

Terrorism Risk

Gordon Woo

Keywords

terrorism; risk; model; game; network; control; global

Abstract

Terrorism risk emerged as a quantitative modeling discipline after 9/11. This chapter describes methods that have been developed for modeling the terrorism risk from Islamist militants. Whereas the damage wrought by a terrorist attack is amenable to engineering loss analysis, the terrorist modus operandi is a function of human behavior, and so requires special methods drawn from fields such as game theory, social psychology, and network analysis. In order to analyze the global terrorist threat from Islamist militants, a coherent global perspective is required that tracks the radicalization of Muslim diaspora communities.

Scientific Overview

Einstein remarked that Nature is subtle, but not malicious. There is no universal definition of terrorism, but all such acts are recognized as being malicious. Not all terrorist campaigns are also deadly and enduring, but these are the words used by the director general of the British security service, Eliza Manningham-Buller, [1] to categorize the global Jihadi threat, at a time when MI5 perceived Britain to be Al Qaeda's No.1 target [2].

The purpose of this chapter is to describe methods for modeling this source of terrorism risk, and to identify research directions, especially in analysis on a global scale. In the latter regard, aviation and maritime risks are given prominence, because of their border protection significance. Skeptics of terrorism risk modeling may perceive terrorism to be simply a Manichaeian struggle between good and evil, or imagine that terrorists are stupid and crazy. Reality is otherwise: capable terrorists are both rational and intelligent. Terrorists have to be intelligent in order to make an impact in asymmetric warfare. Atwan [3] has warned the West not to underestimate the intellectual prowess of the Al Qaeda leadership. Osama bin Laden honored Khalid Sheikh Mohammed, the 9/11 mastermind, with the title 'mukhtar', meaning 'the brain' [4]. 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.

But is it rational for a Jihadi 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 Jihadi to accept 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'*. [5]

Building on the understanding that Islamist militants are rational and intelligent, an overview is presented of the principles of terrorism risk modeling, which govern the frequency and severity of Jihadi terrorist attacks, the choice of weaponry, and the selection of targets.

Terrorist Targeting

A cornerstone of terrorist targeting is target substitution [6]: if a designated target is too hard, an alternative softer target may be substituted. If, however, there is no available alternative of similar status, then efforts at striking the original target may be redoubled. Target substitution operates on all spatial scales, and is a phenomenon very familiar to criminologists (Yezer, [7]). At the street level, the Bali cafés bombed on October 1, 2005, had been chosen for their inferior security. At the town level, the British embassy in Istanbul was bombed on November 20, 2003, in preference to the fortress-like US embassy [4]. At the national level, the IRA switched a truck bomb attack from London to Manchester, when the border security around the City of London was tightened. At an international level, Jemaah Islamiyah switched an embassy attack from Manila to Singapore because of the hardness of the Philippine targets [8].

The malice underlying terrorism suggests applying game theory, as Sandler and co-workers did long before 9/11 [9], and others have done since. Game theory models with just a few variables can be analyzed in elaborate mathematical detail. For example, Kardes [10] has provided solutions to some illustrative stochastic game problems with a small number of states. A basic model of a territory with a handful of terrorist targets, or weapon systems, may be mathematically tractable, but of course the US homeland is dense with terrorist targets. As with models of a few targets, insights into what to protect may be gained from considering a simple model with numerous targets, where all, or almost all, of the targets are equally valuable to the defender (Bier [11]).

To develop a full scale practical model for the entire US homeland, clearly some simplifying assumptions are necessary. These may be coarse, but they can be substantiated from knowledge of the terrorist modus operandi, and validated against information on planned attacks. Al Qaeda operatives are trained to be

meticulous over target surveillance [12], and are very sensitive to changes in security. One may reasonably assume that, through diligent surveillance, they effectively immunize the attack loss potential against changes in security (Major [13]), in the mathematical sense that, to first order, the expected loss from an attack is invariant against such changes.

For various terrorist organizations, such as the IRA, killing large numbers of civilians had very low utility for the terrorists, since such attacks would have severely eroded their popular support base. Thus, as a target, a full sports stadium had a much lower utility for the IRA than for the defenders. However, for Islamist militants, enraged by many thousands of civilian Muslim deaths in conflict zones, mass fatalities are perceived as a legitimate attack objective. Osama bin Laden [14] has indeed encouraged such attacks: *'It is the duty of Muslims to prepare as much force as possible to attack the enemies of God'*.

