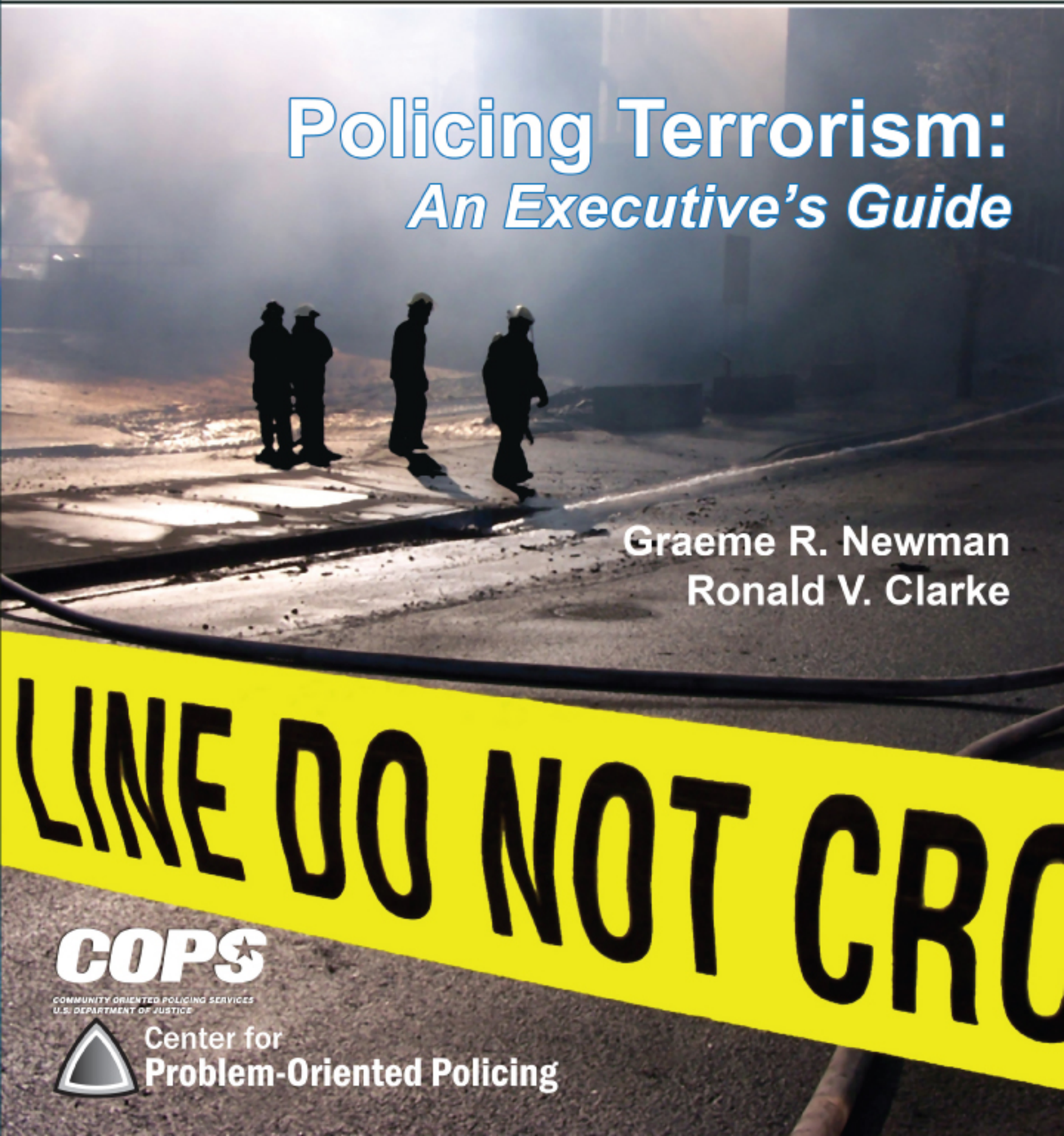
U.S. Department of Justice
Office of Community Oriented Policing Sevices

Policing Terrorism:
An Executive's Guide



Graeme R. Newman
Ronald V. Clarke

COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE
Center for
Problem-Oriented Policing

Policing Terrorism:
An Executive's Guide

By Graeme R. Newman and Ronald V. Clarke

This project was supported by Cooperative Agreement Number 2007-CK-WX-K008 awarded by the Office of Community Oriented Policing Services, U.S. Department of Justice. The opinions contained herein are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific companies, products, or services should not be considered an endorsement by the authors or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

The Internet references cited in this publication were valid as of July 2008. Given that URLs and web sites are in constant flux, neither the authors nor the COPS Office can vouch for their current validity.

Letter from the Director

Immediately after September 11, 2001, I convened a meeting with the heads of the five major executive law enforcement organizations in the United States. Those leaders told me that community policing was now more important than ever. Since then, the Office of Community Oriented Policing Services (the COPS Office) on numerous occasions has brought together federal agencies, representatives from the private sector, law enforcement leaders from around the country, including campus public safety and tribal police, to explore creative solutions to violent crime and the persistent threat of terror. In each of these discussions we were continually brought back to the central role that community policing principles play in preventing and responding to the threats of terrorism.

Since 9/11, state, local, and tribal law enforcement agencies have been tasked with a variety of new responsibilities. The workload of already busy departments has significantly expanded to include identifying potential terrorists, protecting vulnerable targets, and coordinating first response. Whether you are a small town or a large city, as chief, it is your responsibility to ensure that plans are in place to prevent attack and to respond quickly should an attack occur. This manual, dedicated to police executives, sheriffs, and other senior executives, will help you meet the new challenges involved in countering the threat of terrorism. It clearly articulates and summarizes writings on the essential components of a counterterrorism plan.

Renowned authors Graeme Newman, Distinguished Teaching Professor at the University of Albany, State University of New York, and Ron Clarke, University Professor at Rutgers, the State University of New Jersey, offer 50 briefs for preventing terrorism that will prove useful to your agency. Although we believe that the manual will be of use to agencies of any size, it will be particularly relevant to small and midsize police departments who have much more limited resources to devote to terrorism prevention and response. This guide will help agencies develop priorities for their efforts and prepare reasoned and sustainable responses to cope with these additional responsibilities.

After many years in law enforcement and nearly 7 years as the Director of the COPS Office, I have yet to see a successful and sustainable crime-reduction and terrorism-prevention strategy, consistent with our democratic values, that fails to build partnerships with citizens and embraces problem-solving principles. Community partnership and problem-solving in policing are not relics of a bygone era. They're as modern as the war on terror and as current as today's headlines.

After visiting the tragic scene of the 2005 London bombings, the BBC quoted Los Angeles Police Department Chief Bill Bratton as saying:

> *In dealing with serious international crime you need to focus on the community. If police do not have relationships with the communities in a city as ethnically diverse as London, the game is over, we will always be playing catch-up.*

In commenting on the same terror attack, Sir Ian Blair, the Commissioner of Britain's Metropolitan Police said:

> *It is not the police; it is not the intelligence services that will defeat terrorism. It is communities that will defeat terrorism.*

In fighting crime and in securing our homeland, many approaches will be tried and many strategies and solutions will be offered. That is a good thing because we must remain vigilant and always resist the complacency that shadows any long struggle. Nevertheless, as we constantly seek to make our communities safer and more secure, we must hold on to those fundamentals that we know work. We must maintain an unflinching concentration on the immediate causes of the problems we seek to solve, partner with those who can best help us solve them, and align our organizations to better combat those things that most threaten the domestic tranquility of our nation. This manual is intended to help you do just that.

Carl Peed, Director
The COPS Office

Table of Contents

V. Harden Targets

VI. Be Ready if Attacked

Acknowledgments

There is a danger that a manual such as this, written by two academics, might be disconnected from the real life of policing. We have tried to avoid this pitfall, and if we have, much of it is due to the help, assistance, hospitality, and openness of members of the Anaheim (California) Police Department whom we approached early in preparation of this manual. Those who helped us were Chief John Welter, Investigator Christopher Schneider, Lieutenant Chuck O'Connor, Lieutenant David Vangsness, Sergeant Brian McElhaney, and Sergeant James Wilkes. We were also introduced to Thomas J. Wood, Assistant City Manager of the City of Anaheim, who gave us a valuable insight into homeland security issues confronting this mid-sized city, and to Sergeant John Hargraves, Sheriff's Department, County of Los Angeles, Emergency Operations Bureau, who gave us an overview of the operations center. We also gained important insights into the problems facing the private sector in dealing with terrorism from Damion Ellis, Assistant Director of Security and Safety, Hilton Anaheim; Bernard E. Heimos, Guest Relations, Marriott Hotel, Anaheim;and from John J. Amabile, Operations Manager, Resort Security Operations, Disneyland.

We are indebted to the helpful comments of Gary Cordner, John Eck, George Kelling, and Nick Ross; to the anonymous reviewers who aided us in clarifying our message; to Mike Scott, Director of the Center for Problem-Oriented Policing, who not only carefully reviewed the manual, but supported our endeavors over the long period it took us to produce it; to Jon Shane who offered excellent practical suggestions and who drafted Brief 20; and finally to Phyllis Schultze, the pillar of our research, who could always find and provide us with the reading materials we requested.

“It has been said that 9/11 changed everything. This is certainly true for local police agencies and their chiefs.”

Brief 01: Read This First

It has been said that 9/11 changed everything. This is certainly true for local police agencies and their chiefs. It is increasingly clear that federal agencies, such as the FBI and the U.S. Secret Service, can no longer work alone in protecting the United States from further attack. Rather, they must work in partnership with other public and private agencies, and most important, with local police. Local police can identify potential terrorists living or operating in their jurisdictions, they can help protect vulnerable targets, and they can coordinate the first response to terror attacks. These are heavy new responsibilities that significantly expand the workload of already busy departments. Many departments welcome these new responsibilities, but they cannot be shrugged off because elected officials and the public will increasingly expect their police to be prepared.

> *"Counterterrorism has to be woven into the everyday workings of every department. It should be included on the agenda of every meeting, and this new role must be imparted to officers on the street so that terrorism prevention becomes part of their everyday thinking."*
>
> Source: Kelling, George L. and William K. Bratton, *Policing Terrorism, Civic Bulletin 43*, New York: Manhattan Institute for Policy Research, September 2006.

This manual is intended to help police executives and other senior executives meet the new challenges involved in countering the threat of terrorism by summarizing writings on the essential components of a counterterrorism plan. It does not deal with the specifics of such matters as (1) conducting surveillance of suspected terrorists; (2) protecting different types of vulnerable targets, such as ports and chemical plants; or (3) achieving interoperability in wireless communications among different disaster-response agencies, such as fire, police, and emergency medical personnel. Although junior officers need this type of detail, chiefs require more general information about a broad range of issues that can help them develop plans and policies to counter the terrorist threat. This manual seeks to meet the needs of chiefs and other senior personnel by summarizing information about 50 key topics in the form of advice to the chief.

You might feel that you have little need for this manual because your town is too small and insignificant to attract the attention of terrorists. You might well be right, if only because there are many thousands of towns and cities in the United States and terrorist attacks are rare. Some experts, however, believe that it is this very insignificance that might attract terrorists because an attack on an unremarkable and unexpected target might generate more fear—an important objective of the terrorists—than would one on an anticipated target. Whether this is true or not, you cannot take risks with the lives of people in your community: you must make plans to prevent an attack and to respond quickly and efficiently if one occurs.

Alternatively, you might think the manual of little use because you have already had some experience dealing with terrorism or have already undergone some counterterrorism training. You might also have staff capable of developing detailed counterterrorism plans; indeed, you might already have put many of the needed measures and procedures in place. Few of you, however, will be in this fortunate position. It is more likely that you have had no previous experience with terrorism, that you have not had any counterterrorism training, that you have not had time to study the reports and books on the subject, and that your staff lack the expertise to assist you in developing counterterrorism plans. Although the manual is likely to be of greatest help to those who fall in this latter group, we hope that even seasoned counterterrorism experts will find the manual useful in bringing some less-familiar topics and techniques to the fore.

"Counterterrorism has to be woven into the everyday workings of every department."

The manual comprises six parts.

I. Prepare yourself and your agency.

II. Understand the threat.

III. Develop a plan and a support network.

IV. Gather intelligence.

V. Harden targets.

VI. Be ready if attacked.

The first three parts consist of preparatory steps, while parts four through six cover in more depth the three essential components of a counterterrorism plan: (1) developing intelligence on possible terrorists; (2) identifying and protecting major targets; and (3) expanding disaster-response capabilities to encompass the response to a terrorist attack.

Each of the six parts, in turn, is divided into separate briefs that summarize discrete topics or techniques. We have tried to arrange these briefs in logical order, although in the first three parts we introduce some key topics that are developed more fully at the end of the manual.

The manual is short enough to read in a weekend, which would be worth doing, especially if you have little background in counterterrorism. You then should keep it at hand so that you can quickly refresh your memory on a particular topic. Those of you who are experienced in dealing with terrorism might be better served by browsing the Contents pages and reading only those briefs that you think might provide you with new information. Even experienced readers should keep it handy as a ready reference to guide them in their counterterrorism work.

Because most of you typically have little time for additional reading and might not have access to the specialized libraries that hold much of the available information, we have not referenced the manual as fully as an academic paper. Occasionally you might need more information than is provided in the manual; therefore, at the end of many of the briefs we have identified key reports and other publications that can be obtained relatively easily, often from the Internet. If you need help obtaining these references, feel free to e-mail either of us at the following addresses: gnewman@popcenter.org or rvgclarke@aol.com. Also contact us if you feel that the manual omits important information or if you think that some of the advice needs rethinking because of the rapidly changing nature of the field. This will help us in preparing future editions of the manual.

I. Prepare Yourself and Your Agency


LINE DO NOT CR

“After the initial shock of 9/11, you, like many other chiefs, might have begun gloomily to contemplate the future of policing.”

Brief 02: Embrace Your New Role

After the initial shock of 9/11, you, like many other chiefs, might have begun gloomily to contemplate the future of policing. At a stroke, terrorism had replaced crime as the greatest threat to the nation's social order and intelligence agencies had become society's principal guardians, usurping the role traditionally held by police. As the government scrambled to find money for new antiterrorism initiatives, cuts in federal funds for police programs underlined the changed status of policing. But quite soon things began to change again. Although crime-fighting funds did not return to previous levels, police leaders such as William Bratton and George Kelling began to argue for a greater police role in fighting terrorism for two reasons: (1) terrorism is not really much different from conventional crime and (2) local police are in the best position to learn about the emergence of local terrorist threats, to know which targets are most at risk, and to coordinate the first response to attacks.

To fill this role, some of you will have to make considerable changes. If you head a large department in a city with many recent immigrants and many attractive targets, you might have to make sweeping changes—more extensive than if you head, say, a small rural force in America's heartland. Whatever the case, you should embrace the changes because they are consistent with best practice in policing. They put a premium on prevention, on service to the community, on making full use of the data you collect, and on forming partnerships with other agencies and organizations. These practices will not only help you meet the threat of terrorism, but will also help you do a better job of fighting crime.

Crime and terrorism

Some commentators have emphasized the differences between terrorists and ordinary criminals, arguing that terrorists are motivated by a higher cause than criminals and that they are better trained and better organized. In reality, criminals vary greatly in their motivation and commitment. Some serial murderers, for example, plan their crimes just as carefully as any terrorist and are equally as determined to succeed. The differences between terrorists and criminals might be no greater than the differences between various types of criminals. Certainly there are many similarities between terrorists and organized criminals, especially those engaged in transnational crime. In addition, terrorists often commit ordinary crimes—robbery, drug dealing, fraud—not just in furtherance of an attack, but also to sustain themselves. From a policing point of view, there is much to be said for regarding terrorists as criminals with political motives.

Even so, you will need to learn some basic facts about terrorism. (See Part 2 of this manual.) It is particularly important not to accept unthinkingly many of the stereotypes promulgated by some media and politicians (see Brief 6). You will also have to commit resources to coping with some of the new demands that terrorism brings, including managing any terrorism grants that your department obtains. This might mean that you will need to establish and staff a terrorism unit or, for smaller agencies, an intelligence unit that focuses on crimes that contribute to terrorism.

Prevention and security (Briefs 19, 29–36)

Many policing initiatives, especially broken windows and problem-oriented policing, place as much importance on prevention of crime as on detection and prosecution. Given the potential loss of life that can result from a terrorist attack, prevention becomes even more important. Consequently, you will have to increase security at major events and increase patrols at ports, bridges, and other important infrastructure. You might also be asked to conduct security surveys and to provide target hardening advice at vulnerable sites. If so, make sure that the officers who undertake this work are appropriately trained.

Community policing (Briefs 27 and 28)

Like other chiefs, you might utilize community policing officers to foster communication with the residents of certain communities. By patrolling on foot and spending time talking with residents and local business owners, they are likely to learn about newcomers and to notice small changes in their neighborhoods. They are also likely to know responsible leaders in immigrant communities and would be in a position to ask for their help in watching for suspicious activity. These are among the many reasons for developing a community policing program, especially where the threat of terrorism has given rise to tensions between neighborhood residents and police. Special training and skills might be needed to adapt community policing to these new challenges.

Intelligence and information (Briefs 21–28)

In small agencies, information about suspicious activities probably passes freely among officers because they know each other. In larger agencies, however, it is possible that officers who work the same beat on different shifts neglect to share such information; thus, more formal methods of communication might be needed. Terrorism underlines the need for information sharing and, in fact, under the federal Information Sharing Environment (ISE) instituted in 2004, your department will be expected to share information both internally and with the state police, the FBI, Fusion Centers, and other local agencies. To do this, you might need to upgrade your information systems and to employ properly trained analysts. You might also need to assign at least one terrorism liaison officer (TLO) to collate and transfer the information to the appropriate agencies within the ISE. You can obtain information on training your TLO at http://www.tlo.org/training/index.htm. If you have not already, obtain a copy of the *Fusion Center Guidelines*, which was created jointly by the Department of Justice (DOJ) and the Department of Homeland Security (DHS) in an effort to facilitate information

sharing among law enforcement agencies. The guidelines are available online at http://www.fas.org/irp/agency/ise/guidelines.pdf. Another helpful document is *The National Criminal Intelligence Sharing Plan*, published in October 2003 by the Bureau of Justice Assistance (BJA): http://www.it.ojp.gov/documents/NCISP_Plan.pdf. Finally, in October 2007, President Bush announced the new National Strategy for Information Sharing that sets priorities for information sharing and establishes an integrated national capability for terrorism-related information sharing among federal, state, local, and tribal officials, the private sector, and foreign partners. You can find details about this strategy and its implementation at the Office of the Director of National Intelligence, http://www.ise.gov/.

Partnerships (Briefs 17 and 18)

Gathering information about terrorist threats can be facilitated through partnerships with private security and businesses. Banks, check-cashing establishments, and money-transfer stations such as Western Union can tell you about suspicious financial transactions; car rental agencies, motels, and real estate agents can give you information about newcomers and transients; private security practitioners can inform you about organized fraud and cyber crime that might be funding terrorism. These personnel are also immediately responsible for protecting much of the infrastructure in your jurisdiction and are often the first to respond to an incident. Coordination can reduce the demands on your own thinly stretched force.

Preparing for a disaster already requires you to work closely with the mayor or city manager, as well as with other city agencies such as fire, emergency medical, hospitals, and schools. The threat of terrorism, however, means that you will have to modify your plans to account for less-conventional threats. For example, depending on your location, you might have to consider the possibility of attacks by weapons of mass destruction (WMD), including chemical, biological, nuclear, or radiological devices. You might also have to plan for the possibility that bridges or tunnels on possible evacuation routes will be destroyed deliberately. The likelihood that such attacks will be made without warning requires stepping up the frequency and sophistication of training exercises.

You might want to establish partnerships with local newspapers and radio stations. The media can help allay public anxiety by reporting what you are doing to counter the threat of terrorism. It can also help reassure immigrant groups that they will be treated fairly and that police will deal firmly with any hate crimes. Last, the media can play a vital role in an emergency by keeping the public informed about the situation and your response to it. They are much more likely to help if they see themselves as partners in dealing with terrorism.

Much of the above is consistent with regular community policing (Brief 28), so if you already have a community policing program, it will be simply a matter of expanding its focus to take account of the terrorist threat.

How the Long Beach (California) Police Department Has Adapted to the Terrorism Threat

- Created a counterterrorism unit and appointed terrorist liaison officers.
- Reassigned officers to assess and protect critical infrastructure, such as the port, airport, and water treatment facilities.
- Sent officers to train in new skills, such as WMD response and recognizing signs of terrorism.
- Established a port police unit equipped with small boats.
- Reassigned officers to respond to areas with high population growth.
- Increased visibility and response times by switching officers from two- to one-person cars.
- Reduced staffing on lower priority programs, such as Drug Abuse Resistance Education (D.A.R.E.).
- Reduced foot patrols and staffing in the narcotics division.
- Requested additional resources to cover additional demand, both from the city for local needs, and from the Federal Government for national needs.

Source: Raymond, Barbara, Laura J. Hickman, Laura Miller, and Jennifer S. Wong., *Police Personnel Challenges After September 11: Anticipating Expanded Duties and a Changing Labor Pool.* Santa Monica, California: RAND Corporation, 2005.

Brief 03: Know That Fear is the Enemy

In the depths of the Great Depression, Franklin D. Roosevelt rallied Americans by reminding them that "the only thing we have to fear is fear itself—nameless, unreasoning, unjustified terror which paralyzes needed efforts to convert retreat into advance." His words are even more apt in the aftermath of 9/11 because many people are now frightened that they will become the victim of a terrorist attack at some time in their lives. In fact, they worry far more about the truly tiny risk of being killed by terrorists than they do about the much greater risk of being killed in a car crash or some other accident.

As you well know, the same disconnect between risk and fear holds for crime. Fear of crime increased steadily in the 2 decades beginning in the mid 1980s, while reported crime declined steadily. Those who are most fearful of crime—the elderly, for example—are often the least likely to be victimized. In fact, most people do not judge their risk of falling victim to crime and terrorism (or any other calamity) on the basis of statistical data; instead, they are more likely to be influenced by newspaper and television coverage of terrifying events. Thus, people are often more fearful of being killed in an airplane crash or a shark attack than in more commonplace ways, such as a car crash. Many also seem to be frightened of being killed in large-scale disasters, such as terrorist attacks, when this again is unlikely.

The more frightened we are, the more successful will terrorists judge their attacks. Not only does undue fear lower our quality of life but, as argued by David Altheide in *Terrorism and the Politics of Fear*, it also "limits our intellectual and moral capacities, it turns us against others, it changes our behavior and our perspective and it makes us vulnerable to those who would control us to promote their own agendas." This fear can lead the country to spend untold billions of dollars on protective measures, to restrict important liberties, and to make radical changes in foreign policy.

This might not seem relevant to you, but the local response to the threat of terrorism is as much affected by public fear as is the national response. Although a little fear might make it easier to get things done, an unrealistically high level of fear—what one academic described as a "false sense of insecurity"—can lead to a waste of resources and manpower. To stem this waste, you might even be tempted to follow Senator John McCain's advice in *Why Courage Matters: The Way to a Braver Life*: "Get on the damn elevator! Fly on the damn plane! Calculate the odds of being harmed by a terrorist! It's still about as likely as being swept out to sea by a tidal wave….You're almost certainly going to be okay...."

Although this might be the rational response to the threat of terrorism, you would likely find it counterproductive: people admire brave leaders, but they value even more those who understand their fears and show appropriate caution. You should say "Many people are understandably frightened," not "There's nothing to be afraid of," and reducing fear should be an important part of your counterterrorism plan. Fortunately, it is easier to reduce the fear of attack than the actual risk of attack because how can you reduce further what for most jurisdictions is a truly tiny risk? Moreover, most of the actions you can take to reduce fear are not costly, as you can see from the following list of fear-reduction measures.

1. Deal as openly as possible with your partners in developing a counterterrorism plan for the community (see Briefs 17–19). Fully explain the reasoning behind your decisions and graciously accept their input, agreement, and cooperation. You are more likely to succeed if you treat them as full partners, including allowing them responsibility for implementing elements of the counterterrorism plan. If you feel that you cannot be as forthcoming with the public, explain your reasoning to your partners.
2. Evaluate all proposals for both fear reduction and risk reduction. In jurisdictions where risks are negligible, focus first on proposals that promise fear reduction. Once fear is reduced, you will be able to formulate a more rational risk-reduction plan.
3. Be sure you can explain and defend your plan in public.
4. Pay special attention to the fears of minority and immigrant communities, particularly the fear of being victimized by hate crime. At especially sensitive times, such as when terrorist alerts are heightened, announce that you will not tolerate hate crimes; but at the same time, be aware that some minority communities will feel unjustly targeted by the police, no matter what steps you take to assuage their concerns.
5. Enlist the help of local media outlets in communicating your plan, avoiding scare tactics in reporting terrorism, and helping in the unlikely event of attack.
6. If another terror attack occurs, in the United States or elsewhere, be clear about the implications for your town or jurisdiction—in most cases there will be none. Carefully evaluate the local significance of national terror alerts and, if necessary, balance the required actions with efforts to reassure the community and members of your own department.
7. Deal with your own fears about terrorism harming yourself or your family (most unlikely); your professional competence in your new counterterrorism role (we are all learning); and being blamed for taking unnecessary precautions or for failing to take necessary ones (hindsight is a wonderful thing).

