN security adviser credited with routinely raising concerns about the threat. His warnings went unheeded. For several years, UN officials had questioned the consolidation of the organization within one building, and its vulnerable location in a small narrow street in downtown Algiers. The August 2003 UN Baghdad bomb had made it all too evident that UN facilities or individuals were likely terrorist targets.

On 11 April 2007, a vehicle bomb had targeted the main Algerian government building. On the same day, a similar attack was conducted against a police station just outside the city, and a third attempt failed in the vicinity of the World Bank and Danish Embassy. This prompted a UN request to the Algerian authorities for the installation of speed bumps and bollards, and the introduction of a local one-way traffic system. Police presence was increased, but the request was not implemented. The UN considered moving premises, but did not identify a suitable new office. A security risk assessment in October 2007 rated the risk of terrorist attacks, including vehicle bombs, as critical and very likely, with a predicted critical impact. But under pressure from the Algerian Government, the UN failed to raise the threat level.

Following the bombings, a panel of enquiry was set up, headed by the senior UN official, Lakhdar Brahimi. The panel concluded that institutional safety culture demanded personal accountability of those entrusted with the safety and security of personnel. This precipitated the resignation of the eminent international security expert, Sir David Veness, UN under-secretary-general for safety and security, and former head of counter-terrorism at the Metropolitan Police. UN Secretary-General Ban Ki-moon said Sir David accepted personal responsibility for the failures, and that the enquiry report recognized *'that risk management is not consistently understood or applied.'*

How should this best be accomplished? All risk management should be informed by a risk assessment. Typically, this is qualitative and subjective. But the desire for risk management to be consistently understood and applied points to a more structured and objective approach to risk assessment: one which uses the quantitative methods of risk modelling. Exposition of the basic concepts underlying such an approach is the purpose of this paper.

Quantitative risk modelling allows uncertainty in judgements to be accounted for explicitly, and exposes behavioural frailties such as group-think and cognitive dissonance. It also helps to detach risk analysis from external political pressure over the setting of threat levels. Furthermore, through the capacity to evaluate key risk metrics, the efficiency of crisis and disaster management can be gauged and then improved.

A terrorism risk model encompasses analysis of the threat, modus operandi, choice of weapon mode, targeting, and human and economic loss estimation. Any quantitative model has to be based on the best conceptual understanding of the underlying behavioural processes, without the bias of value judgements about political militants. This sentiment is well put in a quote from the Dutch philosopher, Spinoza, cited by Gilles Kepel in his exposition of the roots of radical Islam:

*'In order to preserve in political science the freedom of spirit
to which we have become accustomed in mathematics,
I have been careful not to ridicule human behaviour,
neither to deplore nor to condemn, but to understand'.*

The search for a risk-informed understanding of conflict and cooperation is supported by the award of the 2005 Nobel Prize in economic sciences to Thomas Schelling. He applied game theory principles to the real world problem of nuclear deterrence, and it is natural to seek practical applications to another potential existential threat, which also presents a spectre of a nuclear detonation: terrorism. If terrorism were simply a Manichaeian struggle between good and evil, or if terrorists were stupid and crazy, theorizing would be futile. Belief in the one goes with belief in the other.

Reality is otherwise: terrorists posing a significant threat are both rational and intelligent. The latter attribute is well attested. Terrorists have to be intelligent in order to make an impact in asymmetric warfare. Dr. George Habash, co-founder of the Popular Front for the Liberation of Palestine, categorized terrorism as a thinking man's game. Osama bin Laden honored Khalid Sheikh Mohammed, the 9/11 mastermind, with the title 'mukhtar', meaning 'the brain'. Indeed, it may be argued that the most powerful biological weapon in the terrorist's arsenal is not any deadly virus but the human brain itself.

In applying game theory to terrorism, it is important 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 a great political power 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.

