

*An analysis of international security issues compiled by security professionals for business leaders and those who advise them*

Faced with the prospect of suicide terrorism at home and abroad, businesses are increasingly forced to rely upon physical deterrence and business continuity planning as their primary defences. This issue of *Janusian Thinking* considers additional measures that businesses can take to identify and disrupt terrorists during the reconnaissance and planning phases of their operations- when they are most vulnerable. For the first time, the idea that businesses can adopt proactive counterterrorist measures is gaining real currency.

This issue is produced in collaboration with Dr Kevin A. O'Brien, Senior Policy Analyst, RAND Europe, reflecting research he has been conducting during 2003. During 2004 Janusian will be launching a major initiative on countersurveillance and terrorist target reconnaissance.

## The New Face of Terrorism

Exactly 800 days after 11 September 2001 British diplomatic and commercial interests were finally the direct and overt target of a successful attack by Islamist terrorists. After more than two years of dire warnings, the attacks came in Istanbul rather than London, but the message was very clear: Britain is a target at home and abroad for the 'new terrorism', that knows no bounds.

The recent arrests of 16 suspects around the UK under the Terrorism Act 2000, and the discovery of explosives at the Gloucester home of Sajid Bajat, underlined the mounting concern felt by the police and Security Service that attacks on the UK mainland may be imminent.

Naturally, British businesses are concerned that they will be targeted by affiliates of Al Qaeda and other proponents of the 'new terrorism', and many are seeking ways to respond to this renewed and transformed terrorist threat. As we have argued in this forum on previous occasions, the private sector has far greater ownership of the Critical National Infrastructure (CNI) than 20 years ago, as well as a continuing strong stake with their own infrastructures and commercial assets.

The 'new terrorism' has expanded this range of targets across society – including hospitals, shopping-centres, schools, public transportation systems, tourist centres, large accommodation blocks, and so forth. In many cases mass casualties are achieved either by design or as a side effect of these target selections. The UK government, like most Western governments, is confronting this new threat through a variety of initiatives, including new protective measures, public-education and awareness efforts, civil contingency and resilience planning, and improved co-ordination between the police and intelligence services.

Within this new paradigm of awareness, there is an increased role for UK businesses. As the terrorists widen their gaze to encompass everyday targets, businesses and public-sector entities, every citizen in society must become a 'counter-terrorist'. Governments can no longer be relied upon solely to take responsibility for – and attempt to mitigate against – threats against all aspects of society. What this means for Western businesses – both

domestically and externally – is that they must become ever-more-involved in countering today's 'new terrorism'.

### **Terrorist Target Reconnaissance Against Businesses**

One of the challenges for any organisation seeking to protect itself against the threat of terrorism, and in contributing to the wider public effort, is to discover practical measures that can be implemented in the face of mass casualty terrorism, conducted by protagonists who are prepared to perish in the process of carrying out attacks. Person-borne or vehicle-borne suicide attacks are very hard to defend against in the immediate pre-attack phase- i.e. just before detonation. However, considerable planning, often drawn out over several months, normally precedes sophisticated terrorist attacks. It is during this early pre-attack phase that terrorists are themselves vulnerable, as they select their targets or attempt to gather greater information on their target's situation.

Even unsophisticated terrorists will almost always scout targets before an attack. Al Qaeda affiliated groups plan meticulously. This is done to determine target suitability, levels of protection and noticeable patterns in the target's movements, physical security, and the surrounding environment. Terrorists are opportunistic: exploiting vulnerabilities as they find them. The time, place and methods of attack are selected according to weaknesses they observe. Increasing security has a significant deterrent effect on terrorists during the planning phase, hence the much-noted preference for "soft targets".

Any commercial establishment can be a target, as well as – most unfortunately – many societal locations, such as schools, shopping malls, restaurant districts, movie-theatres and anywhere else large numbers of people gather. As in-depth planning and surveillance by terrorists – which includes assessing the target's security arrangements – precede most attacks, detecting such activity is crucial to thwarting attacks. Even if reports turn up no evidence of terrorist activity, the investigations may act as a valuable deterrent: many cases have been documented in which terrorists turned to an alternative target when their surveillance of a primary target indicated a high risk of detection or failure.

A number of technological 'solutions' are now being tested to detect terrorists and their reconnaissance activities. For example, many airports are beginning to implement biometric recognition devices to look for either known individuals or patterns in crowds. Biometric technologies, such as face-recognition technology, are based around the digital analysis of biological characteristics such as facial structure, fingerprints and iris patterns, using cameras or scanners and computers that in some cases are as small as a computer mouse. Biometrics have already caught-on in other areas, such as among security agencies and government authorities: in Swindon, some automatic bank tellers use iris scanners to verify customers. In addition, a security company in Sydney, Australia, has integrated fingerprint scanners into armoured trucks. Officials at the 1998 Nagano Winter Olympics in Japan scanned the retinas of security guards before outfitting them with rifles and ammunition.

