## The Foreign Policy Centre

The Foreign Policy Centre is an independent think-tank launched by Prime Minister Tony Blair (Patron) and former Foreign Secretary Robin Cook (President) to revitalise debates on global issues. The Centre has developed a distinctive research agenda that explores the strategic solutions needed to tackle issues which cut across borders – focusing on the legitimacy as well as the effectiveness of policy.

The Foreign Policy Centre has produced a range of **Publications** by key thinkers on world order, the role of non-state actors in policymaking, the future of Europe, international security and identity. These include: *The Post-Modern State and the World Order* by Robert Cooper, *Network Europe* and *Public Diplomacy* by Mark Leonard, *NGOs Rights and Responsibilities* by Michael Edwards, *After Multiculturalism* by Yasmin Alibhai-Brown, *Trading Identities* by Wally Olins and *Third Generation Corporate Citizenship* by Simon Zadek.

The Centre runs a rich and varied **Events Programme** at The Mezzanine in Elizabeth House – a forum where representatives from NGOs, think-tanks, companies and government can interact with speakers who include Prime Ministers, Presidents, Nobel Prize laureates, global corporate leaders, activists, media executives and cultural entrepreneurs from around the world.

The Centre's magazine, **Global Thinking**, is a regular outlet for new thinking on foreign policy issues. Features include profiles, exclusive interviews with decision makers, and opinion pieces by the Centre's permanent staff and associates.

The Centre runs a unique **Internship Programme** – the UK's most competitive route for new graduates into the foreign policy arena.

For more information on these activities please visit **www.fpc.org.uk**

# About the Sponsors

**BAe Systems** employs nearly 100,000 people including joint ventures, and has annual sales of some £13 billion. The company designs, manufactures, and supports military aircraft, surface ships, submarines, radar, avionics, communications, electronics, guided weapon systems, command and control systems, specialised sensors and a range of other defence products – many with international partners.

BAe Systems offers a total solution capability, the company's experience in integrated surveillance and security systems, aligned with a proven capability in the provision of crisis management and information assurance systems allow BAe Systems to take a prime role in the homeland security and asymmetric warfare environment. Experience in dealing with emergency services, MoD, the armed forces and governments place the company in a unique position across the broad spectrum of defence, from civil emergencies through to the more military conflict situations.

BAe Systems has a major presence internationally, with offices and facilities around the globe, particularly in Europe and the USA, as well as in the Middle East, Asia-Pacific and Australia. The company has a full in-service support and logistics organisation, enabling it to work with customers, both in specifying solutions to their needs, and offering the management and operation of their facilities, as well as training, repair and overhaul of products and the provision of professional logistic support.

**Control Risks Group** is the leading specialist international business risk consultancy. Founded in 1975, Control Risks has since worked with more than 5,300 clients (including 86 of the Fortune 100 companies) in over 130 countries. Control Risks aims to enable its clients to take risks with greater certainty and precision and to solve problems that fall outside the scope of mainstream management resources. Control Risks offers a full range of value-added services to companies, governments and private clients world-wide, including:

- political and security risk analysis
- confidential investigations
- pre-employment screening
- security consultancy
- crisis management and response
- information security and investigations

Control Risks has grown to a company of over 400 employees with 16 offices worldwide. Our people come from a wide variety of backgrounds, including: business, law, accountancy, the diplomatic service, the military, law enforcement and journalism.

The **Risk and Security Management Forum** is a non-partisan, non-profit making organization established in 1990 with the aim of promoting professionalism in risk and security management and to provide a forum in which members can discuss problems in an atmosphere of confidentiality (all meetings are held under the Chatham House Rule). Its aim is to bridge the gap between public, private and government arms of the security profession in the UK and to maintain contact with similar organisations in Europe.

The Forum consists of some 60 senior security practitioners and risk managers drawn from a wide range of commercial and industrial organisations, government departments, the armed forces, the police and academe. Membership is by invitation only and most members hold posts at a senior level in their organisations. It holds four seminars a year with eminent guest speakers and sessions in which topics of mutual interest are discussed and ideas and information exchanged.

## Acknowledgements

I would like firstly to offer special thanks to the authors. Each contributed considerable time and energy, not only to their own essays, but also towards the project as a whole.

Secondly, thanks to the team at The Foreign Policy Centre. In particular Caroline Holmqvist, Abi Tyler and Laura Vaughan for hard work in the commissioning and production of the collection. Also to Mark Leonard, Veena Vasista and Rob Blackhurst for valuable advice during the editing process.

Special thanks to David Carroll at Interbrand for creating the cover.

Finally, thanks to the RSMF, Control Risks Group and BAe Systems, without whose support this collection would not have been possible. In particular, Norman Ridley, Eric Westropp, Simon Stringer and Matt Brake.

Rachel Briggs November 2002

# The Unlikely Terrorists

**Edited by**
**Rachel Briggs**

The Foreign Policy Centre

First published in 2002 by
The Foreign Policy Centre
The Mezzanine
Elizabeth House
39 York Road
London
SE1 7NQ
Email info@fpc.org.uk
www.fpc.org.uk

This collection ©The Foreign Policy Centre November 2002

All rights reserved
ISBN 1-903558-21-2

Cover by David Carroll

Typesetting by John and Michael Breeze

# The Unlikely Counter-Terrorists

About the Editor viii

About the Authors ix

**Foreword** by *Ken Livingstone* x

1 **Rachel Briggs –** *Introduction: The Unlikely Counter-Terrorists* *1*

2 **Roger Davies –** *An Evolution of Terror: Extreme events and Al Qaida* *8*

3 **Bruno Brunskill –** *The Emergence of New Threats: Cyber-terrorism* *19*

4 **Dr Sally Leivesley –** *The Impact on the Business Community: Building resilience against chemical, biological, nuclear, radiological, explosives and electronic attacks* *31*

5 **John Smith –** *The Company Response to Emerging Terrorist Threats* 43

6 **David Veness –** *The Role of the Police* 52

7 **Bruce George MP and Natalie Whatford –** *Overcoming the Threat: Public-private partnership* *59*

8 **Richard Sambrook –** *Broadcasting Threats: The media and transmission of risk* *70*

9 **John Bray –** *Tackling the Sources of Conflict: What can companies do?* *78*

## About the Editor

**Rachel Briggs** runs the Risk and Security Research Programme at The Foreign Policy Centre. Her work focuses on how the changing security environment impacts on personal and corporate safety and risk. Her report, *The Kidnapping Business* puts forward a practical policy agenda for all the major groups affected – the Foreign Office, business and NGOs. The report received considerable attention among these policy groups. As a result of the report, the Foreign Office has changed the way it organises its travel advice for those visiting hot-spot countries, and the report is used as a training tool for NGOs exposed to risk. *Travel Advice* discussed in wider terms the content of Foreign Office travel advice and the extent of personal responsibility, the report argues that if the Foreign Office is to continue with its current responsibilities to Britons overseas, prevention is better than cure. Rachel's work has been covered in newspapers, such as The Sunday Telegraph, The Financial Times, The Times, and The Sunday Express; and in specialist publications, such as Energy Day, Insurance Day and Foreign Policy magazine. Rachel regularly broadcasts and writes on international security, kidnapping and other aspects of criminal economies.



## About the Authors

**John Bray** specialises in political risk and corporate accountability issues at Control Risks Group. His report '*Facing up to Corruption: a practical business guide'* was published in October 2002.

**Bruno Brunskill** is an Executive Consultant with Anite Modernising Government Division and a board member of the Information Assurance Advisory Council.

**Roger Davies** MBE QGM is a former British military counter-terrorist officer with significant operational experience. He provides analysis of terrorist incidents and threats to UK and US government departments as well as to the commercial sector.

**Bruce George** has been MP for Walsall South since 1974. He chairs the House of Commons Defence Committee and was recently elected as President of the Parliamentary Assembly of the Organisation for Security and Cooperation in Europe. **Natalie Whatford** BA MSc is a researcher and heads the parliamentary office to Bruce George MP.

**Dr Sally Leivesley** is Global Continuity Manager for Risk Analysis (UK) Ltd. She was formerly a scientific advisor, consulting to the Home Office on protection of the population, on projects such as the Channel Tunnel, Thames Barrier, and the City of London.

**Richard Sambrook** is Director of News for the BBC, responsible for all news output on radio, TV and online. He has been Deputy Editor of the 9 O'Clock News, News Editor, Head of newsgathering and Director of Sport before taking his current position in 2001.

**John Smith** is the Head of Group Security at Prudential. He has been in commercial security since 1978 before which he was with the Royal Military Police, specialising in close protection and investigation.

**David Veness** CBE QPM is the Assistant Commissioner for Specialist Operations at New Scotland Yard. He joined the Metropolitan Police in 1964 and has handled hostage negotiations since 1979.

# Foreword by Ken Livingstone

The threat of a catastrophic incident in London remains with us. London's emergency services have a well-deserved worldwide reputation for emergency response. But sound threat analysis and risk assessment; robust and fully resourced consequence management arrangements; properly integrated communications; and consistent security policies and practices right across London are also essential.

As Mayor of London I have been closely involved over the past year in building up our capacity to handle a catastrophic incident. I have been working with the wide range of public and private sector stakeholders who are involved in the array of actions that are in hand. A fully co-ordinated London-wide approach is a key requirement.

Through the work of the London Resilience Team, which was set up to facilitate the work of the Civil Contingencies Committee, a new partnership has been created which encourages key stakeholders to work together in planning their response to a major terrorist threat in London. The London Resilience Team provides the necessary bridge between strategic thinking and action on the ground needed to improve London's resilience. This collection of essays, co-ordinated by The Foreign Policy Centre, represents a positive step in the same direction.

The contributions in this volume are a small example of the concerted efforts of many individuals throughout local, regional and central Government and those in business, industry and the voluntary sector. To the authors of individual chapters, and to those making the policy and practical changes happen, I offer my thanks on behalf of London.

Increasing the resilience of London depends upon on three fundamental principles. First, the security of London can only be improved by working in partnership – both public and private sectors need to be actively involved. Second, rapid, honest and consistent communication is central to increasing safety and gaining public trust. Third, industries and sectors must be aware of their co-dependency on each other – that business continuity in one industry will affect the business continuity of others and improving security preparedness for each will improve security preparedness for all.

We cannot be complacent; the devastating attacks on 11 September represent a qualitative change in terrorist threat. All organisations must play their part in increasing London's resilience by ensuring they have effective and up-to-date contingency systems. As Mayor of London, I will work to improve the resilience of London: heightening security awareness and re-assessing security measures – ensuring that London remains a safe place in which to live and work.

Ken Livingstone London, August 2002

# 1 Introduction: The Unlikely Counter-Terrorists

Rachel Briggs

> **"There is little point in protecting Whitehall if the City of London is devastated"**
>
> *John Smith, RSMF and Prudential*

Counter-terrorism is currently the preserve of the state. Traditionally the main target for terrorists, the government and its agencies lead the UK's fight against terrorism. However, as the threat, most notably that posed by Al Qaida, becomes more diffuse and increasingly determined, business is more likely than ever before to be targeted.

This is now received wisdom. More rarely explored is the role that companies could play in minimizing the impact of terrorism – ensuring that terrorists, if they penetrate our security net, do not succeed in inflicting massive human and economic casualties. The cinematic scale of 11 September, the randomness of office workers beginning a normal Tuesday morning and never returning home, have led to a sense that homeland security cannot defeat a determined terrorist threat. If thousands can be murdered in downtown Manhattan, it can happen anywhere. What use are the old precautions – bomb-proof curtains or fire alarms – if we face flying bombs full of aviation fuel or, worse, biological and chemical weapons? This is to ignore the real, practical lessons of 11 September. The death toll might have been far worse if the Twin Towers hadn't practiced evacuation procedures after the unsuccessful bomb attack to bring the towers down in 1993. And those companies with contingency plans – new accommodation from which to resume operations almost immediately after an attack and insurance against losses – were far more likely to weather the storm in the short- to medium-term. Though business can never predict terrorist attacks or even stop them from succeeding, evidence shows that it can limit their impact. Therefore the UK requires a new breed of counter-terrorist – based not in Sandhurst, but in the City of London.

The case for business involvement in counter-terrorist activities in the UK is a combination of self-interest and social responsibility. The corporate world is an increasingly important target for Al Qaida. Intelligence in this collection shows the group has been linked to plots against a number of companies, including Microsoft and US companies in Singapore. Targeting companies not only achieves economic disruption, it also creates fear and panic among the population at large. Some companies are more attractive targets than others, most notably those companies comprising the UK's so-called critical infrastructure, such as water and energy suppliers, transport and telecommunications networks and financial institutions.

In 2000, the scale and speed of disruption caused by the fuel crisis illustrated vulnerabilities within these infrastructures – but the damage caused by peaceful blockades would be dwarfed by the impact of a determined and ruthless terrorist network. Even where the business community is not directly targeted, companies may suffer collateral damage from an attack on government, military, cultural or religious buildings, especially given the scale of impact sought by Al Qaida. Roger Davies suggests that for this reason the embassies of certain countries – particularly the US, Israel and the UK – should reconsider their location within cities, and buildings within their immediate vicinity should certainly review their security and contingency plans.

Companies have a responsibility to their staff, shareholders, investors, suppliers and neighbours to take their risks seriously and do everything they can to tackle the threat head-on. David Veness rightly points to the financial sector's response to the threat from the IRA/RIRA as an

example of corporate responsibility. This needs to extend across the business community as a whole.

Many companies, though, are shirking their responsibilities to tackle terrorism. In a recent survey of 5,000 companies, just 45 per cent had business continuity or consequence management plans in place. Bruce George observes, "many have decided either rationally or out of indifference that little requires to be done." Some companies may wrongly assume that the scale of the threat is so large that it can't be managed. Others may assume the policies they already have in place will be able to cope with new and emerging threats. In fact, the authors show that adopting these policies against some new threats could at best prove ineffective, and at worst actually worsen the impact. Ultimately, there is little pressure exerted on companies that choose not to act. There are no agreed standards of best practice, and this makes it difficult for a company's stakeholders – its staff, shareholders, suppliers, neighbours, and so forth – to question the policies it adopts. Bruce George recommends that the insurance industry could offer incentives to companies that take security seriously. In the area of terrorism insurance this might require a leap of faith by the market, but could be one way of encouraging good behaviour.

Dr Sally Leivesley stresses that it can take up to two years to implement risk management into business operations. Maintaining the momentum over this period – particularly if there is not an attack or there are long periods between them – requires buy-in from the board. John Bray observes that Chief Security Officers are a new feature on boards in some US companies, and debate continues about whether this is necessary to ensure security is a key strategic concern for boards.

Terrorism is a risk that companies must learn to live with. They cannot withdraw from all areas where there is a risk of terrorist activity, especially as the threat becomes more diffuse and widespread across the world. And while there is little they can do to detect or interdict planned attacks – that is indeed still the role of the state – they can



prepare contingency and crisis management plans to ensure their response reduces rather than exacerbates the impact of a successful attack.

Preparation is key. 'Thinking the unthinkable' has been a much-used phrase since 11 September; companies must not just be prepared for the last attack, they must anticipate what's coming next. Dr Sally Leivesley recommends that companies run regular scenario sessions, preferably in collaboration with the government, and should have a trained and permanent crisis management in place to take ownership of this work. These plans must then be revisited on a regular basis. John Bray quotes Joe Allbaugh, Director of the US Federal Emergency Management Agency, speaking in Brussels in March 2002. Referring to the experience of emergency services in New York, his comments apply equally well to companies and governments, "They need to take their plans off the shelf, dust them off, get them up-dated and be prepared because when there's an incident it's too late."

The authors highlight a number of specific policies – many of which were developed in response to the threat from the IRA – which must be revisited in the light of the threat from Al Qaida. Companies must prepare for losses and damage on a much larger scale than they have ever faced before. It is highly unlikely they will receive a warning, and there is evidence that Al Qaida has tried to obtain weapons of mass destruction. As John Smith remarks, "It is now prudent to consider and plan for damage on the geographic and time scales of Chernobyl, Bhopal or Toulouse. A police cordon for 3-4 days some 400 metres around the site of a conventional vehicle bomb explosion may be a thing of the past. Successful chemical, biological or radiological attacks may deny access to large segments of cities for significant periods." The possibility of large-scale loss of life requires companies to take succession planning seriously. Loss of the entire Board is a risk that should be planned for, and John Smith recommends that companies have succession plans in place for this possibility. The so-called 'golden hour' after an attack is now more important than ever

before; a company's response in the minutes after an attack will determine whether or not they survive.

Companies must also revise their relocation plans. Many establish alternative offices where they can relocate operations in the event of an attack – so-called 'hot' and 'warm' sites. These tend to be near enough to the original office to limit the amount of disruption to staff and operations. In the event of a large-scale attack, though, access to such 'hot' sites may also be denied, as was the case with some companies in the World Trade Center.

Even with the best crisis management plans in place, a successful response depends on the willingness of the workforce to follow instructions. For example, in the event of a chemical or biological attack, workers may be safest remaining inside the building. But with the images of the Twin Towers firmly etched in their minds, some may choose to vote with their feet and leave the building. Not only would this put the individual at risk, it would also increase the movement of air, thus spreading the substance yet further. The role of the media in such situations will be key, as individuals look to trusted news sources for guidance about what to do. As Richard Sambrook comments, media organisations strike a delicate balance between spreading fear and panic and holding back information that might help people survive.

Much more attention must be given to the question of how companies will fund their recovery, as this will determine whether they can survive. The government extended the remit of Pool Re insurance in 2002, but this is limited to the commercial sector and to institutions that accept the cover and increased premiums. The availability of compensation for death, injury and loss of assets by the workforce could be crucial after attack to ensure that companies – and even cities – can still function.

Commercial practice is, of course, to transfer losses to the insurance sector. As Dr Sally Leivesley suggests, it may be that in the event of an extreme attack it is those companies that are able to carry a higher proportion of their risk and recovery financing internally that will be less likely to fail under an extreme attack. This is an area that needs urgent examination.

