SAFE CITIES PROJECT

Hard Won Lessons: How Police Fight Terrorism in the United Kingdom



December 2004

Safe Cities Editor

Paul Howard, Ph.D. is the writer and editor of Safe Cites, *Hard Won Lessons: How Police Fight Terrorism in the United Kingdom*, based on presentations made at the Police Institute at Rutgers University in June 2004. Dr. Howard is the Deputy Director of the Center for Civic Innovation at the Manhattan Institute.

Acknowledgments

The Manhattan Institute would like thank The Achelis and Bodman Foundations for their ongoing support of the Safe Cities program and its publications. We would also like to thank Brian Howat (Head of Unit, National Counter Terrorism Security Office), Kevin Bolton (Detective Sergeant, National Counter Terrorism Security Office), and Vincent Smith (Inspector, British Transport Police) for their cogent presentations on U.K. counterterrorism procedures and assistance in the preparation of this report.

Table of Contents

Introduction: Do Police Matter?

By George Kelling, Ph.D.

Do police matter? Can they prevent crime—or, for that matter, terrorism? The long-prevailing view of the police department's role in society was spelled out in the famous "Principles of Law Enforcement" of Sir Robert Peel, founder of London's Metropolitan Police (Scotland Yard). "The basic mission for which the police exist," Peel wrote in 1829, "is to prevent crime and disorder." Accordingly, Peel proposed that the test of police efficiency should be "the absence of crime and disorder, not the visible evidence of police action dealing with them."

As Peel's model of Anglo-Saxon policing was adopted in U.S. cities during the nineteenth century, this assumption prevailed as well. Police could prevent crime by their presence, by persuasion, by reducing opportunities for crime, and by law enforcement—arresting wrongdoers. Although U.S. policing narrowed its focus almost exclusively to law enforcement during most of the twentieth century—or at least tried to—few police doubted that police really mattered in crime control.

In the 1950s, however, researchers began to ask basic questions about the police "business"—what they did and what it accomplished. Initially, they studied "the law in action," focusing on "what police actually did." These police-function studies showed that police actually spent most of their time providing services, such as managing disputes, rather than "fighting crime." Later, during the 1970s, research on widely practiced tactics—including rapid-response calls for service and automobile patrols—suggested that these tactics had little, if any, significant impact on crime.

These empirical findings became grist for the mill of new theorists who posited that crime was the result of collective "root causes" like social injustice, racism, and poverty. The practical implication of such root-cause theory was that crime could only be prevented if *society itself* were radically changed. These views became memorialized in President Lyndon Johnson's Commission on Law Enforcement and Administration of Justice and became the virtual dogma of criminal-justice thinking. In academia, many scholars wedded this root-cause thinking to the empirical research: police, *as the research shows*, can have little impact on crime. All police and criminal-justice agencies could do was react to crime after it occurred—much like firefighters reacting after the outbreak of a fire. When it came to *preventing* (and thus reducing crime), police did not really matter.

Though root-cause theory dominated official criminology during the 1970s and 1980s, the consensus was not absolute. A dissenting movement of criminologists wondered whether the root-cause theorists, in their "de-policing" of crime control, had not perhaps thrown out the proverbial baby with the bathwater. Indeed, without anyone really being aware of it, the groundwork was slowly and quietly being laid for a return, in the 1990s, to an updated "Peelist" model. This new model accepted the empirical research but interpreted it against a background theory that retained

Peel's time-honored assumption. Rather than concluding from effectiveness studies that policing did not matter, these dissenting theorists incorporated the empirical findings into several "big ideas" that might make police matter more effectively. Three of these ideas, in particular, greatly influenced police work in New York City during the Giuliani years.

The first was the idea of "problem solving," advanced by Professor Herman Goldstein of the University of Wisconsin Law School. Goldstein—who had been among the first empirically-oriented police theorists—argued that the proper business of police was *problems*, not incidents. Response-oriented policing, in Goldstein's view, approached police work as a series of disconnected incidents that had neither history nor future. In fact, most police incidents had both: they had evidenced themselves before in one form or another and likely would resurface in similar terms. Thus, incidents of spousal abuse, noisy and boisterous bars, prostitution, burglary, to give just a few examples, were often, in reality, signs of an ongoing problem that, if suitably addressed by police, could be managed or solved.

The second idea, "broken windows," was formulated by Professor James Q. Wilson (then at Harvard and later at the University of California, Los Angeles) and myself in an article published in 1982. In that article, we suggested that failure to control minor offenses such as prostitution and disorderly conduct destabilized neighborhoods by creating a sense of public disorder. Pushing the theory further, we argued that people were likelier to turn to crime in neighborhoods where toleration of petty crimes—such as graffiti scrawling and window breaking—indicated a lack of effective social control. Restoring order, we believed, would not only reduce neighborhood fear but would substantially reduce crime. In 1989, I worked with New York City transportation authorities and later in 1990 with Transit police chief William Bratton to implement the "broken windows" theory in the New York City subways—and when Bratton became NYPD chief in 1994, he moved to make the theory part of standard NYPD practice.