Aviation experts say facial recognition is perhaps the most promising biometric technique for overcrowded airports, as it relies on long-range cameras to identify people, unlike fingerprint scanners or other devices requiring people to click, touch or stand in a particular position. Thus far, biometrics has not caught on in airports because the devices, though relatively inexpensive, would consume time and space as passengers move through, potentially resulting in more airline delays and cancellations. There are also concerns about the potential for 'false positives' resulting from such mass-scanning. However, where such systems have been trialled, they have been successful. Keflavik International Airport in Iceland installed facial-recognition technology in June 2001. Authorities use the cameras and computers to help identify known criminals, potential terrorists on secret-service rosters and false asylum-seekers from the European Union.

Such processes and devices should contribute greatly towards thwarting – even by their very presence – potential terrorist reconnaissance in the future. However, more basic practices can be implemented that can disrupt terrorist activity during the early pre-attack phase. Beyond the technological ‘solutions’, very few countries have publicly-admitted to doing any work on developing effective ways to counter terrorist reconnaissance; while it is known that the Israel has considered this issue in great depth – but also in great secrecy – the United States is, as part of its public counter-terrorism information and awareness campaign, developing a number of public warnings which include indicators towards spotting terrorist reconnaissance activities.

### **Indicators of Terrorist Reconnaissance: Business Pointers**

In noting “all terrorists have to plan and prepare for an attack, which can make them vulnerable to discovery. They may seek anonymity, or other identities, in making these preparations”, the UK Home Office offers some advice for companies concerned about the terrorist threat. This includes:

- Be alert and observant and report any unusual or suspicious activity to the appropriate people or departments. Encourage your staff to do so, too.
- Have a good look around your workplace and establish an awareness of what should and should not be there. This will be very important if you need to search your premises at any time (for example, if there were a bomb threat).
- Develop links with neighbouring businesses and share information so that, together, you are able to cover a wider area.
- Trust your instincts; if you feel something is wrong, ring the police.
- Be aware of the companies and the people who come and go in the delivery of goods or services in your workplace. If anyone or anything causes you serious concern, report the incident to your managers or to the police.

Similarly, companies should be alert to unusual transactions that raise questions about their purpose or intent – would accounting practices pick up such anomalies? Similarly, is there a possibility that your business could unwittingly support terrorist activity – perhaps through insecure computer systems and access to them. Companies must also ensure that they have checked references and employment records on staff to ensure that they “are who they say they are”.

In February 2003 the FBI warned “Al-Qaeda is reported to be actively seeking opportunities to launch attacks using both traditional (explosives) and non traditional (chemical, biological, radiological and nuclear – CBRN) weapons”. In such a case, the FBI advises companies that, as “terrorist planning may begin months or years before an actual terrorist attack”, companies should “consider previous unusual incidents – such as possible surveillance – when evaluating yourself or your customers as to whether you are a potential target”. Companies should consult information that is readily available, particularly on the Internet, regarding their operations and facilities, and consider how such information might assist terrorists interested in planning an attack. If such information could prove useful, companies are advised to consider revising or removing such information from public access. Companies are also advised to vary their security routines, as terrorists are clearly opportunistic and look for routines that they can identify and then exploit. Finally, companies are similarly warned to consider the potential ‘insider’ threat, as terrorists may attempt to infiltrate a facility or potential target.

In March 2003, the new US Department of Homeland Security (DHS) introduced *Possible Indicators Of Al-Qaeda Surveillance*, stating that "Al-Qaeda operations have been characterized by meticulous planning, a focus on inflicting mass casualties, and multiple, simultaneous suicide attacks", it went on to warn that "Operatives are highly trained in basic and sophisticated surveillance techniques". Through the course of assessing previous al Qaeda operations, US authorities believe that certain patterns of behaviour have begun to emerge – these include:

- Unusual or prolonged interest in security measures or personnel, entry points and access controls, or perimeter barriers such as fences or walls.
- Unusual behaviour such as starting or quickly looking away from personnel or vehicles entering or leaving designated facilities or parking areas.
- Observation of security reaction drills or procedures.
- Indications that terrorists observed any changes in security procedures after e-mailing or telephoning anonymous threats to their intended target.
- Foot surveillance involving two or three individuals working together.
- Mobile surveillance using bicycles, scooters, motorcycles, cars, trucks, sport utility vehicles, boats, or small aircraft.
- Prolonged static surveillance using operatives disguised as panhandlers, demonstrators, shoe shiners, food or flower vendors, news agents, or street sweepers not previously seen in the area.
- Discreet use of still cameras, video recorders or note taking at non-tourist type locations.
- Use of multiple sets of clothing, identifications, or the use of sketching materials (paper, pencils, etc.).
- Questioning of security or facility personnel.