But is it rational for a terrorist to undertake a suicide mission? Yes, according to the 17th century French philosopher, Blaise Pascal. Given the promise of eternal paradise after a martyr's death, and a non-zero likelihood of this promise being actually realized, it is perfectly rational for a terrorist to take Pascal's wager, and bet on this outcome of a martyrdom mission. It is known that some terrorists have followed this line of philosophical thought. In the words of one Palestinian: *'If you want to compare it to the life of Paradise, you will find that all of this life is like a small moment. You know, in mathematics, any number compared with infinity is zero.'*

Nobody can predict the precise timing of the next major terrorist attack. Randomness plays a significant part in any human conflict. This is the essence of Otto von Bismarck's perceptive comment that when you draw the sword, you roll the dice. But, as with natural hazards, there are causal non-random factors in man-made hazards 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. Dr. Magnus Ranstorp, Swedish Defence College, 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. 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. Democracies are prevented constitutionally from mounting an unlimited war on terrorism. As director-general of MI5 faced with the IRA terrorist threat, Stella Rimington pointed out, *'It is a feature of a democracy that a security service will follow a new security threat, rather than foreseeing it.'* At such a statement a cyberneticist would invoke Ashby's Law of Requisite Variety:

If a defender's move is unvarying, then the variety in outcomes will be as large as the variety in the attacker's moves; only variety in the defender's moves can force down variety in the outcomes.

With variety in moves to counter a broad diverse range of potential threats, the great majority of terrorist plots in the leading industrialized nations are interdicted through intelligence, public vigilance, and some good fortune. But some planned attacks are nonetheless successful. However, in democracies, counter-terrorism action is commensurate with the threat, whether high or low, and each successful attack is sure to be met with a swift counter-terrorism response which suppresses the threat of future attacks, albeit at a cost of the erosion of some civil liberties, e.g. increased surveillance and screening, stricter immigration checks etc..

1b. Terrorism threat analysis and scenario development

'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 strikes weakness.' This saying of Sun Tzu is a fundamental precept for the terrorist conduct of asymmetric warfare against a much more powerful adversary. Transcribed later in the scientific language of the French savant, Pierre de Maupertuis, *'The great principle is that, in producing its effects, Nature always acts according to the simplest paths.'*

The notion that the principle of least resistance may guide the probability distribution of certain human actions originated in sociology, 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. Terrorists are 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. Terrorists 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 become an attack option. Development of a scenario leads from weapon attack mode to attack multiplicity, targeting, and loss estimation. These are considered in turn.

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..

A hallmark of Al Qaeda operations is having multiple synchronous points of attack. High multiplicity assists Al Qaeda to meet its objective of inflicting maximal loss, and success is still claimable even if some of the synchronous attacks fail, as happened on September 11, 2001 in the USA and March 11, 2004 in Spain. Furthermore, multiple benefit can be gained from deployment of a specific surprise attack mode; defence against such an attack mode would be hardened afterwards, as with aircraft impact. Money and materiel continue to be available for multiple attacks, thus the limiting constraint for Al Qaeda on the multiplicity of an attack will be the likelihood of detection.

As the multiplicity increases, so more targets need to be surveilled, more attack weaponry procured, and more terrorists involved in planning and preparation. Progressively, the chance increases that the whole plot will be undermined by a security lapse. At some point, it would be foolhardy to expand the attack size, instead it would be best to call a halt to ambition, and stick with the existing multiplicity. The dilemma faced by a terrorist organization in increasing attack multiplicity is analogous with other types of criminal activity. Operational research analysis (Haggstrom, 1967) defines when it is optimal to stop, rather than continue and risk losing existing gains.

In a real-time terrorist crisis, after the first attack has occurred, civic authorities will be vigilant over further attacks. Anticipation of the likely multiplicity of attacks is helpful for preparedness, as is insight into likely targets. Terrorist targeting of synchronous attacks is generally gauged from the history of previous successful or interdicted attacks, terrorist communications and interrogation, as well as from terrorist open publications in printed, broadcast and virtual form. The range of targets may be narrowed by intelligence relating to an imminent attack. The efficient deployment of resources to respond to such intelligence would depend on constructing scenarios consistent with the threat update.

1c. Criticality analysis

As a general rule, the more attractive a target is to the terrorist, the better security it needs to have: offered two targets of equal security, the terrorist will typically prefer to attack that which is more attractive. The marginal cost of extra security is that which would encourage a terrorist to substitute a softer equivalent target. A major challenge for governments is to protect critical infrastructure, which is essential for the maintenance of basic societal functions and thereby attractive to terrorists.

Some critical infrastructure can be accorded enhanced protection: principal government buildings, power plants, oil and gas installations, water utilities etc.. Site perimeters of important properties can be made secure against intruders through advanced surveillance technology and physical barriers. To protect against malicious visitors, identity checks and baggage can be made routine. But extra monitoring requires additional security staff, which is an additional financial burden on operating expenditure.