The third innovation was a new way of managing police resources and tactics, known as "CompStat." Implemented by Bratton when he became NYPD police chief—and subsequently adopted by police departments across the country—CompStat was perhaps the single most important organizational/administrative innovation in policing during the latter half of the twentieth century. Like other managers of large, geographically dispersed organizations, Bratton had faced the problem of how to ensure that his centralized vision of policing was carried out in all seventy-six NYPD precincts. To solve this problem, Bratton invested enormous authority in precinct commanders, devolving resources and decision making to the precinct level. He also mandated weekly planning meetings, in which precinct commanders had to identify problems as well as discuss their plans for dealing with them. This administrative mechanism focused the NYPD on substantive community problems rather than traditional bureaucratic machinations. Precinct commanders, previously preoccupied with what happened at One Police Plaza (central police headquarters), riveted their attention on their precincts: woe be it to the precinct commander who wasn't on top of his or her precinct's problems. These changes reoriented not only precinct commanders, but borough chiefs and top commanders as well: if precinct commanders looked bad, it reflected on the borough chiefs, and so on up the line.

Shortly after Bratton implemented these new ideas, crime in New York City began its historic dive. From 1990 to 1992, crime in New York City subways declined by 30 percent, with arrests and

ejections rocketing from 2,000 per month to 10,000–15,000 per month. Following the problem-solving approach led to the realization that enforcing laws against turnstile jumping would net more serious criminals. Indeed, one out of every seven people arrested in the subways for fare evasion was wanted on a warrant. Often, these warrants would be for very serious crimes, such as murder or rape. One out of every twenty-one fare evaders, at least initially, was carrying some type of weapon—ranging from a straight-edge razor on up to automatic weapons. This process allowed the police to have a good chance of catching significant offenders without exorbitant effort or expenditure of resources. Now, well over a decade later, crime in the subway system is down almost 90 percent from what it was in 1990. Citywide, homicides are at a forty-year low. Overall, New York City is arguably the safest large city in America.

Subsequent research has shown that each of these ideas, particularly broken-windows policing and CompStat, played an important role in reducing crime in New York City to these unprecedented levels.

Since 9/11, police are facing a new challenge: global terrorists using weapons of mass destruction that could result in thousands—or tens of thousands—of casualties. While enormous amounts of ink have been spilled defining the new responsibilities and relationships that should obtain between federal agencies (FBI, CIA, NSA, and the Pentagon), there has been much less attention paid to the role that police must play in homeland security and protecting critical national infrastructure.

This is unfortunate, because terrorism's equivalent to fare jumping in the New York City subways are illegal border crossings, forged documents, and other relatively minor crimes that terrorists use to fund their operations. Once inside our borders, it is the police—not the FBI or CIA—who have the best tools for detecting and prosecuting these crimes.

Ultimately, homeland security is less dependent on appointing a national intelligence czar than it is on empowering local police with the training and conceptual tools to prosecute potential terrorists in the cities and towns where they live.

Police can use problem solving to identify terrorist precursor crimes, broken-windows policing to create hostile environments for terrorists, and CompStat to collate counterterrorism intelligence and target police resources effectively.

The practices—the know-how—are out there, but they are fractured among the many layers of law enforcement that characterize America's federal system of government. What is needed now is an "all-channel network" where expertise and intelligence can be disseminated quickly and effectively throughout the law-enforcement community, from coast to coast, and from police chiefs to officers at the street level. To paraphrase Benjamin Franklin, we must all learn how to hang together or we will most assuredly all hang separately.

In response to this need, the Manhattan Institute and the Police Institute at Rutgers University have instituted an ongoing series of meetings for police chiefs and state homeland-security officials operating along the I-95 corridor of the eastern United States. These meetings bring together the foremost experts on crime prevention and tactical counterterrorism from the U.S. and abroad to discuss how police can maximize their ability to detect, deter, and, when necessary, recover from terrorist attacks.

The following paper is the first in a series of forthcoming "best practices" manuals for police departments that will be published by the Manhattan Institute. It is based on a meeting held at Rutgers University on June 3, 2004, for the "I-95" group, where counterterrorism experts from the United Kingdom gave presentations on how police can:

- effectively identify critical infrastructure
- work more effectively with the private sector to protect high-risk targets
- create a hostile environment for potential terrorists
- identify precursor crimes for terrorism
- use crime prevention techniques to deter terrorists

Their comments were immensely helpful, and we would like to extend to our U.K. comrades (Brian Howat, Head of Unit, National Counter Terrorism Security Office; Kevin Bolton, Detective Sergeant, National Counter Terrorism Security Office; and Vincent Smith, Inspector, British Transport Police) our sincere thanks for traveling so far to render vital assistance to their fellow officers.

If there was one thing that our friends from the U.K. constantly emphasized, it was that the American police officer doesn't have to abandon any of the crime-prevention tools that he has successfully developed over the past decade to meet the challenge of al-Qaida and its cohorts. Ultimately, it is these crime-prevention tools—along with police professionalism, training, and wealth of real-world experience—that will make America's police forces the nation's most valuable homeland-security assets.

Counterterrorism in the United Kingdom: The Leading Edge

The United Kingdom has decades of experience in effective counterterrorism strategy and tactics, most significantly in response to attacks initiated by the IRA and its various splinter groups. As a result, the primary agencies in the United Kingdom responsible for collecting intelligence and safeguarding the public from al-Qaida and other violent extremist groups—MI5, MI6, and the fifty-two U.K. police departments with their Special Branch offices[1]—remain on the leading edge of counterterrorism best practice and constitute a valuable resource for their counterparts in the U.S. and elsewhere.[2] Perhaps even more important, police forces in the U.K., unlike in the U.S., have significantly more experience in counterterrorism operations than their American counterparts.[3]

On June 3, 2004, the Manhattan Institute and the Police Institute at Rutgers University convened a conference of municipal police chiefs and high-ranking officials from state Departments of Homeland Security along the I-95 corridor of the eastern United States to hear presentations from leading U.K. officials tasked with planning and disseminating counterterrorism "best practice" advice to the U.K. police departments and private-sector organizations at high risk for terrorist attack.