Read More:

1. Altheide, David L. *Terrorism and the Politics of Fear.* Lanham, Maryland: AltaMira Press, 2006.
2. McCain, John, with Mark Salter, *Why Courage Matters: The Way to a Braver Life*. New York: Random House, 2004.

“a ‘false sense of insecurity’ — can lead to a waste of resources and manpower. ”

Brief 04: Prepare for Terrorism Alerts

The Homeland Security Advisory System (HSAS) was introduced soon after 9/11 to warn the country of possible terrorist attacks. It consists of five threat conditions with associated suggested protective measures.

1. Red: Severe condition.
2. Orange: High condition.
3. Yellow: Elevated condition.
4. Blue: Guarded condition.
5. Green: Low condition.

For most of the time, the country has been at yellow, the mid position, although on several occasions the risk has been elevated to orange (high). You must have a response plan in place for when the nation or your region goes to orange (or when the local airport is placed on orange by the separate aviation security terrorism alert). The plan should consist of common sense measures that you and others—municipal officials, businesses, and residents—can take in your jurisdiction. (See the Box for checklists of these measures.) Regardless of the actual likelihood of an attack—or indeed the effectiveness of the measures—they might help reassure residents that they are being protected against a possible attack.

The HSAS has been widely criticized in the media. You, too, might have to deal with criticism as you are putting a response plan in place. Because it is unlikely that the threat level will be reduced below yellow in the foreseeable future, the system has been criticized for being a three-level rather than a five-level system. It also has been criticized for providing no clear definitions of what constitutes elevated, high, and severe conditions and for failing to provide practical advice about what to do in each case. Its greatest weakness, however, is that it is not based on hard data, as is the case with weather advisories, for example. Weather advisories are based on meteorological data that cover a wide range of precisely measured weather variables—barometric pressure, wind speed, predicted tides, temperature, expected precipitation, and so forth. Hard information about a pending terrorist attack, of course, is very difficult to obtain, and it is even more difficult to tie some threats to a specific target or region of the country. For every suspected attack, therefore, hundreds or even thousands of cities are placed on alert because there is no accepted method of grading targets according to their potential risk. This leads to wasted resources and unnecessary precautions. It also can cause large sections of the population to become needlessly frightened, which, in turn, can lead to the alert system being discredited when an attack fails to materialize. To deal with this problem, some recent alerts have focused on particular regions of the country or particular industrial sectors. Other improvements to the system are being contemplated, and it is being better coordinated with some other state and federal alert systems. Meanwhile, you have no alternative but to work with the HSAS and to persuade others to do the same. Running through the checklists of what to do in the case of an alert—we provide checklists for an Orange Alert, which is the most common—may be useful if only to remind you of the complexity of responding and the wide range of persons and groups involved.

Read More:
Kemp, Roger L., "Homeland Security: Common Sense Measures to Safeguard your Community," *The Police Chief* 73 (February 2006).

Checklists of Recommended Actions in Response to an Orange Alert

Checklist for police executives

- Closely monitor all available security and intelligence data from federal, state, and local law enforcement agencies.
- Limit access to all critical facilities to essential personnel only.
- Ensure that officers enforce restrictions against parking vehicles near sensitive public buildings.
- Increase defensive measures around key structures and for major public events.
- Warn police and fire personnel to be careful when responding to incidents.
- Inspect building and parking areas for suspicious packages.
- Monitor all municipal reservoirs and watershed areas, wastewater treatment plants, and other sensitive public facilities.
- Conduct random road checkpoints in critical infrastructure areas.
- Advise all personnel of contingency plans for shift modifications, assignments, work and relief cycles, and family care and assistance should the situation escalate. Have a family readiness plan in place.
- Disperse and stage department emergency resources, including spare vehicles and command posts, to various locations throughout the jurisdiction.
- Require the field operations bureau commander to identify potential command posts and staging areas across the jurisdiction and to forward that information to the chief's office.
- Coordinate public information with the mayor's office, the municipal emergency management agency, the fire department, and emergency medical services.
- Require commanders to check all equipment for operational readiness.
- Erect barriers and obstacles to control the flow of traffic, where appropriate.

- Work with the city to identify and publicize evacuation routes.

Checklist for city officials (mayors and city council members, city managers, fire chiefs, public works directors, and other emergency personnel)

- Review local emergency response plans and be prepared to activate the emergency operations center.
- Coordinate response plans with counterparts at other levels of government.
- Work closely with county health officials to detect transmittable diseases.
- Place all emergency management and specialized response teams on callback alert status.
- Ensure that employees are especially watchful for suspicious or unattended packages and articles received through public and private mail delivery systems.
- Store critical response vehicles in a secure area; if possible, in an indoor parking facility.

Checklist for businesses

- Ensure that appropriate security measures are in place and functioning properly.
- Instruct employees to report suspicious activities, packages, and people to their supervisors.
- Search all personal bags and parcels and require employees to pass through a metal detector, if one is available.
- Monitor access to underground garages and loading docks; restrict parking near buildings and infrastructure.
- Inspect and activate intrusion-detection systems, exterior lighting, security fencing, and locking systems.
- Inspect all deliveries; where appropriate, accept shipments only at off-site locations.
- Remind employees of heightened security policies and proper building evacuation procedures.
- Have a plan for sheltering in place.

Checklist for residents

- Expect delays because of baggage searches and other heightened security measures at public buildings and other facilities.
- Report all suspicious activities at or near critical public facilities to local law enforcement agencies by calling 911.
- Do not leave unattended packages or briefcases in public areas.
- Organize emergency supply kits and discuss emergency plans with family members.
- Be alert to your surroundings, do not place yourself in vulnerable situations, and closely monitor the activities of your children.
- Maintain close contact with your family and neighbors to ensure their safety and emotional well-being.
- Monitor world events and local circumstances, as well as local government threat advisories.

(For further advice, see http://www.ready.gov.)

Brief 05: Expect More Public Attention

As the threat of terrorism increases your work and responsibilities, it will also substantially raise your public profile in your town or city. The local media will ask you to comment on the risk of attack. You will regularly be asked to speak at meetings of the Lions, the Elks, the Rotary Club, and similar organizations. Minority communities will seek assurances that they will be protected from hate crimes and that they will not be singled out unfairly by the police. You will work with local businesses and corporations to improve their security. And you will have to consult with hospitals, clinics, and schools (whether they are under municipal control or not) to ensure that they are doing all they can to protect themselves.

More significant than any of this, however, is that the municipal authorities are likely to rely on you to respond to the threat of terrorism. They will see you as the local expert on terrorism and as the main conduit of information from federal authorities. They will expect you to develop local intelligence capacities, to provide advice on securing the municipal infrastructure, to enter into mutual aid agreements with neighboring police departments for sharing critical resources (e.g., SWAT teams, bomb disposal squads, and, often overlooked, interpreters), and to enhance departmental and municipal resources by obtaining and managing federal and state terrorism grants.

You will also have to play a more significant part in emergency operations. Under the emergency operations plan that most cities now have, police departments and other municipal agencies have certain defined responsibilities. A typical plan (as described by the International City/County Management Association) is described in the list below. In this plan, departmental responsibilities include criminal investigation, property protection, traffic control, and evacuation management. These duties will be expanded if the disaster is the result of a terrorist attack. In fact, nearly every aspect of the plan will require modification because a disaster resulting from terrorism differs from other disasters in some important respects (see Brief 38): for example, there usually is no advance warning, public fear will be much greater because of the risk of another attack, and the media attention will likely be greatly magnified, with significantly more foreign coverage. If the attack involves nuclear, chemical, or biological agents, there will be many important repercussions, including protecting responders from contamination and providing treatment for those injured in the attack.

From your point of view, a terrorist attack will require modifying disaster-management responsibilities in three important respects.

1. **Site security.** Following the initial attack, terrorists might plant bombs to kill emergency workers. After the 9/11 attacks on the World Trade Center, police searched vehicles entering the disaster site for explosives and other weapons.
2. **Emergency operations center security.** In addition to tightening security at the disaster site, you will need to tighten security at the emergency operations center (EOC), lest the mayor, community leaders, and other municipal officials are targeted by terrorists.
3. **Crime-scene protection.** Unlike natural disasters, terrorist incidents lead to criminal investigations; hence, you will need to move quickly to obtain and secure evidence. Establish a list of people who will be granted access to the site and do not allow volunteers and civilian responders to move in and out of the site as freely as you would in a conventional disaster. You must do all you can to preserve the integrity of evidence. Make sure that evidence is not introduced into the scene or taken away from it and maintain a thorough record of the evidentiary chain of custody. In cases of arson, ensure that exhaust fumes from generators and other motorized contrivances do not contaminate debris and preclude the use of evidence that shows that accelerants were used.

One last point about recovery: emergency operations plans often neglect the role of businesses in responding to a disaster. Businesses have a vested interest in the community's rapid recovery, they often command vast resources, and they sometimes can provide help far more efficiently than can government agencies (see Box). Your relationship with private security professionals constitutes an important link between government and business; make sure that the city takes full advantage of their potential contributions in responding to disasters.

"In response to Hurricanes Katrina and Rita, companies like Wal-Mart and Home Depot proved far more nimble at providing manpower, materials, and logistics than many parts of the Federal Government. While truckloads of ice contracted by the Federal Emergency Management Agency (FEMA) were stranded for days with no direction on where to go, national retailers were organizing important distribution points for food, water, clothing, generators, and other supplies. Mississippi Power, a subsidiary of Southern Company, was able to restore electricity to hundreds of thousands of customers well ahead of schedule. The security services company Guardsmark tracked down all of its missing employees who lived and worked in the storm-struck area within a week and provided them with cash, emergency supplies, and help with relocation. Johnson Controls bought recreational vehicles in Wisconsin and shipped them to campgrounds in the disaster zone so its employees had temporary housing. Even though Katrina and Rita were natural disasters, not man-made

ones, they illustrate that the nation will be far better served when the Federal Government is organized to fully integrate the private sector as a partner in preventing and responding to catastrophic terrorist attacks."

Source: Flynn, Stephen E., and Daniel B. Prieto, *Neglected Defense: Mobilizing the Private Sector to Support Homeland Security, Council Special Report No. 13*. New York: Council on Foreign Relations, 2005.

Sample Emergency Operations Plan—Who Does What?

Mayor/city manager

- Activate the city emergency plan
- Suspend ordinances, if necessary
- Use all city resources where necessary
- Transfer city personnel, equipment, and functions, as necessary
- Work with public information officer to relay information to the public

Emergency manager

- Serve as advisor to the mayor and city manager
- Direct development of city plan with other departments
- Establish information collection, analysis, reporting, and dissemination system
- Conduct exercises with all agencies and organizations in the community
- Coordinate donations and mutual aid
- Establish a warning system
- Oversee evacuation
- Direct EOC operations
- Work with public information officer to relay information to the public
- Document all response actions

Fire

- Fire suppression
- Emergency medical service
- Search and rescue
- Radiological assessment

Police

- Law enforcement
- Criminal investigations

Code enforcement/engineering

- Assess damage
- Condemn damaged structures
- Coordinate utility restoration
- Public works
- Debris removal
- Water and sewer service restoration
- Heavy equipment

Engineering

- Parks and recreation
- Debris removal

Public buildings and facilities

- Provide offices for state and federal resources

Shelters

Coroner

- Victim identification
- Mortuary services
- Finance
- Accounting
- Procurement
- Personnel
- Ensure well-being of responders' families
- Coordinate volunteers
- City planning department
- Urban planning
- Damage assessment

Legal

- Public information
- Credentials for media and site control
- EOC representation
- Evacuations
- Communications
- Traffic control

Brief 06: Question Assumptions

Sometimes it is difficult to know what to believe about terrorism. For most of us, the main source of information is the media, which bombards us with stories of terrorist atrocities, mostly in far-flung parts of the world, spiced with comments from experts of sometimes questionable authority. Remember that the main job of the media is not to provide information: it is to hold and entertain the audience. Stories, therefore, are presented to make them seem relevant to the everyday experience of the audience and to engage the audience's emotions. TV newscasters will typically follow a story—let us say about a suicide bombing in Sri Lanka—by asking an alleged expert whether we are adequately prepared to deal with such events in the United States. By making the tacit assumption that suicide bombings are to be expected here, the interviewer makes the story immediately relevant to the viewers' lives and raises their levels of fear, whereas in truth, we are almost never adequately prepared for rare and unforeseen events. As a result, viewers are more likely to tune in again, seeking either reassurance or further titillation. "Experts" might have their own reasons for stoking fear, and you can be sure they have an axe to grind, either pro or contra the current administration, with the result that viewers end up less-informed or more confused than ever.

Always try to identify and critically examine the underlying assumptions in the information you receive. We list below some of the most common and most questionable assumptions about terrorism.

1. **Myth: Anyone might be a terrorist.** Although it is true that terrorists come in many shapes and sizes, most terrorists are young males. It is most unlikely that a white-haired grandmother from the Midwest is a terrorist, even if she is behaving in a suspicious manner. She is much more likely to be confused or ignorant of the rules, and that should be the assumption when your officers approach her. They should reserve their suspicions for those who most closely fit the terrorist profile.
2. **Myth: Every immigrant is suspect.** Those who fit the terrorist profile best (for the present at least) are young male immigrants of Middle Eastern appearance. Even among this group, of course, only a tiny minority are terrorists, wannabe terrorists, or even terrorist sympathizers. Treating them differently in casual encounters can jeopardize relations with a group that could otherwise provide your officers with valuable information about truly suspect activity.
3. **Myth: Terrorists are crazed fanatics.** However much you disagree with the reasons for their actions, you should remember that cold rationality guides much of terrorist behavior. Like all organized criminals, they plan their acts carefully, they try to avoid capture, and they are determined to succeed.
4. **Myth: Terrorists are eager to die.** As we have discovered to our cost, some terrorists are willing to die for their cause. But many terrorists are careful with their lives. Not only do they have the same ambitions for success and happiness as everyone else, but they would prefer to escape and strike again rather than to fail and die.
5. **Myth: Terrorists are evil geniuses.** Not every terrorist has the mind of an Osama bin Laden. Most are ordinary, fallible individuals. They might plan their acts carefully, but they are engaged in a risky business. They cannot anticipate every setback and on occasion will be forced to improvise and take chances. Some of their decisions will lead them to fail and perhaps be killed.
6. **Myth: Terrorists might strike anywhere.** In theory, terrorists can strike anywhere, but in practice they must conserve their resources and strike where they will achieve the greatest effect. If we think like terrorists we can anticipate their choices and act accordingly to protect the most vulnerable targets.

"Always try to identify and critically examine the underlying assumptions in the information you receive."

7. **Myth: Terrorists are unstoppable.** Most terrorist groups last only 1 or 2 years before falling apart. There are also plenty of examples of terrorism being substantially reduced. Aircraft hijackings in the 1970s and embassy takeovers in the 1980s are just two examples. If we carefully study the steps that terrorists must take to complete their acts, and then intervene to make these acts more difficult or risky, and if we protect the targets that are most attractive, we can make the terrorists substantially less successful.

8. **Myth: We can win the war on terrorism.** Although we can hinder the terrorists and make them much less successful, we can never win the so-called war on terror. Winning implies that terrorism will be forever eliminated from our world. That is about as unlikely as winning the war on crime.

9. **Myth: If it can happen in Israel (London, Madrid, Delhi), it can happen here.** It is a serious mistake to assume that a form of terrorism that is possible in London or Delhi (or anywhere else overseas) can be reproduced in the United States. Each form of terrorism depends on the opportunities provided by the environment in which it is committed. This environment is rarely the same from country to country. The routine suicide bombings committed against Israel by the Palestinians are made possible by the steady supply of willing bombers and the small size and close proximity of the two countries. Such conditions do not exist here.

10. **Myth: We must prepare for nuclear attack.** Most experts agree that terrorists are unlikely to attack us with a nuclear bomb. The logistics of building, buying, or stealing a bomb, and then delivering it, are just too difficult. On the other hand, most experts agree that terrorists could easily plant a suitcase bomb (a radiological dispersal device) in any of our large cities. It is doubtful that this would lead to mass casualties, although it might result in widespread panic.

11. **Myth: Fighting terrorism is a job for the feds.** However effective they might be, the FBI and the CIA cannot defeat terrorism on their own. Rather, they must garner the support of the public, the private sector and, above all, local and state police agencies. As this manual makes clear, local police agencies play a key role in gathering intelligence about terrorists, in helping to protect vulnerable targets, and in responding to attacks.

12. **Myth: Sharing intelligence is the key to defeating terrorism.** The report of the 9/11 Commission made glaringly obvious the failures of federal intelligence agencies to coordinate their operations. Since then, much has been done to improve communication between the FBI and the CIA and also to improve intelligence sharing among local, state, and federal agencies. However much we improve the gathering and processing of intelligence, we should never rely on intelligence alone. We also need to reduce the opportunities for terrorism by protecting the most vulnerable targets and by controlling the tools and weapons that terrorists routinely use.

Brief 07: Recognize the Limits of "Take Them Out"

Criminal justice scholars have been critical of the idea that we can arrest ourselves out of crime—that we can best reduce crime by aggressively arresting offenders and throwing the worst of them into prison. Here are some of the reasons why scholars believe this policy is flawed.

- Despite the best efforts of police, only a tiny proportion of crimes are followed by arrest and punishment. Further, it is unclear how this proportion can be increased significantly. Crackdowns and increased patrols can be maintained only for short periods and, in any case, produce only a handful of arrests. Detective work is so time-consuming that it can be used only in the most serious cases. Even faster response times do not help the police much because perpetrators are usually long gone by the time the police are called.
- Decades of criminological research have failed to establish a relationship between severe punishment and reduced crime. The best known example is the lack of statistical evidence that capital punishment deters murder. Because most offenders do not believe that they will be caught, they do not take the risk of severe punishment seriously; others do not care if they are caught because they are drunk or enraged when they commit their crimes.
- High rates of imprisonment do not guarantee lower rates of crime. The rates of imprisonment in the United States, for example, are much higher than in many other Western countries, but overall our crime rates are no better; in fact, our rate of violent crime is much worse.
- The supply of offenders is never ending. With each generation of youth, 5 to 10 percent will turn out to be regular offenders; so however many offenders we arrest and imprison, others will soon take their place.
- High rates of imprisonment carry high economic and social costs, both for society in general and for prisoners and their families.

Some of the same reasons explain why we cannot rely on taking out terrorists—i.e., identifying them and then capturing or killing them—as our main defense against terrorism. Catching terrorists is not easy. They take even more care than regular criminals to conceal their activities and tracking them down has sometimes led to the use of questionable procedures. Even when we know their identities, we cannot always catch them. This is especially so when they operate overseas, in countries sympathetic to their cause: witness the fruitless efforts to date to find Osama bin Laden. Those who are willing to die for their beliefs are unlikely to be deterred by the risk of death or punishment. They cannot be tried in open court because of security concerns, and even when convicted, they make difficult prisoners. In fact, perhaps the greatest cost of imprisoning terrorists is that their supporters feel justified in planning fresh outrages to force their release.

Killing terrorists carries even greater costs. It creates more bitterness among already hostile populations, making the conflicts that underlie terrorist acts even harder to resolve. It justifies the use of violence and supports the claim that they are fighting ruthless enemies. It turns them into martyrs and, therefore, into potent recruiting symbols among the impressionable young men whom terrorists seek to attract

None of this means that we should not punish terrorists once they are caught. They deserve punishment because of their evil deeds, and it is right to hunt them down. Some might argue that it is also right to kill terrorist leaders, particularly charismatic individuals who hold considerable sway over their followers and who cannot be replaced easily. Killing these leaders might effectively decapitate the organization and leave its body to wither, saving the lives of many innocent people.

It is not right to let the "take them out" approach dominate our response to terrorism. Imprisoning or even killing terrorists will not eradicate terrorism any more than severe punishment has stopped crime. As a nation we must pursue a multifaceted approach to terrorism. We must pursue diplomatic and military solutions. We must try to improve economic and educational opportunities for foreign populations, both those at risk of becoming disaffected and hostile and those at risk of takeover by terrorist organizations. We must work to prevent terrorists from succeeding in their attacks by hardening targets and controlling the tools and weapons they use. And when they attack, we must respond rapidly and efficiently to reduce the death and damages that result.

But what does all this mean for you? How does this knowledge help you protect your community from terrorism? Clearly, as a local police executive, you have no role in foreign policy, whether in the allocation of foreign aid or in the initiation of diplomatic or military action. But you, too, must pursue a multifaceted plan. In your case, the plan should consist of three key elements: (1) developing local intelligence about possible terrorist activity; (2) hardening the most vulnerable targets in your jurisdiction; and (3) developing effective response and recovery procedures. You should try to maintain a proper balance among these three elements. In particular, do not put too much faith in the power of intelligence to protect you from terrorism. It is only part of what you must do to protect your community. You might be excused for failing to unearth a terror plot, but there is no excuse for failing to protect key targets or fumbling your response in the event of an attack.

"Imprisoning or even killing terrorists will not eradicate terrorism any more than severe punishment has stopped crime."

Brief 08: Know Your Local Vulnerabilities

One of the most frustrating things about the threat of terrorism is that it is impossible to know how real it is. Thankfully, terrorism is rare; so rare that you might think that there is very little chance of your city being singled out for attack. Going on past history, you would almost certainly be right. True, you might have targets that could attract terrorists—a reservoir, the town hall, schools, and bus or train stations—but as the Table below shows, most cities have such targets. Ask yourself if there is any reason for terrorists to be more attracted to your city than to hundreds of other similar ones. Because terrorist attacks are so rare, research alone cannot help you answer this question. For other crimes, it is possible to analyze a sample of occurrences to identify risk factors, but it is not possible to do this for terrorism, at least in the United States.

Having said all that, it is possible to draw some reasonable conclusions about what puts a city at risk of attack. To do this we must analyze two key points: first, the goals of terrorism (to inflict casualties, to create a climate of fear, and to attract media attention); and second, the logistical problems faced by terrorists in mounting an attack (for example, acquiring appropriate weaponry, gaining access to the target, and the difficulties of attacking from overseas). Thus, a city is generally at greater risk of attack when: (1) it is famous—because terrorists want to attract the greatest possible attention; (2) it is important—because terrorists want to harm the country; (3) it is accessible—because terrorists want to minimize their risk and effort; (4) it has a substantial immigrant population—because foreign terrorists find it easier to operate by merging into an immigrant community; and (5) in the case of domestic terrorism (see Brief 11), it is the home of research universities or institutions that contain animal laboratories or commercial establishments that ecoterrorists perceive as threatening to the environment. This means that your city's risk of attack will be increased if it is any or all of the following:

- Historical
- Center of tourism
- State capital
- Large, with many people
- Identified with an iconic product
- Near a large military base
- Federal office center
- Financial, commercial, or manufacturing center
- Near a port of entry to the United States
- Near an international airport
- Center of recent immigration (especially Islamic)
- Site of animal research laboratories
- Major site for petroleum refineries, cogeneration plants, or nuclear facilities
- Major communications and computing center
- Transportation hub.

Even this does not help a great deal because even if your city is at a higher risk than others, its risk of actually being attacked is still very low. The terrible consequences of being wrong mean that you cannot gamble on its being overlooked by terrorists. The temptation to ignore the very small risk will not be countenanced by municipal authorities or the community at large. If nothing else, you may well find it difficult to convince them that the risk is indeed tiny. What can you do to save yourself from having to invest a great deal of time, energy, and resources in trying to prevent an extremely unlikely event from occurring? We suggest the following:

- Put the small risk of an attack on one side and focus on the terrible consequences.
- Focusing on the consequences will help you deal with cynics and naysayers who argue that prevention is a waste of time—that terrorists will never attack your city, that you cannot stop them if they choose to, and that no one will ever know whether your precautions reduced the risks.
- Put as much time, effort, and resources into preventive action (including improving intelligence) as you can, while still being able to meet your core policing responsibilities.
- Strive to improve basic security at all at-risk facilities.
- Ask municipal authorities, business and community leaders, and other stakeholders to rank those targets thought to be at the greatest risk. Use EVIL DONE and CARVER to assist in this process (see Briefs 29 and 30). These acronyms capture the characteristics that put buildings and facilities at risk of attack. There is some overlap between these features and those that put your city at risk; for example, it matters to terrorists that both the buildings and cities that they target are important and famous—but some of the other characteristics relate only to buildings.
- Try to determine the form an attack is most likely to take. Look at the situation from the terrorists' point of view: think about how such an attack could be carried out and which specific vulnerabilities could be exploited.
- Starting with the facilities at the top of the list, consider a range of measures that go beyond improving basic security and develop a plan for implementing these measures. This includes actively searching for new resources from business, state, and federal sources.
- Imagine your personal nightmare: what kind of attack do you most dread? We mean by this a specific kind of attack against a particular facility in your jurisdiction. It might be a gang of terrorists armed with automatic weapons attacking the elementary school; a dirty bomb left in the

park downtown; a truck bomb rammed into the local chemical plant. Whatever it is, you should confront the problem in the cold light of day, rather than after an attack has occurred, when morale is at its lowest. Either you will realize that such an attack is so unlikely that it can be ignored, or you will identify real vulnerabilities that you can do something about. Having taken the necessary action you will at least be able to take comfort in the fact that you have done your best to protect your community.