By contrast, open access to public transportation limits the scope of significant security improvement. It is notable that, on the modern Beijing metro, security against Uighur and Tibetan separatist violence extends even to comprehensive passenger bag screening. However, in the western democracies, such heightened security would neither be feasible nor affordable, even if it were publicly acceptable. Crisis management plans need to be developed to cope with disruption to metropolitan transport infrastructure. This is too open to be affordably protected – it would require at least three thousand policemen to provide round-the-clock security across the London Underground. Preparedness must make do for protection: optimally from a risk perspective, CBRN disaster preparedness exercises in UK focus on an attack at a London Underground hub.

1d. Vulnerability Analysis

The efficiency of metropolitan crisis management depends on a reliable up-to-date image of urban vulnerability to the different modes of terrorist attack. Mobile security assets should be deployed where they are most needed. With intensive counter-terrorism measures instinctively taken by a government to protect its own critical property, there will be a deflected terrorism risk dispersed among softer commercial targets. Commercial property is generally not heavily defended. Organizing protection requires a clear understanding of terrorism risk, so that efforts at corporate risk mitigation are prioritized in a financially optimal manner. More than for government and civic authorities, terrorism security expenditure for commercial organizations has to be justified on a cost-benefit basis. Security is costly, both in terms of manpower and equipment, hence security measures at a particular location should match the local terrorist threat. In the aftermath of the Mumbai hotel attacks on 26 November 2008, negative security comparisons have been made with Jakarta hotels, where security has been markedly upgraded since the Marriott was bombed in August 2003.

Apart from at military bases, security guards are not normally trained or authorized to use deadly force as a response. The great majority of buildings allow vehicle access right up to the building; a minority have vehicle stand-off limits of 15 to 50 metres, with the upper distance rarely imposed. Although it may be thought profligate to have large stand-off limits, for obviously attractive targets this may be a price worth paying. Retrospectively, after Glasgow air terminal was rammed by terrorists on 30 June 2007, stand-off distances at airports have been increased. The list of buildings protected in this way has been progressively extended since 9/11: military facilities; government offices and embassies; critical industrial facilities; high-rise commercial properties and sports stadiums.

Military manuals guide terrorists in the effective use of bombs, but no training camp tutorial can compare with lessons from actual attacks. In October 2003, at the Baghdad Hotel, a car crashed through the security barriers. Security guards responded by shooting out the tyres, and the half-ton bomb detonated 50 metres from the hotel itself. The blast still killed eight people, ripped cladding from the hotel, and broke windows for two blocks. But had the car reached its objective, the impact would have been far worse. Blast modeling indicates that the half-ton bomb detonated 50 metres away generated a blast pressure of about 5 to 10 pounds-per-square-inch at the hotel. Up close, the bomb would have generated blast pressures almost eight times as severe, which would have caused double the damage and many more casualties.

Where standoff is limited, physical barriers provide a key line of defence. Visible security in the form of gates, chicanes, planters, trees and street furniture, now a familiar aspect of post 9/11 urban architecture, will be readily observable during terrorist surveillance operations, and will serve as a deterrent, encouraging the search for a softer target. The ring of steel built around the city of London is known to have deterred the IRA. Furthermore, enhanced blast-protection is increasingly featured in building construction. As with all risk exposure, it is prudent to have multiple layers of protection against terrorism. These may be summarized by the three D's: Deter, Detect, and Deny. Should an attack be launched, CCTV cameras and electronic equipment should be at hand to detect unauthorized intrusion. In the event of a terrorist break-in, opportunities for sabotage, fraud, or other criminal business disruption should be denied the terrorist through tight internal security measures.

1e. Capability analysis

The May 11, 2009 appointment of asymmetric warfare expert, Lt.Gen. Stanley McChrystal, as the top allied commander in Afghanistan affirms US resolution to suppress the capability of Al Qaeda to plan spectacular attacks from its mountain strongholds in Afghanistan-Pakistan. His predecessor, Gen. David McKiernan (2009) had stated succinctly, but not resolved, the politico-military challenge: *'NATO and regional stakeholders simply cannot allow the Northwest Frontier Provinces, Federally Administered Tribal Provinces, and Baluchistan to remain areas of sanctuary for extremists and places for planning and training global terrorists.'*

Al Qaeda operational decision-making is decentralized from this conflict zone with many technical and tactical skills learned online from Jihadi websites. But as in real space, terrorist use of cyberspace is subject to counter-attack by security services, which are assiduous in taking down extremist propaganda websites, and limiting the ability of terrorist groups to recruit members, and plan and perpetrate damaging attacks.