The Al Qaeda chief strategist, Dr. Ayman Al Zawahiri, has explained the influence of the Umma, (the global community of Muslims), in their targeting strategy: *'Al Qaeda wins over the Umma when we choose a target that it favors'* [15]. Opinion poll surveys show that a significant proportion of Muslims around the world condone terrorist attacks against western targets as a reprisal for western indifference to the loss of Muslim lives. The Leeds clique of British-Pakistanis who bombed London on 7/7 held a celebration party straight after 9/11 [16]. Cities with international name recognition are collectively favored by the Umma, as is affirmed by the list of post-card cities attacked since 9/11: Bali, Mombasa, Casablanca, Riyadh, Amman, Madrid, and London. By contrast, towns are not favored by the Umma if they are unknown to most Americans, let alone on the Arab Street.

The Jihadi preparedness to use maximum force, and the Umma's perception of Crusaders' pain as Islam's gain, suggest that, as a first approximation, target utility valuations, based on economic and symbolic value, and casualty potential, are broadly similar for Jihadi attackers and Western defenders. If only Jihadis were motivated to attack a Western target that had low defender utility. A cartoon in Punch Magazine once depicted London's royal Albert Memorial as being an ideal honey-pot IRA target. To the regret of architectural aesthetes, this undefended monument to Victorian garishness was never targeted by the IRA. The Statue of Liberty is a prime example of an iconic terrorist target that is well protected, even though its economic value and casualty potential are comparatively modest. Unlike the undefended Albert Memorial, it is known that the defended Statue of Liberty is a Jihadi target.

If it is posited, as with the Statue of Liberty, that defensive resources commensurate with their utility are applied to protect targets, then a parsimonious targeting model is derived (Woo [17,18]). This is a phenomenological model: the few parameters are estimated through elicitation of the judgement of international terrorism experts. Cities are grouped into discrete tiers by the experts, e.g. New York and Washington D.C. comprise the first tier. A similar style of discrete target tiering is developed for types of targets, e.g. hotels, government offices, airports etc..

The model automatically yields targeting likelihoods akin to a Pareto 80/20 rule, in that it forecasts that the great majority of attacks will be against a minority of potential targets. This focusing of attacks against a small proportion of targets is consistent with historical experience of major prolonged foreign terrorist campaigns, such as the IRA bombing campaign in England, which concentrated terror in its leading cities: London, Manchester and Birmingham.

This baseline model can be updated with site-specific information on whether security is relatively better or worse than the norm for a potential target of a particular ranking. The essential characteristics of terrorist targeting are captured by the model:

- Terrorists may substitute one target with another, according to the relative security of the targets.
- Local security enhancement transfers threat elsewhere: excessive site protection may be undesirable on a societal level. For example, some government buildings may be protected against vehicle bombs well beyond terrorist capability, whereas there may be insufficient expenditure on protecting private offices, or public infrastructure.
- There is safety in numbers: increasing the number of targets of a specific type dilutes the individual risk. By contrast, where there are few targets of a specific type, for example tourist hotels in a city, then the risk is increased, as with the Amman, Jordan, bombings on November 9, 2005.
- Terrorist attacks are geographically focused, with attack likelihood decreasing logarithmically for descending target tiers. This is exemplified by the IRA's choice of English city to attack: the first tier being London; the second tier comprising Manchester and Birmingham, etc..

Weapon Attack Modes

Rationality pervades the operational modus operandi of terrorists. The handbook of all guerrilla movements is Sun Tzu's 'The Art of War', which identifies optimal modes of combat: *'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 dictum echoes the principle of following the path of least resistance that governs the dynamics of the universe, including terrorist activity [19]. This elegant principle was first enunciated by Pierre de Maupertuis: *'The great principle is that, in producing its effects, Nature acts always according to the simplest paths.'*

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 terrorist 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. Accordingly, it inclines towards off-the-shelf, ready-to-use weapons, (such as MANPADS, mortars, hijacked aircraft, and propane tankers), or improvised conventional explosive devices, which do not involve intricate and potentially failure-prone technological development. Al Qaeda is known to be highly adaptive in learning from past terrorist successes and failures from all terrorist organizations around the world [4]. Neural network simulation models can represent the social learning process [20].