- Having dealt with your personal nightmare, focus the same attention on the next worst scenario and deal with it in the same way, and so on, over time.

Further Reading:
Probably every police jurisdiction contains one or more risky facility. You can learn how to identify and eliminate them from the COPS Office's Problem-Oriented Guide for Police, *Problem-Solving Tools Series No. 6: Understanding Risky Facilities*, by Ronald V. Clarke and John E. Eck, 2007. http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=410

"What types of facilities to be secured in your city, or nearby?"

(Answers from 725 cities to a mail survey, September 2002)

	In city (percent)	Nearby (percent)
Water supply	39	82
Government buildings	25	77
Schools	26	66
Transportation	33	66
Hospitals	35	62
IT Infrastructure	27	61
Stadiums/Arenas	28	31
Ports	37	29
Other large buildings	22	28
Power plants	38	26
Other federal facilities	31	21
Military	29	17
International borders	8	5

Source: Hoene, Christopher, Mark Baldassare, and Christiana Brennan, *Homeland Security and America's Cities, Research Brief on America's Cities, Issue 2002-2*. Washington, D.C.: National League of Cities, 2000.

II. Understand the Threat


LINE DO NOT CR

“Terrorists are criminals, too… the behaviors that comprise terrorism—even suicide terrorism—are little different from those that conventional criminals display.”

Brief 09: Think of Terrorism as Crime

Obviously, police departments deal with crime every day; depending on the size and type of jurisdiction, they experience a full range of crimes, from homicide to petty theft and disorder. Because terrorism is so rare compared to other crime, one might expect that the average department would have to learn a whole new approach to crime fighting in order to deal with it. But is this true?

Terrorists are criminals, too. Many terrorist groups carry out ordinary crimes such as bank robbery, drug trafficking, identity theft, and money laundering to support their terrorist activities. Furthermore, the behaviors that comprise terrorism—even suicide terrorism—are little different from those that conventional criminals display.

> *"Many terrorists, especially foreigners who are in the United State illegally, have to live a fugitive lifestyle—that is, they have to commit crimes not just to carry out an attack but simply to sustain themselves. They maintain themselves with illegal documents, committing burglary and robbery, dealing drugs, committing fraud, and so on. In other words, not all illegal immigrants or fugitives are terrorists, but many terrorists have to live underground like illegal immigrants or fugitives to get by in the U.S."*
>
> Source: Kelling, George L. and William K. Bratton, *Policing Terrorism, Civic Bulletin 43*. New York: Manhattan Institute for Policy Research, September 2006.

Terrorism is crime with a political motive. What must a terrorist do differently than an ordinary criminal to carry out his crime successfully? Consider the following example that compares a suicide bomber to a serial murderer.

1. **Terrorist behavior**: A suicide bomber must take several steps in order to carry out his task. He must obtain an explosive belt that can be concealed on his person; he must choose a target; he must figure out how to reach that target without being caught; and he must have a contingency plan should he be apprehended before he reaches his target or before he can detonate the bomb.
2. **Criminal behavior**: A serial murderer must take several steps in order to kill his victim. He must select a target and figure out the best way to approach that target and carry out the murder without being caught; he must decide on the method of killing; he must decide how to dispose of the body; and he must plan his escape route.

The common element in these two examples is the logical sequence of steps that both the terrorist and the criminal must take to see their missions through to successful conclusions.

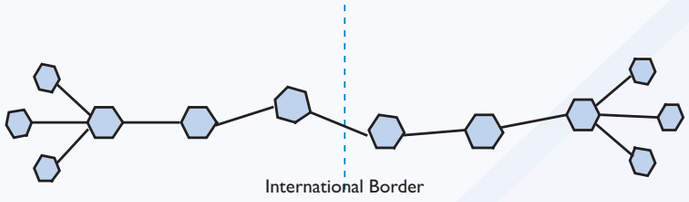
Opportunity makes the terrorist. The specific opportunities and circumstances that each criminal or terrorist act requires will depend on the specific requirements of that particular crime. For example, if firearms are readily available, an offender might choose a gun as his means of carrying out a crime (e.g., a liquor store holdup); this might, in turn, change his

assessment of his opportunities and targets. Similarly, if plenty of explosives are available, but no explosive vests, a terrorist group might plant a bomb in a car or bus, rather than carry out a suicide bombing. In all cases, the plans of attack, whether criminal or terrorist, depend on the opportunities at hand.

There's crime, and then there's crime. Although the general category of crime comprises a tremendous range of activities, most criminals are driven by the same logical impulse: the desire to commit the crime without being apprehended. Nevertheless, each particular criminal opportunity gives rise to a completely different set of choices and acts; that is, the sequence of actions needed to carry out the burglary of a residence in a suburban neighborhood is quite different from that required for a burglary in a high-rise apartment complex. In fact, the differences between various types of conventional crime are as great, and perhaps even greater, than the supposed differences between crime and terrorism.

A group affair? Some argue that the essential difference between crime and terrorism is that terrorism is always carried out by an organized group. Many and perhaps most books on counterterrorism focus on the organizational structure and reach of terrorist groups. Police departments have dealt with organized crimes of many varieties for decades, although with limited success. Recent research on organized crime groups has shown that they generally are not the monolithic organizations that were previously supposed (see Box), but rather that they emerge and disappear according to opportunity and circumstance. Similarly, research has shown that most terrorist groups disintegrate within 2 years. In this regard, the claimed organizational differences between crime and terrorism are inconsequential, although the challenges facing police at the local level in dealing with organizational crime are considerable.

In short, if you think of terrorism as another form of crime and analyze it accordingly, a major barrier to solving the problem is removed. Just as there are many different types of crime that require a variety of tailored responses, so it is for terrorism.



At the local level, terrorism networks are quite similar to organized crime networks, particularly those that operate across borders. The chain network depicted above is common in criminal organizations (including terrorist groups) that move illegal products or services (guns, drugs, illegal immigrants, money) from source to customer. Each actor in the chain serves a dual function: he buys from the previous actor and sells to the next. The obvious point of intervention is the border; whether this is the most efficacious interdiction point depends on a variety of factors, including federal, state, and local laws and the relationship between local police and border agents. End-point arrangements between sellers and customers might be a more effective intervention point for local police. In any event, identifying the tools and conditions that facilitate such activities can be an important first step in protecting the local community from terrorist attacks and exploitation by organized crime.

"The differences between various types of conventional crime are as great, and perhaps even greater, than the supposed differences between crime and terrorism."

Brief 10: Terrorism Comes in Many Forms

Crime is a convenient construct for the media and for laymen in everyday discussion, but it is of limited use in any serious discussion of crime reduction because it encompasses many different types of acts committed by a vast array of offenders, each of whom possesses very different skills and motives. When trying to identify effective crime-control measures, it is essential to focus on specific types of crime, whether bank robbery, rape, drug dealing, extortion, burglary, arson, or identity theft. Although the number of different acts encompassed by the word terrorism are not as varied as those encompassed by the word crime, the same point applies: in thinking about how to defend yourself from terrorism, you must consider both the many different forms that it can take and the type of attack to which you are most vulnerable—because measures taken to prevent one form of attack might not prevent another. Although we tend to think of acts of terrorism as large, spectacular events, many are also mundane criminal acts, such as kidnapping or murder. This is a short list of the different forms that terrorism can take.

- Car or truck bombings
- Suicide bombings
- Ram bombings (truck, plane, boat)
- Improvised explosive devices (IED) and other planted bombs
- Letter bombs/anthrax
- Dirty bombs (radiological dispersal devices)
- Chemical/nuclear/biological attacks
- Assassinations
- Sniper attacks
- Ambushes
- Drive-by shootings
- Hostage takings
- Kidnappings
- Airline hijackings
- Train hijackings
- Ship hijackings
- Rocket and missile attacks.

Which action will the terrorists choose? The type of attack a would-be terrorist chooses depends on the anticipated benefits of the act, as well as on the opportunities for carrying out the attack successfully. Box 1 lists these possible benefits. Not every terrorist act will return every benefit. For example, an airline hijacking can result in the taking of hostages whose lives can then be bartered for government concessions. On the other hand, although bringing down an airliner with a bomb can kill a large number of victims and create a climate of fear, it leaves little room for negotiation. So, depending on other factors—the

Box 1. The Goals of Terrorists.
Terrorists act to further both long-term and short-term goals. It is clear, however, that terrorists have great difficulty directly linking what they must do to carry out a successful operation to long-term goals, such as toppling a government. Understanding these long-term goals generally provides us with little guidance as to which targets they will choose. The exception to this rule is single-issue terrorists. Here is a list of possible long-term and short-term benefits of terrorist acts.

- Cause as much destruction and death as possible.
- Create a climate of fear.
- Create a media sensation.
- Disrupt everyday life.
- Disrupt a specific activity (e.g., recruiting police cadets).
- Disrupt commerce and industry.
- Demoralize security forces.
- Extort concessions (e.g., release of prisoners, removal of troops, policy changes).
- Eliminate an ideological opponent or an offensive icon.
- Humiliate officials and governments.
- Force an extreme government reprisal.
- Exaggerate the perception of the terrorist threat so that a relatively small terrorist group can exert great leverage.
- Create the impression of an all-pervasive force: "the enemy within."
- Show off to supporters, thereby strengthening the terrorist group.
- Intimidate rival political or terrorist factions.
- Maintain discipline within the group.
- Test or "blood" new recruits; train followers.
- Intimidate the population in the base of terrorist operations.
- Exploit perceived democratic weaknesses (i.e., the rule of law, free speech, laws against torture and pretrial detention).
- Break the enemy's will.

Read more on long-term and short-term goals: Headquarters, Department of the Army. Field Manual 7–98, "*Operations in Low-Intensity Conflict,*" Section 3.6, Combating Terrorism. Washington, D.C.: U.S. Government Printing Office, October 1993.

availability of weapons, accessibility of targets, and so forth—a terrorist group might find the timed detonation of a roadside bomb to be more effective than a suicide detonation inside a restaurant. The benefits of each of these bombings are different, even as the targets are different. Each of these acts also requires a different set of decisions and a different set of actions. Single-issue terrorists will choose targets that are directly linked to their issue. But even in these cases, terrorists must still choose from among a wide variety of options. Which animal laboratory? Which university? Which city? (See Box 2 for a comparison of the likely benefits for the terrorists from two notorious attacks.)

Single versus multiple attacks. The complexity and difficulty of a terrorist attack constrains how often the particular type of attack can be used. The major difficulty is distance from the target (see Brief 14). If the target is far away from the home base of the terrorist (e.g., the World Trade Center in the United States, al-Qaida in Afghanistan) sustaining multiple attacks is especially difficult. If the targets are close to home, however, as was the case with the Irish Republican Army (IRA) in Northern Ireland, then multiple attacks of a similar kind can be used and might even become routine. It is important, therefore, to distinguish between routine terrorism and one-off attacks. Routine terrorism has not taken hold inside the United States. The three major terrorist attacks in recent history—the attacks on the World Trade Center in 1996 and 2001, and the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma in 1995—were one-off attacks. One was domestic; the two on the World Trade Center were engineered by foreign terrorists (al-Qaida) who utilized domestic conditions to facilitate the attacks (that is, immigrant communities provided cover for foreign operatives).

Box 2. Terrorist Benefits from Attacking the World Trade Center and the USS Cole.

	World Trade Center Attack (New York City, September 11, 2001)		USS *Cole* Attack (Port of Aden, Yemen, October 12, 2000)	
Objective	Score*	Considerations	Score*	Considerations
Destroy and kill	10	Target completely destroyed; approx. 2,750 people reported killed.	3	Ship substantially damaged, but did not sink. Twelve servicemen killed.
Fear	9	Fear has declined with time.	3	U.S. citizens not directly affected because the act occurred at a distant location.
Create media sensation	10	Needs little comment.	4	Received considerable media coverage because of lives lost and innovative method of attack.
Disrupt everyday life	9	Immediate disruption in New York City, but security precautions have now merged into everyday life.	1	Disruption confined to USS *Cole*, the U.S. Navy, and diplomatic and government personnel.
Disrupt commerce	9	Drastic impact with some longer term effects.	1	Event confined to naval and military operations.
Force government compliance with demands	1	No demands made, but al-Qaida had consistently demanded the U.S. withdraw from the Middle Eastern region.	1	Security was improved; the United States did not withdraw from the harbor.
Force government overreaction	9	United States adopted the doctrine of preemptive war.	1	No powerful government reaction that gave succor to the terrorists.
Exploit weaknesses of democracy	9	The Iraq invasion led to fierce political discord at home and among allies.	1	People galvanized to support families and military.
All pervasive force	9	Constant concern about sleeper cells in the United States.	4	Event confined to military target in foreign waters, though sleeper cells were involved.
Humiliation	10	U.S. government exposed as vulnerable to a handful of foreign operatives.	3	Although lives were lost, naval personnel were seen to have acted courageously.

10=highest score; 1=lowest score

Source: Clarke, Ronald V. and Graeme R. Newman, *Outsmarting the Terrorists*. Westport, Connecticut: Praeger Security International, 2006.

Brief 11: Don't Waste Time on Motives

We have argued that terrorism is crime with a political motive. There are, of course, exceptions to this definition; for example, an offender who broke the election law for political motives would not be considered a terrorist. Others maintain that terrorists are driven by religious fanaticism although even here the overriding motive remains political because the ultimate goal is to topple secular governments. In any event, our point is that it is more productive to think of terrorism as crime than it is to think of it as an entirely different enterprise driven by a fanatical or extreme ideology—because even if the latter is true, there is little you can do about it, whereas if you think of terrorism as crime, your police experience can serve as a useful guide to dealing with terrorist acts.

The root causes of terrorism. Trying to understand the deep-seated motivations of criminals is not especially important in stopping them from doing what they want to do. This is because such analyses invariably lead away from the real-time actions of the offenders as they carry out their crimes. After a lengthy investigation, for example, we might find that a criminal was driven to serial rape because he was abused by his father as a child. But to what preventive action on the part of police can this discovery lead? We cannot change the past; neither can we alter family life so that parents no longer abuse their children. Economic or political oppression is the most popular cause ascribed to modern-day terrorism. This cause is unproven; but even if it were true, what relevance does it have to a police executive in a small town who is trying to decide what to do in the here and now?

Motivation and ideological commitment. The popular view of terrorists is that they are far more committed to their missions than are common criminals. Here the goal of the terrorist is viewed as superior to that of the criminal—the terrorist is driven by a religious or political ideal, whereas the criminal is driven merely by greed. Who is to say which goal is the most worthy? Knowing the motivations of terrorists and criminals does not tell us how committed they are. Do not confuse commitment with motivation.

It would seem that a suicide bomber is far more committed to completing his task than is a bank robber; however, the research on suicide bombers does not support this idea. In fact, people become suicide bombers for many reasons other than religious fervor—money for their families and public acclaim to name but two. Moreover, because a suicide bomber must die to successfully complete his task, the degree of his commitment to his ideal is a moot point: he gets only one chance at success. Bank robbers, on the other hand, have multiple criminal opportunities—at least until they get caught. Thus, one could conclude that persistent bank robbers are more committed than are suicide bombers. In short, whatever the ultimate motivation, both the terrorist and the criminal are committed to the successful completion of their acts. Without such commitment, the terrorist would not be up to the task—but neither would the bank robber.

Ideologies and target selection. If we were to study terrorist ideologies, would it give us any indication of when and where they will strike? We know that in Palestine, for example, suicide bombers rarely attack religious targets. They prefer crowded restaurants, buses, and markets. Their targets are operationally driven; that is, they wish to kill as many people as possible in places with which they are well-acquainted. In fact, although terrorist groups are driven by political or religious fanaticism, their ideology is often overridden by operational factors when it comes to choosing a specific target or weapon. This is why the 9/11 terrorists did not target the White House (too small a target), even though Osama bin Laden wanted them to. Thus, where resources are scarce, expending manpower on the study of the intricacies of terrorist ideology takes resources away from what really counts: assessing the operational factors that terrorists use in the successful completion of each task and designing ways to make each step in the terrorist attack more difficult. This can be done without a profound understanding of the terrorists' fanatical or extremist views, as we will see in subsequent steps.

The big picture. Many factors come together to create an act of terrorism. Some, such as the economic background and family upbringing of the terrorist, occur at a great distance from the actual terrorist act; others, such as the availability of targets and weapons, occur in close proximity to the terrorist act. Many of the factors that contribute to the causes of terrorism are distant from the point where police make decisions about the deployment of resources and manpower. Local police cannot hope to deal with these distant causes; but by focusing on the four pillars of terrorist opportunity—targets, weapons, tools, and facilitating conditions—all of which are accessible to intervention, police can control the opportunities for terrorist action and planning. This means that the opportunities for terrorist exploitation must be identified at the local level where actions can be taken to reduce these opportunities. As a local police executive, therefore, you are a significant player in countering terrorism.

"the opportunities for terrorist exploitation must be identified at the local level where actions can be taken to reduce these opportunities"

Brief 12: Think Terrorist

Terrorists are ordinary people. The first step in understanding the mind of the terrorist is to understand that terrorists are ordinary people with ordinary needs and ordinary limitations. They make decisions about their missions just as we make decisions about the tasks we carry out each day in our work and home environments. Terrorists must decide on their choice of target, how they will reach it, what tools they will need, and which weapons will do the job. In any given situation for any particular terrorist act, these decisions are extremely difficult because the circumstances that prevail in the place and time of the mission provide both opportunities for success and limitations on what the terrorist can achieve.

Planning an attack on the World Trade Center. The objective of the first attack on the World Trade Center in 1993 was to blow up one tower and topple it onto the other. Carrying out this mission required a number of steps.

1. Surveil the buildings inside and out to estimate how much explosive would be needed.
2. Assess the best place to detonate the explosive.
3. Obtain the necessary amount of explosive.
4. Obtain the tools for transporting the explosive (in this case, a large rental truck).
5. Obtain the necessary technology and skill to detonate the explosive.
6. Choose and train the operatives to carry out the mission.
7. Plan an escape route.
8. Gain access to the building (through the parking garage) and place the explosive in the desired location.

Although the attack caused considerable damage and loss of life, it was deemed a failure because it did not fully achieve its objective: the destruction of the Twin Towers. In planning the second attack, the challenge to the terrorists—in this case it seems to have been Osama bin Laden—was to overcome the weaknesses of the original plan. This was done by conceiving of commercial airliners as guided missiles and directing them at their targets in kamikaze style. The terrorists succeeded because they changed weapons, not because they changed targets.

Poor defenses make terrorism possible. The attacks on the World Trade Center were made possible by poor defenses. The first attack took advantage of poor security in the parking garage beneath the Twin Towers, which made them accessible to the truck bomb. The second successful attack took advantage of lax airport security, which had been implemented on the assumption that those hijacking an airliner were not prepared to die doing so.

Why were the Twin Towers targeted? At least two factors were at play: in the first attack they were accessible because of poor security; in the second, they stood out rather like sitting ducks. As we shall see later, there are a number of attributes that make some targets more attractive than others.

Every terrorist act goes through planning stages similar to the ones outlined earlier in this document, although the actual decisions terrorists make are specific to the particular form of terrorism that is contemplated. The accompanying Box shows how complex it can be to prepare for a simple suicide bombing, such as occurs in Israel on a routine basis. And even this example is considerably simplified.

From these observations we can draw some important conclusions that affect how to respond at the local level to the threat of terrorist attack.

- Terrorist targets are not chosen randomly. The common cry that 'We can't protect everything' is based on a false premise that terrorists choose their targets randomly. It is true that we cannot protect everything; but it is also true that we do not have to protect everything. Terrorists face tough decisions, just as we do. They must decide which targets to attack, and they must choose them based on their estimate of success, which is, in turn, informed by the availability of the weapons, tools, and conditions that will allow them to complete their mission. Furthermore, they operate for the most part in a hostile environment, one in which they are the hunted, particularly if they are trying to mount an operation in a foreign country a long way from their home base.

- There are many opportunities to stop terrorists from reaching their targets. Because of the complex logistics of terrorist operations—and especially their need for tools, weapons, and community support close to their intended target—local police can play a major role in identifying

the points of vulnerability in terrorist operations. Police departments that have a close working relationship with local communities that can be exploited by terrorists stand a better chance of stopping terrorists from reaching their targets.

- The availability of attractive targets will determine the type of terrorist attack. The harder a target is to reach, the more esoteric and innovative are the tools and weapons needed to reach it. It follows that the harder the target, the more difficult the planning, and the greater the resources needed to support the operation.

Preparing a Suicide Bombing Mission

There are three basic stages to carrying out a classic suicide bombing attack, such as when a terrorist with a bomb vest walks into a restaurant:

1. Preparation: personnel, targets, and tools.
2. Operation: getting the bomber to the target.
3. Aftermath: claiming responsibility and planning a new attack.

The Table outlines the steps needed to prepare for such an attack. Note that we chose this example because there is more information available about these kinds of attacks, not because it is likely that such an attack (common in Israel) is likely to occur in the United States.

Action needed	Resources needed
Step 1. Arrange a safe base of operations	
• Identify a friendly location for a safe house • Arrange its use	• Warehouse for storing bombing apparatus • Community collusion to support safe house
Step 2. Select target or targets	
• Find attractive targets that fit mission • Choose appropriate route to reach target • Visit target to assess logistics and accessibility	• Maps and reconnaissance of target areas • Intelligence sources from target location and proposed route to target
Step 3. Select bomber candidate	
• Use network to select candidate • Begin indoctrination of bomber • Payments to parents of bomber	• Supply of young zealots • Organizational network to identify candidates
Step 4. Specify exact location for detonation	
• Choose location (e.g., at bus stop X in front of busy market Y) • Choose alternative location if plan is thwarted	• Detailed information from local inhabitants at target location; reconnaissance
Step 5. Specify route to target	
• Plan exact route to target and method of transport (bus, taxi, on foot) • Prepare alternative routes	• Detailed knowledge of target area and routes • Support of local inhabitants helpful
Step 6. Establish group commitment	
• Group commitment sessions to bond conspirators to each other and to mission	• Trusted volunteers to encourage group commitment process
Step 7. Train bombers	
• Use of bomb vest and detonation procedures • Rehearse routes to targets	• Explosives and covering garments • Experts to assemble bomb vest
Step 8. Prepare propaganda	
• Proclaim bomber's martyrdom • Shoot video of bomber expressing commitment to carry out the mission	• Video camera, computer and editing software, poster materials • Photographs of bomber

Source: Clarke, Ronald V. and Graeme R. Newman, *Outsmarting the Terrorists*. Westport, Connecticut: Praeger Security International, 2006.

Brief 13: Counter "What if?" with "How Likely?"

Since 9/11, the specter of another attack from a foreign-based terrorist group has fueled the official response to terrorism and made the public afraid. The daily terror threat level that appears on TV stations at news hours serves to maintain this level of fear. When fearful, we entertain the possibility of all manner of disasters occurring and are likely to be besieged by these possibilities when interacting with citizens, community representatives, and local officials. What if terrorists poison the town's water supply? What if a terrorist set off a dirty bomb at the local sports arena? What if gunmen take over the elementary school? What if? What if? What if? One can imagine all kinds of dreadful scenarios—and they possibly could happen. But the important question is: how likely are they to happen in your particular jurisdiction?

How should you respond to every nightmare possibility? The truth is that any terrorist attack is highly unlikely. To respond to the threat as though an attack of the worst kind is imminent will only breed fear among your constituents and might well hinder you from developing an orderly plan to protect your community. To develop a logical plan you need to assess which special characteristics of your town—what particularly attractive targets—might lead terrorists to attack. You can identify such targets by applying the same sort of logic that is used to identify the types of products that are attractive to thieves.