Companies can also be part of the solution on the ground, helping to tackle the factors driving terrorism and sympathy for the cause. John Bray cites the example of a business-sponsored NGO, the Philippine Business for Social Progress. It works on a series of projects in Minanao, home of the Islamic extremist guerrilla group Abu Sayyaf, a group suspected of having links with Al Qaida. Amongst other things, it provides business training and work placements to young Muslims to provide opportunity for those who might otherwise become radicalised by poverty. Companies also need to check their own behaviour to ensure they do not exacerbate the problem on the ground.

Of course, the role for the government is still as important as ever. David Veness rightly argues it has a responsibility to provide a framework within which companies can carry out their counter-terrorist responsibilities. This framework would create the momentum needed to maintain this important work into the long-term. As David Veness comments, the foundations for this framework have been set but there is much more work to be done.

If the government is to embrace the concept of business acting as counter-terrorists it must not let companies face the threat blindfolded. As Bruce George observes, corporate security managers only have access to relatively low-level intelligence, which undoubtedly impacts on their work. While some, through personal contacts, may have access to more, the government must address this deficiency and ensure that access to intelligence is deepened and widened and delivered in a more systematic way. Of course, there would continue to be sensitivities around certain types of intelligence and it would need to balance often-opposing concerns. But ultimately, the government has a responsibility to make information sharing work. Towards this end, Dr Sally

Leivesley recommends establishing a 'one-stop shop' link for companies within government and the creation of a link between the Cabinet Office and industry leaders to share information and intelligence. John Smith recommends up-dating the well-respected Home Office pamphlet, *Bombs: Protecting People and Property* to include information about chemical, biological, radiological and nuclear (CBRN) attacks.

A co-ordinated response necessitates co-ordinated planning. Dr Sally Leivesley also calls on the government to initiate joint government-business scenario planning sessions and exercises to test their plans, managed through what she calls a 'Cities and Regional Resilience Exercise Programme'. A national programme of this type would allow lessons learned and experience in one area to be transferred to other parts of the country. This practical partnership would also help to build the trust between public and private sectors that is often lacking, especially in relation to matters of security.

Public-private partnership should not be regarded as being one directional – the government depends on business in a number of ways. The business community is responsible for developing the software and technology that can help tackle cyber and other forms of terrorism; many of the country's critical infrastructures are now privately-owned; the long-term stability of the UK following an attack depends on the business community getting back on its feet as quickly as possible; and there are now infinite dependencies between systems. Public-private partnership in tackling terrorism must be based on genuine principles of partnership. Businessmen may be unlikely counter-terrorists, but a national policy without them will make the UK a softer target for attack.



# 2 An Evolution of Terror: Extreme events and Al Qaida

Roger Davies

## Introduction

The nature of terrorism is such that it acts against the security of the individual and the state. On 11 September 2001 the vulnerability of both the state and the individual citizen were brought into sharp focus as Al Qaida simultaneously hit the heart of US security – the Pentagon – and brought to the ground one of the world's biggest office complexes and symbol of the global economy. Some have suggested that the attacks of 11 September represent a "new" form of terrorism, one that is a significant departure from anything that went before it. However, by reviewing examples of current threats and past attacks from open source material, this chapter will show that what we have seen is not the arrival of a brand new threat, but a continuing evolution of existent threats. Al Qaida (and other groups) have used suicide bombers before – such as the embassy bombings of 1998 and the attack on the USS Cole. Large aircraft have been blown up on numerous occasions resulting in significant numbers of casualties. The World Trade Center itself wasn't a new target for Islamic extremist terrorists, who in 1993 had planted a bomb there with the intention of bringing the buildings down. Even the later anthrax attacks in October 2001 weren't an entirely new threat. It would appear, for example, that Aum Shinrikyo considered anthrax as a weapon and perhaps even mounted unsuccessful dispersions of some form of anthrax spores in Japan in the 1990s – thus chemical/biological attacks were hardly new, in principle, even then.

The role of protective, mitigating and recovery systems is to reduce the vulnerability of potential targets against threats. The fact that we are unlikely to come up against an entirely new threat is a positive for

policy-makers and practitioners who have to implement and utilise these systems. However, the fact that we can never be sure how terrorists will use the tools at their disposal or which direction they will take next presents us with significant challenges. Terrorists, of course, seek out the chinks in the armour of the societies and the individuals against which they operate. It is therefore crucial that our responses are constantly up-dated, because if we develop rigid responses that assume a static terror threat the terrorist can easily adapt their tools and strategies to find new chinks in the armour. This requires that the very policy and decision-making machine itself is fluid and able to drive the process forward rather than playing catch-up with the terrorists. As this chapter will show, the public and private sectors are in this together – it is now often impossible to isolate direct targets from those affected indirectly – and the need for co-operation and co-ordination between them is crucial if the UK as a whole is to reduce its vulnerabilities and increase its resilience against attack. This is a theme that will be picked up in later chapters.

The evolving threats we face perhaps provide governments and businesses with new and challenging situations. Terrorists are now seen to have global reach and global links. This is no longer some theoretical concept for academics to chew on. It is a personal and active threat to every member of the population. Whilst terrorists have always been able to carry out mass casualty attacks (and in many cases have done), there is now a realisation that the threat can reach the doorstep of every home and business across the globe. It is this realisation that is new, not the threat.

### The Evolving Threat posed by Al Qaida

As Table 1 below shows, Al Qaida has continued to pose a significant danger in the months since 11 September. The group is thought to have targeted a number of different targets, from embassies to banks and shopping malls, and is still believed to be highly active. It should be remembered, though, that the attacks of 11 September did not occur "out of the blue". Indeed, there were frequent warnings about attacks resulting in regular closure of US (and in some cases British) embassies and heightened security at US military bases, particularly in the Gulf region. Ahmed Ressam, believed to be an Al Qaida cell leader, was arrested in late 1999 in the US, where he was believed to have been planning attacks over the Millennium. There are other reports of Al Qaida linked attacks in Strasbourg and in Jordan planned to occur at the same time. There were successful Al Qaida attacks against US Embassies in Nairobi and Dar es Salaam, the USS Cole and a number of others since the early 1990's that in retrospect appear to be linked to Al Qaida, even if that organisation did not theoretically exist at the time. It is now apparent that planning for a major attack by an Al Qaida linked organisation in Singapore, that was prevented in January 2002 began as long ago as 1993 when "sleeper cells" were established there.

Open source material clearly shows that US diplomatic interests are the most important targets for Al Qaida. US embassies, particularly in countries where there is a significant Islamic population, are at the highest risk. US embassies are not alone though; other countries to have had their embassies targeted include the UK and Israel. Many of these embassies appear to have been targeted with large truck bombs, often containing upwards of 500kg of explosives, which could be expected to cause significant damage to other buildings, often commercial, in the vicinity of the target. As such, buildings within 400m of a US, UK or Israeli embassy anywhere in the world – or near to any high-profile government building, such as the Houses of Parliament – should review appropriate evacuation and crisis procedures as they should be considered to be potentially at risk of collateral damage. Given the determination of Al Qaida to cause as much damage and terror without warning, this may raise a long-term question over the location of certain embassies within cities. Clearly capital cities need to have response plans to deal with a number of simultaneous no-warning truck bombs.

US military targets are also at significant risk. This includes naval ships, such as the attack on the USS Cole; plots in the Gulf and Singapore; and land bases such as the 1996 Khobar Towers bombing in Saudi Arabia. Due to the remote location of many of these installations,

**Table 1**
**Targets believed to have been subject to attention from Al Qaida plots between September 2001 and September 2002**

| Country | Targets |
|---|---|
| **Albania** | US Embassy in Tirana |
| **Austria** | US Embassy in Vienna |
| **Bahrain** | Attack on US Naval facility |
| **Belgium** | NATO headquarters |
| **Bosnia** | US Embassy (more than one plot), UK Embassy in Sarajevo and a NATO base |
| **Cambodia** | US Embassy |
| **France** | US Embassy (suicide attack) |
| | Richard Reid, the "shoe bomber" attempted to blow up a transatlantic flight |
| | Possibly Notre Dame cathedral |
| **Germany** | Attack on unknown railway station |
| **Indonesia** | US Embassy, followed by attacks on German, British, Dutch and Singapore diplomatic missions. Attacks were also said to be planned on the State Secretariat |
| | Attacks said to be planned on foreign and local banks and shopping malls |
| | Attacks said to be planned on train stations |
| **Italy** | US Embassy |
| | Threats to Vatican targets and churches in Bologna, Venice and other cities |
| **Jordan** | Attack on unidentified US target and other attacks planned, including on the US Embassy and the Israeli Embassy |
| **Malaysia** | Various embassies in Kuala Lumpur |
| **Morocco** | Attack on US and UK Naval shipping in the Straits of Gibraltar |
| **Philippines** | US Embassy |
| **Singapore** | US Embassy, UK Embassy, Israeli Embassy, US military targets |
| | Transport infrastructure targets such as a railway station and a taxi stand. Possibly to be co-ordinated with attacks in Kuala Lumpur and Jakarta |
| | A list of 200 US owned companies based in Singapore was recovered from the terrorists. Attacks would have caused significant collateral damage on businesses |
| **Turkey** | Attack on St Sofia cathedral, Istanbul and rumours of interdiction of an attack on a US target |
| **UK** | Undefined targets linked to simultaneous attacks in Germany |
| **Vietnam** | US Embassy |
| **Yemen** | US Embassy |

*Source: TRITON database, HMS Ltd.*



it is much less likely that an attack will result in secondary indirect impact on civilian victims. Yet public areas with a concentration of military personnel are also attractive targets for terrorists, as they are able to hit both the intended target and cause widespread fear and terror among the population at large. Particularly vulnerable to terrorist targeting are population-dense areas, such as airports, bus and railway stations, as well as the aircraft and military buses themselves. Increased security on aircraft has resulted in ingenious methods of circumventing protective measures, and may ultimately result in a displacement of attacks to other population-dense targets.

Other targets that could cause direct or collateral damage on businesses are buildings with cultural or other national status. Aircraft and airports offer both high user density and an additional motivational driver in the perception of fear engendered in the flying public and business community. Capital city airports and national flag-carrying airlines are attractive to terrorists because they present an opportunity to damage national interests as well as corporate and public entities. While the failed attempt of the shoe bomber on board an aircraft has focused attention on the aviation sector, there have also been credible reports of serious threats to rail stations in both Singapore and Germany.

Commercial targets are at threat, directly as well as indirectly. In one of bin Laden's video statements, released after the World Trade Center attacks, it was clear that he viewed the economy of the United States as a key target for his organisation. The investigations into the Al Qaida-linked plot in Singapore apparently uncovered a list of 200 US companies based in Singapore compiled by the group. Three had been highlighted, possibly because of the high profile that these CEOs had in Singaporean society. In March 2002, information emanating from Afghanistan suggested that Microsoft was a possible intended terrorist target. The business community must accept that it is now a possible direct target for organisations such as Al Qaida, which recognises the significance of these targets and the impact their disruption would cause around the world. While it might be more likely that US

companies will be targeted by Al Qaida, there are clear implications for the UK both at home, where many US companies have offices, as well as around the world, where UK interests might find themselves the indirect targets of a hit on a US company.

There appears to be a pattern of threats against religious buildings, as has been seen in Paris, the Vatican, Venice, Istanbul and Strasbourg. The form of these possible attacks has not been clear from open source material, but there may be indications that different forms of attack have been planned such as highly public hostage situations that result in a massacre.

### Tools

The most likely threat from Al Qaida continues to be of an explosive attack. Evidence from Afghanistan has demonstrated that Al Qaida bomb makers were relatively skilled in constructing a range of explosive devices, including postal bombs, other booby traps and radio controlled bombs. Although these threats have not yet materialised, they could do at any time.

Although there was much concern that Al Qaida was attempting to develop other weapons of mass destruction in Afghanistan, it would appear that while they have an aspiration to develop chemical biological or radiological weapons, they have not yet succeeded. That is not to say that we shouldn't be cautious, particularly as apparently conflicting evidence continues to emanate from Afghanistan and elsewhere. In Italy, during the summer of 2000, alleged terrorists had a cyanide compound in their possession, which shows that we should take such threats seriously. It is unlikely that the compound recovered in Rome would have made any sort of effective weapon. But even if the capability is not yet there, the intent is. The anthrax attacks of October 2001 demonstrated that terrorists do have the capability of acquiring and using biological agents. The lesson to take from this is not that the attack was ineffective, but that the agent exists in the hands of evil people who might develop the capability of utilising it in a much more effective manner. The fact that this attack used a relatively ineffective technique should not deflect our concern for dealing with a much more efficient use by terrorists of the same weapon. Regardless of who is responsible for these attacks, they do not necessarily constitute a "new" threat. In the 1990s, it is thought that Aum Shinrikyo may have mounted an unsuccessful dispersion of some form of anthrax spores. The impact of this type of method of terror should never be underestimated though. Whilst relatively small in terms of fatalities, the disruption to the US postal system and government offices was certainly significant. The consequences of a successful widespread dispersal of such material (and we have to assume that the perpetrator still has spores for such an attack) demand that both governments and businesses examine carefully our responses to such an incident.

From the public responses of governments, it is clear that there is a rising concern regarding a radiological dispersion device or even a nuclear device. The real threat from these devices is difficult to ascertain from open source, but it is apparent that:

- Al Qaida had or has a clear interest and intent to develop mass casualty weapons, including chemical biological and radiological weapons.

- Iraq has had and may continue to have the means, technology and motives to present a significant threat either by military or terrorist attack modes.

Weapons of mass destruction pose two key challenges for companies: mass casualties and contamination. The consequences of these attacks could indeed be mass casualties and this demands that governments and businesses examine their continuity plans to ensure they are able to continue operating in the event of significant casualty levels. In some ways, though, the more difficult challenge on a practical level will be decontaminating whole areas of cities. This is a hugely complex task needing massive resources, whatever the nature of the weapon, and any

government will struggle. Thus businesses need to consider their responses in the event of a contamination, especially in the event of an attack that affects headquarter buildings in major cities. Simply sitting back and expecting the government to hold their hands and have them back in business after a couple of days is unrealistic. If businesses are interested in retaining shareholder value they need to demonstrate effective crisis plans to cope with this scenario. Not only could this stop shareholder value collapsing, it may even give them a competitive edge. Practical, inexpensive plans are indeed possible.

Whilst it is tempting to concentrate on those threats that pose the biggest potential impact on society, it is important that other forms of terrorist attack are also considered. Over the last few years the lone suicide bomber, who carries their bomb strapped to his or her chest or perhaps in a bag, has brought fatalities and terror to societies in Sri Lanka and more recently in Israel and Palestine. This form of attack has also been seen in a number of other countries, but largely not yet in the West. There is a perception that because Al Qaida has mounted large-scale attacks using suicide bombers or suicide hijacked aircraft, smaller-scale attacks by individuals with small bombs are not of interest to them. This perception is probably wrong. The "shoe bomber", Richard Reid, appears to be linked inextricably with Al Qaida and his suicide bomb was also a small device, but he or his mentors had identified a "chink" in the security of their target allowing them to maximise the effect of such a small device. Al Qaida also used another concealed suicide device to assassinate Commander Masood in Northern Afghanistan. The largely free and open society that we treasure is particularly vulnerable to lone bombers exploding devices in crowded shops, tube stations, restaurants or commercial reception areas, and it is particularly effective at spreading genuine fear and panic among the public.

## Methods and Implications

Governments and businesses are challenged by the evolved threat but an understanding of the terrorist modus operandi allows the first steps to be taken in increasing resilience.

Firstly, while most UK facilities and organisations within London, especially those within the City, do have bomb incident plans, many are based on the premise that a warning of some sort will be given. With Al Qaida attacks, no warning will be given. This has enormous implications for the effectiveness of current plans and procedures, which must be reviewed. Businesses and organisations within areas of high risk must consider scenarios beyond the traditional evacuation drills. Simply placing desks a metre or two further away from windows sounds like a trivial solution, but it really can help in some circumstances. Covering windows with a plastic film is another, as is improving tannoy systems and crisis plans for establishing 'hot' sites elsewhere in the country, in the event of a London business headquarters being damaged or contaminated. John Smith has more detail on this topic in his contribution later in this collection.

It is apparent that Al Qaida has the intent, as was seen in Singapore, and the capability, as was witnessed in Dar es Salaam and Nairobi, to mount multiple co-ordinated attacks – in these cases, truck bombings. This capability was, of course, also seen on 11 September and may have been planned for the Millennium. The implications for those planning responses are important. Multiple co-ordinated truck bombings within a single city will stretch emergency services significantly, and the threat demands that appropriate resources are available and that procedures are rehearsed to ensure that potential targets are prepared and able to respond. A speedy alert system might also be warranted, to warn other potential targets when a single explosion or attack occurs. Other targets – either public or private sector – would then be able to batten down the hatches for a period. The single event that triggers this response might even occur in another country.

Al Qaida, of course, does not present the only terrorist threat to society. In the UK we have had more experience than most nations of the damage and horror of terrorism. But there are lessons to be learnt here

as well. Throughout the Irish republican terror campaign, the terrorists regularly changed tactics, from assassinations, to letter bombs, to car and truck bombs, to military targets to transport and infrastructure targets, in a continually changing spectrum of threat. We need to apply the lessons learnt here on the national scale to a broader threat spectrum from Al Qaida on an international scale. We can expect Al Qaida to continue to attempt extreme catastrophic attacks, but we can also expect them to adopt the military maxim of surprise. It is vital therefore that our responses are driven by careful monitoring of the dynamic, constantly changing threat, to ensure that surprise is kept to a minimum and our resilience is increased by effective protective, mitigating and recovery plans. Perhaps we also need to revisit the spectrum of conceivable terrorist threats, identify those elements which might be used again by terrorists in different circumstances and design our responses accordingly.

The breadth and scale of the terrorist threat we face means that businesses cannot assume that a government response on its own will be enough to tackle the threat or create preparedness on the part of companies. The government will face its own challenges, especially in the immediate aftermath, but also in the longer term if there are significant casualties or contamination of some form. The primary obligation of the governmental response will not be to enable business to continue – it will be with casualty management and repairing the "infrastructure", such as power, communications and transport systems. Businesses are therefore obliged to address the issue of how their business will continue to function themselves.