The loss of individual operatives is rarely a significant setback; there is no shortage of Muslim recruits ready to fill the ranks. Even though Islamist militants may minimize or disguise communication, such links may become manifest through clandestine surveillance of their meeting places and modes of interaction. Human intelligence, by way of tip-offs, moles, or double-agents, may provide some information on Islamist militants. Otherwise, information can be gleaned from data mining and eavesdropping, such as communication interception. Any communication between two operatives, whether via a meeting, letter, phone, email, or internet, and however secretive, carries a finite risk of interception by security services.

Finding terrorists is easier if the network is larger and more network connections can be identified. Intuitively, the larger the community of active operatives, the larger the number of random detected links that may arise between them, and the easier it becomes for counter-terrorism forces to join the dots, make arrests and accumulate sufficient evidence to make charges and to secure convictions. The organizational worry for terrorists is that if there is excessive planning activity for one spectacular attack, or for a wave of attacks during a short period of time, there will be a greater likelihood of more links being randomly detected, so making the security services' task of joining the dots much easier. It only takes one operative to be seen to be acting suspiciously to jeopardize an entire operation. Too ambitious or too many planned attacks would prove ultimately to be counter-productive, and wasteful of terrorist resources.

Organizing less ambitious planned attacks would be a more resilient and patient approach, better capable of withstanding concerted counter-terrorism efforts at network disruption. Recent armed attacks in Mumbai and Islamabad illustrate the tactical advantage. There has yet to be a successful Jihadi terrorist attack using chemical, biological, radiological or nuclear (CBRN) weapons, notwithstanding the intent to develop such attack capability, and the readiness to deploy such weapons. Under sustained counter-terrorism pressure, the terrorist capability remains low.

1f. Risk calculation

Especially during a terrorist crisis, decision-makers should be taking calculated, rather than reckless risks. Information overload can lead to poor decisions. Processing of risk information is expedited by prior risk calculation, which involves extensive computer simulation of large numbers of possible threat/counter-terrorism outcomes, graded according to plausibility. To quantify a terrorist threat, a number of risk metrics can be calculated. Serving as a medium-term reference baseline is the annualized average human or economic loss, segmented according to geography, and attack mode. A key risk metric during a terrorist crisis is the likelihood of mass casualties or enormous economic loss, and the cost-effectiveness of risk mitigation measures or crisis management action. Red-teaming exercises can be extended in a risk direction by evaluating the risk implications of alternative terrorist moves.

Common to all risk metrics is an estimation of loss consequent on a terrorist attack being successful. Loss estimation involves 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 are technically complex and challenging, but at least the core computational models for blast analysis; conflagration; atmospheric dispersion, pollution transport, epidemiology etc. are founded on consensus scientific principles.

Demanding more innovative thinking is the task of estimating the likelihood of rare attacks. For this, risk modelers use probabilistic event-tree models that delineate the multitude of branches and pathways by which such attacks might occur. Even with insights of intelligence experts, there remains significant modeling uncertainty over the possibility of novel spectacular attacks. However, counter-terrorism constraints on the plot effectiveness of terrorist networks limit the range of practical possibility, and intelligence information can update the likelihood estimates during a time of crisis.

1g. Comparison and evaluation of terrorism threats

A quantitative approach provides a direct means of comparing terrorist threats, once they are evaluated in a probabilistic sense. But what about unknown threats? Donald Rumsfeld's enigmatic and celebrated Department of Defense news briefing on February 12, 2002, brought to public notice the intelligence conundrum of dealing with the 'unknown unknowns'. The public perplexity which this briefing generated reflects the quagmire entered when words alone are used to analyze reports of questionable reliability. Rumsfeld's philosophical reference to 'known knowns, known unknowns and unknown unknowns', was a commendable if confusing attempt to address what are fundamentally deep epistemological issues. Faced with interpreting the most complex dubious baffling evidence, intelligence officers would benefit from quantitative analytical methods that combine statistics with philosophy, specifically evidence science with epistemology - Bayesian epistemology.