Identifying attractive targets. Items that are the most popular targets of theft are defined by the lives of the people who own them and the businesses that make them. The popularity of these goods (e.g., automobiles, iPods, DVDs) means that there are many such items available to be stolen and many people available to buy them from the thief. Using this approach, we can identify the attributes that make products attractive and infer from these attributes the chances of their being targeted by thieves. The acronym **CRAVED** helps identify the attributes of products that are targeted by thieves.

1. **C**oncealable (thief hides iPod under coat).
2. **R**emovable (iPod snatched from chain around neck of victim).
3. **A**vailable (suddenly everyone has an iPod).
4. **V**aluable (iPods are expensive).
5. **E**njoyable (iPods are cool).
6. **D**isposable (everyone wants one).

In principle, every product can be stolen; but as we can see from this analysis, not every product will be stolen. In fact, most products are hardly ever stolen. Similarly, although it is possible that every building or person might be attacked by terrorists, the probability of most being attacked is vanishingly small. Most buildings and people simply do not make attractive targets for terrorists who want to maximize their benefits from every attack. Although it is true that we can't protect everything, it is also true that not everything needs to be protected, or at least protected to the same degree.

The attributes of targets that are attractive to terrorists can be summarized by the acronym **EVIL DONE**.

1. **E**xposed (the Twin Towers were the tallest buildings in the vicinity).
2. **V**ital (electricity grids, transportation systems, communications systems).
3. **I**conic (of symbolic value to the enemy, e.g., the Statue of Liberty).
4. **L**egitimate (terrorist sympathizers cheered when the Twin Towers collapsed).
5. **D**estructible (the Twin Towers were thought to be indestructible).
6. **O**ccupied (kill as many people as possible).
7. **N**ear (within reach of the terrorist group; close to home).
8. **E**asy (the Alfred P. Murrah Federal Building was targeted by a car bomb placed within 8 feet of its perimeter).

How we go about protecting targets from theft follows rather obviously from the analysis of their attractiveness. For example, iPods should not be displayed on open counters, should be packaged in large boxes, should not be worn around the neck, and so on. The same follows for the targets of terrorists. A simple concrete barrier at the right distance from the Murrah Building would have made it much more difficult for Timothy McVeigh to blow it up. Imagining how terrorists might find a way to make the Twin Towers exposed and easy to reach might have led to the anticipation of an aerial attack; in fact this approach was considered, but the warning was not heeded.

Of course, not every terrorist target will display every attribute to the same degree. Furthermore, new or innovative weaponry or tools can affect the destructibility and accessibility of targets. For example, a "ring of steel" composed of concrete barriers and steel fences has been placed around the White House, but this would not have protected it from the aerial attack that convicted al-Qaida terrorist Zacarias Moussaoui says he had planned for 9/11.

EVIL DONE allows us to make some pretty good guesses about targets that are likely to be attacked and the form such attacks might take. (See Brief 29 for more details about EVIL DONE.) This means that we do not have to protect everything to the same degree, even in the face of a nightmare attack. There are other logical ways to predict which targets are more likely to be attacked and which targets, if attacked, will cause the most grief. Insurance companies have been dealing with this problem for as long as they have operated: it is a matter of assessing the target's vulnerability to attack and the expected loss from a successful attack.

Vulnerability refers to the inherent features of a target that attract terrorist attack, such as is described in EVIL DONE. We can reduce the vulnerability of targets by taking the following steps.

- Assessing the attractiveness of potential targets and applying the appropriate preventive techniques.
- Reducing the opportunities for terrorists to obtain weapons that make it easier for them to take advantage of the inherent vulnerabilities of targets.
- Reducing opportunities for terrorists to take advantage of tools, such as new communications technologies, that can make it easier for them to organize their attacks and to reach their targets.
- Monitoring local conditions that can facilitate the terrorists' access to targets, tools, and weapons.

Expected loss refers to the anticipated injury or damage from a successful attack. For example, an attack on an electricity grid might be disastrous because it is an integral part of the infrastructure on which society depends; however, the availability of a backup system can minimize the loss. Although it might be inconvenient, an attack on an electricity grid might not directly kill or injure many people, as would the destruction of a large occupied office building. The frequency of attacks, of course, increases the loss. For example, the number of lives lost during the past 30 years to IRA terrorism (domestic terrorism) is about equal to the number killed in the single 9/11 attack (foreign-based terrorism). In contrast to Northern Ireland, however, the rarity of foreign-based attacks on the United States means that they cannot be predicted with certainty. Indeed, they are less predictable than are earthquakes—but they have the potential to create as much destruction. This is why we need to focus more on reducing vulnerability because by reducing vulnerability we also reduce the expected loss. At the local level, an attack by foreign-based terrorists is extremely unlikely, although there may be some places that are more at risk than others, such as large cities that contain many attractive targets.

Brief 14: Don't Overstate the Risk of Foreign Attack

Although rarely confronted with terrorist acts in their jurisdictions, police departments, unfortunately, are confronted daily with the threat of terrorism. Reports of terrorist attacks are graphically featured in local and national media, and police departments are expected to be prepared for another 9/11. Some large departments, such as the New York City Police Department (NYPD), have their own well-staffed counterterrorism departments, as do station officers in Israel and other places around the world where terrorist attacks regularly occur, so that they can get information quickly about terrorist activity.

Distance from the target. Proximity is probably the most significant factor in terrorist planning. The shorter or easier the journey from base to target, the better it is for the terrorist. This is why there have been so few terrorist attacks by foreign-based terrorists on U.S. soil and why there have been many more directed at U.S. embassies and businesses in parts of the world that are closer to terrorist bases, or where terrorist organizations have well-established satellite bases, such as in the Middle East. To sustain frequent and routine terrorist attacks, the following conditions must apply:

- The terrorist group must be well-organized and disciplined.
- The terrorist group must have strong support from the community in which it operates.
- The terrorist group must operate a financial system that collects and disburses money.

The IRA in Northern Ireland and the various terrorist factions in Palestine meet these conditions. Indeed, these groups have become so well-established that each has managed electoral victory. There is no way at present that a foreign group could establish itself in the United States to conduct terrorism on a routine basis. Instead, a foreign-based terrorist group must overcome the obstacles of distance if it is to attack the United States on its own soil. In the case of the 9/11 attack this required the following:

- Communications technologies that enabled monitoring of operatives from afar
- Placement of an al-Qaida point man and other recruits in the United States
- Recruitment and training of operatives to carry out the attack
- Financial support, including transfer of money to operatives
- Immigrant communities close to the target where operatives could hide and take advantage of local community services
- Selection of a suitable weapon that was undetectable by U.S. authorities.

The botched second attack on the London subway in 2005 exemplifies the difficulties of orchestrating an attack from afar. The operatives in the second attack were poorly trained and had poor logistical support; in fact, according to some reports, they might have had no support at all from al-Qaida. The subsequent

"a foreign-based terrorist group must overcome the obstacles of distance if it is to attack the United States on its own soil"

foiling of the attempt by terrorists to blow up aircraft bound for the United States in August of 2006 underscores the importance to foreign-based terrorists of well-established immigrant communities. In this instance, it was not necessary to place foreign operatives inside the target country, as had occurred in the 9/11 operation. The inherent difficulty of carrying out foreign-based terrorist attacks suggests that the chances of another attack in the United States of the scale and expertise of 9/11 are remote, although not impossible. And if it were to occur, it will be a long time in preparation, as was the case with the 9/11 attack.

Will it happen here? Should we study overseas terrorist events because their methods might be used against the United States? Indeed, top counterterrorism officials have repeatedly warned that suicide bombers will descend on New York or other large U.S. cities. The NYPD counterterrorism squad presses restaurant owners in downtown Manhattan to install Kevlar curtains for protection in the event of an explosion. Does it follow that particular methods of attack used overseas they will be used in the United States? Because of the obstacles of distance, they probably will not; and because suicide bombers choose restaurants as their targets in Jerusalem, it does not follow that a suicide bomber operating in the United States will choose such targets, even in small or medium-size cities. There is a huge range of targets from which to choose. If you have just one or even two opportunities to blow up a target, why choose a restaurant when there are more attractive targets available?

Taking too much notice of attacks that occur overseas also runs the risk of causing reactions at home that far exceed the threat. Richard Clarke, counterterrorism chief under both the Clinton and Bush administrations provides us with a good example. Based on the occurrence in 1996 of a rash of suicide bombings in Israel, the Khobar Towers bombing in Lebanon, and the explosion of TWA 800 on take-off from JFK Airport in New York, Clarke jumped to the conclusion that the 1996 Olympic Games in Atlanta were a likely terrorist target. Consequently, millions of dollars were spent upgrading security in Atlanta, but the only terrorist act was the detonation of a small bomb placed in a trash can by an antiabortion fanatic. This enormously expensive exercise in security has been copied in subsequent Olympic Games and repeated at major sporting and entertainment events, including the Republican and Democratic conventions. Of course, all of these events require security, but questions that have never been asked are how much security is sensibly necessary and what kinds of attacks are anticipated? There have been very few attacks or even attempted attacks by foreign based terrorists on U.S. soil during the last 40 years. In contrast, domestic terrorists have been more active.

Brief 15: Beware the Domestic Terrorist

The immediate reaction of law enforcement and the media to the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, was that it must have been the work of a foreign fanatic. Instead, it turned out to be a domestic fanatic. From 1998 to 2004 there have been 98 incidents of domestic terrorism, resulting in 177 deaths. Unfortunately, 2,817 people were killed in the handful of foreign attacks that have taken place in that time. So although there have been many more incidents of domestic terrorism in the United States, their lethality has been considerably less than those of foreign terrorist attacks.

Single-issue terrorists. With some minor exceptions, domestic terrorism in the United States is confined to single-issue terrorists who use violence to advance their causes. These include ecoterrorists, antiabortionists, and various hate groups. Of these, the Earth Liberation Front (ELF) and Animal Liberation Front (ALF) have been the most active in recent years. Neither of these groups has caused the death of any individual, although they have caused considerable property damage. A number of deaths have resulted from the activities of antiabortionists, who tend to act alone. Other than the Oklahoma City bombing, there have been few militia attacks, with the attack by Timothy McVeigh being the most lethal.

The planning of these attacks generally follows the major principle of terrorist (and criminal) planning described earlier: domestic terrorists attack targets that are close to their bases of operations. It is no coincidence that McVeigh attacked a federal office building in Oklahoma City, rather than one in Washington D.C., the center of the government that he despised so much. McVeigh felt comfortable in Oklahoma City, which was close to his militia-based connections, which made managing his bomb-making that much easier (see Box). Similarly, ELF and ALF conduct their activities in particular locations—generally the far west, the Great Lakes region, and the northeastern United States. Moreover, their single-mindedness makes it easier to predict which targets these groups are more likely to attack. For ALF, any structure or organization that uses animals is a possible target, including research universities with animal laboratories. For ELF, SUV dealers and property developments near wilderness areas are possible targets. In these instances, we can narrow considerably the targets that need to be protected.

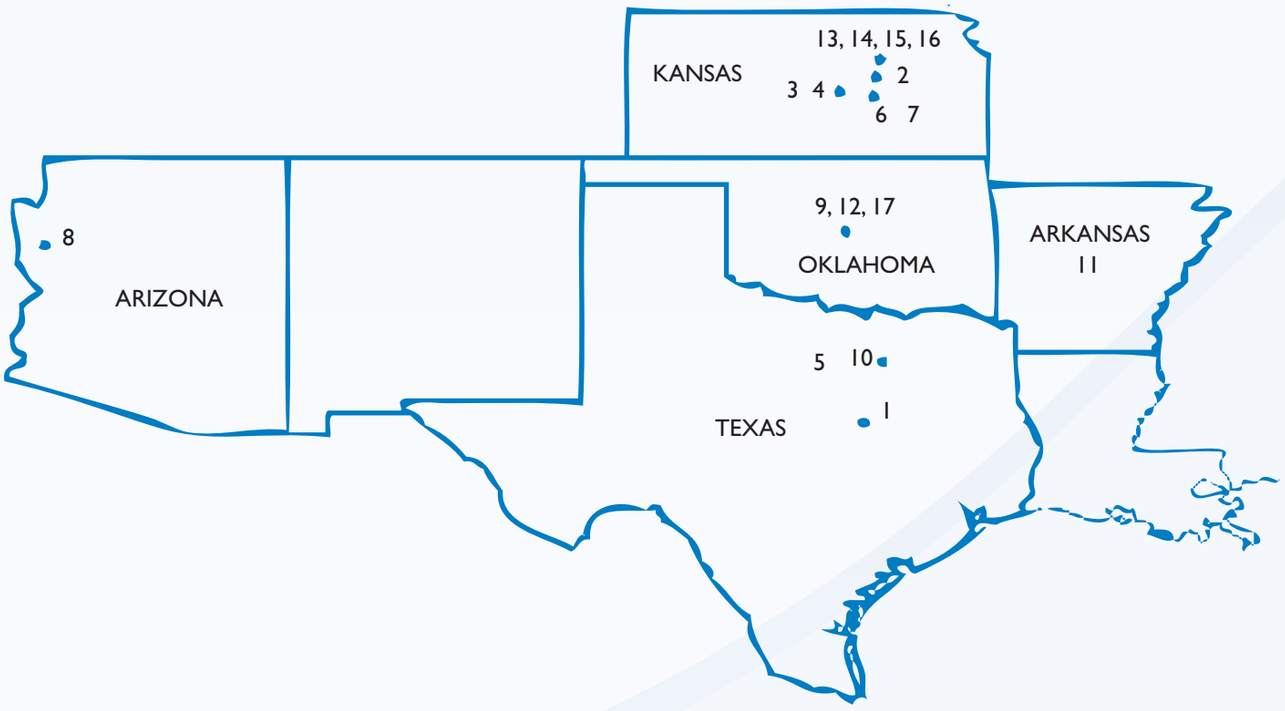
Routine terrorism in the United States. None of these domestic terrorist groups has shown the ability to conduct routine and repeated attacks on the scale of the IRA in Northern Ireland or the various terrorist groups in Palestine. This is probably because they lack the organizational capability to sustain many attacks. It might also be that they are not as committed to violence as are other terrorist groups. Exceptions to this general truth were the violent antiwar and black power protests that took place during the Vietnam era and the series of bombings that was carried out in New York City by the Puerto Rican Liberation movement during the 1960s and 1970s. The latter was a coalition of domestic and foreign-based terrorist groups that exploited the cover provided by New York City's well-established Puerto Rican immigrant community to conduct repeated small-scale bombings of banks and other buildings. The terrorists were few in number and were eventually caught and imprisoned or killed in action. The attacks died out quickly.

Could something similar happen again? If so, what weapons, tools, and facilitating conditions might make domestic terrorism easier? There are several possibilities.

- The widespread availability of small arms in the United States, especially among inner-city gangs.
- The long history of gang violence among Latino and other gangs in large U.S. cities.
- The existence of gangs composed of former paramilitary extremists such as the Mara Salvatrucha, which originated in El Salvador.
- The deportation of gang members to their home countries, thus creating de facto international criminal networks.
- The existence of well-established immigrant communities that provide cultural cover for potential terrorists.

Nobody knows whether—given a cause and a leader—these conditions will result in a significant homegrown terrorism problem.

Journey to a Bombing



Key to Map

1. March 1993: McVeigh went to Waco to see the standoff between the Branch Davidians and Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). The Waco incident allegedly fueled his decision to attack the federal building in Oklahoma City.
2. September 22, 1994: McVeigh rented a storage unit in Herington, Kansas. McVeigh and coconspirator Terry Nichols collected bomb-making materials and stored them in the unit before assembling the device.
3. September 23, 1994: McVeigh purchased 10 bags of fertilizer from the Mid-Kansas Cooperative Association in McPherson, Kansas.
4. September 30, 1994: McVeigh and Nichols purchased forty 50-pound bags of ammonium nitrate in McPherson, Kansas.
5. September 30, 1994: McVeigh purchased three drums of nitromethane at $950 each from V.P. Racing, located south of Dallas, Texas.
6. October 1, 1994: McVeigh and Nichols stole explosives from a storage locker in Marion, Kansas.
7. October 3, 1994: McVeigh and Nichols stole sticks of dynamite, 544 electric blasting caps, and 93 conventional blasting caps from the Martin Mariette Quarry, Marion, Kansas.
8. October 3, 1994: McVeigh and Nichols transported the stolen explosives to Kingman, Arizona, where McVeigh rented another storage locker.
9. October 10, 1994: McVeigh and Nichols drove through Oklahoma City on the way to buy nitromethane at a Dallas racetrack.
10. October 10, 1994: They drove by the Murrah Federal Building and estimated how long it will take McVeigh to walk away from the bomb site.
11. November 5, 1994: McVeigh and Nichols robbed a firearms dealer in Arkansas.
12. December 18, 1994: Accompanied by old friend Mike Fortier, McVeigh traveled to Oklahoma City and confirmed the targeting of the Murrah Building, having previously rejected buildings in Kansas City, Kansas, and Little, Kansas.

III. Develop a Plan and a Support Network


LINE DO NOT CR

“Ironically, responding to an attack is the least problematic component of any counterterrorism plan.”

Brief 16: Cover the Three Bases of Counterterrorism

This brief provides an overview of the three main components of a counterterrorism plan, which we then describe in detail in the final three parts of the manual.

1. Collecting intelligence about possible terrorist activity (Briefs 21–28).
2. Hardening targets (Briefs 29–36).
3. Being ready to respond in the event of an attack (Briefs 37–50).

Ironically, responding to an attack is the least problematic component of any counterterrorism plan. No doubt you already have well-established procedures for dealing with conventional disasters. With some adjustments, your existing emergency operations plan can help you cope with the possibility of a terrorist attack. For example, you will need to anticipate possible follow-up attacks on rescue workers and consider the possible use of weapons of mass destruction, but even here the necessary actions are relatively clear and specific. Provided that established procedures are followed carefully and that you work in close partnership with those who bear the ultimate responsibility for the emergency plan, your community should be well-prepared to respond to, and recover from, a terrorist attack. If you do not plan carefully and things go wrong, you can expect to be criticized, and deservedly so.

Matters are not nearly as clear-cut for the other two components. Far less guidance is available on how to determine which targets to protect and how to collect intelligence about terrorists. It is especially unclear how much effort you should put into intelligence gathering. You should, of course, encourage your community policing officers to watch for possible terrorist activity in their neighborhoods—particularly immigrant neighborhoods—and you should immediately communicate any information they report to the FBI, which has the ultimate responsibility for investigating terrorists in your jurisdiction. For the common good, you should also participate in the local Joint Terrorism Task Force, and have one of your officers trained as a terrorism liaison officer (http://www.tlo.org/training/index.htm). Whether you invest in more formal methods of gathering and sharing intelligence will depend on the size of your jurisdiction and your judgment about its vulnerability. For most small jurisdictions, it is doubtful that the investment would be justified because the risks of terrorism are so low that any special system to collect and share information would yield very little benefit and quickly lapse into disuse. Perusing the National Criminal Intelligence Sharing Plan may help you decide on how much of your resources to invest in information sharing and collection. (http://www.it.ojp.gov/topic.jsp?topic_id=93)

In small, low-risk jurisdictions, target hardening is also somewhat problematic. For a start, it is still unclear how to read the 9/11 attack. At the time, it was widely believed that the attack signified that the United States would be under continuous attack from overseas terrorists for the foreseeable future. Seven years on, however, there has been no repetition of the attack in

the United States. Whether this is because security forces have been successful in intercepting and deflecting all further attacks, or whether it is simply a reflection of geography—the United States is very difficult for terrorists to attack from overseas—is not known. So, although global terrorism is probably here to stay, it is impossible to know when or whether the United States will be attacked again. This uncertainty undermines the argument for extensive target hardening, particularly in light of the costs and effort involved. All those underground nuclear shelters, which became redundant at the end of the Cold War, warn against letting fear drive policy.

Very little guidance exists about which targets to harden, how to harden targets, and how to prioritize target hardening. In 2006, for example, the Department of Homeland Security's (DHS) National Asset Database (NAD) listed 77,069 critical sites that were nominated by states making pitches for federal terrorism funds. Included were many unlikely targets, including Old Macdonald's Petting Zoo, the Mule Day Parade, the Mall at Sears, and Nix's Check Cashing. Indiana's list contained 50 percent more sites than did New York's, including businesses such as Amish Country Popcorn. When questioned about its inclusion by reporters from *The New York Times* (July 12, 2006), the owner of this five-employee establishment seemed as puzzled as everybody else: "Only Amish buggies and tractors here. Maybe because popcorn explodes?" This occurred 1 month after the DHS announced the completion of its National Infrastructure Protection Plan (NIPP), a plan based on a risk management approach (see Brief 19; for further information on vulnerability and risk assessment, two key concepts adopted by the NIPP, see Briefs 29–33). In line with the NIPP, which is still awaiting implementation, it probably makes sense for you to pursue a three-tiered approach to target hardening.

1. Protect obvious targets as soon as possible. Because some targets are privately owned, your role is to liaise with the owners, offer advice that you feel qualified to offer, encourage owners to engage professional security consultants, and serve as a broker between businesses and state and federal agencies that can offer assistance in implementing hardening measures.
2. Draw up both a prioritized list of other targets that require extensive hardening and a timetable for ensuring that this is done.
3. Develop a longer list of all possible targets that should be protected by some basic hardening measures, and monitor plans by the owners of these facilities to put basic security measures in place (Brief 33).

In persuading facility owners to take security measures, explain that such measures will provide protection against both terrorism and conventional crime. Procedures that make it harder for terrorists to gain access to a facility will also help keep out burglars and vandals. In fact, a touchstone of your counterterrorism effort should be to implement those target-hardening measures that will afford dual benefits. Because the risks of a terrorist attack in any particular place are quite low, counterterrorism measures that benefit normal policing operations will be easier to justify, both socially and financially.

"Because the risks of a terrorist attack in any particular place are quite low, counterterrorism measures that benefit normal policing operations will be easier to justify, both socially and financially."

Brief 17: Work with Business

Government and business make uneasy partners, and this is no less true when it comes to crime. Police have often been content to let businesses protect themselves from crime and deal with offenders in their own ways. Occasionally, this arrangement breaks down, as when merchants complain that the local police do not prosecute shoplifters or when police claim that stores do too little to protect their goods.

In the case of terrorism, however, government and businesses must forget old habits and work together for several important reasons. First, businesses own 85 percent of the country's infrastructure, such as reservoirs, chemical plants, transport systems, ports, airliners, communications, etc., which are highly vulnerable to terrorist attack. Second, terrorists often select targets for their symbolic or iconic value—the 9/11 terrorists targeted the World Trade Center because it was a symbol of capitalism—and some companies are uniquely identified with the American way of life. Prominent examples include McDonald's, Wal-Mart, Starbucks, Nike, Hilton, and Marriott. Thus, some Internet web sites claim that Starbucks is anti-Muslim and despite its efforts to address environmental ills, the company has become a target for the radical left. Last, some domestic terrorists target businesses such as mink farms, butchers, and abortion clinics (see Brief 15). As former Homeland Security Secretary Tom Ridge stated: "We are a target-rich environment, and the private sector owns most of the targets."

Businesses are inextricably linked with civil life in the United States. They are located in communities where many of their employees, clients, and customers live. They are often located near enough to their neighbors that an attack on the business is tantamount to an attack on the community. Just as businesses strive to protect their own employees from catastrophic harm, they should strive to protect their neighborhoods and communities, too.

Businesses are not merely targets: they are also an important source of information and resources. Banks can provide information about the financial transactions of suspect organizations, telephone and credit card companies can assist in keeping track of suspect persons, car rental companies and motels can tell you about recent visitors, and agricultural supply stores can track sales of combustible fertilizers. Businesses also invariably step in to help when a major disaster occurs. More important than any of this, however, is that business leaders are as loyal and patriotic as are any other members of the community (see Box 1).

Box 1: Corporations Are Not Just Buildings, Machines, and Paper.

"Corporations are not just buildings, machines and paper; they are employees and shareholders and managers and directors who are all influenced by patriotism; loyalty; and an overarching commitment to our nation's social values, individual freedoms and market economy. When a business takes steps to protect itself and others, part of the calculus for doing so should, and inevitably will, include an interest in supporting our country and protecting its people."

Source: Susman, Thomas. *Terrorism: Real Threats. Real Costs. Joint Solutions.* Washington, D.C.: The Business Roundtable, 2003. http://www.businessroundtable.org/pdf/984.pdf.

Work with businesses to: (1) make their premises, facilities, and operations more secure; (2) develop an emergency plan in case of a direct attack; and (3) involve them in rescue and recovery planning in the event of an attack elsewhere in your jurisdiction. Your points of contact with businesses might include the following:

- Routine calls on businesses by beat officers
- Regular presentations on terrorism at meetings of the Lions, the Elks, the Rotary Club, and similar organizations
- Physical surveys of retail businesses and other commercial establishments by officers trained in site security
- Meetings with the chief executives of large companies and contacts with local and regional managers
- Regular meetings with the security managers of larger businesses.