What Police Need to Know: An Evolving Threat from a Determined Enemy

Terrorism dates practically from the invention of dynamite, and many Western nations are all too familiar with groups promoting political change through violent means—for example, the IRA, the Beider-Meinhoff Gang, and Basque separatists (ETA) in Spain. Still, it should be noted that the threat from al-Qaida and other international Islamist groups is different in scope and in kind from previous threats faced by Western nations. For instance, the IRA in the 1990s carried out its operations through a relatively well-defined geographic corridor in the U.K. that could be monitored to an appreciable degree. The IRA was also focused on a political agenda that did not emphasize mass civilian casualties; often, IRA large explosive attacks were preceded by warnings to local authorities that allowed them to evacuate targeted areas. In short, however dangerous the IRA was (and it remains very dangerous), its attacks evinced a certain logic and predictability that mitigated the lethal consequences of its attacks.

In contrast, al-Qaida and its offshoots operate comfortably in a global theater that makes their movements highly unpredictable. Al-Qaida in particular has created a sophisticated, diffuse, and skilled network of covert operatives that can blend into immigrant communities in Western nations and remain dormant for months or years before carrying out their attacks. Their motives are global and ideological rather than local and nationalistic and thus are not amenable to political persuasion or compromise. Their favored modus operandi are spectacular suicide attacks that seek to inflict mass civilian casualties and disrupt the critical national infrastructures that sustain democratic societies.

September 11 taught law-enforcement agencies in the U.S. that in order to respond to this new threat effectively, they would have to expand their mission portfolio in unprecedented ways—primarily because police departments in the U.S. have not traditionally seen themselves as part of the national security apparatus. Whatever the exact relationships that exist between the FBI, CIA, and local police (now and in the future), police will always bear a significant responsibility for terrorism prevention

and response in the event of an attack. Our colleagues from the U.K. emphasized that police departments are in the best position to:

- identify and protect local and regionally important vulnerable sites
- develop intelligence leads based on targeted criminal investigations and community policing programs
- create security partnerships with private industry and commerce in high-risk areas or industries
- use reality-tested crime analysis and crime-prevention technologies such as CompStat, Automatic Number Plate Recognition, and community policing to interdict terrorist planning and funding operations

Some of these missions—for instance, protecting critical national infrastructure (CNI) will be new to American police forces. Others, such as using CompStat to target criminal activity with potential terror links, build on well-honed police capabilities. But all of them depend on police departments thinking of themselves as valuable and proactive assets in the struggle to defeat, deter, and, when necessary, recover from terrorist attacks.

American police departments are just beginning to understand their new roles and adjust to them. The bad news is that there is much to learn, and not much time to learn it. The good news is that much of what U.S. police departments must learn will build on well-honed crime-prevention and public communication skills that play to their unique strengths in the American civil justice system.

It is no exaggeration to say that large urban police departments in particular are well suited to the complex task of counterterrorism because of their deep involvement in and familiarity with local communities; ability to gather intelligence on complex criminal operations; and, most important, their long-standing experience in deterring, investigating, and prosecuting crime through reality-tested methodologies.[4]

Creating a Hostile Environment for Terrorism

The U.K. police focus on creating a hostile environment for terrorists to operate within. This means embracing a dual strategy of effectively targeting crimes and behaviors associated with terrorist activities and developing a public communications strategy that can make the public an effective partner in counterterrorism intelligence gathering.

The first half of this strategy, crime prevention and analysis, means using CompStat technology[5] and other database tools that can specifically target the ancillary crimes associated with terrorist activities and allocate police resources to prosecute those crimes effectively.

Police can bring tremendous leverage to bear on this front because terrorists do not operate in a logistical vacuum. They do not typically enter their host countries with access to large amounts of hard currency and therefore must engage in a wide range of illegal activities to finance and prepare for their operations. Consequently, they will have been taught at terrorist bases in Afghanistan and elsewhere how to abuse the welfare systems in Western nations, engage in credit-card fraud, and

traffic in forged and stolen documents. They will also often sell counterfeit goods. In short, they will create a long trail of preliminary crimes that police can use to dismantle their operations. If the police are aware of these linkages and factor them into their everyday crime-prevention activities, they can disrupt terrorist networks at their roots. Criminal activities engaged in by terrorists include but are not limited to:

- credit-card fraud
- counterfeiting
- ID theft
- narcotics trafficking
- welfare fraud
- smuggling[6]
- money laundering

Successful prosecution of these crimes includes effective intelligence sharing not only between state, federal, and local agencies, but with the cops on the beat and their supervisory officers. Every officer in the department, when stopping a car, spotting a fake ID, or uncovering a counterfeiting ring, needs to think terrorism first.[7] It has to become part and parcel of every officer's decision-making process when he or she is prosecuting criminal activities that could be linked to terrorists.