## Conclusion

There is a strong, but entirely human, psychological response to these horrific threats that business and to a lesser extent governments have to overcome. This response is characterised by two attitudes, both of which enable people to go into denial of their responsibilities and avoid addressing the issue:

- "It won't happen to us" – people feel that the chances of terrorism directly affecting them are small and that they can get away with doing nothing.

- "If it does happen, the consequences will be so big there won't be anything I can do it mitigate it".

The fact is, however, that the scale of this evolved terrorist threat is so large it can no longer be discounted. The chances of people being affected by a large-scale terrorist event are increasing. It is therefore vital to convince companies, governments and individuals that there are very real, practical and simple measures and activities that they can take that will protect, mitigate against and enable them to recover from a wide range of terrorist attacks, even the most horrific and challenging. The changing and evolving nature of the threat means that we need a dynamic response that can cope with the challenges ahead, and this response needs to be adopted by businesses as well as governments. At the time of writing, the increased threat levels from today's terrorists have been apparent for nearly a year. Governments and businesses will both perhaps have some explaining to do if they get caught without having considered their response. There may be an instinctive reaction for an ostrich to stick its head in the sand. But the threat is real, immediate and requires action from all, now.

# 3 The Emergence of New Threats: Cyber terrorism

Bruno Brunskill

## Introduction

Decision makers are not convinced that cyber threats are worth taking seriously. In part, this may be due to the apparent non-event that was the Millennium bug. This paper makes no pretence that risk assessment of cyber threats, from terrorists or others, is straightforward but aims to give a frank and objective summary of the issues.

The first anniversary of 11 September gave rise to eminent specialist groups questioning the sufficiency of US protective measures against terrorist cyber attack. The American Association for the Advancement of Science reported that the American scientific community, private sector, government and industry must all become more prepared for a cyber attack. A survey of nearly 400 IT professionals showed that over 50% thought it likely that the US would be hit by an attack in the next few months. Intelligence reporting is low volume but there has been a rise in the number of reports of terrorist groups using and being trained in electronic attack methods. The US draft *National Strategy to Secure Cyberspace*, published in September 2002, recognises that the number, sophistication, severity and costs of cyber attacks are increasing.

Meanwhile, Western society is now wholly dependent on electronic systems. They provide everyday services to citizens; they hold and manage all organisations' valuable information assets; many systems are nationally critical to the delivery of electricity, fuel, water and communications. These systems are increasingly complex and interdependent – when one system fails it is almost impossible to contain the impact.



Cyber terrorism is not rocket science, although some types of attack require specialist skills that terrorist groups can acquire. This paper does not say that a cyber attack by Al Qaida is imminent (the evidence in the public domain does not support that contention), rather the paper shows as objectively as possible that there are serious areas of vulnerability that can be exploited by those with malicious intent, be they terrorists, spies or criminals. A key point is that critical electronic systems in western societies would appear to be attractive targets for terrorists sharing the Al Qaida ideals.

Governments, companies, public sector bodies and others face a number of obstacles in trying to mount an effective and efficient defence against this threat. But there are a number of positive steps to be taken to reduce the risk from cyber terrorism in the UK: security standards in software products can be improved; the Government can improve the take-up of its guidance and support; organisations need to work much more closely by sharing threat and early warning information.

## Impact

There can be little doubt about the severe potential damage that a cyber attack can deliver. These have been summarised in numerous papers, most recently in the OECD Security Guidelines published in August 2002 and will not be repeated here. Suffice it to say that electronic systems are now the lifeblood of developed Western societies. They play an essential part of almost every aspect of our daily working and social life; they are the sinews of the UK economy; they are at the heart of almost all control systems; they are vital to our military, law enforcement and emergency services. It is, nevertheless, worth emphasising some of the particular features of a cyber attack.

Critically, the impact of an attack may begin to be felt only some time after the attack has taken place. For example, viruses have been infiltrated into target systems with timing delays to cause their release some time after infiltration. An attacker may try to divert suspicion that an attack has been staged by delaying activation of a malicious malfunction.

A successful cyber attack is like the delivery of a weapon of mass destruction but without the immediate and widespread loss of life. A cyber attack against health facilities will cause loss of life even if most cyber attacks do not directly cause casualties. It is an indiscriminate form of attack because no one can tell exactly how widespread the impact of one attack will be. The widespread disruption of services will make people feel that their life support features are all under threat. The shadowy nature of a cyber attack has the capacity to create the widespread sense of demoralisation, lack of confidence in the authorities and panic in developed societies that would suit the ambitions of many of today's terrorist groups.

This is not simply a potential threat; impacts from cyber attacks are being felt every day by organisations around the world. The manifesto of the Information Assurance Advisory Council (IAAC), launched on 16 March 2002, listed many contemporary examples. PwC calculated that US companies lost $266bn to viruses and hacking attacks in 2000. In 2001, attacks put Yahoo!, e-Bay and Amazon temporarily out of business. The 2002 DTI/PwC survey records that 44% of UK businesses suffered one malicious security breach in 2001-2002.[1] The average cost to each business was £30,000 with some security incidents costing over £500,000. More concerning is the attempt by a security guard in 1999 to hack into a UK nuclear plant's IT system.

## Threat

The attacks of 11 September and the public rhetoric of terrorist groups associated with Osama bin Laden show intent to strike at Western societies in their totality. This is a change from the more traditional intent of IRA and other terrorist groups that have in the past eschewed mass civilian attacks. Disruption of the business and socio-political lives of Western societies seems, to Western analysts, to be an attractive vision for Bin Laden associated terrorist groups today and there is increasing mention of electronic attacks in their literature as well as in reporting of their activities. Cyber attack is a method that is well suited to non-state actors and perfect for 'armies of irregulars' because the 'weapons' are freely available.

There are different types of terrorist cyber attack: terrorists could break into a computer or communications network and introduce a new virus. Viruses take many forms and the most damaging is one that destroys data on a system and/or destroys the electronic processes that handle the data; terrorists could flood the link between an organisation and the Internet with so much e-mail traffic that the organisation's system cannot cope and crashes; terrorists could introduce an 'insider' to an organisation in order to steal or tamper with information on the system; terrorists could break into a computer or communications network and surreptitiously steal or tamper with data on the system.

The tools to carry out damaging cyber attacks are readily available for would-be attackers to use. There are plenty of sites on the Internet that provide the tools for easy download. There are also a large number of discussion groups and other 'chat rooms' where attacking expertise and knowledge is shared and developed. An expert user of everyday computer or communications equipment would have sufficient expertise for some types of attack, attacking websites for example. Many sites have poor password protection, or non at all, allowing an attacker to enter easily and deface the site with obscenities, divert subsequent visitors to a site of his choosing and/or create a new vulnerability to future virus attacks. These straightforward attacks are damaging to reputation and costly in terms of lost business.[2]

Specialist skills would be needed, however, to carry out a surreptitious attack without risking revealing the attack to the system owner. Terrorist groups will be capable of hiring, recruiting or blackmailing people with the skills and experience to undertake highly damaging cyber attacks. They will be most likely to obtain these people through organised criminal groups who have developed cyber attack capabilities. Some groups have the resources and the incentive to invest in high quality collaborators and to train them well. Many of these

groups have developed high quality IT skills to facilitate the surreptitious electronic laundering of their funds.

### Vulnerabilities

Vulnerabilities in systems and in software correlate with the level and type of threat to systems. Threats follow vulnerabilities much more in this cyber threat area than in other threat scenarios. News of a potential weakness in a software package spreads rapidly to system administrators all over the world to alert them to the problem and it is inevitable that people in the hacking communities learn about it as well. Furthermore, hackers put great efforts into probing software packages for weaknesses and may well discover a weakness that the manufacturers and the user communities have yet to find. Once a weakness has been found, it is common for cyber attackers to probe all the instances of a particular software or system in the search for an opportunity to exploit it. Scanning a vast number of potential victims is so much easier electronically than in other potential attack situations.

Information systems are highly complex entities comprising many separate elements. The complexity makes it difficult to judge whether the system is working satisfactorily and is undamaged; it is surprisingly hard to be confident that a system is in a normal and/or good working condition. This makes early detection of the attack difficult. Major crashes and defects are all too obvious but most systems in organisations have functionalities that are not in regular use by the organisation's staff. A system defect or some forms of attack might remain unnoticed for some time in rarely used parts of a system.

Marketing pressures encourage the rapid production of new software and upgrades of existing packages. Costly quality control and security features often take second place to market pressures for quick production and low cost products and many defects may still exist in the software products; there were thousands of defects in Windows 2000 when it was first introduced. These are often found first by the hacking community who commit time and energy to finding ways to exploit these vulnerabilities.



Almost all information systems in business and public use are highly dependent on others. For example, in early 2002 a breakdown in a major piece of BT equipment in Hampshire was followed by the failure of a power back-up system and resulted in the total failure of the emergency 999 systems in some areas. Not only is there a huge number of mutual dependencies between systems, but also there is little information about these dependencies. The fuel crisis, albeit not primarily an information system crisis, showed vividly that dependencies almost invariably take the emergency response managers by surprise.

Many large companies, government departments and major service providers outsource many of the business and technical services to third parties. These arrangements create a number of 'many-to-many' relationships. A successful terrorist 'hit' on one organisation immediately increases the risk of a subsequent cyber attack on another supported by the same outsourcing provider. And a successful terrorist cyber attack on a third party supplier will impact on a number of their customers. Outsourcing will remain a feature of the IT industry and the relationships involved need to take more account of security issues than they do at present.

### Risk

It is both easy to over-hype the threat and to underestimate the likelihood of an attack taking place. Much of the media and some security product manufacturers tend to exaggerate the cyber attack threat; conversely, many organisations appear to assume that only other people or organisations will be targets of cyber attacks – it will not be them. We know that cyber attack tools with a potentially highly damaging impact do exist but there is no clear way of predicting the likelihood of them being used.

Even though it is hard to measure, the consensus amongst expert and academic analysts is that the risk is serious and should be taken seriously. The level of government activity supports this judgement.

The risk of a terrorist cyber attack should, therefore, be included in all organisations' risk assessments.

## Obstacles to effective response

Managing the risks posed by cyber threats is a complex matter. No single organisation can achieve this alone. A high degree of co-operation and co-ordinated responsive actions by a wide range of organisations is needed to achieve significant protection against this threat. Many senior managers and board directors are anxious about making decisions involving information systems. These systems represent major investments for organisations and the issues involved in these decisions often feel alien to many of the would-be decision makers. The 2002 DTI/PwC survey reported an increase from 53% (in 2000) to 73% of businesses believing that information security is a high priority for senior management. But few of the decision makers have competence in these matters and even fewer still have experience of handling security or safety issues as corporate matters. The language involved in information systems inhibits easy communication of risks between corporate decision makers and specialist staff, consultants and product vendors.

Most organisations are reluctant to give information about attacks and, even more so, about the degree or amount of damage inflicted on them. A recent UK attempt to establish a prototype Information Sharing and Analysis Centre (ISAC) within the IT communications sector has failed. In spite of creating a secure and trusted environment, members of the industry turned out to be unwilling to commit themselves to sharing information.

It is also difficult to provide boards with a convincing business case for investment in protective measures. There is a negative feel to security in that it seems to cost money but does not necessarily provide business benefits. Specialists in the field are confident that good information security brings potential competitive advantage but they do not succeed in convincing many at board level.



## Some ways forward

Conference speakers and academic papers have been saying for a few years that managing the risks from cyber threats requires a coherent, co-ordinated and joined-up approach from public, private and not-for-profit sectors. Regrettably, very little substantial progress has been made to make tangible and practical progress on this.

The possibility of a severe cyber attack has prompted most Western and other governments to invest in protecting critical national infrastructures (CNI). States have sought to identify the electronic systems on which their whole nation depends and endeavour to find ways to increase the protection afforded to these systems.

The UK's National Infrastructure Security Co-ordination Centre (NISCC) was founded in 1999 to take forward this work. Their work has led to identification of the UK's critical infrastructure and establishment of security standards necessary to provide protection against the prevailing threats. The National Hi-Tech Crime Unit (NHTCU) was established in 2001 to be a focus of law enforcement work against cyber crime. NHTCU is both a centre of investigative excellence and a support to all police forces in England and Wales for their work against computer crime. The Office of the e-Envoy (OeE) was appointed in May 2002 to lead and sponsor all the Government's work on the protection of information and data systems from cyber attack. This is a valuable development.

But much more needs to be done. The OeE is working on a UK strategy for information assurance; this product is needed as soon as possible for two main reasons. Firstly, there is lack of clarity about the roles of the numerous government agencies because their remits overlap. Their functions are clearly defined and are fine in theory, but when engaging with UK industries, businesses and the citizen, their roles become very confusing. In addition, each of the public bodies have to put resources into harmonising their various activities and these resources could be better used directly confronting the problems of risk.

Part of the information assurance must be to build a real and effective community of interest involving all the public bodies associated with this work. A committed sense of shared endeavour is needed to change the public sector culture of cutting up the business between departments and then defending each piece of 'turf'. One of the many tools needed is a shared information environment where all public sector organisations involved in cyber threat protection can share information within the constraints of each one's privacy and security regimes. Such a system is being developed for the anti-fraud community using the UK Government's 'Invest to Save' funds and could be applied to the information assurance business too.

Secondly, the strategy is needed to provide urgent impetus to bringing much more effective joint working between UK public bodies, not-for-profit organisations and the private sector. Most recognise the need, in theory, to work together but meetings are laced with a sense of wariness and few people attempt to overcome the first hurdle of talking a common language. Public bodies put a high priority on processes while the private sector focuses on outcomes. Both approaches are valid in their own way but what is needed is a commitment to working together to achieve practical benefits.

The private sector businesses and industries must also show stronger commitment to joint working. A good example of where this approach is needed is in the manufacture of secure software products. There is little market incentive for vendors to build in high levels of quality or security features to their software products (for reasons that have been touched on earlier in this paper), but it is not in the national interest for the software industry to continue to produce products that are shot-through with defects. Easily said but much harder to tackle; an integrated and holistic initiative by government in partnership with the private sector is an essential factor for success.

The private sector is not making best use of the existing resources because their response to this threat is too segmented. Industries and businesses tackle the risk as they think it affects them individually and do not recognise that the dependencies between systems and organisations are so extensive that they need to work much more together in responding to this threat. Industries and businesses are locked into silos, communicate little and work together only occasionally. There are excellent initiatives by the CBI, IoD and others but these are covering only a tiny minority of the organisations that need to take a much more active role in tackling this threat in a shared way.

One of the most important initiatives is information sharing, where a group of organisations or individuals enter into an arrangement to share information for the good of the group. This has to be a highly trusted sharing process because much of the valuable information will involve embarrassing and potentially damaging knowledge about one of the participants. For example, businesses or companies will only be prepared to share information for the good of a group if they can be certain that the information will not leak out and damage reputation, sales or share value.

There are a growing number of such sharing entities in the US but, as mentioned earlier, the first prototype in the UK has failed. Large sections of the US private sector have recognised, albeit after a few years of pressure from Washington, that sharing information is much more likely to achieve individual and corporate greater good than hiding it. There are some UK initiatives for information sharing but much more commitment and support from the UK government and the private sector is needed.

NISCC is promoting Warning and Reporting Points (WARPS) as a particular way of establishing the necessary organisation for information sharing. IAAC has been pushing the concept of information sharing too. In 2001, IAAC completed a study that argued the benefits of sharing threat and early warning information.[3] The annex to the paper contained analysis of the benefits and disadvantages of about 20 different information-sharing models that have been tried.

Information sharing has particular relevance in a counter-terrorist context. It can be described as a market differentiator for potential targets of terrorist cyber attack. In most situations, terrorists work in secret and in compartmentalised cells – to avoid the globe's major intelligence organisations who are hunting for them. This can give their targets a marginal advantage by developing communication networks to provide early warning of attacks; by being well informed about the cyber terrorist threat and by sharing information about actual attacks.

Yet, information sharing is a significant challenge for the way Western businesses and citizens normally behave. The marketing of products relies to a large extent on competing organisations 'talking-up' the quality of their products through advertising and other means. Information about problems, shortcomings and crises is withheld because of the damage it could do to an organisation's prospects. This market-driven urge for confidentiality is the greatest weakness of Western organisations that face cyber threats. Terrorist groups and other cyber attackers continue to have opportunities to attack because most potential targets are building protection in isolation.

There are many dependencies between organisations and it is just as much in the interests of the yet-to-be-victimised organisations as it is for those already damaged to encourage information sharing to reduce each organisation's vulnerabilities to future attacks.

## Conclusion

The terrible events of 11 September have justly focused security managers' attention on further measures to reduce the risk to people. Just over one year on, businesses, citizens and security professionals should be encouraged to look afresh at the types of threats they face. We all need to move our attention away from focusing solely on the last threat to predicting the future sources of terrorist damage to people, property and ways of life.



The thrust of this chapter is intended to be a challenge to an accepted way of Western working hidebound by confidentiality. If companies and governments do not rise to this challenge they will miss their main advantage over the cyber terrorist: their ability, collectively, to be smarter than the attacker. Sensible defences can only be achieved through developing trusted sharing practices and other ways of working together on threats and vulnerabilities. Successful protection in the face of what looks like an increasing threat of cyber terrorist attack needs much more imagination, collaboration and energy on information assurance than is today's norm.

[1] "Information Security Breaches 2002"available at www.pwcglobal.com/ie/eng/about/press-rm/news-rel/info_sec02.html

[2] www.alldas.org

[3] IAAC Threat Assessment & Early Warning Working Group's 'Information Sharing Review' available at http://www.iaac.org.uk/Wgs/InfoSharingSummary.pdf

# 4 The Impact on the Business Community: Building resilience against chemical, biological, nuclear, radiological, explosives and electronic attacks

Dr Sally Leivesley

## Introduction

The business community is a strategic target for Al Qaida. By striking commerce, terrorists are able to impact upon world markets, local economies and therefore societies around the world. Economic terrorism is not new, but because of the growing threat from CBNRE[2] attacks the business community faces new challenges and must reassess the effectiveness of its current continuity and crisis response plans.