The logistical burden of alternative weapon systems can be evaluated in terms of the terrorist demands on finances, equipment, materiel, trained personnel and sleeper cell support. Calibration against actual experience is possible for conventional attack modes, but not for exotic attack modes, such as CBRN. Event-tree methods have been devised to elaborate the alternative foreign and domestic pathways by which such unconventional weapons can be manufactured or procured.

Frequency of Successful Macro-Terror Attacks

Macro-terror attacks are acts of terrorism, such as perpetrated on 9/11, that aim to cause substantial loss, and require significant logistical resources, and considerable time for planning and preparation. Al Qaeda is renowned for meticulous detail over its centrally organized attack planning, which involves diligent reconnaissance, surveillance and rehearsal. Most notably, Al Qaeda has developed a long-term strategy, and is extremely patient in planning its military campaign over decades. Indeed, patience is half of the Islamic concept of faith, that covers action, (for which gratitude is due to Allah), and abstinence from action, (for which patience is demanded). Dr. Ayman Al Zawahiri [15] has explained the Al Qaeda goal: *'We must inflict the maximum casualties against the opponent, for this is the language understood by the West, no matter how much time and effort such operations take.'*

It turns out that the number of operatives involved in planning and preparing attacks has a tipping point in respect of the ease with which the dots might be joined by counter-terrorism forces. The opportunity for surveillance experts to spot a community of terrorists, and gather sufficient evidence for courtroom convictions, increases nonlinearly with the number of operatives - above a critical number, the opportunity improves dramatically. This nonlinearity emerges from analytical studies of networks, using modern graph theory methods (Derenyi et al. [21]). Below the tipping point, the pattern of terrorist links may not necessarily betray much of a signature to the counter-terrorism services. However, above the tipping point, a far more obvious signature may become apparent in the guise of a large connected network cluster of dots, which reveals the presence of a form of community. The most ambitious terrorist plans, involving numerous operatives, are thus liable to be thwarted. As exemplified by the audacious attempted replay in 2006 of the Bojinka spectacular, too many terrorists spoil the plot (Woo, [22]).

Intelligence surveillance and eavesdropping of terrorist networks thus constrain the pipeline of planned attacks that logistically might otherwise seem almost boundless. Indeed, such is the capability of the Western forces of counter-terrorism, that most planned attacks, as many as 80% to 90%, are interdicted. For example, in the three years before the 7/7/05 London attack, eight plots were interdicted. Yet any non-interdicted planned attack is construed as a significant intelligence failure. The public expectation of flawless security is termed the '90-10 paradox.' Even if 90% of plots are foiled, it is by the 10% which succeed that the security services are ultimately remembered.

Thanks to the diligence of the security services, which deter the planning of large numbers of attacks, and interdict most of those that are planned, the frequency of successful terrorist attacks is kept low. Only a small proportion of attacks succeed, and these tend to be those involving fewer active operatives. Through this control process, which comes at the cost of some personal civil liberty, the uncertainty in the frequency of successful terrorist attacks is constrained. As happened after 9/11 and 7/7, after each major terrorist attack, democracies will respond by rebalancing the desire for liberty with the need for security.

Research on Terrorism Risk

Terrorism is a global phenomenon. Where activists cannot effect political change through peaceful means, they coerce through political violence. Terrorism research has a wide international agenda: the structure of terrorist organizations; weaponry; targeting; vulnerability and security, counter-terrorism etc. Terrorism risk assessment forms part of the research agenda, and is shaped and directed by the practical needs of the public and private sectors.

The insurance industry operates worldwide. Accordingly, global models of terrorism risk have been developed to assist risk managers of insurance companies and captive insurers. These models vary in resolution from one country to another, depending on the degree of commercial interest. Insurance risk management requires control of aggregate loss potential. Accordingly, models cover all terrorist groups and all plausible attack modes. Although their adoption is discretionary, risk models are used quite widely by insurers, in recognition of which the insurance industry has funded a considerable amount of research on terrorism risk. Notable is the research carried out by the RAND Center for Terrorism Risk Management Policy, which is a joint project of the RAND Institute for Civil Justice, RAND Public Safety and Justice, and Risk Management Solutions (RMS).