The next critical step in creating a hostile environment for terrorists is developing a public awareness strategy that gives citizens a forum for reporting particularly suspicious behavior to the police when it happens. For instance, the London Metropolitan Police have initiated an ongoing campaign to educate the public on a few simple, but critical indicators of terrorist activity. They remind the public that terrorists need:

- *Places to live*—Experience shows that these types of places are often rented on a short-term basis. If you are a landlord or hotel manager, do you have any suspicions about your tenants or guests?
- *To plan and prepare*—Terrorist attacks around the world have involved a great deal of planning and preparation. Have you seen someone paying an unusual amount of attention to security measures at a location, e.g., a major financial or government institution, a shopping center, or part of the transportation network?
- *Vehicles*—Cars and trucks have been used to devastating effect in terrorist attacks around the world. Terrorists also need to move around. If you are a car dealer or rental agency, do you have any suspicions about the persons you sold or rented a car, van, or truck to? Did they pay in cash or otherwise act secretively? Did the purchaser seem to make any attempt to conceal his or her identity?
- *Money*—Terrorists need money to live on and to fund their activities and often raise this by committing check and credit-card fraud. Individuals may create identities to set up bogus bank accounts, then acquire checkbooks to buy goods that are later returned to stores for cash refunds. Credit cards are also cloned and used to buy goods that can later be returned for cash or sold. If you are a retailer, do you have any cause to be suspicious?[8]

- *Rented storage*—Terrorists have used short-term and secure storage accommodation to keep their munitions and bomb-making equipment. Do you have any suspicions about the materials being stored or the activities of the renters?

By targeting the crimes associated with terrorist funding and helping raise public awareness of how terrorists prepare for their operations, police can go a long way toward creating a hostile environment for terrorists without disrupting the lives of law-abiding citizens. The U.K. police have focused on finding ways of increasing the likelihood that terrorists will come into contact with law-enforcement officers, either through targeted operations or through intelligence gleaned from the public.[9]

Protecting Critical Infrastructure and Creating Partnerships with Private Firms

One new, and widely heralded, component of counterterrorism efforts in the U.K. has been the installation of full-time, dedicated counterterrorism security advisors (CTSAs) in every U.K. police force. The National Counter Terrorism Security Office train and support CTSAs in delivering intelligence on emerging threats to the business sector and providing advice on counterterrorism best practices. Their advice relates to such matters as:

- dealing with bomb threat telephone calls
- building searches and evacuation
- contingency planning for terrorist incidents
- dealing with suspect packages
- physical building and location security
- protection of key assets
- terrorist acquisition of materials

By designating the equivalent of a full-time CTSA, American police departments can allocate staff to disseminate intelligence and help promote "best practices" to private-sector firms, particularly firms dealing with CNI or businesses in high-risk areas such as financial districts. The CTSAs provide a focal point of contact and advice for such organizations.

Working successfully with private firms to detect, deter, and respond to potential terrorist incidents depends on cultivating trusted contacts at private firms and developing channels for regular communications. For instance, in London the Metropolitan Police hold regular briefings for key members of the business community to discuss potential threats and provide guidance on appropriate security measures. They have also created a wider e-mail and pager alert program that can, when needed, provide several thousand key business personnel in London with real-time instructions in the event of an attack or suspected attack. Both these measures have helped facilitate intelligence sharing between the police and the private sector and helped coordinate effective contingency plans in the event of an attack.

Obviously, police-business partnerships are particularly important in the area of protecting CNI. In the U.K., the CTSAs have been tasked with helping to identify new vulnerable sites post-9/11 for increased security advice as well as police protection and response. This is because U.K. policymakers have recognized that, in a modern economy, technology and business relationships change so rapidly that there is a real need for local and regional advice on potential vulnerabilities. Once these vulnerabilities have been identified, the police should identify "trusted contacts" at these sites who will receive more classified intelligence information than is available to the general public and who can work closely with the police to develop contingency plans in the event of an attack. This is a continuation of the work undertaken by MI5 following the IRA attacks against the economic infrastructure in the 1990s.

Broadly speaking, the U.K. has designated a number of sectors comprising CNI, and the police can use this as a template (together with advice from other central government and local agencies) to develop their own lists:

The sectors include:

- Communications
- Emergency Services
- Energy
- Finance
- Government and Public Service
- Transport
- Water

Of course, no level of government—national, state, or local—can ever deploy enough resources to protect every potential terrorist target. Worse, when forces are deployed too thinly, there is a risk that truly essential sites will not receive the protection that they deserve. As a result, MI5 and the National Counter Terrorism Security Office, along with representative government departments in the U.K., have developed a fairly stringent set of guidelines for classifying such sites. U.K. CNI sites are identified as being critical to national economic or social survival, whereas other sites are identified, for example, as being either attractive to terrorists because of their materials held or the status that they hold nationally or locally. Police in the U.S. should find these subdefinitions helpful in categorizing their own local CNI lists:

Economic Sites: Installations or systems are selected for additional protection and advice if it is assessed that the loss of the products or services from this site would have widespread and critical economic consequences to the U.K.

Vulnerable Sites: Facilities that if attacked or exploited would give terrorists the ability to acquire materials or generate mass casualties. This category includes sites where chemical, biological, radiological, or nuclear materials are available. It also includes certain iconic/tourist locations.

Further advice is available through the National Counter Terrorism Security Office. E-mail: nactso@btopenworld.com.