This piece argues that a company's size and sector will be important influences on both its risk profile and its ability to recover from an extreme event. Business size and sector may be critical factors in the event of an extreme attack on the City of London or other key financial centres in the UK. Certain sizes of business may be more successful in business continuity and some industry sectors may be stronger or weaker after such an attack. A company's size and sector will influence its vulnerability to public and corporate fright; the extent to which it will be a direct terrorist target; and whether it will fail as a secondary consequence of an attack. However, regardless of size and sector, there is still more that companies can do to raise their resilience and improve the way they respond to attacks so as to minimise losses. Business continuity planning, effective risk financing, and well co-ordinated and practiced crisis response plans will all improve a company's ability to recover.



Companies must respond and up-date their risk management responses to tackle the threat of extreme terrorist attacks. Once the leading companies develop strategies, relevant protections will become known to small and medium enterprises. Ultimately, a genuine national resilience against the threat of terrorist attack must work on three different levels – strategic, operational and technical. This essay puts forward a number of concrete recommendations about how this could work in practice.

This essay predicts an optimistic outcome in response to the terrorist threat for the first decade of the new millennium. Terrorist threats can act as a global stimulus on governments and international companies to protect critical public and private infrastructure and the workforce, and this will have secondary strengthening effects against other disruptions and can create a new and unexpected efficiency in risk management with uplifting of profit margins. The business community and national governments must now rise to the challenge.

## The business community as a key strategic target for terrorists

Airline attacks in the late 20th Century caused losses, high insurance and protective security costs. But with this exception, the impact of terrorist attacks prior to 11 September tended to be contained within national boundaries. However, the rapid globalisation of terrorist capability in the 1990s has created forces capable of affecting the balance of world markets. A continued campaign by Al Qaida and other globalised groups would have long-term impacts on markets and a significant influence on global economic performance. Terrorist groups have strategic capabilities for targeting and organisation, although weapons and attack delivery may remain simple. It is as though a rogue global corporation (Al Qaida has been compared to a corporation in its structure and operations) with revenue of millions of dollars is acting outside all national and international laws. There are no regulatory constraints and management has business, chemical engineering, information technology and medical expertise. The rogue corporation

can envisage, plan and carry out simple but devastating forms of attack on critical public and private infrastructure. Corporate fright from these attacks may weaken the global market place. Media transmission of mass casualties around the world can also cause 'public fright' that translates into low levels of confidence in the market, movement of investments into cash and currency fluctuations.

Unpredictable, but economically focused targeting by these globalised groups may now threaten sensitive pillars of the modern economy. Possible targets are transportation (airlines, shipping, railway stations and infrastructure); global financial centres; nuclear power stations, electricity and other utility infrastructure; and buildings symbolic of economic or religious power. Attacks may also focus on command and control facilities within government, such as government buildings, embassies and the defence forces; civil infrastructure, such as telecommunications towers and vital equipment; and computing and information systems.

Economic terrorism is not new. However, the growing threat from CBNRE[2] attacks threatens the viability of cities unless business continuity is practiced in a new and invigorated manner with close co-operation between government and the private sector. Suicide delivery of some extreme attacks by an individual or team poses entirely different problems for prevention and continuity planning. Failures in warning systems and recovery planning could cause long-lasting impacts on the market and global economic performance. The pre-11 September continuity plans in Britain are not an adequate preparation for the severe impacts of CBNRE[2] and the scale of threat from these weapons requires that both the government and the private sector recognise that resources, knowledge and technology are of primary importance for national resilience. The table below outlines examples of some of the types of threats that the business community faces.

Ironically, although many weapons of 'mass destruction' as conventionally understood will be inefficient or intercepted by the



**Table 1**
**Examples of Extreme Threats to Business Operations**

1 **LARGE TONNAGE / MULTIPLE BOMBS:**
4-tonne vehicle bombs; multiple mortars with kilometre range; airplanes into tall buildings

2 **SUICIDE ATTACKS:**
Firearms and explosives attacks on groups at entry to buildings, markets; chemical/biological/radiological materials released in buildings, roads, civic infrastructure and on planes, buses, trains and tunnels.

3 **CHEMICAL/BIOLOGICAL ATTACKS:**
Anthrax, Sarin, VX, ricin, cyanide, smallpox, plague; hazchem tankers.

4 **RADIOLOGICAL:**
Caesium-137, Uranium 235.

5 **CYBER TERRORISM:**
SCADA systems; e-business; public & market confidence.

6 **ATTACKS ON CRITICAL INFRASTRUCTURE:**
Telecommunications, water, power transmission, nuclear reactors, pipelines, buildings, transportation.

authorities, the efforts of Richard Reid, the shoe bomber, showed innovation[1] in the delivery of new weapons of mass destruction – as did the use of planes on 11 September itself.

## Winners and losers in the market

Some business sectors are more vulnerable than others to the globalised terror threat due to conditions inherent within their markets or the nature of their operations.[2/3] Vulnerabilities of some sectors to extreme attacks are summarised in Table 2, which is extracted from unpublished analysis of impacts on 38 sectors from the FTSE Index. The analysis is based on an assessment of a potential sustained campaign by globalised terrorist groups, with consideration of direct attacks on some sectors; responses of corporate fright; public fright after highly visual and shocking attacks; and supply chain consequences. The extract from the 38 sector guide includes recommendations for continuity planning. Sectors with the most serious vulnerability are those directly dependent

on public confidence in the market, for example, banks, retail, property, construction, and leisure. Other losers are sectors directly vulnerable to terrorist attacks, for example, transport, water, oil and gas, chemicals, electricity and gas distribution. Some sectors may fail as a secondary consequence of attacks, for example, insurance, investment companies and pharmaceuticals.

The winners – not shown in the table – are those sectors that are less dependent on public confidence, for example, food and drugs, forestry and paper, mining, tobacco and telecommunications. Some sectors can show increased strength because of changes in demand under sustained attack conditions, for example, IT hardware, media, aerospace and defence.

**Table 2: Losers and Continuity Solutions**[4]

| Business Sectors | Extreme Terrorist Threat Analysis (2002–2010) | Examples of Potential Continuity Solutions |
|---|---|---|
| **Banks** | Reputation sensitivity /direct disruption from extreme cyber attack on systems/ telecommunications loss | Global continuity plans –to be discreet and not publicised, to provide decision making protection of critical personnel |
| | Production and distribution are sensitive to attacks on transportation and utilities. | Alternative providers of telecoms and net banking |
| | | International partnerships and hosting agreements for branches of banks, public information pre-prepared |
| **Chemicals** | Sites and transportation are potential weapons against populations | Two hemisphere locations for back-ups or partnerships to guarantee critical production outputs |
| | Increased regulatory pressures and costs to reduce mass casualty risks | Redundancy planning for changes in transport modes |
| | | Pre-emptive planning with governments on self-regulation arrangements, adoption of on-line risk information and management systems and opening of these to regulatory scrutiny. Closer monitoring of high volume movements or storage that could be extreme weapons |
| **Electricity and Gas Distribution** | Attack sensitive | Government encouragement of household dual systems |
| | | Regional industry planning. Trans-national contracts for increased resource inflow |
| | | Extreme threat analysis and key point protection with public awareness campaigns |
| **Insurance** | Secondary losses from attack liabilities, reputation sensitive globally | Development of new financial instruments for companies as risk financing, reduction in risk transfer practices and support for enhanced internal continuity practices |
| | | Separation of extreme events causation from other loss categories to preserve general insurance market |
| | | Government insurance bonds for catastrophic loss cover, taxation levies on workforce or home insurance to compensate losses for individuals |
| **Oil and Gas** | Attack sensitive | Response as for electricity sector |
| | Loss of assets | Key point protection |
| | Higher production demands balanced by losses and local attacks in some countries at enhanced level | Local awareness. Hardening of workforce capability for response to disruption. Exercising with emergency services of extreme threats and hardening of protection |

As well as a company's sector, a number of other factors influence its ability to survive following a major terrorist attack. These can be termed as 'survival indicators' and are shown in the table below. The survival indicators include controls against terrorism applied by the company itself and some of the independent variables that will affect trading, such as external resourcing, services and human factors. Human factors include the risk appetite of investors, public fright experiences by consumers who modify purchase (e.g. retail) or avoid activities (e.g. leisure, house building). Continuity responses to the independent variables are difficult, examples include significant changes in product, accepting a write-off of some parts of the business, or trading from other countries.

**Table 3: Survival Indicators**

| | |
|---|---|
| 1 | Communications redundancies, trans-national and inter-hemispheric |
| 2 | Protection of decision-makers |
| 3 | Risk financing resources |
| 4 | Protection of critical company infrastructure |
| 5 | Low sensitivity to market confidence |
| 6 | Low dependency on risk transfer |
| 7 | Successful history of risk management |
| 8 | Crisis response capability and CBRNE[2] plans |
| 9 | Tested capability within 'golden hour' of attack |
| 10 | Protection of personnel and families |

## Business continuity planning

Currently, business continuity planning concentrates on relocation to 'hot' (parallel information systems) or 'cold' sites (staffing and data recovery after an attack). This planning is insufficient to fully offset extreme threats that are now foreseeable since 11 September. As John Smith argues elsewhere in this collection, there are limits to the current organisation of these resources and new threats continue to challenge a company's ability to cope in the aftermath of an attack.

Since 11 September a new continuity 'mindset' is required in the boardrooms. The focus of information security personnel needs to be on protection of their lives as well as building distributed networks. Some groups in the workforce, including IT personnel may be located in environments that make them more prone to being casualties of extreme attacks. The location of CEOs and executive directors on top stories of tall buildings, for example, can cause losses – their protection may not be possible in locations such as these, which may be strategic targets for terrorists. The media has differential exposures where persons may be located in soundproof areas for broadcasting or in glass clad structures. In all buildings, physically challenged groups also have special protection requirements.

The issues of compensation for death, injury and loss of assets by the workforce are other factors critical to the continuity of cities and companies. The availability of risk and recovery financing requires close attention by the private sector in consultation with government. A general rule may be that the higher the proportion of risk and recovery financing that is carried internally by the company, the lower the risk of failure under extreme attack conditions. This goes against the commercial practice of encouraging companies to transfer losses to the insurance sector.

Risk financing by government as the 'insurer of last resort' creates challenges to competition but protects critical economic activities. Under sustained and extreme attacks, risk financing by government in the form of compensation may be more efficient in the form of levies on the public and private sector employers or employees. This would balance compensatory payouts with economic functioning. Consideration could be given to pooled funds for recovery of small business. The prioritisation of critical infrastructure recovery and

international financing would need to be considered by the government in association with key trading partners. Pool Re financing has been extended to cover all risks but this arrangement is limited to the commercial sector and to institutions that accept the cover and increased premiums.

### Crisis response

In the next decade, organisations that are able to introduce, within relatively short periods, a strengthened response may end up being the survivors in their sector. Physical assets for delivery of crisis response include a control room to co-ordinate communications and planned operations or a virtual control infrastructure and on-line crisis communications and plans. There are key crisis roles and it is important to appoint, train and exercise these leaders and any number of deputised persons to give cover during crisis operations and recovery. Even within small business, there needs to be a back-up of leadership plus recovery finances and knowledge of survival.

Special technical plans may be required for recovery after or protection against certain types of attack and distribution of information for the protection of workers and their families. The maturing of business operations to implement general risk management can take up to two years of planning, training and testing.

While there is much that companies can do themselves to raise their resilience against an attack, the business community needs the assistance of the government.[5] The operational resilience of British business will require the 'one stop shop' approach recommended by the House of Commons Select Committee on Defence.[6] The strengthening process described above will be more successful if there is an emphasis within national governments on providing a communication point where the private sector's critical recovery requirements can be prioritised and serviced. A 'one stop shop' would activate government assistance, support to local agencies and co-ordinate central government's response.



Strategic resilience can be established through a formal connection between the Cabinet Office as co-ordinator and leaders of industry, which could provide a continuous feed of intelligence to industry on hardening against weapons effects and near real time information on threat assessments. Recovery after any 11 September scale attack would be effective if prioritisation was planned in consultation with industry leaders on a strategic level. This would contribute to rebuilding the most critical parts of the private sector and protect the national economy.

Shelter and evacuation under extreme threats will also significantly enhance survival of the workforce and family members. A key priority is the co-operation between government and the private sector, aimed at minimising losses within the emergency services during response. The loss of emergency service leaders and response teams creates very serious problems for the resumption of normal life and business within city areas. Losses can be minimised by pre-attack exercising and preparedness within the private sector with co-ordination by government. A significant risk to continuity will be self-evacuation by the workforce out of central business districts and relocation by economically mobile high performing personnel to areas that are perceived as safe and outside inner city areas.

Exercising and testing appropriate protection systems, including first aid, can be undertaken regularly and in association with emergency services and local government. Exercising is an option that is psychologically reassuring, creates a readiness for survival and prepares business managers for the massive changes brought about by extreme attacks. Operational resilience requires positive decisions, drills by companies and the public, and proactive measure for the protection of life and business in the 'golden hour' after an attack. After an exercise, businesses understand which critical parts of their operations need to be protected. A policy initiative to establish what can be termed a 'Cities and Regional Resilience Exercise Programme' would bring together the public and private sectors and enhance information sharing.

## Public communication

The question remains as to whether populations should be informed in advance of the possibility of an attack or under emergency broadcast conditions either after an attack or when an attack is imminent. Even basic information can have a dramatic effect on casualties inflicted. Time is an essential element in survival. Immediate decisions have to be made by populations within the 'golden hour' in order to survive. Although spreading additional fear can add to the terrorist threat, the basic question is, can mass populations survive at a higher rate if given pre-attack personal protective information? Chemical/biological and radiological information is rarely produced for public consumption in the UK. In contrast, the US has emphasised chemical/biological risks in recent years and has introduced central co-ordination by the Department of Homeland Security post-11 September to protect the population. Emergency communications to threatened populations require government emergency media preparations with in-the-box visual or broadcast media information. Richard Sambrook's essay has more on this important issue.

## Conclusion

The current outlook for the business community is positive. There is a lot of momentum for a strengthening of resilience and there are concrete recommendations that can be taken up by both the commercial world and national governments that will make their responses more effective to extreme terrorist attacks. Partnership is key to a successful response to the current threat posed by Al Qaida, so business and government must move forward together.

[1] Triton Terrorist Report (Monthly Issues June 2001 to September 2002 of an open source global terrorist incident database), special threat data and media report and the HazMan on-line system concept for risk and crisis response. HMS Ltd., info@hazmansol.com

[2] Sector Watch 2000, Peace in our time?, July 1999 and Herd and Hype, September 1999, co-authored by Dr Sally Leivesley and Teather and Greenwood Limited

[3] The Safety Audit, January and February editions 2002, produced by Dr Sally Leivesley, sally@newrisk.com

[4] Winners and Losers in the Market Place, 2002-2010, Dr Sally Leivesley, Unpublished Research

[5] Consultations with security advisers within the private sector in multinational companies, academic leaders, security and risk consultants, government planners and leading private sector legal advisers.

[6] The United Kingdom Parliament, House of Commons, Defence-Sixth Report, http://www.publications.parliament.uk/pa/cm200102/cmselect/cmdfence

# 5 The Company Response to Emerging Terrorist Threats

John Smith

## Introduction

Commerce is the lifeblood of the United Kingdom. Damage commercial confidence sufficiently and UK plc will grind to a halt, slowly perhaps, but inexorably. The recent corporate collapses in the US have severely affected confidence in the markets across the world and Osama bin Laden might be forgiven for wondering whether he should have continued his business career in order to destroy America. Al Qaida chose a different tactic on 11 September but the real target was the destruction of commerce through fear and chaos. The protection of human life necessarily takes priority at such a time, but strategically the protection of commercial life must run a close second. The business community recognised quickly that the threat evidenced on 11 September changed its world. It must continue to react and adapt to this change in terrorist tactics just as it responds to the ever-changing business environment. Business managers now must think and plan for the unthinkable. Government too must realise that whilst it is the role of business to survive in fiercely competitive market conditions, some active assistance is urgently needed where terrorism is concerned. Given the UK's experience of domestic terrorism over the last 30 years much should already be in place. The threat was always there – it simply has a new face and different tactics – and whilst we look to government for clear guidance, as ever in the commercial world, self-help is the key.

## The business community as a terrorist target

Most politically motivated terrorist groups in the world have learned the value of targeting commerce. The concept is not new, conventional forces have made use of it for centuries. In the hands of terrorists it has taken on a new significance. In the UK, the 1992 St. Mary Axe/Baltic Exchange attack by the Provisional IRA marked a step change; a major, catastrophic attack targeted on a key business area, the City of London. Photographs of the Commercial Union headquarters building appeared on the front page of newspapers worldwide and featured large on the world's TV channels.

So successful was this change of tactics that even serious attacks on security forces and government became almost a sideshow. They were deadly and tragic for those involved and for their families, but usually rated substantially less coverage in the media than the series of attention-grabbing "spectaculars" on commercial and business areas. Suddenly, the targets were no longer simply soldiers and policemen in Northern Ireland or elsewhere. Suddenly the attacks happened in centres of population like London, Manchester and Warrington. Civilians at work and at play felt themselves literally in the firing line. There were some terrible events – probably most notably the bombing of the town centre of Omagh in August 1998 by the 'Real' IRA which resulted in 29 deaths – but overall these attacks caused surprisingly few civilian casualties. The intention was clearly to cause severe disruption to businesses and commercial life. Over the last 30 years and despite the hoaxes and false calls, the emergency services, the utilities and ultimately business and the civilian population have all learned to cope with the telephone bomb warning, the incendiary and the car bomb. The stories of those who experienced attacks became the fodder of the lecture circuits and the terrorists' aim of influencing political thinking was clearly understood by anyone who chose to analyse events.

## The changing threat – and its impact on incident management

This type of terrorism, the "old face", has not gone away. Nationalism still prompts committed individuals around the world to violent action and the one-off pipe bomber or nail bomber will occasionally surface to expurgate some grudge, genuine or otherwise. Yet the world changed for most people on 11 September. There have been previous serious

terrorist attacks on US interests outside mainland US and one previous, largely unsuccessful attack on the World Trade Center, but some had failed to understand that these were attacks on an ideology, rather than attempts to influence political thought. The attacks of 11 September demonstrated clearly that terror, brought through mass civilian casualties, is the aim of the "new" terrorists. There is no longer a political agenda, valid or invalid, with which some parts of some populations could sympathise, as with Irish Nationalism. The aim on 11 September was simply to terrorise, it has not changed since: *"What is coming to the Americans will not, by the will of God, be less than what has come. So beware, America. Get ready. Get prepared."* (Al Qaida spokesman, Sulaiman bu Ghaith, June 2nd, 2002).