The security managers of large businesses are likely to prove one of your most useful partners (see Brief 18); but remember that large businesses are not necessarily at greatest risk of attack. The businesses most at risk fall into four main groups and these are the businesses on which you should focus your energies: (1) those responsible for infrastructure, such as reservoirs and power stations; (2) those responsible for facilities in which many people gather, such as mass transit hubs, malls, sports arenas, and theme parks; (3) those that will inflict collateral damage if attacked, such as chemical and biological plants; and (4) those that are commercial icons, such as McDonald's and the other companies mentioned above.

You might be surprised by the lack of cooperation from a particular business. There are a number of possible reasons for such a reaction: some companies might simply be willing to live with the unknown and probably very small risk of attack; other

companies might have developed a false sense of security in the 7 years that have passed since 9/11; still other companies might be willing to risk substandard security because they believe that the government will bail them out if the worst happens. In addition, some companies might be constrained by their financial and managerial environments, such as the following:

- Businesses that belong to national chains might have to conform to the security practices laid down by headquarters.
- Companies might fear that incurring substantial security costs will put them at a significant competitive disadvantage.
- In today's just-in-time markets, anything that delays a company's operations is seen as anticompetitive.
- Companies might be reluctant to initiate costly new security procedures that are likely to change in the wake of a terrorist strike.

"you should emphasize dual benefit measures: those that will protect the business not just from terrorism, but also from crime"

Many companies fear that a thorough security assessment will reveal serious shortcomings that they will have to spend vast amounts of money to fix, lest they be accused of willful negligence if something bad occurs (see Las Vegas example in Box 2).

Box 2. A Failed Briefing.
In 2004, information received by U.S. intelligence agencies indicated that Las Vegas casinos were being targeted by Islamic terrorists. In an effort to be proactive, the FBI called a meeting in Las Vegas and invited the security directors of all major casinos to attend and be briefed on the information. The only people who attended the meeting were two local police officers. Internal Justice Department memos allege that the casino's desire to avoid liability was one reason that no casino security directors attended.

Source: Garcia, Mary Lynn, "Risk Management," in *The Handbook of Security*, ed. Martin L. Gill, Basingstoke, England: Palgrave Macmillan Ltd., 2006.

For all these reasons, you should emphasize dual benefit measures: those that will protect the business not just from terrorism, but also from crime, which might help to increase profits. Such measures go beyond the first level of security preparedness— perimeter security, intrusion detection, and guards and patrolling—to include know-your-customer bank policies, strengthened customer ID requirements for car rental businesses and motels, and criminal record checks on prospective tenants by managers of apartment complexes.

Brief 18: Partner with Private Security

Despite the common concerns of police and private security, community police officers are more likely to meet with clergy, business groups, and neighborhood associations than with local security professionals. In fact, private security professionals can provide invaluable help in securing your community from attack. They are responsible for the security of most of your jurisdiction's infrastructure and provide visible crime control in the places where people spend much of their daily lives: at work, on public transport, in educational facilities, in shopping malls, and even in gated communities. Indeed, it has often been observed that although the public sector controls terrorism information and intelligence, it is the private sector that controls the most vulnerable and likely targets of attack.

Benefits

In the United States, private security employees outnumber the police by three to one. Partnering with private security in your jurisdiction will allow you to call on a much larger body of men and women to help meet your antiterrorism responsibilities. Specifically, it will help you to do the following:

- Safeguard the critical infrastructure in your community that is protected by private security and ensure rapid recovery in the event of an attack.
- Obtain effective help from private security in emergencies. Because security officers are often the first responders, police can coordinate private security efforts with regard to evacuation, food, and other emergency needs.
- Improve the flow of information—in both directions. Partnering will allow you to communicate threat information to the private sector efficiently and, conversely, it will allow the private sector direct access to the right people when they need help or want to report information.
- Make use of private-sector knowledge on topics that your department might know little about, such as fraud and cybercrime.
- Obtain access to private-sector resources and facilities that will help you meet training and operational needs.

Trust

Take charge of the partnership, but to obtain full cooperation be sure to give your private sector colleagues public credit for their contributions. Deal with them as equals. This might be easier for you than for some of your officers, who might feel that private security personnel are untrained, particularly in handling weapons; that they are poorly regulated and insufficiently accountable for their actions; and even that they are wannabe police officers who could not get a badge. These perceptions reflect a limited understanding of the role of private security personnel and a limited appreciation of their capabilities, expertise, and resources. For their part, private security officers might see the police as arrogant and uninterested in their field—until they are looking for a retirement job. Working together might have the effect of dispelling these misperceptions and prejudices.

Perhaps the most critical issue concerns the handling of sensitive information. Your officers might be uncomfortable sharing threat information with companies owned by foreign entities; other information, such as criminal histories, is protected by privacy laws. For their part, private security might fear that proprietary business information will become public under freedom of information laws. They might not speak candidly at partnership meetings lest competitors learn about their problems or because they fear being charged with antitrust violations or even criminal wrongdoing. Finally, they might not report instances of cybercrime lest your department seize their records or computers. In a word, it all boils down to mutual trust, which takes time and patient negotiation to develop.

Organization

As mentioned in Brief 17, one of the best ways to approach the larger businesses in your community is through their corporate security officers, but there are many other security professionals in your community, including local security consultants, the suppliers of guard services, managers of burglar alarm companies, and installers of security hardware and systems. You might think you already have good informal contacts with these groups, facilitated by the many retired police officers employed within their ranks; however, senior private security posts are now increasingly filled by managers promoted from within; the "good ole boy" networks are disappearing. According to the DHS, the goal of preventing terrorism is better served by formalized relationships between police and private security, whether though coordination agreements or memoranda of understanding. Formalization shows employees on both sides that the partnership is an organizational priority.

Getting started

- Involve the top security professionals in your area. Let them suggest others who should be involved.
- Clarify the purpose of the partnership and set goals for improved collaboration and coordination.
- Spell out what the partnership must do to accomplish its mission. (See the Box for typical activities.)
- Identify the resources the partnership will need to meet its goals and find ways to secure these materials.
- Find a physical and logistical home for the partnership and appoint a police officer to coordinate its activities.
- Decide how the partnership members will communicate, both routinely and in emergencies.

- Create an identity for the partnership through the use of a logo, brochure, or web site, and use this identity to obtain funds and recruit members.

Read More: Office of Community Oriented Policing Services. National Policy Summit: *Building Private Security/ Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2004.
http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RIC=246

Some Activities of Police/Private Security Partnerships

Networking

- Regular meetings to discuss problems and to help each side understand the problems and motivations of the other.
- Lectures by private security professionals at police training centers.
- Speeches by one group at conferences of the other.
- Directories of local police and private security contacts.
- Honors and awards from one group to the other.

Information Sharing

- Information provided by police on criminal convictions, threats, and incidents, where permitted by law.
- Information provided by the private sector on business crime and suspect employees.

Crime Prevention

- Joint participation in security and safety for business improvement districts.
- Consultation on situational crime prevention and community policing.
- Special operations on local concerns, such as check fraud or false alarms.
- Joint support of Neighborhood Watch and National Night Out.

Resource Sharing

- Technical and logistical expertise.
- Specialized equipment and facilities, such as auditoriums, classrooms, and conference rooms.
- Office space for community policing activities, such as storefront ministations.

Training

- Hosting speakers on topics of joint interest.
- Exchanges of training and expertise. Corporations can offer management training to police, private security can train law enforcement in security measures, law enforcement can teach security officers how to testify in court or how to gather evidence in accordance with prosecutorial standards.

Legislation

- Drafting and supporting laws and ordinances on such topics as security officer standards and licensing, alarms, and computer crime.
- Tracking legislation of importance to law enforce-ment and security operations.

Operations

- Joint investigations of complex financial fraud and computer crime.
- Critical incident planning for natural disasters, school shootings, and workplace violence.
- Joint sting operations.

Source: Bureau of Justice Assistance, *Operation Cooperation: Guidelines for Partnerships between Law Enforcement & Private Security Organizations*. Washington, D.C.: U.S. Department of Justice, 2000.

Brief 19: Know About Risk Management

If you have not already done so, identify the targets in your jurisdiction that are at the greatest risk of terrorist attack and, therefore, are most in need of protection. In small towns, this might not be difficult because there might be only a few targets to attract terrorists—say, the reservoir, a chemical plant, and the two or three local schools. Together with the managements of these facilities, you should be able to develop a plan to protect them from feasible threats. If your jurisdiction is larger, the process of identifying threats and determining priorities becomes much more challenging simply because there are so many more targets to consider and so many more threats and consequences to weigh. In these circumstances, you might want to institute a formal risk assessment as part of a risk-management program.

Risk management is a procedure used by corporations to identify, prioritize, and deal with major threats to their profitability and continued operations. These threats might be the result of natural causes (hurricanes, snow storms, failure of telephone and computing systems, viral epidemics, or even the unexpected death of the CEO) or malevolent human action (sabotage, robbery, fraud, hacking). Risk management is being used increasingly by government agencies, and the DHS advocates its use in assessing and responding to terrorist threats.

Risk management can be highly technical, especially when data exist to support quantitative assessments of threats and countermeasures. Institutes, professional associations, and journals exist to serve the needs of its practitioners. We will not attempt to provide a detailed description of the technicalities; instead, we will provide you with enough information to judge whether you need to commission a formal risk-management study in your jurisdiction. We will also tell you how to undertake a risk-management study that might not meet professional standards, but that might satisfy your immediate needs. To do so, we draw heavily on an excellent guideline (see Box) produced by ASIS International (formerly, the American Society of Industrial Security).

The first step in a risk-management exercise is risk assessment. In a terrorism risk assessment, the analyst attempts to answer the following questions. What targets might be attacked and how? What is the likelihood that the targets will be attacked? The answers to these questions assess the vulnerability of the targets. What would be the consequences for your city, in both the short and long term? The answer to this question assesses the expected loss. Answering these questions, therefore, helps in identifying, evaluating, and prioritizing risks. Risk management builds on these answers to address a second set of questions. What actions can be taken to reduce the risks of attack? What are their associated tradeoffs in costs, benefits, and risks? How would their choice constrain future options? This is called mitigation.

You might question the value of undertaking a risk-management study based on this process. There are so many difficulties involved in making the estimates needed at each of the seven steps that the results will necessarily be fraught with uncertainties and qualifications. Although this is true, it might still be worth going through the process because this will force you to look carefully at each potential target. The results might be both surprising and helpful. You might discover, for example, that the target that everyone believes is most vulnerable has already taken security precautions that considerably reduce its risks. In light of this information, you would be able to concentrate your attention on less-vulnerable targets that have not taken minimum precautions.

Read More: Department of Homeland Security, *National Infrastructure Protection Plan*. Washington, D.C., 2006. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Dewar, James A. *Assumption-Based Planning: A Tool for Reducing Avoidable Surprises*. New York: Cambridge University Press, 2002.

The ASIS International Guideline on General Security Risk Assessment.

Although this guideline is intended to help security professionals identify crime risks at a specific location and to assess possible solutions, it can be adapted to identify the risks of a terrorist attack. If you cannot hire a professional risk-management consultant, you can use the guideline to undertake your own study, especially if you can obtain the help of a knowledgeable security professional.

Once you have identified the targets most at risk of attack, apply the seven-step guideline to each. We have modified the description of the seven steps to make them more relevant to terrorist attack.

1. **Identify the people and assets (property, networks, and information) at risk for each target.**

- People include all those involved with the enterprise and in neighboring communities.
- Property includes buildings and intangible assets such as intellectual property.
- Networks include all systems, infrastructure, and equipment associated with data, telecommunications, and computer processing.
- Information includes various types of confidential and proprietary data.

2. **Specify the types of attack and vulnerabilities.** Terrorist attacks can come in many forms (truck bombs, hostage takings, shootings) and for each facility that is at risk try to identify the form of attack to which it is vulnerable. The vulnerability analysis should take into consideration anything that might be taken advantage of to carry out an attack. This process should highlight points of weakness and will assist in the construction of a framework for subsequent analysis and countermeasures.

3. **Estimate the probability of each form of attack.** Here is where you enter the realm of guesswork—with the safest estimate being zero. It will be easier to rank the forms of attack than to establish their likelihood. For example, a reservoir is more likely to be contaminated than it is to be attacked with bombs.

4. **Determine the impact of an attack.** Determine the likely impact of each form of attack for each target. Try to estimate likely deaths and injuries, property losses, disruption to everyday life, rescue and recovery costs, and the emotional effect (chiefly fearfulness) on the community.

5. **Develop options to mitigate risks.** Identify options available to prevent or mitigate losses. These might range from passive acceptance of the risk through a range of security options, including installing equipment or hardware; altering policies, procedures, and management practices; and hiring and training security staff.

6. **Study the feasibility of implementing your options.** The practical considerations of each option or strategy should be taken into account at this stage of the assessment. Financial cost is an obvious factor, but equally important is whether the strategy will interfere substantially with the operation of the enterprise. For example, stringent access control procedures at a mall or arena might create a negative environment that effectively discourages people from entering the facility. The challenge is to find a balance between a sound security strategy and the operational needs of the enterprise, as well as the impact on the people affected by the security program.

7. **Perform a cost-benefit analysis.** In this final step, consider the costs and benefits of a given security strategy. Determine both the costs of implementing a strategy (financial, managerial, social, environmental) and the various benefits, not simply reducing the harms that might result from an attack, but also other benefits, such as reducing the risk of crime.

Source: ASIS International, *General Security Risk Assessment. An ASIS International Guideline*. Alexandria, Virginia, 2003. http://www.asisonline.org/guidelines/guidelinesgsra.pdf

Brief 20: Go After Terrorism Grants

Grant funds can help you meet your responsibilities regarding terrorism by paying for equipment, training, and overtime. If you are successful in obtaining grants, your overall budget will increase substantially. As well as helping you to meet your responsibilities, these funds might allow you to develop your department in ways that you have always wanted.

If you establish a terrorism unit, writing grant applications and managing grants can be one of its principal duties. With so much money at stake, make sure that you choose an energetic and ambitious officer to head the unit. He or she will be very busy applying for and managing grants and might make a considerable contribution to your bottom line. Grants are available from federal, state, and private sources.

Federal sources. Federal agencies that offer counterterrorism grants provide different levels of funding, offer different opportunities, and have differing eligibility requirements and application processes. The following is a list of some potential sources. Sources for more specific purposes are detailed elsewhere in this manual.

- **Department of Homeland Security** (http://www.dhs.gov): The DHS makes millions of dollars in grants available each year for equipment, technical assistance, and training.
- **Counterterrorism** (http://www.counterterrorismtraining.gov): This source originated with recommendations made by the U.S. Department of Justice's Counter-Terrorism Training Coordination Working Group. It offers counterterrorism tools to the law enforcement and first-responder communities.
- **Grants.gov** (http://www.grants.gov): This source originated from a 2002 Presidential Initiative to improve access to government services for the public. Law enforcement agencies can review grant solicitations and apply online.
- **State and Local Anti-Terrorism Training** (http://www.slatt.org): The SLATT program is a joint effort between the FBI and the Bureau of Justice Assistance (BJA). Coordinated by the Institute for Intergovernmental Research (http://www.iir.com), it is intended to provide specialized training to police in dealing with terrorism and criminal extremism.
- **Bureau of Justice Assistance** (http://www.ojp.usdoj.gov/BJA): BJA is one of the largest sources of federal funding. Its Programs Division coordinates state and local grants.
- **Office of Community Oriented Policing Services** (http://www.cops.usdoj.gov): The U.S. Department of Justice Office of Community Oriented Policing Services (the COPS Office) has expanded its original role of providing resources for community policing to include providing resources to combat terrorism.
- **National Institute of Justice** (http://www.ojp.usdoj.gov/nij): Although the National Institute of Justice does not make programmatic grants, it does make research and evaluation grants. Law enforcement agencies usually are required to partner with a research institute or university before funding will be granted.
- **Office for Victims of Crime** (http://www.ojp.usdoj.gov/ovc): The Office for Victims of Crime is unique because it expressly provides resources to support crime victims. It, too, has expanded its role to include the provision of funds for victims of terrorism and mass violence.

State grant funds. State administrative agencies (SAA) are responsible for coordinating state and federal funding and for passing federal funds to local jurisdictions. Designated SAAs vary from state to state. In New Jersey, the designated SAA is the Office of Homeland Security and Preparedness; in California, it is the California Office of Homeland Security. Visit http://www.ojp.usdoj.gov/odp/contact_state.htm to find your designated SAA contact.

Private foundations. The thousands of foundations that fund program areas each year are often overlooked by law enforcement agencies. An Internet search will swamp you with possibilities; fortunately, guides that will help you target foundations that finance programs in your state and geographical area are available from: Research Grants Guides, Inc., P.O. Box 1214, Loxahatchee, FL 33470 (Telephone: 561.795.6129; Fax: 561.795.7794). You need only review the guides for specific categories (e.g., equipment grants, building grants) to find a funding source and request a grant application.

Applying for funding. The several steps in the life of a grant typically include strategic planning and command staff meetings before the actual writing begins. The Chart illustrates the steps that comprise a typical grant application. Depending on local conditions and the type of grant application, your development team might be able to shorten the process.

Writing the grant. Before beginning to write, your team must research the topic using the Internet, beginning with the National Criminal Justice Reference Service (http://www.ncjrs.org). You must support the application with source material, including statistics about the nature and extent of the problem you seek to address and possible solutions that you want to explore.

Supporting statistics must be representative and from a reliable source; remember, you are trying to convince people to invest in your program. The grant proposal itself must meet professional presentation standards: it must include all required forms, with original signatures; it should be neat and logical; and it should be linguistically precise, with proper grammar and punctuation—do not use jargon, do not use the first person voice, and spell- and grammar-check the entire document before giving it to someone else to proofread.

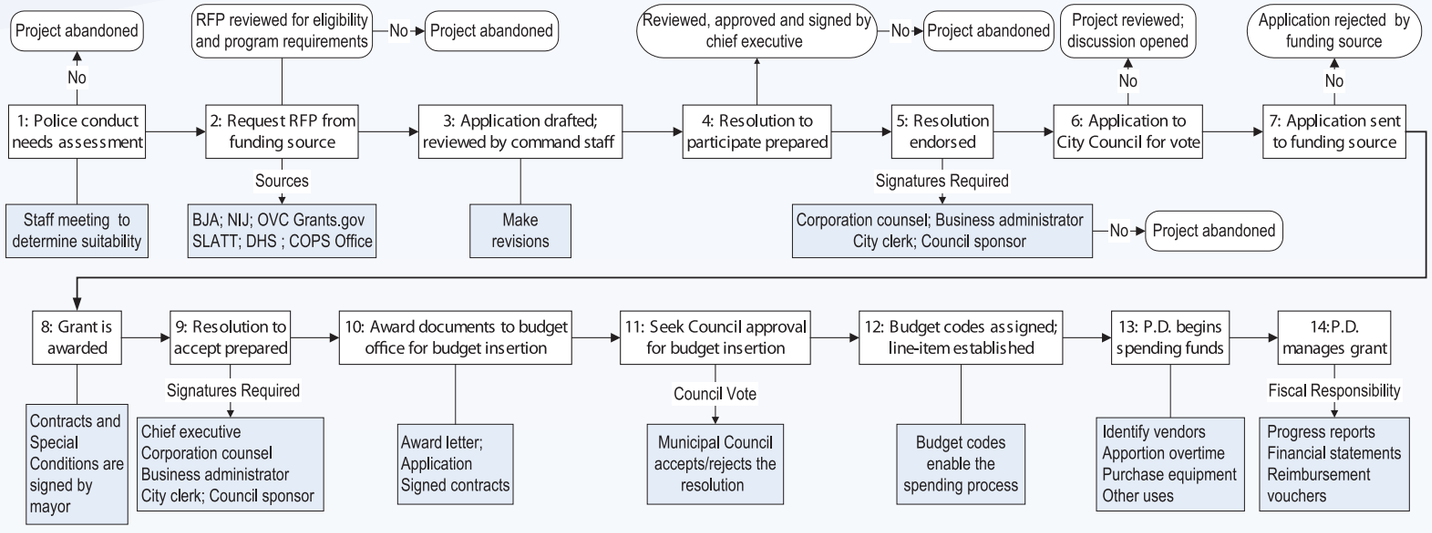
Every grant should be formatted according to the specifications in the request for proposal (RFP); if none is provided, follow the layout below.

1. **Cover Page:** include the program name and agency identifying information.
2. **Contents:** page numbers must match the contents.
3. **Abstract:** a short description of the grant application and funds requested.
4. **Problem Statement:** define the problem and support your findings with relevant statistics.
5. **Goals and Objectives:** ensure that the goals are achievable and the objectives measurable.
6. **Program Strategy:** describe what you intend to do and how you intend to do it.
7. **Budget Narrative:** in addition to completed budget forms, the narrative should justify how the funds will be spent and why they are necessary.
8. **Appendix:** attach all supporting documents including copies of source material and resumes, as necessary.

Managing the grant. After the grant is awarded, your agency must meet certain administrative requirements to ensure accountability. Each grant program typically comes with an owner's manual that outlines your administrative and accounting responsibilities. It also defines common terminology, terms and conditions of accepting the grant, how to access the funds, financial record maintenance, federal audit requirments, required reports and reporting periods, the length of the grant, and procedures for procuring extensions. Most funding agencies also offer telephone support for technical assistance to ensure smooth grant implentation.

Read More: Shane, Jon M., "*Writing a Winning Grant Proposal*," FBI Law Enforcement Bulletin 72. Washington, D.C.: Federal Bureau of Investigation, May 2003.

A 14 Step Grant Application Process



IV. Collect Intelligence


LINE DO NOT CR

“The U.S. Department of Justice has created a variety of counterterrorism task forces and councils to improve information sharing.”

Brief 21: Help the FBI—Join Your Local Joint Terrorism Task Force

The U.S. Department of Justice has created a variety of counterterrorism task forces and councils to improve information sharing. From your point of view, the most important of these are the Joint Terrorism Task Forces (JTTF). There are now more than 100 throughout the country, including the 56 FBI field offices. Although the first JTTF preceded 9/11, their number has greatly expanded since the attack. Their mission is to coordinate federal, state, and local law enforcement efforts to detect, prevent, and respond to terrorist attacks. Primarily investigative and analytic agencies, JTTF are staffed by FBI investigators, agents from federal agencies such as the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the Bureau of Immigration and Customs Enforcement (ICE), and detectives from local police and sheriff's departments. Several successes have been credited to the JTTF, including the arrest and conviction of the terrorists who mounted the first attack on the World Trade Center in 1993 and of the so-called shoe bomber, Richard Reid.

If an FBI field office is located in or near your jurisdiction, you will almost certainly already belong to a JTTF. The same is likely to be true if you head up a large department. But if yours is a small, rural force in an area unlikely to attract the attention of terrorists, it is unlikely that you belong to a JTTF or, indeed, would obtain much benefit from joining one. Whether to join a JTTF is a difficult decision for medium-size departments serving towns or small cities that are far removed from previous terrorist activity. In practice, joining a JTTF means assigning one or more of your detectives to work in the JTTF full time; part-time assignments are discouraged because the officers cannot participate fully in the work of the JTTF. Upon joining the JTTF, your officers will be deputized as FBI agents. The FBI pays overtime and provides needed equipment and supplies; your department, however, continues to pay the officers' salaries. So there is a substantial commitment of resources on the part of your department. Moreover, officers who are assigned to the JTTF are expected to stay there for at least a year, because it can take 6 months or more to process the necessary top secret security clearance.

The principal benefit of participating in a JTTF is to help make the country safer from attack. Participation helps the FBI in its investigations, which might one day relate to a case in your own jurisdiction. It is unlikely, however, that your participation in the task force will provide you with any earlier warning of a serious terror threat than you would otherwise receive; neither will your participation be of any great assistance in the unlikely event that an attack occurs. There are several reasons for this. First and foremost, the FBI will inform you immediately of any serious threat in your jurisdiction, whether or not you participate in a JTTF. Second, your own JTTF officers cannot always relay information to you, especially when the information is top secret. Third, as noted by William Bratton and other critics, JTTF are primarily investigative agencies: they are not geared to providing real-time intelligence to local agencies. In other words, JTTF do not share FBI intelligence with partner agencies. To serve this need, the FBI has recently begun to create Field Intelligence Groups in all 56 field offices.