Obviously, each of these subcategories requires a different security approach. Vulnerable sites may require more traditional "target hardening" measures, including plans for evacuation or containing the hazard in the event of an attack. On the other hand, making economic sites less vulnerable

should include building redundancy into the system in addition to increasing security, so that even in the event of a "successful" attack, the plant or facility could reroute at least some of its commodities to another facility or system to continue operations.

Police and on-site security managers will not often be able to offer protection to the entire facility. However, by working together with site managers, police should be able to conduct additional analysis and identify key points at the facility that are critical to the survival or protection of the site and protect those areas accordingly.

As suggested above, once the police have identified CNI facilities, they must create ongoing working relationships with these sites through "trusted partners" within the organization with whom they will share intelligence, develop contingency plans, and coordinate operations in the event of an emergency. Police should not be hesitant to involve other relevant agencies in contingency planning—for instance, the local fire and health departments—when they are faced with a site that contains a hazard that is outside their area of competence. Once police have established trusted contacts, reviewed and responded to potential vulnerabilities, and established contingency plans, they should exercise and update those plans on a regular, predetermined basis to ensure that they remain current.

An additional advantage of remaining proactive in the identification and protection of local CNI sites is that these relationships will be valuable in a wide range of scenarios in which the police will be expected to respond—bomb hoaxes, natural disasters, or even severe technological malfunctions (e.g., blackouts). No matter what kind of incident occurs, if the police have credible emergency-response plans in place for local critical infrastructure sites that they have drilled on regularly, they will be in a much better position to react and lessen the inevitable strain placed on their own officers and other emergency responders.[10]

Business Is the New Target

Of course, CNI is not the only target. Police need to be aware that business institutions and financial districts—for psychological reasons as well as economic ones—have become the targets of choice for international terrorists. Terrorists understand the dependence of Western countries on economic and financial networks and are committed to disrupting or destroying those networks. According to the Congressional Research Service, in 2003 67 percent of anti-American attacks worldwide were against American businesses.[11]

More recently, the capture of a high-ranking al-Qaida operative in Pakistan led the Department of Homeland Security to issue specific security warnings for the New York Stock Exchange and the Citigroup headquarters in Manhattan; the Newark headquarters of Prudential Financial, Inc.; and the Washington offices of the World Bank and the IMF. Police operating in American cities with significant business or financial centers will likely have many similar targets within their jurisdictions. Undoubtedly, the hardening of targets in Washington, D.C., and the New York metropolitan area are likely to redirect terrorists toward other high-value targets in localities that are seen to be more vulnerable.[12]

In order to deter these attacks, police should first conduct an analysis of the business assets within their jurisdiction to determine which are most likely to be viewed as high value (either

economically or symbolically) by terrorists. Then they must conduct a vulnerability analysis of potential targets. Which are protected, and to what degree? All police departments, even in rural localities, should invest the time to create a list of potential targets and assess their vulnerabilities.

Once they have established a threat list, they should establish ongoing partnerships with security managers and senior business managers to monitor security and exchange intelligence on presumptive threats. Police, however, should always be aware that private firms that may be outside the CNI sector are likely to be leery about increasing resources devoted to security without clear rationales for doing so. As such, the police should be very forthright about disclosing potential threats to business partners as soon as they become aware of legitimate concerns.

However, after having created an ongoing relationship, police can take advantage of the fact that terrorists will conduct extensive reconnaissance on their targets in preparation for an attack. They will probe business security procedures and infrastructure to look for weaknesses. They may attempt to secure employment at private firms to facilitate access and better explore vulnerabilities. All these tactics will bring them into contact with private security or business managers, *not* with police personnel. By keeping businesses apprised of terrorist tactics, reviewing and updating security and employment practices, and exchanging timely intelligence with financial institutions, the police can make them much more secure and resilient. Besides working on specific measures unique to particular targets (for instance, CCTV or glazing windows to resist bomb blasts), police should encourage businesses to take the following general precautions:*

1. Businesses should conduct a reasonable **risk assessment**. What kind of threats might the firm face? What is the likelihood of these events happening? Where, on premises or through your IT systems, are your vulnerable points?

2. Target hardening from building design onward. When at all possible, police should encourage firms expanding or constructing new facilities in their jurisdiction to **plan security measures from the outset**. This is likely to make target hardening more efficient (in time and expense) and effective than adding more security on an ad hoc basis later.

3. Police can work with businesses to make **security awareness** part of the firm's ongoing routine. Firms should task a senior manager or head of security to liaison with police and distribute police briefings to critical members of the firm. This should help ward off complacency and keep private firms confident that they are receiving credible information on a real-time basis.

4. Police can encourage firms to implement **crime prevention** measures by ensuring that perimeters around the firm's location are clean, well lit, and devoid of any obstructions that make the target more vulnerable to terrorist or criminal activity.

5. Firms must be reminded that **access points to their premises should be kept to a minimum. Access control is a key feature of security.** Firms that have not done so should consider introducing passes for employees and procedures for booking in visitors and contractors. Searching of bags may also be desirable but, as with other measures, should be proportionate to the threat and also carefully explained to staff. Firms should also look carefully at vehicle access and parking arrangements for vendors and employees. High-risk targets should consider

introducing a barrier system and arranging that garage or parking lots are located so that unauthorized vehicles cannot get close to the premises.