Besides the insurance industry, the US government has a direct stake in assessing terrorism risk on a national scale, among other purposes to improve counter-terrorism resource allocation. Any implementation of a risk-based allocation procedure must address concerns over uncertainty as to terrorist

targeting. A detailed RAND study (Willis et al. [23]), based on the RMS terrorism risk model, has developed an approach for making allocation decisions robust against uncertainty in model parameterization.

A considerable volume of academic terrorism risk research has been undertaken to support national public policy, notably at the University of Southern California's Center for Risk and Economic Analysis of Terrorism Events (CREATE), a DHS University Center of Excellence. At spatial scales below the national level, terrorism risk assessment is potentially useful for state and local public officials, for managers of transport infrastructure, utilities, critical facilities, as well as major buildings. Absent prescriptive terrorism mitigation standards, a risk-based approach to decision-making on security improvement is relevant. For major transportation systems, cost-benefit analyses for project prioritization and resource allocation have been conducted (e.g. King et al., [24]).

The challenge of terrorism risk assessment varies according to scale. On one hand, the more restricted the geographical scope, the narrower is the spectrum of possible targets. On the other hand, the dynamical coupling of terrorism risk across regional boundaries and between diverse targets is lost. The same applies with research focusing on specific weapon systems: the more restricted the military scope, the harder it is to address the coupling and switching between alternative choices of weaponry. An analogy with weather forecasting is apposite, since meteorological conditions are dynamically coupled across regions. Local weather forecasting is possible, but only if a large scale model of the atmosphere is used to define regional boundary conditions.

The problem of scale manifests itself particularly acutely in frequency estimation. An absolute measure of frequency cannot be generated internally from within the confines of a research project that has a reduced scope. However, setting aside discussion of the absolute probability of an attack against a specific target, risk assessments can usefully focus on the conditional probability of an attack.

Aviation and Maritime Risk Assessment

Just as the fighter jet is symbolic of militarism, so the passenger jet is symbolic of terrorism. Civil aviation is a vulnerable link in the global economy. The continuous adaptation of attack modes to evade security enhancements is a conundrum of aviation risk assessment. A wide range of airport security measures have been analyzed by Martonosi [25] from an operational research perspective. The cost-effectiveness of MANPAD counter-measures has been investigated by von Winterfeldt and O'Sullivan [26], using decision analysis techniques. Their analysis shows that measures to deflect SAM missiles might be cost-effective if the probability of an attack exceeds 0.5 in ten years; the losses are large (\$100 billion); and the countermeasures are relatively inexpensive (< \$ 15 billion). It turns out that the RMS estimate of the ten year MANPAD attack probability for shooting down a plane in the US falls around the threshold criterion. Given also that the scale of economic losses and the cost of countermeasures might also straddle the criterion levels, any decision on

implementing countermeasures remains awkward, bearing in mind the inevitable prospect of terrorist threat shifting to another alternative aircraft attack mode. Since 9/11, there has been an intermittent series of foiled plots against civil aviation, several of which have involved the smuggling of explosives.

Like aircraft, ships can be attacked or converted into floating bombs. Apart from these maritime dangers, US ports face a considerable challenge in preventing illicit terrorist cargo or personnel from entering the USA, whilst allowing the free flow of maritime commerce. Security standards are tightening at foreign ports, but the possibility exists that an inbound vessel might have terrorist connections. It is impractical for the coast guard to search more than a small percentage of inbound vessels, so an intelligence-led risk-based procedure is needed to improve the search selection.

With access to a global database of all commercial vessel movements, (such as maintained by the Lloyds Marine Intelligence Unit), a threat-ranking system can be devised, based on public information on ownership, flag of registration, crew nationality, last ports of call, etc.. Like any profiling system, it can be subverted by an adaptive terrorist intent on surprise, except that intelligence leads may give reason to revise this threat-ranking. A risk-based methodology for incorporating available intelligence leads, and treating surprising data of dubious reliability, has been devised by Woo [27] using the conceptual framework of Bayesian epistemology.