As with other dangerous adversaries, Al Qaeda places a high strategic value on surprise as an attack weapon. As the war theorist Clausewitz remarked, surprise confuses the enemy and lowers his morale, and furthermore, it invigorates the forces conjuring up the surprise. Surprise can be inflicted on an unwary adversary at many levels. Alas, surprise, almost by definition, may be one of the hardest weapons to overcome. The 9/11 Commission report stated that *'it is crucial to find a way of routinizing, even bureaucratizing the exercise of imagination'*. In the interpretation of intelligence information, the exercise of imagination is impeded by the human frailty of cognitive dissonance. If evidence conflicts with one's prior world view of terrorism, it is simplest to resolve this dissonance by downgrading the reliability of the evidence.

In the domain of communications monitoring, a natural endeavour is to attempt to tune in to that part of the communications spectrum that might be used by evasive smart terrorists, and amplify the electronic signal received. An analogous endeavour in the domain of human behavioural psychology is to attempt to *'tune in'* to terrorist behaviour, and step up the gain on the corresponding behavioural signal. The terrorist behaviour to which counter-terrorism officers would be especially keen to *'tune in'* is of a devious, imaginative and surprising kind.

To be surprised is to be caught unprepared. Inadequate preparedness takes many forms: lack of physical security; lack of security personnel; poor intelligence etc.. Clearly, access to direct intelligence information about potential surprise terrorist plots would always be welcome. But, even in the absence of such intelligence, there is much that counter-terrorism forces can do to prevent strategic surprise, which is first and foremost a reaction of the human mind. Those who are mentally well prepared are much less likely to be surprised.

Counter-terrorism information is intrinsically uncertain, and consists of occasional threat reports of varying degrees of confidence, plausibility and reliability. In order to treat such soft information in a systematic manner, minimizing subjectivity, one needs to address fundamental epistemological issues concerning differing states of counter-terrorist knowledge. Specifically, one needs a method for weighing the likelihood of the truth of a threat hypothesis according to various criteria:

- How many information sources are there? Does the information come from a single source, or from several sources? Are the sources independent?
- How reliable are each of the sources? How likely is it that a source would make a false report?
- How coherent is the information? Are the source reports collectively consistent with each other, or are they partially contradictory? To what extent do the reports confirm each other?

- How surprising is the information? Are several sources providing the same surprising information?

Also, if intelligence happens to be very specific, it should make an intelligence officer wonder why and how the source originated it. The surprise/specificity index can be assigned with reference to qualitative descriptions of the kind tabulated in Table 1.

TABLE 1: SURPRISE / SPECIFICITY INDEX

SURPRISE/ SPECIFICITY INDEX	EQUIVALENT QUALITATIVE DESCRIPTION
0.1	Extremely precise and weird
0.2	Very precise and surprising
0.3	Moderately precise and surprising
0.4	Quite precise and surprising
0.5	Neutral or no opinion
0.6	Unsurprising
0.7	Vague and imprecise
0.8	Uninformative
0.9	Very uninformative
1.0	Extremely uninformative

In the aftermath of the 7/7 London transport bombings, organized at cell level by a well respected primary school teacher, Mohammed Siddique Khan, the metaphor of a chameleon has been used to portray the adaptive capability of Jihadis to blend into the background and avoid suspicion. A merit of Bayesian epistemology is that no such adaptation, however cunning and resourceful, would be impervious to counter-terrorist action, provided there were some fragment of prior intelligence. Such indeed was the case regarding the organizer of the 7/7 plot, who was briefly tailed by MI5 through links with another terrorist conspiracy under investigation.

The value of surprising information can be analyzed more systematically using the methodical principles of Bayesian epistemology, which provides a formal quantitative framework for considering whether surprising information should be believed. Sometimes, a report can be too odd not to be true. In scanning the horizon for Rumsfeld's 'unknown unknowns', the epistemological realm of the proverbial black swan, additional telescope capability is provided within the framework of Bayesian epistemology. By definition, an unknown unknown is off the threat radar screen. However, it is often the case that there are vague dubious precursory signals of the looming black swan. Inevitably, such signals are surprising, as well as being of questionable reliability, and thus hard to detect using conventional methods.

2 TERRORISM THREAT MANAGEMENT

2.a Identification of preventative measures and strategies for terrorism threats

Preventative measures start with counter-terrorism operations: plot interdiction is an optimal policy. As far as counter-terrorism security services are concerned, the group of active supporters of political violence constitutes a very large social network, interlocking sub-networks of which may be involved in terrorist plots at any given time. Key to the disruption of plots is the discernment of links between nodes of a terrorist sub-network. The higher the likelihood of identifying a link between terrorist two nodes, the clearer a pattern of connections will become, and the easier it becomes to ‘join the dots’ to disrupt a terrorist plot, and gain the necessary corroborative evidence for criminal proceedings. As a conspiracy expands in size, or as a series of conspiracies are interlocked, so the discernible signature of plotting becomes increasingly recognizable. The intuition that too many terrorists spoil the plot, can be expressed in a quantitative way utilizing modern developments in network analysis.