6. Police can advise firms on which **physical measures** for building security may be most effective and appropriate—locks on windows and doors, CCTV, alarms, or improved lighting—and install them according to context and need. Firms should ensure that physical countermeasures are working by examining them on a regular basis.
7. Firms should implement security procedures for **mail handling**. High-risk targets should consider setting up a mail room away from their main premises and train staff in emergency procedures.
8. When **recruiting staff** or hiring contractors, ensure that they are who they say they are by checking documentation. Private firms and police can work together to check terrorism watch lists for employees who have access to sensitive areas or materials.
9. Firms should also set up firewalls and other electronic measures to **protect critical information and vital IT systems**. Firms must ensure that those who supply, operate, and maintain IT systems are reputable and reliable.
10. Police can encourage private firms to construct **business continuity plans,** designating how the firm will continue to function if something happens that destroys or degrades critical systems or facilities or prevents access to its site/office. Realistically, for some firms this may be the only measure that they can undertake.[13]

*This information was adopted from the MI5 website www.MI5.gov.uk. More information on this and other security and business continuity issues can be found at http://www.mi5.gov.uk/output/Page167.html.

As noted previously, security is very expensive, and businesses even in high-threat areas may be reluctant to incur large ongoing expenses for an indefinite period of time. However, police can encourage businesses and building owners that are located at or near high-profile targets to form working groups to share information, diffuse security costs, and implement best practices without disgorging vital trade secrets. Even competitors within an industry are apt to recognize that terrorists are their common enemy and that an attack on one facility or building—as in the World Trade Center attack—can impair or disable surrounding firms if they have not prepared adequately for these types of events.

Canary Wharf, in London, is one example of a leading global financial center where businesses have joined together to share security costs and explore ongoing methods to improve common security. The Canary Wharf Group[14] has reviewed procedures for simultaneous building evacuation at One Canada Square (home to major banking and media firms), practiced a mass evacuation of a fifty-story tower, and used computer software to model the best escape routes from buildings. As evidenced on September 11, planning and evacuation drills can be critical in minimizing the loss of life from a terrorist attack and should be emulated at all other high-risk targets.

Police and private firms should also develop evacuation planning that takes account of several different contingencies (for instance, in response to a radiological or "dirty" bomb, as opposed to

conventional munitions) and plan accordingly. Police should also compile (and update regularly) lists of key personnel at private firms in high-risk areas to contact in the event of an emergency in order to coordinate business responses ranging from immediate employee evacuation to defending in place.[15]

As mentioned earlier, in the unfortunate event that police and businesses are unable to deter an attack, business continuity plans will enable firms to resume normal business operations as quickly as possible. Unfortunately, many businesses seem blithely reliant on the police or other law-enforcement agencies to prevent attacks and few have developed adequate business continuity plans. According to one British study, 80 percent of large businesses in London had some form of continuity plan. Nonetheless, 20 percent of blue-chip companies did not. Even more worrisome, 83 percent of medium-size businesses—with between fifty and 500 employees—did not have a business continuity plan. While these businesses may not be economically critical taken individually, they are often key suppliers for larger firms, and disabling two or three medium-size firms may have the same effect as disabling a large corporation.

Although it is, obviously, not the responsibility of the police to ensure business continuity, financial districts are linchpins in many urban economies, and ensuring that they return to normal operation as soon as possible is critical to protecting national infrastructure.[16]

In the final analysis, building successful police-business counterterrorism partnerships is about establishing trust and avoiding complacency when the threat is murky and highly unpredictable.

Integrating Crime Prevention and Counterterrorism Strategies: A U.K. Model

In the U.K., the British Transport Police (BTP) are responsible for the safety of passengers and cargo on 10,000 miles of track, comprising some 3,000 stations. This task seems scarcely possible for the 2,000-man force, which has a budget of only £162 million.

However, the BTP has managed to leverage its effectiveness through crime-prevention strategies; building effective partnerships with the private firms that operate the railways; and the efficient use of available crime-prevention technologies and computerized threat analysis. Naturally, the same systems that are deployed to reduce theft, sabotage, and vandalism can be used to deter, detect, and respond to terrorist attacks. In short, the BTP is an admirable model of how to protect CNI with limited resources.

Secured by Design

Crime-prevention technologies and principles are best deployed when a system or site is being designed—not when it is already in operation. Retrofitting can be very expensive and time-consuming. Police should also be cognizant of the fact that CNI sites may be operated by private firms dependent on the ongoing generation of revenues from the site in question.

However, persuading a private firm in a CNI sector to employ crime-prevention principles and technologies is possible by reminding the firm that crime prevention is a loss-control mechanism that adds value to the system by securing and protecting valuable assets—including the firm's

reputation for safety and reliability. When analyzing the need for designing in security, called "crime prevention through environmental design," the police should ask project managers to carefully consider the following at the design stage:

- What exactly are you protecting?
- What could be vulnerable? What is vulnerable?
- When do you start protecting your investment?
- What finances are available for security measures?
- How do you protect your investment?

Answering these questions at the design stage will make site security more effective and less expensive in the long run. The BTP have learned through experience that crime-prevention technology, no matter how attractive in the abstract, should only be deployed when there is a real operational requirement, its role is well defined, and it can be effectively managed. Once security management at the site has been tasked into the chain of command, there are several practical design questions than can be employed to improve the safety of the local environment:

- Are there clear sight lines around the facility that will allow for easy monitoring of the surrounding premises, including exit and entry points?
- Is there sufficient lighting at the premises to deter attempts at unauthorized entrance or the placing of unauthorized items?
- Does the landscaping plan help to protect the site, or does it make it more vulnerable?
- Is a fence or other perimeter protection needed?
- How easy or difficult is it to gain entrance to the roof? Is the roof monitored in any way?
- Where is the parking lot or garage located? Is it monitored?
- Have the premises been constructed to resist attacks and minimize casualties—through reinforcement of load-bearing structural elements, glazing for windows, and so on?