Critical Needs Analysis

Of all the various measures that may be taken to protect the US homeland against terrorism, securing national borders is a priority. Somewhat indeterminate is the specific contribution made by specific border security measures, such as the US VISIT program, which involves the gathering of personal identity information about people in transit to the US, or at US border posts. A strict regime of personal identity checking casts a virtual security net around the entire US that takes advantage of the small-world phenomenon of social networks: terrorists may be separated by thousands of miles, but connected instantaneously by a computer database of suspected or known terrorist links.

The potential to unravel a terrorist network may have very substantial deterrent value. A sizeable community of Jihadis involved in planning a large-scale technically complex operation, e.g. a CBRN attack, would come under heavy counter-terrorism pressure. Given that a major US operation carries a significant risk of network unraveling, there should be a strong impetus for terrorists either to lower the attack scale to reduce their detectability footprint, or to switch the attack to a softer country within the western alliance. Through its unwavering support for US foreign policy, Britain is seen by Islamists as forming an axis of evil with the U.S. and Israel. The UK is an obvious substitute target: the UK is politically

almost exactly aligned with the US on the war on terrorism, has a far more radicalized Muslim community, and yet is far behind on biometric border security. Already, the terrorist threat to London is comparable with that to New York or Washington. Because Al Qaeda has a global franchise, and terrorist target substitution operates on a trans-national scale, there is a critical need for risk assessment which is conducted on a global basis [28].

Global Scale of Terrorism Risk Modeling

Global terrorism models are needed to comprehend the terrorist threat to the US homeland from Islamist militancy. This is obvious for international aviation and maritime transportation attacks, but it is true for all threat modes, since foreign policy is a prime driver of Muslim discontent and Jihadi recruitment. Further research on global terrorism risk modeling will benefit efforts at focusing counter-terrorism action. Terrorist social networks; weapon procurement and transport; and the security of US assets abroad are important concerns that merit analysis from an international perspective.

The Umma has been galvanized collectively by Al Qaeda to seek redress for the plight of Muslim brothers and sisters in conflict zones. The global social networks of Muslims provide a support framework for radicalism, extremism and terrorism. A crucial role in facilitating terrorism in the western democracies is played by Muslim diaspora communities: Pakistanis in UK; Algerians in France; Moroccans in Spain; Somalis in Italy etc..

Improved models need to be developed for the evolution of terrorist support. Transcending the boundary between sociology, social psychology, and physics, is the modern discipline of sociophysics. This offers a scientific methodology for incorporating the social dynamics of diaspora communities into terrorism risk assessment. Basic rules of social interaction, akin to the dynamics of physical systems, are capable of enhancing understanding of complex social behavior. The formation of ghettos is a classic paradigm of sociophysics; one which is relevant to terrorism risk. 'Jihad' and 'Osama bin Laden' are the favorite Google keywords in some British Muslim ghettos. It is no surprise that as many as 100,000 British Muslims considered the 7/7 London bombings to be justified [1].

With the same objective, large scale agent-based computer simulations of the collective behavior of Islamist militants have been developed (e.g. MacKerrow [29]), but there is much room for advancement in the understanding of Islamist militancy. The discourse on this subject is beset at the highest level by political autism – the inability to think what others are thinking. Mathematical psychologists like Vladimir Lefebvre have found mathematical ways of encoding the recursive sequence of thinking what others think. Terrorism risk assessment will be distorted if its political components misrepresent the underlying root causes of terrorism (Richardson [30]).

Research Directions

Terrorism risk analysis is no longer a fledgling discipline. The core principles that govern terrorist actions are subject to observation and empirical validation, and, with the passage of time, the database of planned attacks is becoming more amenable to quantitative analysis. What is already clear is that, in the asymmetric warfare waged by the western democracies against militant Islam, the forces of counter-terrorism are achieving considerable success in controlling terrorism. The record is not perfect, as illustrated by the rail bombings of Madrid in March 2004 and London in July 2005. As the authorities remind their citizens: it's not a question of if, but when the next attack will occur. But at least, the question is thankfully not: how many major attacks will there be?

Research into global counter-terrorism is needed to elucidate important aspects of the dynamics of the terrorism control process. The close cooperation between security services in the G8 countries contributes significantly to the successful interdiction of the great majority of planned terrorist attacks against these countries by Islamist militants, and to restricting their international operations. The dynamics of terrorism control depend on the global political environment, which is easily destabilized, and subject to the law of unintended consequences, even if politicians would hope otherwise. To be meaningful for homeland security decision-making, cost-benefit analysis should be broadened in scope from having a restricted internal domestic frame of reference to having global coverage of US interests and actions. The terrorist threat is integrated across the globe. Accordingly, terrorism risk research must also be directed globally.