Previously bomb warnings, however cynical and flawed, allowed many to escape the worst effects of the explosions in the UK. The negative consequences of mass civilian casualties to a political agenda were well understood. Without a political agenda and with perpetrators prepared to die, the escape of innocent civilians need form no part of the terrorists' planning. Surprise attacks are significantly more difficult to resist, even more so when the attackers are willing to sacrifice their own lives. Military strategists know the value of unexpected attacks carried out by committed forces; in the hands of terrorists embracing martyrdom and seeking mass civilian casualties, the value is significantly enhanced. Careful timing, choice of targets and modern technology enabled – almost forced – a significant proportion of the world's population to watch horrific events unfold in colour and in real time. This factor alone raised awareness of the threat to unprecedented levels and clearly placed business continuity and survival on the boardroom agenda.

The 11 September attacks affected a significant proportion of two of the world's major cities. Future attacks may affect even larger areas of any target city. It is no longer safe to assume, if it ever really was, that an attack will only have a major and lasting effect on an area the size of a couple of football pitches. The damage may deny access to areas of a square mile or far, far more. The possible use by terrorist of chemical, biological, radiological or nuclear (CBRN) weapons takes the issue further still, bringing with it a fear that may affect millions – in itself a potent terrorist weapon. The anthrax letters in the United States received 24-hour news coverage, provoking numerous hoaxes and even more false alarms.

It is now prudent to consider and plan for damage on the geographic and time scales of Chernobyl, Bhopal or Toulouse. A police cordon for 3 or 4 days some 400 metres around the site of a conventional vehicle bomb explosion may be a thing of the past. Successful chemical, biological or radiological attacks may deny access to large segments of cities for significant periods. The "target hardening" techniques advised in the excellent Home Office pamphlet *"Bombs: Protecting People and Property"* may now be insufficient in themselves to cope with post-11 September attacks, even though the "filming" of glass continues to be excellent advice. Sound, well researched, comprehensive and clearly laid out Home Office guidance on dealing with CBRN attacks is now overdue. *"Bombs: Protecting People and Property"* has been updated with advice on dealing with postal devices. It urgently needs significant update and expansion to cover, in one place, the best available advice on the new threats to commerce and to the population at large.

The use of chemical and biological weapons is by no means new, nor is the intention to cause mass civilian casualties, vide the 1995 sarin gas attack on the Tokyo subway system by the apocalyptic sect Aum Shinrikyo. The difference with "new" terrorism is that the world, including the business world, now accepts that the unthinkable can, and may, happen. Prior to 11 September it was difficult for the business community, many of whom hardly remember the Cold War let alone World War II, to conceive that a catastrophic attack on one of the world's greatest commercial symbols could possibly succeed.

Prudent businesses have long had well prepared, practised and exercised "all hazards" plans to deal with major incidents. Key

individuals at every level have been identified and trained in the management of incidents, communication cascades are in place and have been tested regularly, bomb threat and evacuation procedures have been published and practised, and flexible incident management and business continuity plans have been drawn up. Businesses in traditional target areas such as the City of London, West End and the London Docklands have developed these skills even further, liaising closely with the emergency services to understand how they respond to major incidents. They are familiar with the principles detailed in the London Emergency Services Liaison Panel Manual "*Major Incident Procedures"* and may have adopted similar command structures to those used by the police, fire and medical services. Some have taken things still further and have worked directly with the emergency services to hone the incident management skills of both groups. All of this remains relevant and important and has already proved its value for many businesses. The knowledge, techniques and training are transferable, but the "new" characteristics – mass casualties, no warning, suicidal perpetrators, CBRN weapons – mean that prudent businesses have been reviewing their arrangements for business survival very carefully since 11 September.

Before 11 September there was an almost universal assumption that most staff would survive a terrorist attack. The use by terrorists of conventional improvised explosive devices (IEDs) meant that the company manager responsible had simply to decide, often based on distance from an identified or strongly suspected IED, whether to evacuate the building or to keep staff inside and under cover in "shelter areas". If the building was to be evacuated the decision was whether to instruct people to cluster in a pre-ordained location, as for a fire evacuation, or to disperse as far away as possible. Experience indicates that short-term panic and confusion are an inevitable result of terrorist attack but, since 11 September, the situation has become more complex. In a conventional IED explosion people on the upper floors of very tall buildings may conceivably be safer remaining in situ. Post-11 September, when terrorist action is suspected or apparent, building occupants are likely to vote with their feet. The possibility of the use of CBRN weapons in a modern city brings a whole new set of factors into play. Evacuation as a result of a suspected chemical or biological attack may exacerbate the situation by causing major movement of air, increasing and aiding the spread of any air borne contamination. The evacuation of contaminated individuals into the streets and onto public transport may accelerate the dissemination of a chemical or biological weapon more widely than any response system can possibly absorb and the damage may be substantially longer lasting.

## Business continuity

After the St. Mary Axe/Baltic Exchange bomb in 1992 the prudent corporation drew up business continuity plans. These had previously often been heavily weighted towards the recovery of information technology systems in situ. A new industry sprang up to provide "hot" and "warm" sites[1] furnished with basic office furniture, telephones and IT systems to which businesses could decamp should they be denied access to their building. There was an assumption that staff would survive an attack and be available reasonably quickly to return to the office or to move to the temporary warm site facility, not too far from their normal place of work. The main problems revolved around ensuring that the information systems at the warm site were up to date, information and data were accurate, backed up and available when required and plans were kept up to date. Although some "icon targets" like the London Stock Exchange, the BBC at White City or the Vauxhall Cross MI6 building were attacked, most businesses were not the specific targets of the attacks they suffered, they were merely "collateral damage" – in the wrong place at the wrong time. Planning often reflected this. The emergency services reduce their cordon to the minimum as quickly as possible, traffic flow would be re-established and site re-entry could generally be obtained in less than a week unless the damage was particularly severe. Warm site requirements often specified the selection of a location only a few miles from the building being supported. It was considered important that staff could easily get to the site in little more than the time it would normally take for them

to get to work. New York demonstrated that recovery sites in close proximity to the supported building may be affected and therefore be placed out of use. Warm site providers have traditionally found their customer base from the same city, possibly separated by only a few hundred metres. This solution requires reassessment after the World Trade Center. Customers in the same city may all be affected and all require the same service at the same time. The warm site itself may be in the same zone of damage and its use denied. Companies must now consider much more flexible arrangements. Any staff left alive, willing and capable may need to be transported to any one of a number of warm sites, be accommodated and may need their family commitments dealt with. Technology will need significant flexibility to cope. The attacks of 11 September led to the failure of some complex company networks. In contrast, the internet continued to function despite heavy user-traffic, especially to news sites. This survival reflects the internet's origins as a centreless communications system that was developed by the American military in order to survive a failure at any one point. The internet could provide a critical tool if companies are to communicate with customers and staff in the event of a terrorist attack.

Many financial sector businesses have already developed the ability to move their centres of operation onto other continents, rather than just a few miles, on only a few minutes notice.

Business must now think the unthinkable and plan to cope with the loss of a number of staff. In this context plans for staff welfare will need to be particularly robust. The consequences of clustering key staff in the same building in the same city need re-examination. Nowhere is this truer than with the board itself. Until now the protection of the board of any major organisation has centred on well-known, fairly simple principles: board members should not all travel in the same aeroplane, board meetings would require physical protection if held in high-risk locations. Consideration now must be given to the possibility of all board members being in the wrong place at the wrong time. Succession planning has taken on a new significance. It is not helpful to suggest that Board meetings should not take place in London, Paris or New York in view of the possibility of another attack similar to 11 September and it is still not practical to conduct all meetings electronically. The benefits of direct face-to-face contact when planning or agreeing strategy and accountability are immeasurable. Boards should review their succession plans, confirm what needs to be done (and by whom), should they all become casualties and like all business continuity planning, they should exercise for the event. This does require a degree of sanguinity on behalf of existing board members; after all, they may not themselves benefit from their foresight.

## Conclusion

The commercial world can do little to prevent terrorist attacks, but it can and must be prepared to deal with them, as with any other risks to business, when they occur. The establishment of efficient processes to deal with a major incident is no different to the methods used for dealing with any other business problem. As with any project a Board level sponsor and a project director committed to the process are essential, as is the clear identification of responsible and accountable individuals to take it forward and to respond in the event of an attack. These individuals must understand their responsibilities in an emergency and must be trained to respond appropriately. Plans should be reviewed dispassionately in the light of the lessons learned at the World Trade Center and must be rehearsed. Prudent corporations will have all this in place but there must be closer liaison between government and commerce on security matters, especially on the problems posed by "new" terrorism. There is little point in protecting Whitehall if the City of London is devastated. The last few years have seen much more open relationships between some areas of government and the private sector but we have some way to go in the UK before we achieve the free interflow of information between the two sectors enjoyed by some of our allies. The commercial world can and will solve many of the problems without help, but in this area we are all at risk. Not since World War II have the two sectors been so dependent on

each other, possibly some of the lessons learned then may be of value now.

[1] A 'Hot' site is one that can be occupied almost immediately, with IT telecoms etc, running as a 'mirror image' of the systems they are intended to replace. A 'warm' site will probably require up to 24 hours preparation.



# 6 The Role of The Police

David Veness

The new threshold of terrorism threatens to impact upon the public at a level of danger which demands action from both "likely" and "unlikely" counter-terrorists. "Likely" counter-terrorists are mainly state actors. They are the traditional players of counter-terrorism working in intelligence agencies and police forces. These include both nations and assets within nations, such as military and security. They constitute the coalition of countries now allied to combat international terrorism on the new scale. "Unlikely" counter-terrorists are equally important. Post-11 September their role has moved from the wings to centre stage. These unlikely actors are predominantly the potential victims of terrorism. They include business, commerce, and local communities. Their endeavours to prevent and reduce harm are critical to the new counter-terrorism.

The reason that more persons and premises are at risk is the potential scale of the present threat and the terrorist intention to commit mass murder. For the UK this represents a shift from a vehicle bomb, which might devastate a street, to a terrorist attack that impacts upon a neighbourhood or a whole city. Thus people who were less likely to be harmed or effected by past terrorism are now more likely to be damaged and have many more reasons to be part of the defence.

The key word to understanding the new dimension of threat is 'global'. The geographical spread of the groupings linked to Al Qaida ranges from North Africa to Indonesia and the Philippines, spanning South East Asia and including Singapore. Across the line from Marrakech to Manila there is an axis that begins at a north east point in Central Asia and traverses southwest into East Africa and beyond. This near-global range of origins of linked groupings is unique. It also seems likely that

the actual links between these groups and Al Qaida is closer than previously thought. In operational terms, the global origins of the terrorist threat provide global reach and the capability to deliver global impact.

There is also the factor of global intractability. Many terrorist campaigns in the past have involved identifiable root causes accessible to political peace processes. The basic agenda of Al Qaida – including the issues of US presence in the Arabian Peninsula, Palestine, US support for Israel, the suffering of the people of Iraq and oppressive regimes in Muslim nations – is unlikely to be resolved by political means in the foreseeable future. There is the mosaic of aspirations of the groups which were linked to greater or lesser degree with Al Qaida. Put together, resolution via the root cause route, however laudable, remains elusive. There are also no signs that Al Qaida has any intention to negotiate. Rather, the agenda is destructive and riddled with hate.

These global dimensions pose a formidable challenge for counter-terrorism. They included a breadth of possible attack methodologies, from mass casualty assaults against symbolic targets to lesser-scale events, conducted by smaller groupings or even lone individuals. This means that all the traditional terrorist attack methods available to terrorists, such as the gun, the bomb, plus hostage taking and kidnapping remain relevant, but are added to by whatever means the terrorists can acquire and deploy. The stark lesson is that if they can get it and make it work, they will use it to kill people.

Several lines have been crossed since 11 September. They are the intention to cause mass deaths by suicide attackers operating simultaneously against significant targets, without prior notice, but based upon long term preparation and planning. Add to these developments the CBRN dimension. Whatever the connection of Al Qaida to the anthrax attacks in the US in Autumn 2001, the impact was clearly demonstrated and echoed in the caves of Afghanistan as investigators examined the evidence of Al Qaida intentions.



Beyond the global nature of the threat is the reality of its endurance. Future counter-terrorism for both likely and unlikely counter-terrorists needs to be based upon the reality of a long-term challenge.

## Public Defence

The objective of the global war against terrorism is now clear. It is the elimination of terrorism carried out by terrorists with global reach and able to achieve devastating impact as a force in international affairs; It is not the defeat of all terrorism. Global reach terrorism comprises the Al Qaida network, the terrorist groups associated with it and small groups who pursue the same agenda. The hallmark of this collective threat is the determination to cause spectacular impact and public harm.

It remains the role of law enforcement to combat all forms of terrorism. However, at the "war aim" level counter-terrorist endeavour is now a grand alliance, based upon political will, military action, diplomacy, intelligence and financial investigation. The grand alliance has already achieved results: there is a new government in Afghanistan; the logistical base of Al Qaida has been reduced; actual attacks have been disrupted; counter-terrorism has been reinforced in many nations; crisis management has advanced and new laws and policies have been introduced.

In the UK recognition of the need for long-term activity is materialising in the form of policies and resources. There is recognition that future results require action now and that plans are needed for the years ahead. As Dr. Leivesley highlighted earlier in this collection, effective crisis management plans take two years to realise within individual companies. After the frenetic activity of the first months there is also a move towards strategic thinking and more dynamic and proactive endeavour. Underpinning these efforts to reduce threat are harsh realities that will impact on the threat levels for the UK, such as the inextricable alignment between the UK and the US, the certainty of harm to UK citizens abroad (and at home), the pursuit of the "axis of evil" and the "sixty country problem" as described by George Tenet.

Both the UK and the US are obvious members of the sixty countries at risk.

For the police service, the future needs to be based upon the recognition that there are now two roles to perform. The first is the traditional crime-fighting duty of combating street crime, burglary, vehicle crime and other menaces to peaceful life. The new role is professional commitment to internal security. It is unprofessional to move officers back and forth between conventional crime fighting and internal security. This results in both being performed, at best, less effectively than they should be and, at worst, poorly. The new twin roles of the police service create new demands for longer-term resourcing. It is critical that sustained investment is made in long-term intelligence-led counter-terrorism. It is wiser to employ one expert to detect a terrorist before an attack than to employ twenty patrolling officers to combat an unknown attacker.

However, intelligence concerning a global terrorist alliance is a formidable challenge and threats will emerge where precise information is elusive. Attacks will happen.

The need for enhanced dedicated activity within the police service reflects the shift in understanding as to the nature of the threat. As regards the menace to the UK, this will persist – at least at the present level of danger – for the foreseeable future. Preparation, prevention, proactive operations, post-event activity and community involvement all require energy at new levels.

## Public/Private Partnership

The scale of the threat and its likely endurance for many years to come, alongside the limitations of the public response, make team endeavour vital. It is critical that all the energisers of modern society, both the likely and unlikely counter-terrorists are harnessed; the public sector acting alone will not be able to offer a comprehensive solution.



Economic targeting seems to be a persistent thread for international terrorism. Private economic activity must therefore be part of the defence and mitigation strategy. Corporate responsibility and citizenship acquires a new clarity of purpose. In business terms, this means that security should now become a main board issue and should not be delegated to security specialists, striving in isolation. The appropriate defence mechanisms already exist. They now need to be elevated to match the challenge. Prevention, 'good-housekeeping' security, business continuity and disaster recovery provide the framework.

How might these useful beginnings be further developed? Executive master-classes are being developed that explore the new face of terrorism can be understood and look for ways of integrating this understanding into commercial practice. These sessions also help to sustain a new level of partnership activity within and between public and private sectors. The public sector can contribute unique knowledge and the private sector can focus this information into relevant and sustainable defences. International exchanges are also critical. The UK has emerged from thirty years of combating conventional terrorism with a sophisticated system of translating intelligence into threat levels and threat levels into warnings that are understood by the public and lead to useful public-spirited actions. The US, with less experience of homeland terrorism, can learn from this expertise and indeed transatlantic discussion continues on this subject.

The case for enhanced information exchange before, during and after events is clear and provides a genuine opportunity to reduce risks and consequences.

The response of financial institutions has already provided a highly creditable example of corporate citizenship. Such entities are commonly situated in the city centre locations in buildings which are often symbols of economic power and are employers of large numbers of staff. But as well as being potential victims they are also important

defenders. These organisations are tackling their risks through security strategies that look outside the office as well as inside and engender links with neighbouring properties, especially in multi-occupancy buildings.

## What Next?

There is a great deal of valuable prevention activity already underway to protect the most essential aspects of national life. This work has expanded dramatically in recent months and has been advanced by provisions of the Anti-Terrorist, Crime & Security Act of 2001. However, the task of broader social preservation and recovery is greater. New York provides the classic example of the diverse talents and resources needed to restore normality out of chaos.

Business, commerce and community can provide an enormous contribution but require a structure within which these efforts can be channelled and co-ordinated. The reinforcement of counter-terrorism that will be necessary in times of heightened menace or after an attack provides an example.

The UK does not have a national guard, a gendarme or a third force, but there are resources that can fill this gap. Police Community Support Officers will be deployed for the first time in Autumn 2002. Special Constables provide a vital means of sustaining local policing while regular officers perform other duties. The role of the volunteer reserves of the armed forces is being actively debated and promises to develop with up to 6,000 individuals available to respond to specific crises. This will be based upon enhanced linkages between military organisations at the brigade level and local emergency services.

The private security industry has considerable assets already deployed in relevant places and the leaders of this sector have displayed significant social responsibility in the debate as to how teamwork can be made more systematic and focused. There is a clear opportunity for public policing to brief private security on the new era of threat and response. There are practical outcomes that this process will deliver which have not yet been exploited.