Security clearance has sometimes proved to be a stumbling block in JTTF operations. Not only can top secret clearances take an inordinate length of time to process (for reasons described in Box 1), but they can result in professional jealousies, such as if a JTTF field officer has a higher security clearance than his chief. In fact, in at least one case this situation led to a police agency withdrawing its officers from the local JTTF. In 2005, Portland, Oregon, withdrew from the local JTTF because the FBI would not provide top secret clearance to the city attorney (see Box 2). The mayor had sought the clearance because he claimed that without it he would have been unable to determine whether his JTTF officers were in compliance with the state's strict civil liberties legislation.

Box 1: Being Granted Top Secret Security Clearance

In addition to physical verification of birth, education, residence, credit, employment, and military service records, personal interviews must be conducted with the candidate, employers, neighbors, associates, and references. Discrepancies and unfavorable information must be investigated and resolved.

Box 2: One City Withdraws from a JTTF.
In April 2005, Portland, Oregon, became the first jurisdiction in the country to withdraw from a JTTF. This culminated months of disagreement between the city and the FBI over the city's ability to oversee Portland police assigned to the JTTF. Portland is famously liberal, but some background is necessary to understand the decision. In September, 2002 *The Portland Tribune* uncovered a huge number of files that the Portland police had kept on activists from the 1960s to the 1980s. In 1981, a state law was passed that required the city to cease investigating activist groups without reasonable suspicion of their involvement in criminal activity and to destroy any existing records. Not only were the files not destroyed, but the city continued to maintain the files in defiance of the law.

Not long afterwards, the FBI announced the arrest of a local Muslim cleric, Mohamed Abdirahman Kariye, who the FBI claimed had tried to board a plane at Portland International Airport with traces of TNT in his luggage. Subsequent tests showed no explosive residue on the luggage. Thereafter, another Portland resident, Brandon Mayfield, was arrested by the FBI for complicity in the Madrid bombings of March 2004. Mayfield, an attorney, was a convert to Islam who attended the same mosque as Kariye. The FBI claimed that Mayfield's fingerprints matched those on a bag found close to the railway station that had been attacked. The Spanish National Police had apparently told the FBI that this was incorrect; when an Algerian national was later arrested based on the same fingerprint evidence, Mayfield was released without charge. In an almost unprecedented move, the Federal Government subsequently paid Mayfield $2 million and formally apologized to the lawyer and his family.

It was this history of police excesses and bungled FBI investigations that preceded Portland's dissatisfaction with the JTTF. Matters came to a head with the election of a new mayor, Tom Potter, a former city police executive, who had consistently expressed dissatisfaction with the city's arrangements with the JTTF. As is usual, Portland's JTTF officers had been given top secret security clearances, but those who signed their paychecks did not have such clearances, so they were unable to track their employees' official activities. Potter's attempt to remedy the situation broke down when the FBI refused to give the same security clearance to the city attorney as had been given to Portland's JTTF officers. Thus, the mayor would have been unable to determine whether his officers' actions conformed to the state's civil liberties laws, which are stronger than their federal equivalents.

Source: Kershaw, Sarah, "In Portland, Ore., a Bid to Pull Out of Terror Task Force,"
The New York Times, April 23, 2005.

Brief 22: Know Why You Don't Need Behavioral Profiling

Every police executive knows that racial profiling is illegal and highly inaccurate. Although it is true that foreign terrorists are more likely to be young men from Muslim countries, the vast majority of such individuals in the United States have no terrorist leanings or sympathies. Consequently, other means of narrowing the search for potential terrorists are being explored. One of these is behavioral profiling, which seeks to identify signs of lying or prevarication in suspects under questioning. The problem with this approach is that everyone is a little bit accomplished in deception; even the most honest among us is well practiced at saying how much we enjoyed a boring dinner party or liked some dreadful birthday present. White lies of this kind smooth social interaction. To tell them, we must know a little about acting—or at least how to conceal our feelings. As lies become more serious—to parents, employers, spouses—we have to work a little harder to appear sincere. Conversely, to protect ourselves from being deceived we learn to look for telltale signs: blushing, avoidance of eye contact, stammering, inconsistent stories, etc.

Citizens routinely lie to the police, but police officers quickly learn the usual excuses ("I didn't see the stop sign;" "The light was still green;" "I forgot to pay") and generally believe that they can tell from a person's demeanor when they are being lied to. Even if police can distinguish truth from fiction in these commonplace interactions with ordinary citizens, it is much harder to do so when interrogating hardened offenders about serious crimes. Offenders are likely to be more practiced liars with much more to lose if caught. They know how to control their emotions and hide their feelings. Consequently, police have looked for ways to see past these stratagems and uncover the lies they are being told. Thus, thousands of police investigators have been trained in the Reid Technique of Interviewing and Interrogation, which is designed to help them distinguish truth from falsehood; large numbers of polygraph interviews are undertaken each day for the same purpose.

Both the Reid Technique and the polygraph rely on picking up signs of anxiety under questioning: in the case of the polygraph, by measuring physiological skin responses indicative of stress; in the case of the Reid Technique, by close observation of body movements and characteristics of speech (e.g., pitch and rate). Both were designed for use in formal interview situations and are not suited to field interviews; but terrorists can be encountered in the field when they are reconnoitering targets or embarking on a mission, and it would be very valuable to be able to see through their stories. For example, three of the 9/11 hijackers were questioned by police during routine traffic stops, but in none of these instances did they arouse undue suspicion. On the other hand, Algerian-born Ahmed Ressam, the so-called millennium bomber, was apprehended at Port Angeles, Washington, on December 14, 1999, trying to smuggle bomb-making equipment over the Canadian border. During routine questioning Customs Agent Diana Dean became suspicious because Ressam's itinerary seemed unusual, he was uncommunicative and fidgety, and he was acting in a nervous manner.

The arrest of Ressam raises the enticing possibility that officers trained to detect the kinds of signs that Diana Dean observed could detect terrorists under routine questioning. This is the promise of behavioral profiling: looking for signs of nervousness in facial expressions, small shifts in posture, and unusual speech or hand gestures. Israeli security forces have been using behavioral profiling for many years at Tel Aviv's Ben Gurion Airport, from which there has never been a hijacking. Encouraged by this success, a diluted version of the Israeli procedure is now under evaluation at Logan Airport in Boston, the point of departure for the two airliners that rammed into the Twin Towers. But behavioral profiling is only one of the elements in the Israeli success: it is used in conjunction with full mandatory searches of each passenger and intensive interviews about reasons for travel.

"This is the promise of behavioral profiling: looking for signs of nervousness in facial expressions, small shifts in posture, and unusual speech or hand gestures"

Although behavioral profiling has been authenticated to a degree by the work of Professor Paul Ekman of the University of California, San Francisco, even he cautions about using it on its own. For more than 40 years, Professor Ekman has been exploring the relationship between facial expressions and emotion and has catalogued more than 10,000 possible combinations of facial muscle movements that reflect feelings. He has learned how to catch involuntary "micro-expressions" that flicker across the face when a person is lying. Unfortunately, few people without his years of experience can accurately detect these micro-expressions. Most groups he has studied, police included, did little better than chance when attempting to catch a lie being told. U.S. Secret Service agents as a whole did better than other groups, but even their accuracy was only about 10 percent better than chance.

Although intensive training can teach people to become better at detecting lies, training can also help people conceal their anxiety when they lie. In any case, anxiety under questioning has many sources. A person who is telling the truth, for example, might be fearful of police or might merely fear that he will not be believed. It is easy to confuse anxiety with lying, a mistake that Ekman calls "Othello's error" (see Box). Othello's error not only calls into question the validity of behavior profiling, but also that of the polygraph, which detects anxiety rather than lying. In fact, scientific evaluations have not supported the ability of the polygraph to detect lying, although it can still be a valuable adjunct to interrogation, particularly when offenders believe that it is accurate.

Othello's error
In Shakespeare's play, Othello falsely accuses his wife, Desdemona, of infidelity and threatens to kill her. Othello misinterprets her fearful expression as a confirmation of guilt and murders the unfortunate woman.

There is little reason to believe that police officers can be trained to detect lies by terrorists they encounter in the course of routine patrols. Together with the inherent improbability that any particular officer will encounter a terrorist, this suggests that it would not be worthwhile for you to invest in such training for your officers. You would be better off ensuring that your officers are alert to suspicious behavior, such as loitering near or attempting to gain unauthorized access to sensitive facilities. This does not mean that customs officials, airport screeners, and others who are more likely to encounter terrorists in the course of their routine jobs would not benefit from such training. Although, again, it is unlikely that it would be cost effective to give many of them the 9-week training that the carefully selected Israeli security officers at Ben Gurion Airport receive.

Read more: Schubert, Siri, "A Look Tells All," *Scientific American Mind*, October/November 2006.

Brief 23: Promote Intelligence-Led Policing—But Know its Limits

In the words of the academic commentator Vincent Henry: "Most police officers assigned to patrol or enforcement duties informally gather, analyze, and disseminate basic criminal intelligence on a daily basis. They interact with the public, casually or actively obtaining information about the community and the people who inhabit it, and they typically conduct some sort of rudimentary analysis to achieve a better understanding of the community and its crime problems. In many cases, they share this basic intelligence with other members of their agency."

Intelligence-led policing is the attempt to capitalize on this routine work, not for its traditional purpose of solving crimes, but proactively, to prevent and deter crime—and now terrorism. To do this, computerized systems are needed to capture and structure the scraps of information in an easily accessible format. In this form, the scraps of information are called collated data; and data are not intelligence. To become intelligence, the data must be analyzed by trained officers who use their knowledge and experience to recommend actions based on patterns in the data. For example, they might notice a number of small purchases of bomb-making materials and link the onset of the purchases to the arrival of a suspect group in the area. This intelligence can then be used to target the group for intensive surveillance and to ask stores to keep systematic records of such purchases. Ultimately, the intelligence might be used to support legislation making it more difficult to purchase such chemicals.

The term intelligence-led policing was coined by the Kent Constabulary in the United Kingdom, which developed the concept in response to sharp increases in burglary and automobile theft at a time when police budgets were being cut. Senior managers believed that a small number of individuals were responsible for many of these crimes and that the crime rate could best be cut by creating intelligence units to target the offenders for investigation and prosecution. They freed resources for these units by deemphasizing the response to calls for service. Within 3 years, crime had dropped by 25 percent. Intelligence-led policing is now the basis of the National Intelligence Model, which has established new data-collection and processing standards for the 43 police forces in the United Kingdom.

In the United States, intelligence-led policing has captured attention as a way to "connect the dots," the phrase popularized by the 9/11 Commission. In other words, it provides a way of combining discrete pieces of information about terrorist activities that make sense only when considered together. The New York City Police Department is the leading exponent of intelligence-led policing to combat terrorism. It has more than 1,000 officers dedicated to counterterrorism, it has hired intelligence and counterterrorism experts, it has officers fluent in many languages, it monitors news services and intelligence reports, and it even has agents stationed overseas in terrorist hot spots. No other domestic police department can match this investment, although many large agencies, with hundreds or perhaps thousands of officers, support an intelligence capacity. It requires only a computerized database, intelligence officers and analysts, and an intelligence manager—although these are generally used to support investigations rather than to direct operations.

Some of the remaining 17,000 agencies in the country, having dozens to hundreds of sworn employees, might be capable of developing intelligence products for internal use, but those with smaller staffs generally do not employ intelligence personnel. If they do assign someone to intelligence operations, that person generally has multiple responsibilities and is often a narcotics, gang, or counterterrorism officer. In some cases, these officers have received intelligence awareness training and are able to interpret analytic products, but most have not.

Establish an intelligence function. If you have not yet established an intelligence function within your department, you can probably meet your needs by taking the following steps:

1. Prepare a mission statement to address developing and sharing intelligence on serious crime and terrorism.
2. Designate an officer or a civilian analyst as the department contact for intelligence.
3. Charge that individual with preparing periodic briefings on terrorism using intelligence collected from open-source materials and other police agencies.
4. Ensure that reports of suspicious activity from patrol officers and others are channeled to this person.
5. Join a regional intelligence center; if one is not available, work with other local agencies to form a regional center.
6. Ensure that privacy issues are protected (see Box).

Be prepared for cynicism and resistance. Patrol officers who do not perceive intelligence as immediately useful might see it as a tool to shift policy away from traditional police models, and senior officers with little understanding of intelligence will be skeptical of its value.

Although we encourage you to establish a basic intelligence function, do not expect too much from the investment. There are two reasons for this.

1. Intelligence is highly skilled work, often beyond the capabilities of the officers you can deploy. In the words of Gregory Treverton of the RAND Corporation: "[Intelligence] involves gaining a deep and broad understanding of a problem at hand in order to be able to discover emerging patterns. The objective is to connect the dots on a continuing basis in the knowledge that the nature and position of the dots are in constant flux. It may imply that, instead of deep expertise in a particular slice of a problem, what is required are many pairs of eyes looking at data for emerging threats."
2. Useless information is vastly more common than useful information. Although we often hear stories of intelligence successes that result from tips received or surveillance undertaken, we do not hear about surveillance that showed no results, or all the apparently promising tips that led nowhere.

Read More:

1. Henry, Vincent, "The Need for a Coordinated and Strategic Local Police Approach to Terrorism: A Practitioner's Perspective," *Police Practice and Research 3* (4) (2002): 319–336.
2. Treverton, Gregory F., *The Next Steps in Reshaping Intelligence, Occasional Paper.* Santa Monica, California: RAND Corporation, 2005.

Legal and Privacy Issues

In the 1960s, local police departments got into trouble by illegally spying on antiwar and civil rights groups. To prevent this, the following guidelines have been endorsed in a recent Department of Justice report.

Information entering the intelligence system should meet a criminal predicate or reasonable suspicion and should be evaluated to check the reliability of the source and the validity of the data.

Information entering the intelligence system should not violate the reasonable expectations of privacy or civil liberties of its subjects.

Information maintained in the intelligence system should be updated or purged every 5 years.

Agencies should keep track of who receives the information.

Information from the intelligence system should be disseminated only to those who have a right to it and a need to know in order to perform a law enforcement function.

Source: Peterson, Marilyn. *Intelligence-Led Policing: The New Intelligence Architecture*. NCJ 210681. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Assistance, September 2005.

Brief 24: Separate Dream from Reality in Information Sharing

The 9/11 Commission severely criticized the failure of the FBI and the CIA to "connect the dots" before the attack; that is, to see a pattern in the scattered pieces of information about the hijackers that had come to the attention of various federal agencies. The Commission went on to say that these agencies must share critical information about suspected terrorists on a more coordinated and timely basis. In fact, information sharing should not stop at the federal level. Federal agencies must also share information more freely with state and local police. Furthermore, they must look to these agencies to supply them with leads on suspected terrorist activity in their local jurisdictions—leads that the feds would likely never obtain on their own. As former CIA Director R. James Woolsey noted in testimony to Congress: "The flow of information sharing is likely to be more from localities to Washington, rather than the other way around." State and local agencies also need to find ways to share information with each other. The fact that local police came face-to-face with three of the 9/11 hijackers in traffic stops before the attack is often cited as a catastrophically missed opportunity.

The need to share information is clear; what is less clear is how to go about doing so. There are more than 17,000 state and local law enforcement agencies in the United States, relatively few of which have an intelligence-gathering capacity (see Brief 23). Fewer still have much of an idea how to analyze the information collected so that it can be shared productively with other agencies. Unless these agencies develop an intelligence capacity, they will be left out of the loop. Despite this, various steps are being taken to facilitate information sharing among those agencies that do have an intelligence capability. The FBI, for example, has established Joint Terrorism Task Forces in all regional districts (see Brief 21)—although they seem to be designed less to serve the needs of local law enforcement than they are to assist in FBI investigations.

More in the true spirit of information sharing, the FBI is working on a system that will allow state and local police to determine whether a suspect is on one of the terrorism watch lists maintained by the Federal Government. This will require the integration of the (at the time of writing) nine existing lists and the development of a system that allows real-time access to the consolidated list. The "fusion centers" that are being established in many states represent a third information-sharing initiative. They will pool information from multiple jurisdictions and make it available to patrol officers, detectives, management, and other participating personnel. A center's mission can be limited to antiterrorism, but it often includes other significant crimes, such as identity theft, insurance fraud, money laundering, and armed robbery.

Finally, get up to speed on the many guidelines and documents about information sharing produced by the Office of the Director of National Intelligence, in particular the 100 Day Plan for Integration and Collaboration. http://www.fas.org/irp/dni/100-day-plan.pdf.

"Although the need to share data is not new, exchanging information across jurisdictions and levels of government is more critical in the current threat environment than it ever was in the war on crime. Because state and local law enforcement is decentralized, it must overcome its traditional reluctance to share information."

Source: Kelling George L. and William K. Bratton, *Policing Terrorism, Civic Bulletin 43*, New York: Manhattan Institute for Policy Research, September 2006.

"Local law enforcement often presumes that federal agencies are withholding detailed, relevant and important information, for any number of reasons. I am not convinced that this is the case. The FBI is learning to get back into the intelligence-gathering game just as we are, and we must acknowledge that the information just may not be there sometimes."

Source: Flynn, Edward A., *Protecting Your Community from Terrorism: The Strategies for Local Law Enforcement Series. Volume 1: Local-Federal Partnerships*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2003, p 29.

Impediments to information sharing

The main impediment to the timely sharing of terrorism information is that most local agencies lack both a staff trained in a common intelligence curriculum and the technology to collate, analyze, and exploit raw intelligence data (see Brief 21). In fact, most local agencies lack properly trained crime analysts, let alone intelligence analysts. In most departments, crime analysis is considered more important than intelligence analysis, simply because the former can yield more obvious and consistent benefits for everyday police work. Many local departments also lack the computer equipment and software needed to facilitate a national intelligence data system. Even within the same force there might be little interconnectivity among existing computer systems. Without uniformity and interconnectivity, the dream of an electronic network across which information can be quickly transmitted and collated remains just that: a dream.

Other impediments to information sharing include the following:

1. Secrecy is the stock-in-trade of intelligence agencies; historically, protecting sources and preventing leaks has been of great importance. This is why the need-to-know doctrine drives policy on information sharing. Unfortunately, in practice this doctrine inhibits information sharing and, therefore, inhibits the fresh perspectives and new insights that sometimes occur when new eyes examine old information. Local agencies still complain that information released by the FBI often contains little more than what can be found on cable news stations or in media press releases. Although there is much talk about the need to develop more trust, how to do so among 17,000 agencies is never really discussed. It is more realistic to find ways of sharing information, stripped of details about sources.

2. Particularly in the early stages of an inquiry, it is likely that investigators will guard their information jealously. This is not merely to prevent leaks that might jeopardize the investigation, but also because they (understandably) wish to reap the kudos that will result from successfully apprehending the terrorists. Sharing the information can mean sharing the glory—or even being deprived of it.

3. Terrorism, even suspected terrorism, is rare. It is hard for people to remain vigilant when nothing seems to be happening, and hard to maintain the morale of those doing the watching.

4. The essence of prevention is stopping something from happening. It can be hard to demonstrate that such efforts have been successful when the agency that collects the relevant information is not the agency that takes the action that prevents the thing from happening. Once again, this fact militates against the intelligence function and more specifically against the sharing of information.

Read More: D'Amico, Joseph, "Stopping Crime in Real Time," *The Police Chief* 73 (September 2006). http://www.policechiefmagazine.org/

"It is important to recognize that the responsibility for investigating virtually all bombings and terrorist attacks lies with federal law enforcement. The state or local agency may be called upon to assist the investigation in various collateral ways, but their role will certainly not be that of the primary investigative agency. Given the history of friction between federal and local law enforcement, the tendency for petty jealousies and misunderstandings to escalate into full-blown turf wars, and the tremendous media attention and public pressure that will inevitably accompany the investigation, it is also doubtful that a given terrorist investigation will proceed quickly and smoothly. Conflicts are practically unavoidable in the current law enforcement climate."

Source: Henry, Vincent, "The Need for a Coordinated and Strategic Local Police Approach to Terrorism," *Police Practice and Research* 3 (4) (2002): 319–336.

Brief 25: Know the Limits of Video Cameras

Quite soon after the suicide bomb attack on the London Underground in July 2005, the world's TV stations broadcast video footage of the four bombers entering the subway. The pictures were a vivid endorsement of video surveillance and anyone seeing them could not fail to be impressed by their value to investigators (see Box). It is very likely, therefore, that you will be urged to install video cameras in your city to protect against terrorism, even if people in the United States have been more resistant to video surveillance than have those in the United Kingdom. This resistance is based mostly on knee-jerk privacy concerns that have little basis in reality. Surveys undertaken in the United Kingdom and elsewhere generally find that people welcome the cameras. They could not care less that they are being photographed as long as cameras make the streets safer. People in the United States would probably feel the same if they thought cameras would help protect them from terrorism. In any case, they are already accustomed to seeing cameras in banks, stores, gas stations, office buildings, schools, and on college campuses.

The London Underground pictures vividly demonstrate the value of video surveillance in investigating terrorism. But is there evidence that video cameras can actually prevent attacks from occurring? There is no clear answer to this question, partly because video cameras are comparatively new and evidence of their use is just beginning to accumulate. In conjunction with the COPS Office, however, Dr. Jerry Ratcliffe of Temple University recently reviewed research on the effectiveness of video surveillance in preventing crime in public places (see "Read More"). He analyzed the results of more than 30 published studies, most of which were undertaken in the United Kingdom. He noted that it is difficult to prove the effectiveness of video cameras because they are often used together with other crime-prevention techniques, which can make it difficult to separate their effect from those of other measures. It is also difficult to know whether they reduce crime or simply displace it beyond the range of the cameras. Despite these difficulties, he was able to draw the following conclusions:

1. Video cameras can work, but they are not a panacea. They work in different ways in different situations.
2. Video cameras work most effectively when bundled with other situational prevention measures, i.e., measures that increase the difficulties and risks of offending, that reduce its rewards, and that remove excuses and temptations (see http://www.popcenter.org/25techniques.htm).
3. Video cameras work best in small, well-defined sites (for example, parking lots) rather than across large areas (such as downtown districts).
4. Video cameras are more effective in combating property crime rather than violence or disorder.
5. Video cameras work best when closely integrated with police operations.

It is clear from this summary that when tailored carefully to circumstances, video cameras can provide situational crime-prevention benefits. Whether they can prevent terrorism is unclear, although there is good reason to believe that anything that increases the risks of terrorism is likely to have some deterrent value. We, therefore, would be inclined to include video cameras in any plans to improve basic security at specific at-risk targets, particularly because the cameras will have more general crime-prevention benefits. Whether they should be installed in public streets or downtown neighborhoods is a more difficult decision because their crime-prevention value in such settings is less clear. They might serve to reassure the public, however, and would possibly be useful in the event of terrorist activity. Much will depend on the sophistication and size of the system and, therefore, its cost. Dr. Ratcliffe lays out the components of a complete video surveillance system as follows:

- One or more cameras that view a public area
- A mechanism to transmit video images to one or more monitors
- Video monitors to view the scene—usually accompanied by recording devices
- A camera operator, such as a police officer or security guard.

Refinements include the following:

- Ability to transmit images across the Internet
- Motion sensors to activate the camera
- Normal or infrared lighting to enhance picture quality at night
- Pan and tilt capacity that allows an operator to change the camera's viewing direction, zoom, and focus
- Facial recognition technologies and systems to estimate the location of firearm incidents
- Intelligence systems to detect unusual activity, such as fights in the street (these are under development).

The Value of Video Cameras to the Massachusetts Bay Transit Authority

More than 450 security cameras watching for potential terrorists on "the T" are now helping catch alleged criminals. Friday, the Massachusetts Bay Transit Authority (MBTA) transit police arrested a 27-year-old man accused of robbing a passenger at gunpoint at the Back Bay station. Such cases have often gone unsolved, officials said, and the arrest would have been far less likely without digital images from a surveillance camera at the station.

The camera network "has aided us tremendously in identifying suspects that normally would not have been identified in the past," said Sergeant Detective Michael Adamson. "Hopefully, the word will get out that these cameras are in place and people will reconsider their actions before committing crimes on the MBTA."

He said that detectives have been increasingly successful with the cameras, and they are now routinely using them to narrow down suspects. He said that even when police are unable to positively identify a suspect with the digital images, they usually get promising leads by significantly enhancing a suspect's description to include details of clothing and distinguishing features, such as moles and tattoos.

In the Back Bay holdup, on a Saturday late last month, the victim described his assailant as a man with a tattoo on his neck, police said. Transit police showed the victim photos of more than 100 known offenders with neck tattoos. When the victim picked someone out, police checked the digital surveillance cameras at Back Bay and found an image of the same man entering the station around the time of the robbery. That helped police obtain an arrest warrant for the suspect.

Source: Daniel, Mac and Suzanne Smalley, "Antiterror Cameras Capturing Crime on T," *The Boston Globe*, January 29, 2007.