Once these questions have been answered, the CNI firm and the police can work together to identify the systems that can best improve security—for instance, CCTV, perimeter intrusion-detection systems, alarms, video motion detection, and access-control systems. While the police are, obviously, not going to install or monitor these systems, they can provide advice on what works and how security systems can best be managed to deter crime.[17]

Finally, the police should work hard to develop good community relations in the area where the CNI site is located. By interacting with residents of the neighborhood and helping to create an orderly atmosphere near the site, the police can help deter crime as well as potential acts of terrorism.

Of course, target-hardening measures can only provide so much deterrence, particularly for premises like office buildings, train stations, or other structures that are insecure by definition. Instead, police officers must develop the ability to sort out real threats (the briefcase or luggage bomb) from trivial ones—hoaxes and misplaced laptops.

In the British railway system, there are some 250,000 misplaced items annually. Shutting down a train station every time someone leaves his laptop case on a train is obviously not an option. As a result, it is critical for police to develop procedures for categorizing suspicious incidents (for instance, of persons taking an untoward interest in building design or security measures) and items on relatively short notice. This will inevitably entail developing a program of risk management—deciding what level of insecurity the premises (and police) will tolerate and what level or type of incident will bring about a robust response by police or other security personnel (for instance, evacuation of a building or station). The BTP have been remarkably successful at this. In 1992, 20 percent of incidents involving the discovery of unclaimed luggage or other personal items at train stations in London resulted in a full evacuation. In 2002, this ratio had been reduced to less than 1 percent. However, since information on threat-analysis technologies is classified, police with further questions about BTP procedures and response should contact the British Transport Police directly.[18]

Since attacks on trains have become an item of particular concern after the Madrid bombings on March 11, 2004, we have included the following guides for police on securing railway premises.

Secure Station Planning: The BTP Scheme**

Government research shows that passengers on public transport are most concerned when waiting at stations. To combat this, the government, the British Transport Police, and Crime Concern have launched the Secure Stations Scheme, which encourages Britain's rail companies to improve security at stations and to reassure customers of their commitment to passenger safety.

The national scheme covers all aboveground and underground rail stations (across England, Scotland. and Wales) that are policed by the British Transport Police (BTP). It has established national standards of good practice in security and accredits individual stations that have worked with the BTP and other local partners to implement a package of security measures. These include the following:

Design

Good lighting and secure fencing in station, parking lots, and surrounding entrances and exits
Up-to-date information and clear signs for the public
Clear lines of vision

Management

Security staff presence / CCTV surveillance
Rapid response in emergencies
Regular inspection and maintenance
Special training for staff to deal with conflicts and emergencies

In order to achieve the designation of "secure by design," railways also have to conduct an independent passenger survey to see whether passengers actually feel safe at the stations and provide evidence of low crime rates over a sustained period. American police and other municipal authorities can add value to public transportation by using the secure-by-design model to increase

public confidence in the use of public transport system, reduce overall crime on the railways and subways, and increase the use of public transport.

**Taken from http://www.securedbydesign.com/guides/stations.asp.

Communities Defeat Terrorism

It should also be noted that there is a real danger that, in the campaign against terrorism, Muslim citizens in Western societies will feel themselves unjustly persecuted. The U.K. police have responded to this problem by working hard to build effective liaisons within Muslim immigrant communities. American police officers can also help ameliorate feelings of isolation and suspicion by using community policing techniques to develop relationships between community leaders and local precincts. American police officers, perhaps uniquely among law-enforcement and intelligence agencies, possess the ability to put a human face on America's counterterrorism operations and demonstrate that operations against terrorists do not pose a threat to the civil liberties of law-abiding immigrants.

Furthermore, in America's federal law-enforcement system, the police may not have access to the kinds of day-to-day relationships that develop in the U.K., where local police departments, Special Branch, and national intelligence agencies are in constant contact. As such, police must be proactive, not reactive, in building their own relationships. Police should form call lists and cultivate personal contacts with as many federal and state agencies as possible in their area—for instance, the JTTF, National Guard, FEMA, CDC, and state police. This will facilitate the creation of personal contacts and unofficial channels that build trust and working relationships before a crisis develops, not in the midst of one.

In conclusion, the task facing American police is not so much incorporating new tactics or technologies (although there is certainly much training to be done regarding WMDs) but in incorporating the counterterrorism mind-set into how they approach their everyday operations. This simple strategy—implementing counterterrorism planning, intelligence gathering, and community partnerships into existing police crime-prevention and response procedures—will go a very long way toward making America's communities hostile places for terrorists to operate.

Endnotes

[1] Every police department in the United Kingdom has a "Special Branch" department—ranging from only a few officers in some regional offices to several hundred (at the London Metropolitan Police)—whose primary duties are prosecuting and assisting in counterintelligence and counterterrorism operations. They liaison directly with MI5 (the Security Service) and MI6 (the Special Intelligence Service).