Overall, the business sector is a powerful medium by which the education and awareness of staff can be developed. The desirable outcome is greater awareness rather than public paranoia. The phrase "alert not alarm" which originates from business leaders elegantly describes the way ahead.

The over-arching framework of government leadership, emergency service commitments and productive public/private debate that will advance this agenda is not yet fully formed, but the foundations are evident. What is required now is to combine these actors in a 'seamless' front that recognises that prevention and consequence management are now inextricable and linked components of a revised order of social protection. This is inevitable but success will depend on the extent to which those involved are prepared to take risks in respect to info-sharing and to combat complacency head-on.

## Conclusion

The scale, breadth and longevity of the present and future danger means that no one actor has the answer.

London, for example, has determined a policing priority to increase the security of the capital against terrorism. This priority is informed by two objectives: the first to prevent and disrupt terrorist activity; the second to achieve an effective response to suspected and actual terrorist incidents. In common with all other actors in counter-terrorism the official public services will not achieve these objectives by operating alone. In the months and years ahead, continuing combined endeavour by all actors within society will be essential to mitigate the murderous intentions of new-era terrorism. It is wholly unacceptable to wait for the next attack before such measures are vigorously pursued.

# 7 Overcoming the Threat: Public-private partnership

Bruce George MP and Natalie Whatford

Terrorism has a long and ignoble history that can be traced back at least to the *Sicarii* of ancient Palestine (although it has been argued that modern terrorism derives from the latter years of the eighteenth century). London and some provincial cities were subjected to terrorist bombings 130 years ago. For the last three decades or so the UK has had to deal with terrorist organisations and incidents largely linked to Northern Ireland. There have of course been other terrorist organisations, both indigenous to the UK and from abroad, that have targeted the UK or used the country as a base for their activities and campaigns elsewhere. The Terrorism Act 2000 proscribed 35 organisations operating in the UK deemed to have been linked to both international and national terrorist organisations 'concerned in terrorism, committing acts of terrorism or promoting and encouraging terrorism'. The Anti-Terrorism Crime and Security Act 2001 strengthened the existing legislation.

The attacks of 11 September exacerbated an already deteriorating financial and industrial downturn in the world economy. It has been estimated that Al Qaida spent around half a million dollars to mount the operation. The Milken Institute calculated that the cost directly attributable to the outrage was in excess of $100 billion, including life insurance, damage to property and the loss of production. The cost of damage to property alone was estimated at between $9 and $13 billion.[1] Helminger has added that the cost so far for the 'War on Afghanistan' and the 'War against Terrorism' stands at $1 billion per month. The economic costs, loss of life, consequences for the national and global economies and additional security in protecting both economic and military infrastructure can only be estimated at this stage.



This essay will focus on the impact of the events of 11 September on industry and commerce, mainly in the UK. It will show how and why companies are at risk but will present evidence that many companies are not taking their risks seriously. We will look in detail at two key infrastructures – the nuclear industry and the financial sector and will put forward a number of recommendations about how business and government can work together more effectively to tackle the threat together.

## The Threat and Vulnerabilities

Government, military, police and security establishments and personnel are not the only likely targets of terrorism. Indeed, published research in the US and UK reveals a greater likelihood of commercial premises or establishments within the private sector being targeted. This reflects the fact that much of what is called 'critical national infrastructure' is actually in private ownership. The privatisation programmes of the Conservative Governments 1979-1997 were continued under the present Labour administration. The Ministry of Defence counts a number of commercial premises among 160 'key points' – sites where security is essential to the 'ability of the country and the armed forces'[2] to conduct military operations. There is a further list of economic 'key points' where the prime responsibility for protection rests with the security service. However it should be pointed out that, in the event of a crisis, responsibility for protecting industrial and commercial premises and personnel would fall upon the companies themselves.

Furthermore, business is a strategic target in its own right. As Roger Davies says in this collection, the Al Qaida network recognises "the significance of these targets and the impact that their disruption would cause around the world". Why should commerce and industry feel vulnerable? Paul Wilkinson in his seminal study written before 11 September pointed to its vulnerabilities.[3] More recently, in the US Department of State's 'Patterns of Global Terrorism 2001' published in May 2002, it was identified that 'business' was by far and away the biggest target for terrorists in 2001, with '397 of the 531 facilities struck categorised as 'business''.[4]

In his report to the NATO Parliamentary Assembly entitled 'The Economic Consequences of 11 September and the Economic Dimension of Anti-Terrorism', Paul Helminger reiterated the threat to the business community and the consequences of the vulnerability of the national and global economy.[5] He also warned of the need for most large corporations to reconsider their internal security strategies and predicted that these additional measures would result in new and unanticipated costs to their balance sheets.

While certain companies and sectors are more attractive targets for terrorists, what is striking is the spread of impact. Dean and Yonah Alexander, writing a few months after 11 September, identified the US companies that had been targeted overseas, showing that nearly every type of business sector had been affected:

> 'Corporate America suffered severe initial damage to particular businesses, such as airlines, tourism, hospitality and insurance. Other sectors that witnessed some slump – in certain regions – were real estate, energy technology, media and entertainment and private and public mail carrier firms. Additional industries – transportation, retail, financial services, automotive, health services, pharmaceuticals and biotechnology – were impacted by the terrorist incidents in varying degrees.'[6]

This list of vulnerable commercial sites can more or less be replicated in the UK. The financial sector, nuclear installations, transportation, energy, the chemical industry, pharmaceutical industry, parts of the communications industry and information technology, the venues of major sporting events, ports and harbours, aviation and aerospace including airports and airlines, and the water industry amongst others have all been recognised as being potential targets. However, who can tell with any degree of accuracy what targets will be chosen by international terrorists? Frankly, who would have thought that terrorists would have chosen to destroy a small nightclub in Bali?



## The Response

Despite the scale of the threat, it is truly amazing how many vulnerable enterprises do not appear to have been taking the risk more seriously. A recent study of 5,000 companies revealed that only 45 per cent had business continuity plans (or consequence management plans) in place.[7] Provisional research carried out during the preparation of this piece also shows that the response of commerce and industry had been mixed. Some sectors and companies are treating the increased threat very seriously; particularly those mentioned above, yet many have decided either rationally or out of indifference that little needs to be done.

What factors influence the level of preparedness of a company? Those companies most likely to be taking the threat seriously are those who are designated as high risk. As a result these are the companies that tend to have competent security and risk managers or advisors reporting to their boards, who are aware of the consequences of not taking security and the threat very seriously and have a strong sense of duty of care to their employees. In particular, companies that have in the past been victims of acts of terrorism will be highly attuned to the need for high security budgets. American companies are also more likely to be taking the threat particularly seriously, due to the fact that Al Qaida has identified them as legitimate targets. Lastly, enterprises that are subject to international regulation, such as the nuclear industry discussed below, are most likely to be responding positively to the greatly increased threat from Al Qaida and other international terrorist organisations related to it and to domestic terrorism.

Why might other companies not be taking security seriously? Some might believe they are not inviting targets for Al Qaida, or break away groups of the IRA. Others might be perfectly happy with their security arrangements. Some may believe that, should the unlikely happen, their insurance will take care of the problem. Others place their faith in the role of the military and intelligence services to keep the threat away from them. Others who own premises away from London in other

major cities or in high-target sites feel that geography provides the best form of security.

The authors have anecdotal evidence of companies expending more on security equipment and personnel – although much activity followed immediately after 11 September and may not have persisted – and overall security spending has increased. There is contradictory evidence from the United States. In a recent survey of the international membership of the American Society for Industrial Security (ASIS) about half of respondents reported that their security budgets were up by at least 70% since the 11 September terrorist attacks. Yet, at the recent ASIS 48th Annual Seminar and Exhibits, one of the speakers put the figure considerably lower.

## The Nuclear Industry

The nuclear industry is, for a number of reasons, a critical focus of counter-terrorism efforts. Since 11 September, there has been a radical revision of the idea that terrorists could not conceivably undertake 'nuclear terrorism' – few now doubt this ability and willingness. But in addition the nuclear industry provides a critical case study in how 'unlikely' counter-terrorists can work alongside the government, as this critical infrastructure is owned both by private and public organisations.

The consequences of a successful terrorist attack on a nuclear installation could be potentially catastrophic, not only to the workforce but also to those over a much wider geographical area, national boundaries. In his evidence to the House of Commons Defence Select Committee, Gordon Thompson wrote 'a civilian nuclear facility is a potential radiological weapon'. If a nuclear reactor were to be successfully targeted then significant quantities of radioactive material would be released into the environment. The reprocessing plants at Sellafield in the UK and Cap de la Hague in France have the largest inventories of radioactive material in Europe and could thus be seen as potential terrorist targets. Material in transit, including nuclear weapons, has long been identified as a potential hazard along with the danger of theft of fissile materials and nuclear sabotage.

### *The National Regulatory Environment*

The regulation of the nuclear industry in the UK involves a number of agencies including a civil regulator who is part of the DTI's Office of Civil Nuclear Security, the Nuclear Installations Inspectorate. In the UK it is the DTI that ensures, through national law and regulation, that civil nuclear facilities and material meet international regulations. The legal and regulatory framework for nuclear power stations is contained in the Nuclear Generating Station (Security) Regulations 1996. The DTI is currently undertaking a consultation that will help in enhancing the security of the Civil Nuclear Industry. Within this sector are companies such as BNFL, the UK Atomic Energy Authority, British Energy and URENCO. Listing the legislation and regulations relating to nuclear security including the transportation of radioactive materials would exhaust the reader.

Protecting the above companies and their sites is undertaken by the Atomic Energy Police and private security, both of which are in-house contracts. In the defence sector it is undertaken by Ministry of Defence Police, The Home Department Police Forces and the Security Services play a significant role. As George & Gearson wrote 'it is clear that the British system benefits from the close relationship, through the regulator between the intelligence and security community on the one hand and the civil nuclear industry on the other. It enables the industry indirectly to obtain the latest high level of security necessary to make the right decisions in responding to the threats.'[8]

### *The International Regulatory Environment*

Even before 11 September and particularly following the collapse of the Soviet Union, there were a great many measures to attempt to prohibit nuclear proliferation and enhance the security of nuclear installations throughout the world. Under the Non Proliferation Treaty, the Non-Nuclear Weapons States undertake not to acquire nuclear

weapons and must adhere to the international Atomic Energy Authority (IAEA) safeguards. The IAEA was established as an autonomous organisation under the United Nations in 1957. Various legal documents have been agreed to such as the Convention for the Physical Protection of Nuclear Material that was passed in 1987 to which the UK is a party and the Convention on Nuclear Safety in 1996, along with the Joint Convention on the Safety of Spent Fuel Management and Safety of Radioactive Waste Management, which entered into force in 2001. Currently the IAEA is examining further measures to strengthen international conventions and guidelines relating to the physical protection of nuclear and radioactive materials and nuclear facilities. It must be stressed however, that important though the IAEA is, it offers advice to national governments. It is not obligatory.

### The Financial Sector

11 September highlighted the fact that the financial sector remains an important target for terrorists. While public-private partnerships in relation to traditional critical infrastructures such as the nuclear industry continue to develop, much more needs to be done to foster these types of links within the business community as a whole.

Like most of the business community, the main security issues that face the financial sector range from the need to protect its staff and customers, to its assets and reputation. In aggregate, the destruction of a nation's financial heartland would have devastating consequences for the national and international economy. Crime appears in all forms and guises, from fraud, armed robbery and increasingly from the ultimate crime-the threat of terrorism. It is to the fore in risk management, security, business continuity and resilience. The banking industry, for example, has done much through a proactive management of the security risks and the identification and application of control systems through the establishment of a group to deal with major (terrorist) incidents – the Major Incident Group. Liaison with law enforcement bodies along with seeking advice and guidance through security incident collation, the monitoring of criminal trends, intelligence dissemination and the promotion of awareness of security issues, have all been of importance. A key reference text known as the 'The Incident Document' was written to deal with the scope, planning, monitoring and risks that companies face, as well as the banks' response to such events. A Major Incident Group Framework (MIGF) forms the general structure together with an Incident Liaison Committee (ILC). The ILC was set up in the immediate aftermath of the terrorist attacks on the World Trade Center. Running in tandem are business Recovery Plans that are supported by a Business Contingency Unit, a Business Continuity Unit and a Property Contingency Unit. When trying to manage the risk, there are on-call arrangements in place, together with operational decisions and the management of information that are made by ILC in the event of an incident. Today there is regular communication and the dissemination of key facts between the various companies and the ILC. This highlights the continued seriousness with which the financial industry is taking the issue of terrorism.

The financial sector is largely regulated at national level. One might assume that the commercial sector was taking the necessary precautions, which would include updating its business continuity/ resilience plans and examining where enhanced security was appropriate to meet the increased threat including target hardening, strengthening building structures, an increased security budget including greater use of CCTV, an increased use of numbers and higher quality of security personnel and closer collaboration.

We feel that there is a need to enhance security within both large and small companies. You cannot isolate enhancing security at commercial establishments from organisations that inter-relate with them. There is a network of relationships that comes out of personal links. Links can be made both individually and collectively with the police intelligence and if they are lucky with the security services, the emergency services and the Civil Contingency Secretariat. We can also identify further, that at a local level there are both formal and informal links between the government, the military and emergency planning.

Security companies need to have good links with risk management and business continuity resilience. Companies should have reviewed the areas of security that we have mentioned earlier in the light of 11 September. Physical security, such as building security and their business continuity plans should now be a reflection of the possible risks they face. It seems that companies should look carefully at the quantity and quality of the personnel that they employ and not resort to employing the cheapest that is available along with ensuring that their personnel are well trained and properly motivated. The hirers of security have a strong case for an increased budget. Nevertheless it is no good just writing a blank cheque – increased resources have to be both wisely purchased and used.

There is also a need for more clarity in the deliverance of the government's intelligence information. Security managers frequently criticise intelligence, yet it should be said that they have access to relatively low-level intelligence which undoubtedly has an impact on their work. Managers of large enterprises with senior police or intelligence background might be aware of intelligence that is unavailable to others. The government needs to look carefully at whether access to intelligence could be deepened and widened, and delivered in a more systematic way. The Metropolitan Police area and the City of London are exemplary in terms of the good relations which exist and are developing between the business community and the police. It has been David Veness, Assistant Commissioner for Specialist Operations at the Met, who brought the two together. However, it is far from certain whether this closeness exists in all police authority areas.

## The Insurance Sector

The insurance industry is also critical in 'counter-terrorism'. The insurance sector has a self-interest in influencing those seeking insurance cover to improve their security in light of terrorist threats. The UK's market-based insurance structure is better placed to play this role than others, for example the French state-run structure.



Yet the insurance industry must ensure that it too is adequately protected against the effects of a major terrorist attack. Estimates of the cost of the 11 September attacks to the insurance industry worldwide range from $32 to $58 billion. The industry initially increased premiums to cover the high payouts, although these now seem to be returning to earlier levels. The deeper problem is that some insurance companies have withdrawn their cover in relation to acts of terrorism. This has led to the establishment of an industry-wide solution. 'Pool Re' is a government-backed insurance policy against terrorist incidents impacting on commercial properties. In the event of a large payout, individual insurers pay the first £100,000 of a claim, the rest is covered by Pool Re. The nuclear industry, due to the particular risks faced, has a dedicated Pool Re Nuclear in place.

## Conclusions and Recommendations

In this chapter we have chosen to focus upon the threat to and the response of commerce and industry. There is a critical need for a greater awareness on the part of some sectors of commerce and industry of their increasing vulnerabilities and of the importance of responding appropriately and in a measured way.

However, one cannot see these sectors in isolation from what is being done by the Government, be it central, regional or local, the emergency services, the health system, the police service, intelligence services, the private security industry or the security profession, many who are engaged in the purchase of security services. The Building Research Establishment has recommended that the Government should fund at a higher level. In our view, universities and other research establishments need to take a greater interest in the threat from terrorism. The architectural profession and planners ought to take into consideration the designs of their tall buildings in order to safeguard them from any terrorist attacks.

The private security industry at long last is going to be regulated. However, the process will not be swift and, as the House of Commons

Defence Committee recommended in its report, a regulated industry would indeed be beneficial to all. Statutory regulation of the private security industry and the security profession as a whole should contribute to a greater professionalism.[9]

This chapter was written with the aid of the sources listed below and interviews with 20 Heads of Security in the UK.

The authors would like to thank Mark Button, Senior Lecturer at the University of Portsmouth.

1 The Milken Institute website address www.milkeninstitute.org

2 House of Commons Defence Committee (2002) op., p 23

3 *Wilkinson, op cit,* Paul Wilkinson 'Terrorism versus Democracy: The Liberal State Response' (2000) (London: Frank Cass)

4 'Patterns of Global Terrorism 2001' United States Department of State May 2002

5 A Report for the NATO Parliamentary Assembly on 'The Economic Consequences of 11 September and the Economic Dimension of Anti-Terrorism' By Paul Helminger April 2002 can be found at http://www.nato-pa.int

6 'Terrorism and Business: The Impact of 11 September, 2001' By Dean C. Alexander and Yonah Alexander pp193.

7 House of Commons Defence Committee (2002) op., p 39

8 ibid

9 'Understanding the Private Security Industry Act 2001' By Bruce George and Mark Button



# 8 Broadcasting Threats: The media and transmission of risk

Richard Sambrook

The world changed on 11 September. The violation of so many lives in such horrific and shocking circumstances could never allow a return to the old assumptions and shorthand we used to explain the world and which suddenly felt outdated. Developing an understanding of these changes, and the responsibilities that go with them, is at the heart of the media's role in the post-11 September world.

Today's broadcasting environment presents people with a staggering amount of choice. The connected consumer has access to hundreds of television channels, even more options on radio and, of course, the vast ocean of unregulated information and streamed broadcasting that is the internet. This presents the public with great choice but also the problem of choosing. Following the events in New York and Washington on 11 September, who should they choose to guide them through the unfolding events?

The simple answer is they will choose who they trust. Whoever they trust to be first with information, to be accurate, to understand their fears and explain the facts most clearly. They will turn to a source with which they can identify.