References

- [1] Manningham-Buller E. The international terrorist threat to the UK. Speech at Queen Mary College, London, November 9, 2006.
- [2] The Guardian newspaper. Manchester, October 19, 2006
- [3] Atwan A.B. The secret history of Al Qaida. Saqi books, 2006. 256pp.
- [4] Gunaratna R. Terrorism risk briefing, Washington D.C., 2005.
- [5] Oliver A.M., Steinberg P. The road to martyr's square. Oxford University Press, 2005, 214 pp.
- [6] Drake C.J.M. Terrorists' target selection. Macmillan Press, London, 1998, 272 pp.
- [7] Yezer A. Terrorist attacks and their consequences. Presentation at the CREATE workshop on benefit methodologies for Homeland Security Analysis, June 8-9, 2006.
- [8] Bell S. The martyr's oath. John Wiley & Sons, Ontario, 2005, 254pp.

- [9] Sandler T., Lapan H. An analysis of terrorists' choice of targets. *Synthèse*, Vol.76, 1988: 245-261.
- [10] Kardes E. Robust stochastic games and applications to counter-terrorism strategies. CREATE report, 2005, 64pp.
- [11] Bier V. Choosing what to protect. CREATE report, 2005, 27pp.
- [12] Gunaratna R. Inside Al Qaeda. Hurst & Co., London, 2002, 282pp.
- [13] Major J. A. Advanced techniques for modeling terrorism risk, *Journal of Risk Finance*, Vol.4, 2002:15-24.
- [14] Lawrence B. (Ed.) Message to the world: the statements of Osama bin Laden, Verso, London, 2003, 224pp.
- [15] Zawahiri A. Knights under the prophet's banner, London, 2002.
- [16] The Guardian newspaper. Manchester, June 24, 2006
- [17] Woo G. Quantitative terrorism risk assessment, *Journal of Risk Finance*, Vol.4, 2002:7-14.
- [18] Woo G. Insuring against Al Qaeda, NBER Insurance Workshop Presentation, 2003.
- [19] Ranstorp M. (2006) In the service of Al Qaeda. In preparation.
- [20] Carley K. (2003) Destabilizing terrorist networks, CASOS Working Paper.
- [21] Derenyi I., Palla G., Vicsek T. Clique percolation in random networks, *Phys. Rev. Lett.*, 94, 2005, 160202.
- [22] Woo G. Small world constraints on terrorism attack planning. *RUSI/Jane's Homeland Security & Resilience Monitor*, Vol.5, 2006.
- [23] Willis H.H., Morral A.R., Kelly T.K., Medby J.J. Estimating terrorism risk. RAND Corporation, Report from Center for Terrorism Risk Management Policy, 2005, 66pp.
- [24] King S., Isenberg J., Assessment of urban transportation infrastructure for terrorism risk management. ICOSAR, Millpress, Netherlands, 2005: 2773-2780.
- [25] Martonosi S.E. An operations research approach to aviation security. M.I.T. PhD thesis, 2005, 163pp.
- [26] Von Winterfeldt D., O' Sullivan T.M., A decision analysis to evaluate the effectiveness of MANPAD counter-measures. CREATE report No. 05-30, 2005, 24pp.
- [27] Woo G. Institutionalizing imagination to prevent surprise. Invited talk at the IDSS national security conference, Singapore, 2005.

- [28] Woo G. The terrorist threat to the US from abroad. Presentation at the CREATE workshop on benefit methodologies for Homeland Security Analysis, June 8-9, 2006.
- [29] MacKerrow E. Understanding why – dissecting radical Islamist terrorism with agent-based simulation, *Los Alamos science*, No.28, 2003:184-191.
- [30] Richardson L. *What terrorists want*. John Murray, London, 2006, 288pp.

Further reading list

Wiktorowicz Q. *Radical Islam rising: Muslim extremism in the West*, Rowman & Littlefield, New York, 2005, 288pp.

Cross-references

RA27; RA31; RA42; RA43

Glossary terms

Diaspora

Interdiction

Umma