Suppose that, within the large disparate population of terrorist supporters, there is a group who are actively involved in operational planning at a particular time. It is in the general terrorist interest to tend to randomize network connections, to keep security services guessing about plot involvement, and defeat efforts at profiling. However, even with randomization, there is a tipping point in the size of the group, beyond which the presence of conspiratorial plotting should become increasingly manifest to the security services. Even the most careful plotting may be dashed by excessive numbers of operatives. As Niccolò Machiavelli noted in his discourse on the security of Roman emperors: conspiracies should be kept small.

Population clusters forming within random networks may be analyzed graphically in terms of a basic clique of three people, who all are interlinked. Graph theory analysis reveals a dramatic change in the connectivity features of a graph, i.e. a tipping point transition, when the link detection probability attains the value: $p = (2N)^{-1/2}$, where N is the size of the group. Rearranging this formula, the tipping point arises where the size of group exceeds one half of the inverse-square of the link detection probability. The nonlinearity embedded in the expression for the link detection probability embodies in a concise manner the rapidly escalating dependence of counter-terrorism performance on surveillance capability. The greater the link detection probability, the smaller the size of conspiracies that can be disrupted. Conversely, the smaller the link detection probability, the more tenuous is the prospect of identifying plots.

This new type of terrorist network analysis has been applied to past and present terrorist campaigns. A topical important application is to the Jihadi terrorist threat to London, which has the highest terrorism hazard of any city in the western alliance. According to UK opinion polls, about 6% of adult British Muslims thought that the 7/7 London bombings were justified. Assuming this ratio approximately holds for the half million Muslim visitors, most of whom are from Pakistan, an estimated 100,000 Muslims within Britain might actively support the Jihad. Countering the rising UK threat of Islamist

militancy since 9/11 through the doubling of its pre-9/11 staff, the UK Security Service has around a thousand personnel for Islamist terrorism surveillance operations. With each secret agent being aided by informers and the local constabulary, as well as by receiving tip-offs from the general public, so as to keep reasonable surveillance of approximately five citizens, a surveillance ratio of approximately 100 to one equates to a link detection probability of about 1/10, and a moderate tipping point value N of 50. This serves as a constraint on the number of terrorists actively planning attacks in UK. Indeed, since 9/11, the most complex UK plots, involving many conspirators, have been successfully interdicted.

The conviction rate since 9/11 of those arrested under UK terrorism laws is only about 13%. More than half of detainees are not charged. For the terrorist threat to be lowered in democracies of the western alliance, heightened surveillance is not the answer; there has to be a reduction in the Muslim (Umma) sub-population who consider terrorism against these countries to be justified. Psychology has been an art of war for millennia, but the technological means of strategic persuasion have reached their zenith in the 21st century. Al Qaeda's chief strategist, Ayman Al Zawahiri, wrote as follows to Musab Al Zarqawi in July 2005: *'I say to you: that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the hearts and minds of our Umma.'* Overseeing propaganda is the head of Al Qaeda's Media Committee, Abu Abdel Rahman Al Maghrebi, the son-in-law of chief strategist Dr Ayman Al Zawahiri. Under dynamic leadership, Al Qaeda's media arm, Al Sahab, has substantially increased its annual output of audio and video messages.

For security in UK, with its traditional colonial links with Pakistan and large diaspora community, there is a need to win hearts and minds of young Pakistanis. This was recognized in an address on July 27, 2007, to the Pakistan Youth Parliament, by the British Foreign Secretary. David Miliband delivered the following qualitative message on international relations, which is supported by quantitative terrorism risk analysis: *'Diplomacy needs to change to be about winning hearts and minds, instead of bureaucrats holding meetings behind closed doors.'*

2.b Risk Reduction

Terrorism risk can be reduced systematically by raising the level of security, but it has to be at an acceptable cost. Special protection technology, such as the installation of anti-MANPAD devices on planes, reduces aviation risk, but at a high cost which airlines can ill afford and passengers would generally be unwilling to pay. More affordable on-land vigilance includes installing additional CCTV, hiring extra security guards and marshals, introducing intensive screening, showing of picture/biometric ID, extending police stop-and-search, strengthening border and perimeter security. Risk can also be reduced through decreasing vulnerability to opportunist attacks. Examples include the removal of public receptacles (e.g. waste bins), in which package bombs might be hidden, as they were by the IRA in their London bombing campaign.