Whichever system you choose, you will face a number of logistical questions: where to place the cameras; whether to merge your crime-prevention cameras with existing traffic-monitoring cameras; how to monitor the cameras; how to respond to incidents; how to communicate with officers on the ground; how to store images and for how long; and how to manage public concerns. As we said, the public would likely support their use for counterterrorism and, in any event, most systems will not compromise constitutional protections against unreasonable search and seizure. You might still need to show that strict rules would prohibit officers from focusing the cameras inappropriately, and that stored images will be accessible only to those with a need to know. It would certainly be prudent to seek local legal advice on these matters.

Read More: Ratcliffe, Jerry. *Video Surveillance of Public Places, Problem-Oriented Guides for Police, Response Guides Series No. 4*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2006. http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=226

"Most camera systems will not compromise constitutional protections against unreasonable search and seizure-but seek legal advice on these matters."

Brief 26: Don't Depend on Public Vigilance

Electronic freeway signs near large cities often display an 800 number asking the public to "report suspicious behavior." This might seem like a good idea, but vague exhortations for citizens to be vigilant serve to heighten fear and fuel calls for service that are mostly useless. In fact, there are several reasons for not depending on public vigilance.

1. On mass transit, it makes sense to ask the public to report unattended bags or packages because everyone can recognize these objects and can easily understand that they might contain bombs. In the case of the freeway signs, however, suspicious behavior is not defined and there is little agreement about what it is (see Box 1).
2. Without a clear definition of suspicious behavior, people might be reported or even accosted based on the prejudices or presuppositions of those who define them as suspicious or out of place—for example Black pedestrians in a predominantly White neighborhood.
3. Requesting public help in reporting suspicious behavior is not cost-free. It requires that those requesting the reports answer the phone and speak with the caller or listen to recordings later—which, of course, would be too late if the warning was genuine.
4. After listening to the reports, it is necessary to evaluate and even investigate them. This will waste scarce resources, because the vast majority of reports are groundless.
5. Terrorism is extremely rare. The public will soon grow weary of exhortations to be on guard if nothing happens. Worse, it can engender cynicism about the competence of counterterrorism efforts.

In addition to the concerns detailed above, a number of other factors militate against setting up your own hotline to obtain information from the public. For example, people can use the hot line to harass those they don't like; hot lines attract cranks and pranksters; and finally, you might find that you have to explain yourself to angry callers whose reports you have decided are groundless.

Box 1: Seven Warning Signs of Terrorism

Many postings on the Internet list suspicious behavior (the following list is from the U.S. Attorney's Office in Hawaii), but to what extent they reach and inform the general public is unclear. Although some of the indicators can be useful (e.g., unusual purchases of chemicals), the majority are vague and encompass ordinary, everyday activities that are generally indistinguishable from conventional behaviors (e.g., taking photos; see Box 2).

1. **Surveillance:** suspicious monitoring activities of a target; unusual photography of targets; creation of maps and diagrams; attempts to obtain blueprints of government buildings and utilities.
2. **Elicitation:** attempts to gain restricted information about a place, person, or operation; attempts to place key people in sensitive work areas; efforts to find out target strengths and weaknesses.
3. **Tests of security:** driving by the target or attempting to breach security to discover response times.
4. **Acquiring supplies:** purchasing or stealing explosives, ammunition, or weapons; unlawful storage of large quantities of chemicals, such as nitrate fertilizers; thefts of law official uniforms or identification badges
5. **Suspicious people who don't belong:** behaviors that just don't seem to fit within norms; people who are out of place because of demeanor, self-imposed seclusion, or antisocial behavior; presence of training manuals and anti-American or anti-Semitic propaganda.
6. **Dry runs:** practice sessions at or near target areas to work out bugs and unanticipated problems; these might include mapping out routes, monitoring police frequencies, and determining the timing of traffic lights.
7. **Bomber indicators:**
   Suicide Bombers ***(ALERT)***: **A**lone and nervous; **L**oose and bulky clothing not compatible with weather conditions; **E**xposed wires; **R**igid midsection—caused by explosives belt or harness; **T**ightened hands—might hold detonation device.
   Truck bombers: Purchases or theft of sizeable amount of explosives, fuses, blasting caps, and chemicals such as nitric acid, sulfuric acid, urea crystals, liquid nitromethane, or ammonium nitrate; rental of self-storage spaces to store the chemicals; delivery of chemicals to residential or self-storage facilities; unusual odors, rusted metal, or bright stains in apartments, motels, or self-storage units; rental, theft, or purchase of a truck or van with a minimum of 1-ton carrying capacity; test explosions in remote, rural areas; chemical burns or missing fingers on hands.

Source: U.S. Attorney's Office, District of Hawaii http://www.usdoj.gov/usao/hi/atac/terrorisminformation.pdf

If it is of limited value to ask the general public to report suspicious behavior, is it helpful instead to confine your inquiries to individuals or businesses that are more likely to come into contact with potential terrorists? That is, would it be worth asking car rental agents in your city to inform the police about suspect clients—for example, a group of foreign men renting a large van or truck? Would it be worth asking hotel and motel clerks to inform you when guests check in from Islamic countries? Should you ask realtors to let you know when short-term renters seek isolated properties or pay rent in cash? Is it worth asking bank managers to keep you informed about regular payments of money from overseas?

These might seem like sensible precautions, but you should remember that the overwhelming majority of these activities are lawful and innocent. Consequently, you will need to think hard about the quality of the likely information and how it will be collected and collated. Such requests might initially result in some information trickling in, but your sources will quickly dry up unless you keep sending reminders. A dedicated terrorism unit could ask these questions on a regular basis, although this might waste time that could be better spent in other ways. Although the chance of obtaining useful intelligence from directed inquiries is probably greater than from a general public appeal, it is still likely to be counterproductive because of the inherent improbability of terrorists targeting your city. A better way to engage the public in your counterterrorism effort is by fully exploiting the intelligence function of community policing, the subject of Brief 28.

"A better way to engage the public in your counterterrorism effort is by fully exploiting the intelligence function of community policing."

Box 2: Birdwatchers Beware!
Much allegedly suspicious behavior is entirely innocuous. One of the authors was once detained overseas while taking photos of shorebirds in a yachting harbor that was adjacent to a largely disused military installation. The behavior was entirely innocent, but the large telephoto lens needed for bird photography triggered a report by a member of the public to security personnel.

Brief 27: Serve Your Immigrant Communities

Although immigrants used to congregate primarily in gateway states such as California, Florida, Illinois, Massachussets, New Jersey, New York, and Texas, they have now begun to settle in many other areas. Nowadays, there is quite likely an immigrant community within your jurisdiction.

Because of the difficulties of policing immigrant communities, local police have often been content to let these communities police themselves, intervening only when serious crimes come to their attention. September 11 changed all that. Immigrant communities, especially Arab and Asian communities with Muslim ties, came under suspicion as potential breeding grounds for terrorism. Beginning in November 2001, the U.S Attorney General asked federal, state, and local law enforcement agencies to conduct "voluntary" interviews with thousands of young men from Middle Eastern countries in the United States on temporary visas.

Although the great majority of these men were entirely innocent, the authorities did have some grounds for suspicion. The first attack on the Twin Towers was undertaken by a group residing in a Jersey City, New Jersey, immigrant community close to Manhattan, and the 9/11 attackers lived in or near immigrant areas that matched their ethnic and national backgrounds. There is little doubt that al-Qaida's attacks were facilitated by the presence of immigrant communities in the United States. Federal agencies correctly understood this—but perhaps not that these communities were used unwittingly by al-Qaida. Immigrant communities help new arrivals to find their way in a strange country, particularly when the newcomers cannot speak the language. By the same token, they make it easier for foreign operatives to get bank accounts and credit cards, to get money from abroad, to buy cars, to find places to live, and so forth.

It is likely that some of these communities were a source of financial support for al-Qaida because its extensive revenue raising through charities and mosques in immigrant communities is well-documented. In some cases, it seems that money raised within immigrant communities to assist charities in their home countries has been diverted into the hands of terrorists.

Such operational and financial support for terrorism, even if largely inadvertent, is enough to demand police attention. But might not these communities be involved in terrorism in a much more serious way? Can they not also produce their own homegrown terrorists, just as Muslim communities have in Britain, albeit with some support from al-Qaida? It seems unlikely that this will happen here, at least in the near future. Muslim immigrant communities in Britain are generally older than those in the United States; many of these individuals entered the country to do jobs that the British disdained. It is not from this first generation of immigrants that terrorists are drawn. Rather, it is individuals from the second, British-born generation, who are often disappointed with their employment status and resentful of the fact that their Muslim identity is given little respect. In contrast, the children of Asian immigrants in the United States seem to be doing well in schools, colleges, and the job market, partly because many of their parents had superior educational qualifications that helped gain them entry to the country.

So far we have only considered immigrant communities as possible sources of terrorism, but not as victims of terrorism. Every time there is news of a foiled terror plot or whenever the terror alert is ramped up, immigrants report being fearful—not just frightened of becoming the victims of terrorism, but of being targeted by the authorities with further checks and restrictions and by local populations with hostility and even hatred.

Protecting these communities and providing them with reassurance, while at the same time ensuring that they do not harbor or support terrorism, presents a difficult balancing act. Standard community policing seems to offer the best hope of meeting these twin needs, but some important barriers exist. These include the facts that: (1) immigrants often fear and distrust the police; (2) many immigrants have little understanding of civil rights, U.S. law, or law enforcement; (3) language barriers prohibit effective communication and trust between immigrants and police; (4) immigrants fear that contact with police will threaten their immigration status (a problem that has been exacerbated as local and state police increasingly work with federal immigration authorities); (5) the sense of communal socialization that community policing programs require is lacking because many immigrants are more connected to their native lands than to their new homes; and (6) the lack of voting rights among immigrants limits their relevance in determining the priorities of police and local governments.

Nevertheless, there is much you can do to overcome these barriers and implement community policing successfully in immigrant communities. The following are a few examples:

- Designate community policing officers to work exclusively with immigrant communities. Establish police substations in larger communities.
- Use ethnic radio and television, religious institutions, and employers to communicate with immigrant communities. This will help you reach a larger constituency, as well as community members (e.g., younger immigrants, children of immigrants, and day laborers) who usually do not attend traditional meetings at precincts.
- Employ more interpreters and make police materials available in foreign languages. Check out Limited English Proficiency: A Federal Agency Website at http://www.lep.gov that outlines Executive Order 13166 concerning the improvement of access to federal programs and offices for people whose proficiency in English is limited.
- Involve immigrant leaders in designing and implementing effective cultural training programs for your officers. Train your officers to communicate effectively with the different elements in the immigrant community.
- Work to overcome barriers that prevent the recruitment of officers from immigrant communities, including the dislike of police and problems with administrative and cultural barriers.
- Define clearly and publicize your immigration law enforcement policies.
- Inform community advocates of your department's role and policies. Similarly, make sure the media accurately reports the dialog taking place between police and immigrants.

Rob Davis, chief of police in San Jose, California, a member of the Mormon faith, announced that he would join local Muslims in fasting for the entire month of Ramadan. He was inspired to do so after speaking to 7,000 Bay Area Muslims. He intended to break his fast each night with a different Muslim family at his own home. Chief Davis said: "I need to be a chief for everybody, particularly for those who've felt marginalized."

Source: McDonald, William F., "Police and Immigrants: Community and Security in Post-9/11 America," in Justice and Safety in America's Immigrant Communities, ed. Martha King, Princeton, New Jersey: Princeton University: The Policy Research Institute for the Region, 2006. http://region.princeton.edu

Read More:

Briggs, Rachel, Catherine Fieschi, and Hannah Lownsbrough, *Bringing It Home: Community-Based Approaches to Counter-Terrorism*. London: DEMOS, 2006. http://www.demos.co.uk/files/Bringing%20it%20Home%20-%20web.pdf

Shah, Susan, Insha Rahman, and Anita Khashu, *Overcoming Language Barriers: Solutions for Law Enforcement*. New York: Vera Institute of Justice and the Office of Community Oriented Policing Services, 2007. http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=403 and http://www.vera.org/overcominglangbarriers

Brief 28: Make Community Policing Your First Line of Defense

"Only an effective local police establishment that has the confidence of citizens is going to be likely to hear from, say, a local merchant in a part of town containing a number of new immigrants that a group of young men from abroad have recently moved into a nearby apartment and are acting suspiciously. Local police are best equipped to understand how to protect citizens' liberties and obtain such leads legally."

This quote from former CIA director James Woolsey's testimony to Congress in 2004 is just one of many endorsements of the role of local police in counterterrorism. The essence of his prescription for obtaining vital information is earning the trust of citizens, talking regularly and informally with key members of the community, and protecting the community's rights and freedoms. Written another way, this is the formula for effective community policing. Like many other chiefs, you might already assign beat police officers to particular neighborhoods so that (1) you can better serve the community and (2) the community can help you meet your policing responsibilities. No doubt you expect your officers to spend considerable time in these neighborhoods, getting to know residents and business owners and talking with them about local problems and troublesome individuals. Given the loss of life that can result from a terrorist attack, you might find that citizens are even less reticent to pass on information about suspicious activity than they are for conventional crime. In fact, gathering information through community policing has many advantages over traditional intelligence work. By focusing on community policing you can avoid the following issues:

- Compiling unsubstantiated lists of suspects
- Conducting costly surveillance of suspects and places
- Dealing with charges of profiling
- Dealing with wiretapping and its legal and political encumbrances
- Conducting secret (and therefore suspect) operations
- Undermining community trust
- Working against your own community
- Dealing with charges of entrapment.

By focusing on community policing, you gain the following benefits:

- Trust of the community
- Knowledge about targets most at risk
- Reduced crime as well as prevented terrorism
- Deeper knowledge of your community
- Closer collaborations with businesses
- Reputation for openness
- Respect.

"Local police officers have an everyday presence in the communities that they are sworn to protect. They 'walk the beat,' communicate regularly with the local residents and business owners, and are more likely to notice even subtle changes in the neighborhoods they patrol. They are in a better position to know responsible leaders in the Islamic and Arabic communities and can reach out to them for information or help in developing informants."

Source: Kelling, George L. and William K. Bratton, *Policing Terrorism, Civic Bulletin 43,* New York: Manhattan Institute for Policy Research, September 2006.

Community policing should result in your officers becoming more familiar with local communities and learning quickly about any suspicious activity. This will happen only if they are held responsible for reducing crime in their beats; if they spend most of their working hours in these beats; if they get out of their cars, spend time talking to residents and business owners, and establish relationships with them; and if they pay close attention to what is bothering residents and business owners and do what they can to alleviate the problems.

"Community policing should result in your officers becoming more familiar with local communities and learning quickly about any suspicious activity."

Making an Organizational Commitment to Community Policing.

- Assign officers to specific geographic locations for extended periods.
- Build principles into recruitment activities and selection decisions.
- Incorporate community policing into performance evaluations and reward systems.
- Develop technology and data systems that make information more accessible to officers and the community.
- Train all staff in community policing principles.
- Increase officer discretion and accountability.
- Encourage officers to propose innovative solutions to longstanding problems.
- Simplify hierarchical structures.
- Increase agency transparency for activities and decision-making.
- Incorporate community policing into field officer training.
- Give officers latitude in developing innovative responses.
- Develop technology systems that support problem analysis and evaluation.
- Build community policing into mission and strategic planning.

Source: Chapman, Robert and Matthew Scheider, *Community Policing for Mayors: A Municipal Service Model for Policing and Beyond*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2006.
http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=32

For your part, you will need to make sure that these officers have the resources, the knowledge, and the working conditions to properly fill their roles. This involves the following:

- Selecting officers who are temperamentally suited to community policing
- Leaving officers in place long enough to gain the trust of the community
- Matching officers with neighborhoods (for example, selecting officers who live close by or even in the neighborhoods they serve)
- Ensuring that officers have the language skills to communicate with minority residents
- Establishing a police substation in the neighborhood, wherever practicable
- Allowing officers flexible work hours and, whenever possible, not pulling them from their neighborhoods for emergency duties
- Training officers to serve a terrorism intelligence function.

You will need to monitor your community policing officers lest they become too closely identified with the neighborhood they serve and suborned by its priorities. To make sure that they meet your goals, check on the quality and frequency of their intelligence reports and make sure that they are setting and meeting concrete crime and disorder reduction goals. In addition, you might need to beef up the department's crime analysis capacity by employing a dedicated and properly trained staff and providing them with up-to-date technology. Finally, you will need to make sure that officers understand that problem solving is valued as highly as are detection and arrest—and that it will be equally rewarded with recognition and promotion. The Box lists organizational changes that you might need to make to implement a community policing program.

V. Harden Targets


LINE DO NOT CR

“Distance is of vital importance in understanding terrorism, just as it is in explaining crime.”

Brief 29: Assess Target Vulnerability: Use EVIL DONE

As we indicated earlier, it is possible to identify targets that might be attractive to terrorists by analyzing two essential elements: vulnerability and expected loss. In this brief we provide a way to assess the vulnerability of targets using **EVIL DONE**, an acronym that summarizes important aspects of vulnerability. Remember, vulnerability refers to the inherent features of a target that can attract a terrorist attack, whereas expected loss refers to the anticipated injury or damage that can ensue if the target is attacked. We will discuss assessing expected loss in the following brief.

Elements of EVIL DONE

Exposed: A target sticks out of the city skyline (for example, the Twin Towers or the Statue of Liberty) or stands out in another way: the only multistory building in a small town; a Federal Government building; a large shopping complex; or a nuclear power plant.

Vital: The target plays a critical role in day-to-day functions. The water supply, electricity grid, food chain, and transportation system are vital to any town, small or large. If terrorists believe that their destruction will wreak havoc, they might choose these targets.

Iconic: Targets that have high symbolic value can attract terrorists. The Statue of Liberty, for example, is an icon of New York City in particular, and of the United States in general. In contrast, Tim McVeigh chose the Alfred P. Murrah Federal Building in Oklahoma City because it stood for the Federal Government, which he abhorred. Although not quite as iconic as the Statue of Liberty, it stood for something abstract and important: the Federal Government.

Legitimate: An important factor in the decision to strike a target is how the attack will be viewed by other terrorists, their sympathizers, and would-be sympathizers. If the attack is viewed as illegitimate—as was the murder of Lord Mountbatten by the IRA in 1979—the terrorist group might lose public support. Hamas in Palestine conducts frequent public opinion polls to find out whether their targets are seen as legitimate by their supporters.

Destructible: The target must be destroyed or the targeted individuals killed if the terrorist act is to be regarded as successful. Some buildings are difficult to destroy and some people are too well-protected to kill. Thus, a target might be spared because it is thought indestructible. The Twin Towers were so considered until al-Qaida devised a way to destroy them in its second attack.

Occupied: With few exceptions, terrorists seek to kill as many people as possible, because it is what most frightens their enemies. Targets that will produce mass casualties, whether large venues with many people, or smaller densely packed targets such as cafes and trains, are preferred. Targets with important people present will also be preferred.

Near: Distance is of vital importance in understanding terrorism, just as it is in explaining crime. Study upon study show that offenders typically travel very short distances to commit crimes and often prey on their own neighborhoods and communities. Similarly, if the terrorists live cheek-by-jowl with those whom they hate, their task is greatly simplified; not only are the logistics of attack much easier, but the chance of escape is much greater if the terrorists can melt away into the surrounding community. The example of the Irish Republican Army (IRA) makes the point: from 1970 to 1994 the IRA mounted tens of thousands of attacks in Northern Ireland, but only a handful in England. Distance is of greatest relevance when terrorists are domestic and your jurisdiction is very large. When terrorists are foreign, all the targets in your jurisdiction are equally far away—unless the terrorists are operating from an immigrant neighborhood, as did those responsible for the first attack on the Twin Towers, which originated from nearby Jersey City, New Jersey.

Easy: How easy is it to access the target? For Timothy McVeigh, it was too easy: he was able to park his truck bomb just 8 feet from the Murrah Building. How easy was it for al-Qaida to get at the World Trade Center? For the first attack, it was relatively easy because of the poor security in the underground parking garage. The second attack, however, required complicated preparations, including training pilots to fly commercial airliners into the Twin Towers.

Applying EVIL DONE

The Table applies EVIL DONE to some landmarks in Washington, D.C., as viewed from the perspective of foreign terrorists planning an attack using a plane or a truck bomb. ("Near" plays a lesser role in the choice because each landmark is equally distant from the foreign base of operations.) It is easy to argue with the ratings in the Table; nor would all terrorist groups share the same priorities. Its purpose is merely to show that, in principle, it is possible to rate the vulnerability of targets for any city. You can draw up a similar grid and use it to identify and rate targets in your community. Ask yourself how their characteristics vary according to the method of attack (guns, arson) and the type of terrorist group (domestic, single issue). This is the first step in developing a systematic plan of target protection. In the following briefs we introduce a method for assessing the expected loss if a target is hit.

Target Attractiveness Scale, Washington, D.C. (simulated example)

1=Low attractiveness; 5=High attractiveness

Target Characteristic	White House	United States Capitol	The Pentagon	Washington Monument	Union Station	Washington National Cathedral	Old Post Office	Georgetown University	National Zoo
Exposed	4	5	5	5	3	4	0	2	1
Vital	3	3	4	0	4	0	0	1	0
Iconic	5	5	5	2	0	1	0	0	0
Legitimate	5	5	5	5	3	1	2	1	0
Destructible	4	3	2	4	4	4	4	1	1
Occupied	4	4	3	2	4	1	2	3	3
Near	1	1	1	1	1	1	1	1	1
Easy	2	3	3	2	5	5	4	4	4
TOTAL SCORE	28	29	28	21	24	17	13	13	10

Source: Source: Clarke, Ronald V. and Graeme R. Newman, *Outsmarting the Terrorists*. Westport, Connecticut: Praeger Security International, 2006.

Brief 30: Anticipate the Fallout of an Attack—Use CARVER

The previous brief described how to assess vulnerability—the likelihood that a particular target will be attacked—using EVIL DONE. In this brief, we describe CARVER, a method for assessing the expected loss from an attack on any particular target. Note that vulnerability and expected loss are not necessarily correlative; that is, just because a target is highly vulnerable does not mean that the expected loss from an attack will necessarily be high. For example, an attack on an electricity grid might not directly kill or injure anyone—although it certainly might inconvenience a great many—so the potential loss of life would not be as great as with the destruction of a large, occupied office building.

Introducing CARVER

CARVER is a protocol used by U.S. Special Operations Forces in assessing and targeting an adversary's installations. There are many variations of this protocol, which has been adapted to many locations, targets, and situations. This protocol bears some similarity to EVIL DONE, but it views targets from the point of view of the owner rather than that of the terrorist, which is primarily the viewpoint of EVIL DONE.

CARVER and EVIL DONE provide different ways of assessing target vulnerability; however, CARVER includes an assessment of the expected loss from an attack. Expected loss means the injury, damage, and disruption that can result from an attack, whereas vulnerability means the likelihood of the target being attacked (which is what EVIL DONE assesses). Expected loss and vulnerability combine to provide an assessment of risk:

RISK = VULNERABILITY + EXPECTED LOSS

It might be that a particular target for practical or even budgetary reasons cannot be completely protected. An electricity grid, for example, is quite exposed and covers a large geographical area, but its most crucial points can be protected and backup systems can be installed to ensure the grid's continued operation, even if one critical point is disabled. Thus, although the grid remains vulnerable, the expected loss is reduced because the damage and disruption that might result from an attack are minimized.

Elements of CARVER

Criticality: Will a successful attack have a significant impact on the facility's operation and services? (Expected loss)

Accessibility: How easily can the attacker reach the target? Will special tools or weapons be needed? Have steps been taken to secure the target? (Vulnerability)

Recuperability: How long will it take to replace, bypass, or repair the target? (Expected loss)

Vulnerability: Is the target constructed to withstand an attack? Does it contain combustible materials that will enhance an attack? (Vulnerability)

Effect: What effect will the attack have? Will it shock the local population? Will there be a ripple effect on other critical targets? The destruction of the World Trade Center, for example, affected stock market trading and the economic viability of the airlines. (Expected loss)

Recognizability: Is the target prominent or iconic (e.g., the Pentagon, the Empire State Building)? Is it protected by enhanced security precautions (such as the ring of steel around the White House) that highlight its importance? (Vulnerability)

These criteria provide the basis for a rating scale that can be applied to structures and facilities in your jurisdiction. The scoring is entirely subjective, although some guidelines can be useful in assessing each component. We have provided an abridged form (on the opposite page) for you to adapt to your own local needs. Of course, CARVER is only a rough guide. It can be more or less applicable, depending on local conditions. In any event, using CARVER and EVIL DONE together will be enough to get you started on your own systematic risk assessment.

"...just because a target is highly vulnerable does not mean that the expected loss from an attack will be high."