Terrorists – at least, initially – are most likely to target the highest-profile targets that they can attack; these may include:

- Key national assets such as nuclear power plants, dams and government facilities
- Energy sector installations including power stations or major powerlines, fuel farms, and petrol stations
- Transportation sectors including passenger rail, freight trains carrying toxic industrial chemicals, civil aviation, rail and vehicle bridges, tunnels, and metropolitan transit systems
- Direct attacks on financial institutions

Similar to the Homeland Security 'activities to watch for', other key activities which might suggest possible terrorist surveillance include:

- Foot surveillance involving 2-3 individuals working together.
- Mobile surveillance using bicycles, scooters, motorcycles, sport-utility vehicles, cars, trucks, boats or small aircraft.
- Persons or vehicles being seen in the same location on multiple occasions, or persons sitting in a parked car for an extended period of time.
- Persons not fitting into the surrounding environment, such as wearing unusual clothes for the location, or persons drawing pictures or taking notes in an area not normally of interest to a tourist.
- Persons using possible ruses to cover their activities, such as taking on a disguise as a beggar, demonstrator, shoe shiner, fruit or food vendor, street sweeper, or a newspaper or flower vendor not previously recognized in the area.
- Persons videotaping or photographing security cameras or guard locations, or unusual or prolonged interest in security measures or personnel, entry points and access controls, or perimeter barriers such as fences or walls.

- Finally, an increase in anonymous threats followed by individuals observing security reaction drills or procedures, or questioning of security or facility personnel by an individual(s) that appears benign.

Similarly, the US Air Force – in a warning to its personnel and their families – launched Operations EAGLE EYES, which is based around the ‘neighbourhood watch’ concept. Allegedly ‘taking its cue from the experiences of British and Israeli authorities, who have significant experience dealing with urban terrorism’, EAGLE EYES is premised on the belief that “the best judges of knowing who or what belongs — or, perhaps more importantly, doesn’t belong — in a building, work centre or neighbourhood are usually the people who work or live there”. Information collected on suspicious activities is used by both the immediate-area authorities and the central Air Force Office of Special Investigations analytical centre at Andrews Air Force Base, where it is compared to other Air Force reports, as well as to similar information from the Army, Navy and other federal agencies.

EAGLE EYES outlines seven broad categories of concern for reporting:

- Surveillance, which involves someone recording or monitoring activities. This may include the use of cameras (either still or video), note taking, drawing diagrams, annotating maps, or using binoculars or other vision-enhancing devices.
- Elicitation, which involves people or organizations attempting to gain information about military operations, capabilities or people. Elicitation attempts may be made by mail, fax or telephone or in person.
- Security tests, which include any attempts to measure reaction times to security breaches or to penetrate physical security barriers or procedures in order to assess strengths and weaknesses.
- Supply acquisition, which involves purchasing or stealing explosives, weapons, ammunition, etc. This category also includes acquiring military uniforms, decals, flight manuals, passes or badges (as well as the equipment to manufacture such items) or any other controlled items.
- Suspicious people or people who don’t seem to belong in the workplace, neighbourhood, business establishment, etc. This category includes suspicious border crossings and stowaways aboard ships or people jumping ship in port.
- Dry runs or putting people into position and moving them around according to a plan without actually committing a terrorist act. Dry runs particularly come into play when planning a kidnapping, but they can also pertain to bombings. An element of this activity could also include mapping out routes and determining the timing of traffic lights and flow.
- Asset deployment or putting people and supplies into position in preparation for a terrorist act. This category represents the last chance for people to alert authorities before a terrorist act occurs.

Significant breakthroughs in anti and counterterrorism are relatively rare. Countersurveillance and disruption of terrorist reconnaissance are some of the most significant innovations of recent times, and offers businesses the opportunity to take credible steps to protect themselves.

***Janusian Security Risk Management and RAND Europe provide this article for reference only – it is not suggested as a guaranteed method for defeating terrorist attacks. Janusian and RAND take no responsibility for any events relating to or resulting from the information contained in this article.***

**Further information:** Janusian Security Risk Management is the specialist political risk and security subsidiary of The Risk Advisory Group Ltd. For further information please visit [www.janusian.com](http://www.janusian.com).