In the UK that day, viewers placed their trust in all the main broadcasters but turned in their largest numbers to the BBC. Around half of those switching on television turned to BBC One, which was broadcasting the coverage of news channel BBC News 24. The story was similar on radio, and around four-out-of-ten people using the internet went to the BBC News website.

So why should they trust the BBC, or ITV for that matter, over the hundreds of other alternative sources of information?

Public trust in any broadcaster would have been seriously eroded on 11 September, had they not been on air quickly with serious, informed coverage of what was happening in America. That's why Sky, the BBC and ITN all make the investment in 24-hour news channels. They are not created for the few, they are a reflection of the way modern society consumes news. People today are busier, choosier and less inclined to wait for news – or anything else for that matter. Trust between a public service broadcaster and the audience rests on being there when they need you. And if the judgements you make don't reinforce that trust, they will find someone else to tell them what is happening.

It's not just about television either. As the catastrophe of 11 September unfolded, a large proportion of the UK population were at work – not just in offices but also on the road, on the street, or, for whatever reason, not near a television. That's why it's vital to make news available however it suits the audience, whether it's by investing in online services, radio news or emerging platforms such as mobile phones or other mobile devices. Allowing the audience to choose you as a source of news from an ever-expanding menu of options is crucial to retaining their trust.

The explosion of news services has swept away notions of special broadcast arrangements for civil emergencies that were developed during the Cold War. It's a reasonable assumption that, by the time broadcaster and government might have negotiated the terms of a special broadcast, many others would already be on the air or on the web.

Nor is the relationship based exclusively on us, the media, telling them, the audience, what's going on. The internet has turned what was a one-way process, with the broadcasters informing the public of events, into a two-way connection. Media organisations are no longer the gatekeepers of information and have to be more responsive to events and their audiences. BBC News Online alone received more than 35,000 emails on 11 September – many from survivors and witnesses. By reading their stories and posting them on our site, we began the process of understanding the impact of the attacks and created a gathering point for a shocked world.

Any organisation, public or private, caught up in a terrorist act needs to understand the reality of this rich, volatile information environment. Credibility depends on openness and transparency. The penalty for ignoring the demands of media in these circumstances, however onerous they may be, is to lose credibility and the confidence of the public.

This has some basic implications for relations between the media and the authorities or companies caught up in a terrorist act. First, there is the need for fast and accurate information. If something is not known or unclear, we should say so. What the public need at such time are basic, reliable facts and somewhere to go for more if they believe friends, colleagues or relatives might be involved.

Often organisations involved in a catastrophe believe withholding information is a means of retaining control. This is mistaken. It erodes public trust and confidence in how the situation is being handled. There must be good reason for withholding information – perhaps notifying relatives, or ensuring an investigation is not compromised – but always with the assurance there will be full transparency and frankness in due course.

And in the immediate minutes and hours after an event, the media can be a conduit in the other direction – appealing for help, or information which may prove valuable.

This can take a wide variety of forms, from basic practical information such as an emergency phone line number, to notifying the public of

how to minimise resulting disruption to their everyday lives – for example through traffic and transport warnings. This all helps take the pressure off the emergency services. In the case of dangers to public health, such as through contaminated water or air, the authorities need to use the media to advise the public of what safety measures they should adopt. Giving communities this kind of vital information is a central part of our public service remit. And the media may often help with the arrest of those responsible for incidents – the man who planted the bombs in Soho, Brixton and Brick Lane was caught within a fortnight of the first explosion after a work colleague recognised him from CCTV footage which had been widely broadcast.

Sir Michael Bishop, who ran the airline British Midland at the time of the Kegworth crash in 1989, is rightly held up as the best example of leadership in the face of disaster. By visiting the scene promptly and speaking openly and sympathetically he did much to maintain public confidence in the company. There are many examples of others who failed to follow his example to their cost.

Well-run organisations should have already prepared crisis management contingency plans, which reflect the need to inform the public by providing maximum access and reliable information to journalists as soon as it is available. Some organisations in the past have been found to have kept quiet on embarrassing details, to have misled the press and public about the extent of a crisis or to have frustrated the legitimate attempts of journalists to find out what has been going on. Many have suffered a disastrous sullying of their public image as a result, in some cases never recovering.

News judgements about how much information to broadcast can be far from clear-cut. The anthrax outbreak in America and the scares it prompted here created acute dilemmas for broadcasters. The extreme fears created by bio-terrorism pose one of the greatest tests of the media's ability to strike a balance between the need to constantly update people about a fast-moving story without causing undue alarm.



There were hoaxes and scares caused by caster sugar but beneath it all a very real sense of fear among a population still coming to terms with events of a few weeks earlier.

How should we maintain our connection and the trust with our audiences who undoubtedly feel threatened? Over-play the story and face accusations of scare mongering; report too little and risk eroding the trust among those who may feel they are being kept in the dark. Achieving consensus on the risk is notoriously difficult and the public are often left bewildered by competing claims and a culture of disputation. For instance, when a second contaminated letter was sent to Senator Patrick Leahy, it was said by investigators to have contained enough highly refined anthrax to kill 10,000 people. Compare this view with that of Red Thomas, a retired army officer from Arizona, who wrote what became the definitive article attacking overblown fears about anthrax. The only way, he said, for one letter to kill 10,000 people would be "to find 10,000 volunteers to line up and lay down on a big metal table while a doctor stuck a tube down into the lungs and blew the anthrax in there, and then we'd get all 10,000 of them and fly them to Pango Pango so they could avoid any medical intervention, and then yes, we could kill 10,000 people." Both views are true to some extent but who should the anxious audience believe?

Again, trust is key. The BBC took a policy of not reporting the dozens of anthrax hoaxes as our judgement was that there was no hard evidence that the attacks had spread beyond the US. Had that judgement been wrong, we would have lost much credibility. Sometimes it's a very fine call.

Of course there's a difference between our responsibilities as a part of the media and those of the organisation directly involved in an incident. We expect that organisation to put as much information as possible into the public domain. Our task is to make a selection from that information to best inform our audiences. It is not in our power to keep information secret, unlike the organisation involved. Others can, and

often do, report what we decide not to. We simply have to fulfil our duty of passing on to people what we consider to be the most accurate and reliable picture of events.

For broadcasters, the threat to impartiality is never greater than when nations feel threatened. The BBC's media correspondent Nick Higham, writing in the British Journalism Review, described what many observed in the American media as the "war on terrorism" gathered pace: "However much American journalists may value fair and impartial reporting and the separation of news and comment, there is bias in the US news media, and never more so than when the nation thinks itself at war. It's a bias in favour of patriotism."

This point is echoed by a New York Times critic who wrote: "After two months, American television's cautious approach [to covering the war] has turned into a knee-jerk pandering to the public, reflecting a mood of patriotism rather than informing viewers of the complex, sometimes harsh realities they need to know." It's significant that CNN, normally seen as coming into its own at times of conflict, was said by some to have "lost" this war by being overly patriotic in its coverage and giving viewers what it thought they wanted rather than some of those harsh realities.

Broadcasters and newspapers in the UK were also facing the same pressures to act "in the national interest" which could have compromised the impartiality of the journalism. The Sun and Mirror newspapers fought their own war of sorts, with the latter regularly questioning the war aims and outcomes, while The Sun stood shoulder-to-shoulder with Blair and Bush, caustically attacking everyone and anyone who showed signs of "wobble".

In this atmosphere, to maintain the trust of audiences, broadcasters must be willing to ensure they retain visible independence and impartiality.

The media has to protect its right to reflect all sides of any debate without failing to listen to those who have genuine concerns or



complaints about our reporting. So when Downing Street called together the heads of BBC News, Sky News and ITN to discuss our coverage in the wake of 11 September, we all went willingly. There was a perfectly proper exchange of views about the media's responsibility in reporting the crisis. However, given public comment around the world, it was important to assert that the broadcasters retained the right to decide what they broadcast. The politicisation of information is corrosive – and the public distrust it. In addition, the media have a legitimate role in holding to account those with public responsibility. So in times of crisis the media have to ensure an arm's length relationship with those immediately caught up in events. The media's role and responsibility is not the same as the government's or of any other organisation in the centre of the storm – and never can be.

An essential part of the commitment to being an impartial source of news is creating a forum where minority views can be heard. While public service broadcasters should in times of crisis provide focal points for the majority, they must also seek out the voices of those whose views are not shared by the majority, even if that invites criticism. In the period following 11 September, it was sometimes difficult to broadcast dissenting voices without yourself becoming the target for attack. But seeking out the thoughts of the UK's diverse population and the wider international community in the weeks and months which followed was absolutely the right thing to do and presenting those views fairly and honestly was fundamental to the role of the media in defending democracy.

During the IRA bombing campaign in the 1980's the Conservative government sought to prevent Irish republican views being broadcast by banning them. It didn't work and may arguably have been counterproductive. Reporting Muslim opinion in the UK in the wake of 11 September also highlighted the need to avoid treating ethnic or religious minorities as homogenous groups and to recognise, no matter how inconvenient in preparing a two-minute news report, that there's unlikely to be a single point of view.

The honest reflection of views may be a cornerstone of impartial reporting but it does not mean anything goes. As well as a responsibility to be honest and open with our audiences, we have to be sensitive to what they are feeling. Take, for example, the special edition of BBC One's Question Time, broadcast two days after the attacks on New York and Washington. The panel was chosen to reflect a range of views, as was the audience. But as the live programme got underway, it became clear that the handful of Muslims in the audience were going to be highly vocal and uncompromising in their criticism of America. There was a huge wave of protest from viewers who besieged the BBC switchboard for days afterwards. While the views expressed on the programme were all valid – and were soon being debated across the media – we had to admit we'd got the timing wrong.

Confronted with a new threat, new fears and a lot of confusion, I believe the media has a responsibility to be a trusted guide through a difficult and complicated story, to separate fact from fiction, science from hearsay, and to shine a light fully on the issues raised. The withholding of information needs a clear and tangible justification – and the assumption must be in favour of full transparency.

It is not the media's job to scare the public, nor should we be in the business of underplaying danger for fear of alarming people. And whatever we decide to broadcast we do so in the knowledge there are thousands of other sources of information out there against whom we are judged.

The truth is, if our audiences trust us they are smart enough – given straight facts – to make up their own minds about levels of risk.



# 9 Tackling the Sources of Conflict: What can companies do?

John Bray

Writing soon after 11 September, the American writer Francis Fukuyama pointed out that the terrorist attacks had led to a rapid re-evaluation of the role of the state. Earlier, there had been much discussion about the declining importance of national governments in an era of globalisation. Many argued that major international companies were now more powerful than governments; Wall Street whiz kids briefly saw themselves as masters of the universe. However, as Fukuyama pointed out, 11 September sharply demonstrated the limits of corporate power:

> The weightlessness of the new economy will not protect you from falling concrete; your only hope in this kind of crisis is the heroism of fire fighters and policemen... Microsoft or Goldman Sachs will not send aircraft carriers and F16s to the Gulf to track down Osama bin Laden; only the military will.[1]

Equally, governments acting on their own have a limited capacity to address the deeper sources of terrorism. 11 September has shown how the political and economic failure of states such as Afghanistan can help spawn violence far beyond their borders. Both in Asia and Africa there are many examples of weak states with a high potential for political violence and institutional collapse. It will be difficult to prevent further destabilisation without economic development, and this typically requires the participation of private companies.

Companies cannot replace governments in the struggle against terrorism, but they can play an important complementary role. This

essay argues that companies can make two prime contributions:

> First, they can manage security risks to minimise the impact of terrorism on their own operations, and hence on society as a whole. This involves co-operation with the state, while recognising that governments' resources are finite. Companies must take responsibility for their own security policies.
>
> Secondly, they can help address the deeper social and economic causes of extremism. This includes engagement with weak states whose political and economic failures contribute to international terrorism.

This chapter discusses how companies can best make their distinctive contributions to the wider struggle against terrorism, while also meeting their commercial objectives.

## Company Security Responsibilities

The events of 11 September prompted international companies to take a longer, more sober look at their security arrangements as a whole. Among other long-term questions they are asking themselves whether they really need to be exposed in what are regarded as high-risk regions, such as the Middle East or Central Asia. In sum, how many risks can they afford to take? How much security is 'reasonable'?

### *Setting policy*

The answers depend on the company's nationality, sector and its internal culture. The responsibility for defining and articulating that culture lies firmly with the company board, and not with government.

This is not new. According to the principles set out in the 1999 Turnbull Report on Internal Control[2], companies listed on the London Stock Exchange are required to issue annual statements defining their policy on all aspects of risk management – including security. Similar requirements apply in other jurisdictions, for example under Germany's *Kontrag* regulations. Shareholders have a right to know what steps the company is taking to protect their assets.

What's new post-11 September is the increased emphasis on security as a strategic issue. For example, in some US companies Chief Security Officers (CSOs) are now taking their place on company boards alongside the more conventional Chief Financial Officers (CFOs) and Chief Operating Officers (COOs). Previously, security was often regarded as a secondary concern that could be sorted out once major investment decisions had already been taken. Now this is less likely to be the case.

There may be calculated commercial reasons why some company boards are more willing than others to take high risks. In the petroleum and mining sectors 'major' and 'junior' companies have traditionally taken very different approaches. Smaller exploration companies may see a competitive advantage in operating in difficult areas such as Burma, Sudan and Albania which larger, more risk-averse companies would be reluctant to touch. They hope that their willingness to take higher political and security risks will be rewarded by important geological discoveries and rich commercial returns.

### *Risk assessment*

Whatever a company's appetite for risk, a structured risk assessment process is needed. This should focus both on the likelihood that particular types of event will take place, and the potential impact on the company's objectives.

11 September extended the range of events that are imaginable. Previously, if companies considered terrorism at all, they were more likely to think of kidnaps or relatively small-scale bomb explosions. Osama bin Laden's Al Qaida organisation has demonstrated a willingness to inflict large numbers of civilian casualties. Their 'success' in New York means that companies now have to take

seriously the risk of further high-impact terrorist attacks, for example on oil refineries or nuclear power stations.

Government information is an important source for risk assessment, but it should not be the only one. Officials are understandably reluctant to compromise their sources, so the information they disclose in public is often too generalised to be of much use. Companies will need their own sources, particularly when operating in remote areas.

Risk assessments will need to take account of all kinds of company assets, not just people or buildings. Control Risks recently conducted a threat evaluation for a European bank that was planning to sub-contract its IT support facilities to India. In the course of the review, the risk of political violence and natural disasters in India emerged as issues that were important but not critical to the bank. The greatest risk was reputational: the bank would lose the trust of its customers if subcontractors leaked confidential information. This applied whether its IT specialists were based in India or Idaho. Reputation is a company's most important asset and, in this case, the area where risks are hardest to manage.

The increased attention on terrorism should not distract companies from less spectacular, but more common threats. For example, in Brazil the limited terrorist threat is greatly outweighed by the everyday dangers of violent crime. Car-hijacks and armed robberies rarely make the headlines in Rio de Janeiro, but companies cannot afford to lose the services of key employees who decide to move elsewhere because of crime.

### *Travel security*

Although security has rightly risen up the corporate agenda since 11 September, there need be relatively few occasions where concerns over physical safety serve as a 'deal-breaker' if the commercial conditions are otherwise right. The key is to ensure that security becomes an integral – and routine – part of business planning, not an emergency add-on when things go wrong.



This principle applies as much to day-to-day concerns, such as travel security, as to crisis management. The main lesson has been that companies must know in advance before employees go to potentially dangerous areas so that they can receive up-to-date advice on potential hazards. For example, one UK-based company requires all its employees to receive a special briefing before going to countries rated at Medium risk or above on Control Risks' five-point scale (Insignificant, Low, Medium, High and Extreme). Similarly, companies need to know where their employees are so that they can take prompt action in the event of a sudden crisis such as a coup or a major terrorist attack.

Depending on company policy, business travellers may still visit high-risk regions – and meet the company's commercial objectives – provided they take appropriate security measures. For example, soon after the fall of the Taliban regime, the more entrepreneurial companies wished to send executives to Kabul in the hope of winning lucrative reconstruction contracts. This kind of business trip need not be foolhardy as long as travellers receive special protection, and keep in regular contact with their offices at pre-arranged times by satellite phone.

### *Crisis management*

There is much that companies can do to reduce risk, but it is not possible to eliminate risks altogether. Companies therefore need to ensure that they have effective contingency plans to respond to emergencies. Again, preparation for potential emergencies needs to be an integral part of business planning at every level.

In March 2002, Joe Allbaugh, the director of the US Federal Emergency Management Agency visited Brussels to share the lessons of 11 September with his European counterparts. He explained that the experience of dealing with the World Trade Center disaster had shown up serious flaws in New York's emergency planning. For example, New York's hoses would not attach properly to New Jersey's fire trucks. His

message to his European colleagues applies equally to government and commercial planners:

> They need to take their plans off the shelf, dust them off, get them updated and be prepared because when there's an incident it's too late.

As discussed elsewhere in this collection, it is essential for companies – or groups of companies – to collaborate with officials when drawing up their emergency plans, both at local and national levels. This principle applies both to terrorism response and to other kinds of emergencies, such as evacuation from countries in a state of conflict. Embassies may be able to play an important co-ordinating role, but resident foreign businessmen need to liaise with them in advance, not at the last moment.

### *Beyond complacency*

Overall, company security directors comment that 11 September has made their job that much easier: no-one now questions the need for their expertise. At the same time, many express concern that interest in security may drop if there is a long interval before the next major terrorist attack.

Complacency would be a severe mistake as long as the deeper sources of terrorism remain unaddressed, and this raises the question of what companies can do to mitigate the complex social factors that lead to violence in the first place.

Part of the answer is 'local'. Whether in Bradford, Budapest or Bangalore, companies can best serve the interests of the wider community by providing employment and generating wealth, while treating all their stakeholders fairly. A reputation for good corporate citizenship will not protect them from random, non-selective terrorist attacks (the companies in the World Trade Center were hit because of their location rather than their individual reputations). However, companies with good local networks will be better placed to survive periods of political or social unrest.

The question also has a wider national and international aspect: to what extent can companies contribute to stability in volatile developing countries? This issue is particularly important for weak states that – in the worst case – might otherwise turn into the 'next Afghanistan'.