Relocating staff away from buildings under heightened threat, e.g. Dutch embassy staff accommodation in Islamabad, reduces personnel risk. More drastically, overseas nationals might be repatriated away from a designated threat zone. An alternative is to move offices to sites with fewer security weak points. US embassies are hardened by relocating to more isolated secure sites, e.g. around Istanbul, Hague, London, etc..

The IRA often telephoned coded bomb warnings to provide some time for a target to be evacuated. The area evacuated might be a building, street or city block. Fortunately, the IRA did not contemplate the use of a dirty bomb or other CBRN weapon, which might threaten much larger urban regions, the evacuation of which would have been a logistical nightmare, on a par with large-scale evacuation in a hurricane or volcanic crisis. But what if a terrorist group issued an anthrax dispersal warning for a capital city centre, as might hypothetically happen in the future, perhaps as a political blackmail gambit?

Recognizing that dispersal of an anthrax device would be most effective in a high-density urban area, action to reduce the city centre population might be worthwhile. A decision to mandate a short-term evacuation in the face of an uncertain threat falls within a common important category of economic decisions: pay a sum now to avert paying a larger sum later, contingent on the occurrence of an uncertain hazard event. Evacuation is a form of insurance protection. The significant socio-economic expense of evacuation is the premium deemed worth paying so that, in the event of a terrorist atrocity, the much higher cost of mass casualties is avoided.

The economic character of this class of decisions is exemplified by a basic cost-loss model. Consider a situation where a decision-maker has to choose between two actions: (a) protect; (b) do not protect. The cost of protection is C . In the absence of protection, the decision-maker incurs a loss L , which exceeds C , if an adverse hazard state arises. The corresponding expense matrix is shown below:

TABLE 2: LOSS-COST EXPENSE MATRIX

ACTION	Adverse Hazard State	No Adverse Hazard State
[a] Protect	C	C
[b] Do Not Protect	L	0

Let the probability of the adverse hazard state arising, within a specified time window, be denoted by p . If the expected expense is to be minimized, then the optimal policy is to protect, if $p > C/L$, but not to protect if $p < C/L$. The minimal expense is then $\min\{C, pL\}$. In the present context, protection would be evacuation, which carries a cost of C . The adverse hazard state here is one of a terrorist attack, for which a decision not to protect carries a large loss penalty of L , measured in human fatalities. Given the enormous societal cost associated with urban evacuation, the probability p would have to be substantial for this even to be considered. But this situation might arise if it were known that a viable CBRN device had already fallen into terrorist hands. Indeed, if publicized, this might precipitate an urban exodus.

2.c Risk Avoidance

Most risk avoidance decisions require some basic level of cost-benefit analysis to justify the imposition of any additional corporate or societal burden. The British Airways passenger service from London to Washington DC has been grounded on occasion because of a credible terrorist threat. Following the 7/7 London transport bombings, many travellers avoided the perceived high terrorism risk associated with public transport, but such risk avoidance soon lapsed with the need to resume daily life. To avoid terrorism risk by giving in to specific terrorist demands is morally objectionable, but nevertheless might be prudent. Where risk is avoidable at comparatively modest cost, it makes sense at least to consider this option.

The March 3rd, 2009, gun assault on the Sri Lankan cricket team coach en route from hotel to cricket stadium in Lahore reflects a risk which might have been avoided, had the team been taken by helicopter to the stadium, as they were ultimately taken out. Would the risk have justified this apparent extravagance? Randomness plays its part in inadvertent risk avoidance. Pakistan's leaders were planning to dine at the Marriott Islamabad on September 20, 2008: a fortunate late change of plan saved them from the half-ton terrorist bomb and subsequent fire which engulfed the hotel.

Where financial risk is a major concern, it may be avoided by transferring it to an insurer. Terrorism insurance provides a valuable public function by helping to maintain commercial activity in areas specially threatened, e.g. in key target-rich metropolitan areas. For example, bank loans for business development in high risk areas may require terrorism cover. Recognizing the societal value of terrorism insurance as well as the responsibility of government for national security, public-private partnerships in providing terrorism cover include national terrorism insurance pools and backstops in many countries of the western alliance.