[2] The U.K. has a much flatter structure with fewer police forces and agencies than the U.S., and it has also pursued closer cooperation, integration, and trust between agencies in its work to combat terrorism. There has been a process of evolution rather than revolution, which grew through lessons learned and careful consideration. The U.K. also is keen to apply standards to much of its work in the field of counterterrorism, whether it is the training of K9 dogs or the type of lock or fence guarding a particular site.

[3] This is primarily because of a difference in the national security structures of the U.S. and U.K. In the U.K., the primary agency tasked with counterterrorism operations, MI5, has no executive authority, and there is no national police force per se, i.e., there is no FBI. As a result, MI5, by necessity, must work with local police departments through their Special Branch offices to prosecute terrorism and counterintelligence-related investigations.

[4] We also should not overlook the fact that the FBI employs just under 12,000 agents nationwide. The combined state and local police officers in the U.S. number approximately 650,000, with the New York City Police Department alone having more than 38,000 officers. As far as "boots on the ground" go, police departments have a significant force advantage over federal agencies in their local jurisdictions and thus a far expanded capacity to collect intelligence and instigate counterterrorism investigations.

[5] At the New York City Police Department, "the CompStat Unit generates electronic pin maps of crime locations citywide; analyzes geographical locations of shootings, homicides, and other major crimes; monitors pattern crimes; develops advanced computerized crime-tracking methods; and provides briefing/presentation materials for the Police Commissioner. In addition, the CompStat Unit gauges the crime-fighting effectiveness of field commands by monitoring arrest activity, responses to pattern crimes, bias crimes, and the implementation of crime strategies."

[6] Cigarette smuggling has become a particularly lucrative criminal operation. Federal authorities believe that millions of dollars in illegal cigarette sales are being funneled to al-Qaida and Hezbollah through these smuggling rings.

[7] Two days before 9/11, United Airlines Flight 93 hijacker Ziad S. Jarrah was stopped by a Maryland state trooper for a speeding violation. Jarrah was on a CIA terrorist watch list, but this information was never conveyed or available to the Maryland State Police.

[8] Adapted from the London Metropolitan Police Life Savers campaign, available online at http://www.met.police.uk/campaigns/anti_terrorism/march.htm.

[9] Public communications should also be segmented into several different components. First, it involves media relations and making the media an effective partner in conveying security information. Second, the police must educate the public about the threat that they are facing, how to take appropriate safety measures, and how they can send tips to the police. The police should also make counterterrorism outreach the subject of community policing meetings and talks at schools and other public institutions. Police should go to trade associations and conventions (for instance, for car- and truck-rental firms) and discuss how terrorists can exploit these firms and emphasize what

vendors should watch out for. Finally, the police should be aware that terrorists themselves are listening to these public-service announcements and will react to them, i.e., the police can use communications as an effective terrorism deterrent by making terrorists aware that high-value targets are extensively monitored and protected. Pushing terrorists away from high-value targets in heavily populated areas can help minimize casualties.

[10] These are training opportunities with real-world implications. As such, the police and site-security managers should always conduct after-action reviews and incorporate the lessons learned. The police should also widely disseminate after-action reviews to local emergency-response agencies.

[11] *The Department of State's Patterns of Global Terrorism Report: Trends, State Sponsors, and Related Issues*. Congressional Research Service, June 1, 2004. Available online at http://www.fas.org/irp/crs/RL32417.pdf.

[12] Of course, the psychological value of striking New York and Washington will ensure that they remain at high risk for terrorist attacks for the foreseeable future.

[13] It should also be noted that many, and perhaps all, of these measures have positive business implications for firms that undertake them, i.e., they reduce business vulnerability to liability suits, theft, corporate espionage, accelerate firm recovery time in the event of a natural disaster, and may lower insurance premiums. Police should take the time to make the business case for these measures to ensure that firms and their security managers can justify security improvements to their board and shareholders.

[14] Comprising ten office buildings on an eighty-six-acre business complex housing some 6 million square feet of office and retail space with more than 60,000 occupants.

[15] The police must have a communications system (e-mail, fax, or phone) in place before an emergency occurs, be able to quickly identify and categorize the type of event(s) that they are facing, inform the business community of any necessary information, and then respond according to prearranged contingency plans.

[16] More information on business continuity is available online at http://www.londonprepared.gov.uk.

[17] There is, of course, the risk of a real or apparent conflict of interest when police recommend particular vendors to private firms. Police can avoid this conflict by encouraging federal agencies, the U.S. Chamber of Commerce, or other industry associations to draw up lists of approved providers that meet preestablished third-party certification and technical standards. In the U.K., for instance, the National Counter Terrorism Security Organization can provide firms with technical security standards that they can use to evaluate security vendors. The U.K. Association of Chief Police Officers (APCO) has also established ACPO Crime Prevention Initiatives Limited (APCO CPI), a nonprofit "company [that is] funded through partnership with companies whose products meet technical standards identified by ACPO CPI." More information on APCO CPI can be found at http://www.securedbydesign.com/about/index.asp.

[18] For more information, contact Vincent Smith, Inspector, Force Crime Prevention Officer, British Transport Police at (011) 44.207.830.8994 or via e-mail at vincent.smith@btp.pnn.police.uk.

MANHATTAN INSTITUTE FOR POLICY RESEARCH

52 Vanderbilt Avenue • New York, NY 10017
212.599.7000 • www.manhattan-institute.org