## Commercial Engagement with Weak States

The social case for companies' engagement with weak states is that poverty and political incompetence exacerbate conflict. If weak states become failed states, violence and insecurity may spread beyond their borders, either through terrorism or through organised crime. It will be difficult to provide long-term political solutions without economic development, and the private sector is an essential ingredient. Pakistan is an obvious case in point.

However, companies cannot operate effectively or constructively unless they can make a commercial case for engagement.[3] For petroleum or mining companies the attraction may be access to natural resources. For manufacturers of consumer goods, the hope may be to establish a foothold in large new (commercial) markets. Firms that enter – and stay with – countries in difficult times will be better placed in times of recovery and expansion.

### *Guarding integrity*

Whatever the commercial rationale, companies cannot operate effectively in weak states unless they manage risks effectively. Since 11 September there has, quite rightly, been an increased emphasis on physical security, but integrity risks – in particular the avoidance of corruption – may be even more important.

Integrity links directly to the terrorism debate. Islamist terrorists are hostile to the West because – among other reasons – they accuse

Western governments and companies of propping up corrupt regimes in the Middle East.

In weak states the challenge of maintaining commercial integrity is all the greater because standards of governance are – by definition – likely to be poor. Typically both business and government are dominated by narrow social elites who may not distinguish between the interests of the state and their own personal concerns. Badly run bureaucracy means that 'transaction costs' – the managerial time taken to deal with obstructive officials – are likely to be high. There is a temptation for country managers with tough budgetary constraints, to offer financial inducements, especially if such payments are customary in the country where they operate. However, if they do so, they reward corrupt behaviour, ensuring that malpractice becomes all the more entrenched.

At the very least, international companies need to ensure that they are 'part of the solution' to governance problems rather than 'part of the problem'. At a minimum, they should – in their own self-interest – maintain high standards. They may also be able to work with local business initiatives to improve commercial standards. For example, in the Philippines, the Makati Business Club is currently leading a collective initiative to promote higher standards of business integrity and transparency. This includes an attempt to reach agreement on common standards, and sponsorship of training on techniques to resist corruption.

The link between poor governance and terrorism applies in many parts of the world, not just in the Middle East. Nepal currently faces what at first sight appears to be an anachronism in the 21st century: an expanding Maoist insurgency. The sources of the insurgency are complex but, on a recent research visit to the country, one interviewee after another spontaneously brought up the problems of governance and corruption. Military campaigns may keep the insurgency in check, but there can be no lasting settlement unless the wider problems of governance are addressed. This is primarily a task for Nepali political leaders, but local and international business may be able to contribute through collective initiatives to combat corruption.

### *Neglected regions*

Even in states that have not failed, there may be provinces and regions that are neglected – and are therefore sources of violence. In the Philippines, business people complain that the reputation of the entire country is undermined because of a long history of political violence in Mindanao, hundreds of miles from Manila. Mindanao has recently drawn international attention because of reported links between local Islamists and the Al Qaida movement.

Philippine Business for Social Progress (a business-sponsored NGO) is working on a series of projects in Mindanao. Among other initiatives, it is trying to provide business training and work placements for young Muslims. The idea is to ensure that there is an 'alternative' to violence. Given the depth of social and political alienation in Mindanao, this may be a relatively small contribution but it is a good example of business working with civil society in a previously neglected region. Focused local initiatives of this kind may help address the global problems of trans-national Islamic terrorism.

## New Coalitions: The rules of engagement

If international companies are to operate effectively in high-risk regions, they will need the support of both 'home' and 'host' governments. It is crucial that they achieve the right balance, working with both kinds of government without relying on either of them. They are most likely to achieve this by working with other social actors – not just governments, but also representatives of civil society, such as community groups and NGOs.

As discussed, Western governments may be able to offer assistance with risk assessment, but companies will still need their own sources. Insurance is re-emerging as another important area for Western government support as premiums for both security and political risk

insurance have risen sharply since 11 September and private insurers lack the capacity to provide all the cover that companies need.

However, companies cannot afford to identify too closely with Western home governments. This is partly because international companies do not necessarily have obvious national identities anymore. For example, Royal Dutch/Shell and Unilever have been Anglo-Dutch for decades, and the Swiss/Swedish ABB claims to be 'local' wherever it operates. More critically, too close an identification with a foreign, especially Western, government can increase rather than decrease security risks. Since the 1970s, terrorists across the world have attacked Western companies – particularly banks, airlines and travel agencies – as proxies for Western governments. The risk of such proxy attacks has increased rather than decreased since 11 September, as security concerns rise to the top of diplomatic agendas.

Equally, companies will not – or should not – want to identify too closely with host governments, still less with individuals in those governments. Companies that are seen as clients or – worse still 'cronies' – of a Suharto or a Marcos will face significant political risks when there is a change of government. Companies must identify with the countries where they operate, but not with partisan political interests.

It is particularly important for companies to avoid appearing partisan in cases where security concerns are linked to wider disputes about human rights or the allocation of resources. Some of the most notable cases arise where international petroleum or mining companies are operating in remote areas. Local people receive few benefits from such operations and government security forces suppress dissent with undue force. Such problems have arisen in countries as diverse as Nigeria, Burma, Colombia and Indonesia.

Companies are now finding ways to develop three-way partnerships with governments and civil society to address such problems at both the



local and international levels. In December 2000, the UK Foreign Office and the US State Department helped broker the Voluntary Principles on Security and Human Rights.[4] The signatories include major US and UK petroleum and mining companies, as well as NGOs such as Amnesty International and Human Rights Watch, and the principles cover risk assessment and relationships with both government and private security forces. The signatories are continuing to share experience on implementation of the principles: one of the main challenges is securing the co-operation of host governments.

At a local level the World Bank-sponsored Business Partners for Development (BPD) has been developing case studies of tri-sectoral partnerships between business, government and civil society in countries such as the Philippines, South Africa and Colombia.[5] Examples include a series of joint projects to provide responsive and affordable water and sanitation services in poor communities. All three sectors have contributed their expertise to ensure that the projects are sustainable both environmentally and – bearing in mind the companies' interests – commercially. One of BPD's main roles has been to facilitate the pooling of experience, and develop a common understanding of best practice. This is a field that continues to evolve. From the companies' point of view, one of the clear benefits is that their projects are more likely to prosper – and remain safe – if they can draw on the support of both government and local community organisations.

Terrorism remains a complex problem: it demands multi-faceted solutions involving a range of social actors. Speaking at a conference organised by The Guardian and the Royal United Services Institute (RUSI) in October 2001, UK Foreign Minister Peter Hain argued that:

> 'Global problems need global solutions provided by global coalitions. You can't be secure at home in an insecure and unstable world. Globalisation links our destinies in new and complex ways.'[6]

He went on to argue that coalitions need to extend beyond governments:

> 'We need the innovation and market building that only business can provide; the analysis and legitimacy that only civil society can bring.'

Working alone, neither governments nor business have all of the answers to terrorism, but by working together with local and international civil society, they may be able to begin addressing some of its root causes.

[1] Francis Fukuyama, 'The United State', *Financial Times,* 15 September 2001.

[2] Available online at www.icaew.co.uk. Edward Alden, 'A lesson in preparing for the worst', *Financial Times*; 24 April, 2002.

[3] For a discussion of the business case for engagement in high-risk regions, see: Jane Nelson, *The Business of Peace* (London: International Alert, Council on Economic Priorities, Prince of Wales Business Leaders Forum, 2000), pp. 13-19.

[4] Available online at www.state.gov

[5] www.bpdweb.org

[6] Peter Hain, 'A global approach to peace', *Guardian Unlimited*, 30 October 2001. www.guardian.co.uk.



## Also available from The Foreign Policy Centre

**Individual publications should be ordered from Central Books, 99 Wallis Road, London, E9 5LN tel: 020 8986 5488, fax: 020 8533 5821 email: mo@centralbooks.com**

**To order online go to www.fpc.org.uk/reports**

**(Subscriptions are available from the Centre itself)**

### THE FOREIGN POLICY CENTRE MISSION STATEMENT

March 1999; Free, with £1 p+p, or free with any pamphlet.

*'Likely to be controversial with Mandarins and influential with Ministers',* **Financial Times**

---

### HOW TO REFORM THE COMMON AGRICULTURAL POLICY

Jack Thurston, with an introduction by Chris Haskins
September 2002; £14.95; plus £1 p+p, ISBN 0-903558-1-4.

---

### TRAVEL ADVICE

Rachel Briggs
Kindly supported by Thomas Cook Tour Operations
August 2002; £19.95; plus £1 p+p, ISBN 1-903558-16-6.

This report addresses the travel advice sector in the UK. A growing number of Britons are getting into trouble abroad and British Consulates are often left to pick up the pieces when things go wrong. Many of these problems could be avoided if relevant travel advice was read prior to departure, but there seems to be complacency and confusion among the main groups of travellers about whether they are at risk and whether it is their own responsibility to seek out advice. Travel Advice calls for partnership between the UK government, the travel industry, companies, and the charity sector to ensure targeted advice gets to the people who need it.

---

## THE KIDNAPPING BUSINESS

Rachel Briggs
March 2001; £9.95; plus £1 p+p, ISBN 1-903558-16.
Kindly supported by Hiscox, Control Risks Group, ASM Ltd., Marsh Ltd. and SCR

This report sets out a new policy for economic kidnapping. It puts forward recommendations for the UK government, the business community and the aid community aimed at helping them to prepare better for the risk of kidnapping.

---

## AFTER MULTICULTURALISM

Yasmin Alibhai-Brown
May 2000; £9.95; plus £1 p+p, ISBN 0-9535598-8-2.

*'Yasmin is brave, intelligent and always worth reading',*
***Diane Abbott MP,*** **New Statesman**

---

## RE-ORDERING THE WORLD: The Long-Term Implications of 11 September

Mark Leonard (editor), with essays by Ehud Barak, Ulrich Beck, Tony Blair, Fernando Henrique Cardoso, Malcolm Chalmers, Robert Cooper, Fred Halliday, David Held, Mary Kaldor, Kanan Makiya, Joseph Nye, Amartya Sen, Jack Straw and Fareed Zakaria
March 2002; £9.95; plus £1 p+p, ISBN 1-903558-10-7.

*'Caused a storm…',* **The Observer**

---

## PUBLIC DIPLOMACY

Mark Leonard with Catherine Stead and Conrad Smewing
In association with the British Council, BBC World Service, and the Norwegian Government.
June 2002; £14.95; plus £1 p+p, ISBN 1-903558-131.

*'First-rate. An extraordinarily important book to make the case for public policy that recognises the role of the soft power',*
***Jospeh Nye, Dean, Kennedy School of Government*****, Harvard**

---

## REINVENTING THE COMMONWEALTH

Kate Ford and Sunder Katwala
In association with the Royal Commonwealth Society
November 1999; £9.95; plus £1 p+p, ISBN 0-9535598-4-5.

*'Intelligent and wide-reaching',* **The Times**

---

## THE PRO-EUROPEAN READER

Dick Leonard & Mark Leonard (editors), with essays by Winston Churchill, Jean Monnet, Roy Jenkins, Mikhail Gorbachev, Milan Kundera, David Puttnam and Tony Blair.
Published by Palgrave November 2001; £16.99; plus £1 p+p, ISBN 0-333977211.

*'Here's a book full of cures for prejudice and phobia. Some of the antidotes are bold, some wry, some profound, some sharp – all short. The treatment is worth every Euro',* ***Neil Kinnock***

---

## THE FUTURE SHAPE OF EUROPE

Mark Leonard (editor)
Kindly supported by Adamson BSMG Worldwide.
November 2000; £9.95; plus £1 p+p, ISBN 1-903558-02-6

*"The Europe of Nice is a building site waiting for new master builders. A booklet by The Foreign Policy Centre makes the point more eloquently than any polemicist",* ***Peter Preston,*** **The Guardian**

---

## NGO RIGHTS AND RESPONSIBILITIES:
## A new deal for global governance

Michael Edwards
In association with NCVO.
July 2000; £9.95; plus £1 p+p, ISBN 0-9053558-00-X.

*'Timely and thought-provoking… balanced, objective and written with great sense and flashes of humour',*
***David Bryer*, former Director, Oxfam**

---

## TRADING IDENTITIES:
## Why Countries and Companies Are Becoming More Alike

Wally Olins
October 1999; £9.95; plus £1 p+p, ISBN 0-9535598-3-1.

*'A fascinating pamphlet',* ***Peter Preston,* The Guardian**

---

## GLOBALIZATION – KEY CONCEPTS

David Held & Anthony McGrew, David Goldblatt & Jonathan Perraton
April 1999; £4.95; plus £1 p+p, ISBN 0-9535598-0-7.

*'An indispensable counterweight to optimists and pessimists alike',*
***Will Hutton***

*'This is the agenda on which a new politics must be constructed and new alliances forged',* ***Clare Short, Secretary of State for International Development,* New Statesman**

---

## THE POST-MODERN STATE AND THE NEW WORLD ORDER

Robert Cooper
In association with Demos.
2nd edition 2000; £8.95, plus £1 p+p, ISBN 1-84180-010-4.

*'Mr Cooper's pamphlet explains, lucidly and elegantly, how the emergence of what he calls the postmodern state has changed international relations',* **New Statesman**

## NETWORK EUROPE

Mark Leonard
In association with Clifford Chance.
September 1999; £9.95; plus £1 p+p, ISBN 0-9535598-2-3.

*'A radical agenda for reform from the government's favourite foreign policy think-tank',* ***Stephen Castle,* Independent on Sunday**

*'A welcome contribution to the important debate about Europe's future',* ***Tony Blair***

---

## FROM WAR TO WORK:
## Drug Treatment, Social Inclusion and Enterprise

Rowena Young
In association with Globalegacy.
March 2002; £16.95; plus £1 p+p, ISBN 1-903558-07-7.

*'This report will spark major debate',* **The Observer**

*'An insightful analysis that gets us beyond the anachronistic hard on/soft on drugs debate, and points up the key dilemmas facing governments in the search for an effective drug policy',*
***Mike Trace, Director of Performance,* National Treatment Agency**

---

## THIRD GENERATION CORPORATE CITIZENSHIP:
## Public Policy and Business in Society

Simon Zadek
November 2001; £19.95; plus £1 p+p, ISBN 1-903558-08-5.
Kindly supported by Diageo and Friends Ivory & Sime

*'Zadek strikes at the very heart of this debate',* ***Craig Cohon,* Globalegacy**

---

## THE NEXT GENERATION DEMOCRACY PROJECT

The 'Next Generation Democracy' project explores the theme of legitimacy in an enlarging Europe, organised around five themes: Matching Policies to Public Priorities, Accountability, Political Competition, Participation and Representation.

## NEXT GENERATION DEMOCRACY: Legitimacy in Network Europe

By Mark Leonard and Tom Arbuthnott, November 2001

The framework document for the Next Generation Democracy programme.

*'A most important policy brief... It is good to see new and clear thinking on the future of the EU.'*
***Baroness Nicholson of Winterbourne MEP***

*'It certainly is an intriguing project, which I shall follow with interest.'*
***Sir John Kerr,* Secretary General, the European Convention**

---

## LINKING NATIONAL POLITICS TO EUROPE

By Simon Hix, March 2002

The second output from the series. Hix argues that the European institutions are increasingly disconnected from the citizens they are meant to serve. He maintains in this policy brief that the answer is to allow national parliamentarians to elect the Commission President. This would create a stronger link between national politics and EU politics.

*'Very interesting document.'* ***Ana Palacio,* Spanish Foreign Minister**

*'The Convention may chose not to endorse [Hix'] ideas, but it should at least give them serious consideration.'* **European Voice**

---

## CAN BRUSSELS EARN THE RIGHT TO ACT?

**By Mark Leonard and Jonathan White, July 2002**

In the Matching Policies to Public Priorities theme, Mark Leonard and Jonathan White argue that the European Union is suffering from a delivery deficit, and that EU institutions must earn their powers by proving their ability to execute them effectively.

*'The report provides a robustly pro-European critique of where the EU is failing the delivery test, most obviously in areas such as the Common Agricultural Policy and the delivery of overseas aid',*
**The Observer**

*'Provides interesting ideas for my work at the convention',*
***Gisela Stuart MP***

---

## Forthcoming publications from The Risk and Security Research Programme

## CORPORATE PERSONNEL SECURITY IN EMERGING MARKETS

### Working Paper One: The Legal and Policy Framework for Duty of Care

Rachel Briggs (December 2002)

This paper will examine what a company's duty of care to their employees in emerging markets actually means in practice, and will explore the extent of personal responsibility of staff. It will outline the current legal and policy framework and will suggest a number of changes to improve safety.

---

## CORPORATE PERSONNEL SECURITY IN EMERGING MARKETS

### Working Paper Two: The Role of Third Party Actors

Rachel Briggs (February 2003)

This paper will examine the role of the UK government, corporate security companies, insurance companies and other third party actors, and will put forward a number of suggestions for each of these actors.

---

## CORPORATE PERSONNEL SECURITY IN EMERGING MARKETS

### Final Report and Findings

Rachel Briggs (July/August 2003)

The final report will set out a new policy agenda covering the safety of those being employed by companies in emerging markets.

---

## Subscribe to The Foreign Policy Centre

The Foreign Policy Centre offers a number of ways for people to get involved. Our subscription scheme keeps you up-to-date with our work, with at least six free publications each year and our quarterly newsletter, Global Thinking. Subscribers also receive major discounts on events and further publications.

| Type of Subscription | Price |
|---|---|
| ☐ Individuals | £50 |
| ☐ Corporate and Libraries (will receive ALL publications) | £200 |
| ☐ Diplomatic Forum (Special high-level embassy scheme) | £500 |
| ☐ Europe Embassy Subscription Scheme (Tailored to the Centre's Europe Programme, please contact Tom Arbuthnott: tom@fpc.org.uk) | £150 |

Please make cheques payable to **The Foreign Policy Centre**, indicating clearly your postal and email address and the appropriate package, and send to Subscriptions, The Foreign Policy Centre, Mezzanine Floor, Elizabeth House, 39 York Road, London SE1 7NQ. For further details, contact Rachel Briggs: rachel@fpc.org.uk