2.d Risk Shifting

Terrorist target substitution operates on all geographical scales: from individual to street, to city, to national level. At an individual level, the assassination of Theo van Gogh in November 2004 was a textbook example: a knife in the film-maker's chest affixed a letter addressed to the prime source of the terrorist's fury, Ayaan Hirsi Ali, the self-styled infidel subject of his provocative film. At the other end of the scale, analysis of terrorism threat shifting away from the U.S. shows that the U.S. is not isolated as a target from others in the western alliance: Islamist gunmen who terrorized hotel guests in Mumbai in November 2008 singled out both Britons and Americans.

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. Whilst serving as CIA director, George Tenet, testified on 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.' Target substitution, as this is called, is a prediction about the rational behavior of terrorists, affirmation of which must ultimately come from the terrorists themselves. Indeed, explicit admission of this soft target strategy has come from Khalid Sheikh Mohammed, the Al Qaeda chief of military operations, who was arrested in March 2003.

In November 2003, Islamist terrorists struck yet another city with high name recognition: Istanbul. The local US embassy was too hard a target to hit; it had been relocated out of the city for security reasons. Instead, terrorists struck the much softer target of the British consulate, where a desire to foster closer community links precluded such tightening of security. The lesson of Istanbul was learned fast; concrete blocks were rapidly installed outside the British embassy in Sofia, Bulgaria. An abiding lesson is that, with a terrorist threat to a number of prize targets, the most vulnerable generally have the highest probability of being attacked. As with the installation of burglar alarms, self-protection carries the externality of shifting criminal risk to neighbours.

2.e Acceptance of Risk

For the vast majority of possible terrorist targets, significant expenditure to reduce vulnerability is not justified by the low ambient risk. If security levels in target countries were adjusted approximately so as to equalize risk, the annual probability that any one target would be attacked would be minuscule: as in the jungle, there is safety in prey numbers. Governments should attempt to compare and reconcile the residual terrorism risk level to which citizens are exposed with the ambient risk level from ordinary criminal acts and natural hazards. Terrorism risk is higher in metropolitan areas, and so is the regular crime rate of mugging and burglary.

Conspicuous security presence around soft targets in crowded places may be justifiable if security staff have regular crowd management duties as well, which is the case at night-clubs and casinos, which are known Islamist decadent targets. However, as shown by the attempted club bombing in central London on 29 June 2007, unarmed doormen may not deter determined terrorists, and armed doormen, if legally allowed, might deter customers. Where security is deficient, system recovery must be resilient.

As a showcase for disaster resilience, the HSBC bank headquarters in Istanbul managed to resume business a day after being bombed on 20 November 2003, thanks to the implementation of their earthquake disaster plan. This offered an implicit degree of redundancy of a creative kind which makes residual risk acceptance a tolerable crisis policy. Meticulous disaster preparedness and post-event rapid response are essential for mitigating loss. Cost-effective are new technological advances, such as in personal protective equipment, which protect first responders better against toxic substances, and increase mobility and access. Deploying well-equipped and trained rapid response teams makes excellent counter-terrorism sense, denying terrorists the maximal losses they crave. Risk managers should aim for total security, but settle for resilience.

REFERENCES

- Bovens L., Hartmann S. (2003) *Bayesian Epistemology*, Oxford University Press.
- Brahimi L. (2008) Towards a culture of security and accountability. Report of the Independent Panel on Safety and Security of UN Personnel and Premises Worldwide.
- Buruma I. (2007) *Murder in Amsterdam*. Atlantic books.
- Haggstrom, G. W. (1967), *The Annals of Mathematical Statistics*, 38(6), 1618-1626.
- Kepel G. (2005) *The roots of radical Islam*. Saqi Books, London.
- Machiavelli N. (1517) *Discourses on the first ten books of Titus Livy*.
- McKiernan D. (2009) *RUSI Journal*, Vol.154, No.2.
- Ranstorp M. (2005) *RUSI Journal*, Vol. 150, No.3.
- Taleb N.N. (2007) *The black swan*. Penguin books, London.
- Woo G. (2009) Intelligence Constraints on Terrorist Network Plots, In: *Mathematical Methods in Counter-Terrorism*, Memon, N.; Farley, J.D.; Hicks, D.L.; Rosenorn, T. (Eds.), Springer, New York.