Sample CARVER Protocol

CRITICALITY (result of successful attack)
Immediate indefinite closure of facility, economic dislocation, danger to local community……5
Immediate closure, return to service after several months, danger to local community……4
Return to service within several weeks, some economic dislocation…… 3
Return to service within 2 weeks, inconvenience to community ……2
Facility not vital to community, minimal disruption…1

ACCESSIBILITY
Security of perimeter, entry points nonexistent……5
Perimeter fenced, but many entry points unsecured……4
Video surveillance, untrained security personnel……3
CPTED* applied, trained security personnel……2
CPTED, aerial surveillance, high-tech ID for entry, buffer zone……1

RECUPERABILITY
No redundant systems, equipment, or materials……5
Limited backup equipment or materials……4
Redundant systems in place, no disaster plan……3
Recovery equipment and systems in safe location, disaster plan……2
Extensive redundant systems, disaster plan coordinated with local emergency response plan……1

VULNERABILITY
Contains chemicals or other materials that will enhance destruction, located in densely populated area……5
Not built to withstand moderate explosion, located in densely populated area ……4
Contains glass or other materials that will enhance injuries, located in suburban industrial park……3
Built to withstand major explosion, located in rural area ……2
Built to withstand major explosion or aerial attack, located in rural area……1

EFFECT
Panic in local and national population, severe national and international economic dislocation……5
Collateral damage to other components of the industry or service……4
Emergency response teams and hospitals overwhelmed….3
National and local media coverage……2
Orderly response from law enforcement, local community……1

RECOGNIZABILITY
Target is widely featured in media; national icon……5
Target easily exposed to reconnoiter……4
Target's significance and location known mainly to local community……3
Plans of facility available on Internet, library……2
Targeting point unknown to locals; needs insider knowledge……1

** Crime prevention through environmental design*

Most versions of the CARVER protocol are concerned with the risk to physical structures and installations, but because structures and installations vary considerably in size, shape, and organization, the rating scale should be adapted to suit your local needs. A railway system, for example, entails quite different risks than does an office building or an industrial park.

Finally, this version of CARVER says little about the one significant feature of all targets that is attractive to terrorists: people, who are often the ultimate targets.

We consider this aspect of risk assessment in the following brief.

Brief 31: Save Lives Before Saving Buildings

Terrorists often target people, whether at work in office buildings, gathered in restaurants and market places, or confined in public transportation systems. For example, favorite targets of suicide bombers in Israel include buses, bus stops, market places, and restaurants. In these cases, the destruction of physical facilities is secondary: it is the people whom terrorists want to kill or injure. To do so they construct special bombs that disperse shrapnel to injure as many as possible. The combination of destruction and gore ensures widespread media attention.

Thus said, give special attention to the two attributes in EVIL DONE and CARVER that point to the vulnerability of people as targets: terrorists prefer to attack heavily populated buildings and locations (Occupied of EVIL DONE); and terrorists prefer attacks that will spread fear and panic throughout the community (Effect of CARVER).

Wherever people are. Conduct a preliminary survey to determine which facilities and installations are most likely to attract terrorist attacks, either because they contain many people, or because their destruction will cause severe hardship, injury, or death to people in the local community. In the case of the World Trade Center, both types of targeting were fulfilled. Many occupants of the Twin Towers were killed by direct attack; in addition, many emergency response personnel were killed during the rescue operation. And the aftereffects of the attack—both the cleanup and the pollution caused by the collapse of the towers—continue to claim victims to this day.

Densely populated confined spaces. Densely populated confined spaces, such as buses, railway cars, shopping malls, subway stations, theaters, hotels, convention centers, and stadiums are favorite terrorist targets: the presence of many people in a small area means that even a relatively small bomb can cause a great number of casualties. Fortunately, however, such facilities have a minimal number of entrances and exits that can be monitored by trained security personnel or with modern technology, such as video surveillance equipment.

Heavily populated open spaces. Open public places without controlled access points, such as bus stops, downtown shopping districts, open-air markets, and public parks.

Densely occupied special-purpose facilities. Building complexes that house workers, students, customers, and clients, such as hospitals, schools, office buildings, department stores, and stadiums.

Residential areas adjacent to possible targets. The Bhopal (India) and Chernobyl (Ukraine) disasters caused widespread injury and death among those living close to, or downwind from, the disaster sites. Are there any facilities in your jurisdiction whose destruction could cause injury to surrounding residents in the days and years following the attack, such as chemical factories and other plants that produce toxic materials, including nuclear power plants and oil refineries?

Panic. In the past, al-Qaida has made simultaneous attacks in different locations to cause panic among the populace and overload emergency response operations. When conditions are favorable, terrorists have even arranged attacks that target emergency response teams. This type of attack is unlikely in the United States, at least by a foreign-based terrorist group, because conditions favorable to routine terrorism are required. The preparedness of the emergency response team is crucial in minimizing the panic and injury caused by the attack because it helps neutralize the objective of the terrorists: to kill and maim as many people as possible.

Time frame	Deaths (Score=3 per case)	Major injuries (emergency hospital care; score=2 per case)	Serious injuries (Long-term care; score=1 per case)	TOTAL INJURY SCORE
Immediate				
Next day/week				
Several months				
Several years				
TOTAL				

People first. To make sure that you place people first in your line of protection, conduct an initial survey of your town to identify heavily populated facilities, then rated them according to estimates of how many people might be killed or injured, including emergency response personnel. Use the results of this survey in your CARVER and EVIL DONE assessments. A final assessment might look something like the Comprehensive Risk Assessment (CRA) instrument we have provided below. Adapt it to suit local needs, to the information you have collected, and to the range of possible scenarios you envision.

EVIL DONE, CARVER, and similar protocols require detailed information concerning the structure and functioning of various targets, the services that they provide, their management and organizational structures, and any security procedures that are already in place. To compile these data you will need good working relationships with the owners and managers of such locations (Brief 17); you will also need trained personnel to apply the protocols and to make the assessments. If you do not have trained risk analysts on staff, you will either need to look outside your department for expert advice or you will need to train your own officers to provide it. Injury estimates, in particular, can require input from experts because they will vary with the type of attack (biological, nuclear, conventional) and the particular target at risk. The skills that these individuals have might also carry over to other buildings, locations, and installations. Ask them for help.

Comprehensive Risk Assessment (CRA)

Attack Scenario (Time of day, weaponry, etc.)

Target description and location	EVIL DONE rating	CARVER rating	Injury score	*Total CRA
Suburban shopping mall				
Downtown shopping district				
Railway station downtown				
Bus station in front of market				
Power grid				
Water supply				
Convention center				
Town hall				
Hospital				
High school				
College				
Elementary school				
Middle school				
Buses				
Railway cars				
Theater				
Sports arena				
Chemical factory				
Oil refinery				
Natural gas storage tanks				
Paint factory near residential suburb				
Railway tracks through town center				
Toxic waste dump near school				
Other				

* CRA= (EVIL DONE + CARVER) X Injury score

Brief 32: Don't Be Diverted by the Displacement Doomsters

Some skeptics say that security measures will be unavailing against the threat of terrorism because terrorists can simply shift their attention from hardened targets to those with less stringent security; that is, although it might be possible to upgrade security at an iconic structure such as the Empire State Building to the extent that an attack becomes nearly impossible, other locations, such as ubiquitous shopping malls and restaurants, will always be soft targets. It is not always so simple for terrorists to distinguish between hard and soft targets. Terrorists must consider many factors when planning an attack; perhaps the two most important are the proximity of the target to their base of operations and their ability to easily access the target. A shopping mall that is protected by standard security procedures is likely sufficiently hardened to discourage would-be attackers. On the other hand, a high-rise office building that lacks basic security—where, for example, a truck bomb can be parked in the underground garage—is surely a soft target. Although a target's vulnerability is dependent on the appropriateness of the security measures that are designed to protect it, it ultimately depends on the terrorists' perception of the level of that security. And the fact is that any hard target, no matter how well-protected, can become a soft target if the attacker manages to obtain the tool or weapon needed to overcome its defenses.

Displacement. Will terrorists simply switch to softer, less significant targets if you harden major targets according to EVIL DONE and CARVER? If you tighten security in your jurisdiction—and make sure everyone knows about it— will terrorists merely move on to the next jurisdiction? Criminologists call this movement of crime from one area to another displacement.

Situational crime-prevention studies suggest that displacement is not a foregone conclusion. It certainly happens, but not in a majority of cases. In fact, offenders who are discouraged by security procedures do not simply go ahead with their planned crime. Indeed, security procedures that are introduced to stop crime at one location sometimes result in a diffusion of benefits: the reduction of crime in locations that were not targeted by the original security procedures.

We also know that displacement is not inevitable when opportunities for terrorism are reduced, specifically in the case of airliner hijackings. The Table below shows the number of hijackings that occurred from 1961 through 2003. There was a rash of airliner hijackings between 1968 and 1972 (between the United States and Cuba), at which point passenger and baggage screening was introduced at airports and the United States and Cuba signed a pact whereby each agreed to return hijackers to their country of origin. After 1973, there was a drastic reduction in hijackings. Did this increased security cause hijackers to go to other countries to commit their crimes? Clearly not: there is no hint in the data of an increase in hijackings in other countries; in fact, rates of hijacking were reduced abroad, as well. Did offenders switch to a different kind of terrorism, such as sabotage bombing, when hijacking became too difficult? Not so. As can be seen in the Table, aircraft bombings did not increase after the security measures were put in place; if anything, they decreased.

	Number of Years	Average Hijackings per Year		Average Sabotage Bombings per Year
		U.S.	Foreign	Worldwide
1961–1967	7	1.6	3.0	1.0
1968	1	20.0	15.0	1.0
1969–1970	2	30.5	58.0	4.5
1971–1972	2	27.0	33.0	4.5
1973–1985	13	9.4	22.7	2.3
1986–1989	4	2.8	9.0	2.0
1990–2000	11	0.3	18.5	0.3
2001–2003	3	1.3	5.7	0.0
1961–2003	43	6.7	17.9	1.6

Source: Clarke, Ronald V. and Graeme R. Newman. *Outsmarting the Terrorists*. Westport, Connecticut: Praeger Security International, 2006.

Do not be put off by the displacement doomsters. Hardening your targets according to EVIL DONE and CARVER will help forestall terrorist attacks. It makes life difficult for terrorists, who must consider many factors in deciding when, where, and what to attack. It might make their lives so difficult that they give up trying.

Finer Points of Displacement

Adaptation. There is little doubt that over time terrorists and other criminals adjust their behavior accordingly when new security measures are introduced. This is not so much displacement as it is adaptation. We have seen this process in the area of car theft. Steering column locks were found to be effective in reducing car theft in the 1970s in the United States and elsewhere. As thieves learned how to overcome these locks, new technologies were introduced, such as special alarms, tracking devices, and electronic immobilizers. As a consequence, car thieves are now more likely to rely on methods that get around these technologies, such as breaking into houses to steal the keys or targeting rental cars (i.e., renting them using false IDs). This extended process—a kind of arms race between them and us—is called adaptation. The plot to use liquid explosives on aircraft bound for the United States is a clear example of adaptation. In this case, faced by heightened security procedures at airports, the terrorists exploited the fact that liquids could be carried on board freely.

Alternative targets. Some suicide bombers plan for alternative targets in case the route to their first target is blocked. When multiple simultaneous bombings are planned, alternative targets in close proximity to the prime target might be selected. Mohammed Atta, the leader of the 9/11 terrorist group, observed with satisfaction the nuclear power station at Three Mile Island as he went on a practice flight to New York City. Had he been unable to reach the Twin Towers, he might have tried to destroy that alternative target. Make sure that such alternative targets are also protected.

Different weapon, same target. When it became clear that it was not possible to destroy the Twin Towers with a truck bomb, the terrorists did not switch targets; rather, they devised an unconventional weapon and an unconventional means of delivering it to the target. Why didn't they switch to a target that was easier to hit or destroy? We can only speculate, but one reason might be the almost unique iconic status of the World Trade Center. Another is surely that they had invested much time and resources in reconnaissance of the World Trade Center. If they had switched to another target, in a different city, a whole host of new logistical problems might have arisen.

In sum, although you should be mindful of alternative target selection and the possibility that terrorists will adapt to your defenses, it is not likely that your security precautions will cause terrorists to displace their activities. Adaptation, however, must be viewed more seriously because it is why you must constantly review your defenses in an attempt to anticipate where and how terrorists will try to overcome them.

"Some suicide bombers plan for alternative targets in case the route to their first target is blocked."

Brief 33: Improve Basic Security for All Targets

We all recognize that every potential target cannot be protected to the same degree, but can we protect everything to some degree? There are several ways to do this, but first a brief story about a poisoning attack by unknown assailants in the United States that resulted in seven deaths.

In 1982, seven people in the Chicago area suddenly collapsed and died, including three from one family. It was eventually determined that they had died after taking Tylenol® capsules that had been bought at a local drug store. The tablets had been laced with cyanide by unknown killers, whose identities remain a mystery to this day. Catching the persons responsible proved to be impossible; their motivations were never revealed. Today, this act would be called terrorism because it was a random chemical attack by unknown assailants who chose a drug store as their place of attack. (We should note that neither the choice of a particular drug store nor the method of delivery were random.) Johnson & Johnson, the makers of Tylenol, took steps to ensure that such killings would never happen again. In collaboration with consumer groups and government regulatory agencies, they introduced tamper-proof packaging. With one stroke, the packaging of products in the United States was changed forever. Today, all over-the-counter medicines, consumable products, and many other personal items arrive in tamper-proof or tamper-evident packaging. With one simple innovation, a massive improvement in product security and public safety occurred on a national, and indeed, an international scale. And it occurred to prevent an extremely rare form of murder.

We would not expect a local police executive to introduce a preventive technique of such massive proportions. We tell this remarkable story not only to demonstrate that creative thinking can solve seemingly impossible problems, but to highlight the fact that security interventions can have tremendously positive ripple effects. The introduction of tamper proofing protected people from many other forms of attack involving an incredible variety of products.

Basic security protects against terrorism and crime. On a smaller scale, there is much that can be done to ensure that basic standards of security are maintained throughout all government, public, and commercial facilities. A basic level of security, after all, should be maintained to protect against criminal intrusions and attacks, not just against terrorism. As we pointed out in Brief 7, it is very helpful to think of terrorism as just another form of crime and to approach the problem of prevention in much the same way: through partnerships with citizens, merchants, and government officials. In fact, the basic security measures that can prevent the burglary of a commercial establishment will also work to protect the establishment from a terrorist attack: the perimeter should be secured, adequate lighting installed, and so forth. You should work with local officials and merchants to ensure that they are aware of basic security procedures, including Crime Prevention through Environmental Design (CPTED; see Box). All buildings and locations can benefit from maintaining a basic level of security, regardless of whether or not a terrorist attack is anticipated. In these cases, protection against crime is also protection against terrorism.

"basic security measures that can prevent the burglary of a commercial establishment will also work to protect it from a terrorist attack"

The Basics of Crime Prevention through Environmental Design (CPTED)

CPTED analyzes environmental conditions and the opportunities they offer for crime or other unintended and undesirable behaviors. It attempts to reduce or eliminate these opportunities by using elements of the environment to (1) control access; (2) provide opportunities to see and be seen; and (3) define ownership and encourage the maintenance of territory.

CPTED evaluates the ways in which various features of a particular environment afford opportunities for crime and other undesirable behaviors. CPTED attempts to remove or reduce these opportunities by changing various aspects of the physical and social environment, including the following:

- Building design
- Site layout and site features such as lighting and landscaping
- Facility location and the influence of surrounding land uses
- Target hardening and security measures (or a lack thereof)
- Routine use and activity schedules
- Rules and policies governing use and behavior.

CPTED requires expert opinion and analysis to work properly. If your department does not have such experts, you will need to engage consultants or to train your own officers. Implementing CPTED often requires an extensive involvement with local neighborhood organizations, so you should search out towns or cities where CPTED is used on a regular basis. One example is the Seattle Neighborhood Group (http://www.sngi.org), which has adopted CPTED as its major approach to community safety problems.

General physical security. Depending on where you live, you might require expert assistance on a range of specialized issues, including private security, guards and patrols, loss prevention, executive protection, and CPTED. You can obtain information on training and expert assistance from the following organizations.

- The International CPTED Association is an organization dedicated to crime prevention by environmental design. Publications are available at CPTED Resources: http://www.cpted.net/.
- ASIS International (formerly the American Society of Industrial Security) provides a range of training courses on security surveys, CPTED, and risk assessment. ASIS also provides certification for a number of security areas and makes available listings of professionals who can conduct risk assessment and building surveys. Find ASIS at: https://www.asisonline.org. There might also be a local chapter of ASIS in or near your town.

Read More: Zahm, Diane. *Using Crime Prevention through Environmental Design in Problem-Solving, Problem-Solving Tools Series No. 8*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2007. http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=440

Brief 34: Meet the Challenge of Infrastructure Protection

We think of targets as specific places, buildings, or people. Infrastructures are different: they are complex systems that occupy both space and time and contain many fixed and moving targets. As such, they are better thought of as systems. There are many different ways to classify infrastructures, including the following.

- Transportation: air, sea, roads, rail, subways, ports, bridges, tunnels
- Food and agriculture: farms, processing plants, distribution centers
- Communications: telecommunications networks, postal service, radio and TV stations, Internet service providers
- Water: reservoirs, pipelines, purification systems
- Energy: refineries, generating stations, nuclear plants, electricity grids, oil and gas pipelines
- Industries and manufacturing: factories, warehouses, shops and retail outlets
- Public facilities: malls, restaurants, hotels, stadiums, movie theaters
- Banking and finance: branches, computer systems, offices
- Public health and safety: public records; health, safety, and social security systems.

Because infrastructures are complex, they are not often targeted by terrorists, although there certainly are some exceptions, such as the oil pipelines in Iraq. It is very difficult for terrorists to destroy a specific infrastructure because most have backup and fail-safe systems. Although an attack on infrastructure can be disruptive, achieving any significant level of injury and destruction is difficult. Although terrorists might attack a train or a bus, they do so not to bring the transportation system to a halt, but to kill as many people as possible with a single attack. Attacks against buses, trains, and aircraft are not really attacks on infrastructure, but rather on attractive targets that happen to reside within an infrastructure.

Because much of the infrastructure in the United States is privately owned and operated, a close relationship with local businesses will be essential to your security efforts. Do not assume that private companies or businesses will understand security needs: businesses vary enormously in the extent to which they consider security a part of their regular business activity. Many of the physical elements of infrastructure (buildings, towers, wires, reservoirs) can be well-served by the application of basic CPTED procedures (see previous Brief). Where necessary, call on the help of experts to protect specific infrastructures. We list below some sources of expert opinion for the protection of transportation systems, stadiums, and public events. Expert sources for other types of infrastructures are listed in Brief 36, because their complexity challenges terrorists to use unconventional means of attack, including biological and nuclear methodologies.

Stadiums and Events

Although strictly speaking, these are not part of the critical infrastructure, their protection is critically related to the security of other local infrastructure because a scene of mass destruction can overwhelm an otherwise capable system of communications, transportation, or public health.

- A special event that is designated a National Security Event can qualify for special federal protection and procedures under the direction of the U.S. Secret Service. http://www.secretservice.gov/nsse.shtml. Find out more about special event security from the COPS Office publication *Planning and Managing Security For Major Special Events: Guidelines for Law Enforcement*. http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=441.
- The Information Analysis and Infrastructure Protection Directorate of the DHS (http://www.llnl.gov/hso/iaip.html) provides an online assessment of stadium vulnerability.

Transportation Systems

The main federal source for transportation security is the Transportation Security Administration (TSA). Its web site (http://www.tsa.gov) contains a wealth of information, including links to many transportation security specialists. Another general source is the nonprofit, nonpartisan American Association of Highway and Transportation Officials. Find it at http://www.transportation.org/.

For specific transportation sectors, start with the following:

1. **Rail** - Common railway security issues include the following:

- Security of stations
- Open architecture
- Inspection methods and policies for passengers and baggage
- Security of rail freight and inspection of rail cars and containers.

2. For a general introduction to the issues, go to the TSA passenger rail group on the TSA's web site. This site provides links to rail travel resources, plus a number of helpful pointers. http://www.tsa.gov

3. For a helpful review of passenger security issues, see *Passenger Rail Security: Overview of Issues*, by David Randall Peterman, Congressional Research Service, May 2005. http://www.fas.org/sgp/crs/homesec/RL32625.pdf.

4. For a review of specific risks and ways to counteract them,see *Passenger Rail Security: Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts*. Government Accountability Office, Report No. GAO-06-557T. http://www.gao.gov/new.items/d06557t.pdf

5. **Bus** - For an overview of bus transportation issues, download the School Bus Driver Security Training Program developed by the New Mexico Surety Task Force. Although intended for school bus drivers, many of the points and procedures are applicable to any type of bus. http://www.nasdpts.org/documents/SecurityNewMexicoCourseTrainingGuide.pdf

   In addition, the National Association of State Directors of Pupil Transportation Services offers many useful links and articles. http://www.nasdpts.org

6. **Truck** - If your town is situated on a busy highway, roadway security can be important. Check out the Federal Motor Carrier Safety Administration for pointers on safety, security, and border issues. http://www.fmcsa.dot.gov

7. **Air** - Visit the TSA's Transportation Security Research and Development Center at http://www.tsa.gov/research/index.shtm.

8. **Sea** - If your town is close to a seaport, you will likely need special help, especially because of overlapping jurisdictional issues among federal, state, and local agencies. For further information, see *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*. Government Accountability Office. Report No. GAO-02-993T. http://www.gao.gov/new.items/d02993t.pdf

Brief 35: Know About MURDEROUS Weapons

Despite the terrifying scenarios generated by weapons of mass destruction, they are rarely used in terrorist attacks for reasons we discuss in the next brief. Instead, the vast majority of terrorist attacks are carried out using guns and explosives. The sometimes subtle differences between the various types of conventional weapons make each more or less suitable for different types of attack. To protect targets properly, you must decide which type of weapon is most likely to be used for each particular target. To assist in this process we offer the acronym MURDEROUS, which summarizes the attributes of weapons that terrorists seem to value.

Multipurpose: Most firearms are designed for a specific purpose. For example, a high-powered rifle is generally used to hit a single target located at a great distance from the shooter; a shotgun, on the other hand, is designed to provide a wide field of fire, but is useful only when the target is located near the shooter. Explosives have a much broader application: a car bomb, for example, can be used to assassinate a single individual, whereas a truck bomb can be used to demolish a large office building. Obviously, explosives cannot be reused, so their supply must be replenished. It is possible, however, to achieve the destructive effect of an explosive by using small arms that can fire explosive ammunition, such as dum-dum bullets or rocket-propelled grenades.

Undetectable: Because of enhanced security at airports and other likely targets, terrorists must generally use weapons that are concealable and undetectable. This helps explain the popularity of Semtex, a small, lightweight, and largely undetectable explosive. It took only 11 ounces of Semtex packed into a small tape recorder to bring down Pan Am 103 over Lockerbie, Scotland. Because it is easily concealed, it is an ideal weapon for suicide bombers, who must often penetrate layers of security to reach their targets.

Removable: The weapons of terrorism must be portable, which means that they must be light enough and small enough to be lifted and carried by one or two people. This portability and size also makes such weapons easy to steal. We know from studies of hot products that portability is highly valued by thieves. For example, when high-quality stereo equipment was very expensive it was a favored target of burglars because it could be carried off and resold easily. Although terrorists are not interested in the resale value of the things they steal—a weapon is prized because it is destructive, not aesthetic—the same principle applies.

Destructive: Guns are most suited to killing a targeted individual. Because terrorists generally wish to kill as many people as possible as quickly as possible, their weapon of choice is often the explosive. In Iraq, for example, the insurgency has killed many more U.S. soldiers using improvised explosive devices (IED) than it has using bullets. See the Box for a summary of the lethality of various types of weapons.

Enjoyable: Terrorists enjoy their weapons and seemingly get a great deal of excitement and pleasure out using them. Of course, it is not just terrorists who enjoy weapons: many ordinary people do, too.

Reliable: To be useful a firearm must be reliable, which is why new military recruits are thoroughly trained in caring for and using their weapons. Civilian users find out whether a weapon is reliable through continued use. If they are familiar with a particular weapon (or one like it), they are likely to favor that weapon over another. This means that terrorists will likely shun unconventional or unfamiliar weapons unless their mission cannot be accomplished in any other way. Thus, it is likely that routine terrorist attacks will take place using familiar, conventional weapons.

"...terrorists will likely shun unconventional or unfamiliar weapons unless their mission cannot be accomplished in any other way."

Obtainable: Availability is perhaps the most important of all weapon characteristics. How easy is it to get the weapon? Can it be easily bought or stolen? Can it be manufactured in house? The world is awash in small arms, which are the most widely used terrorist weapons. And because there are so many of them, there are plenty of places from which they can be stolen; theft is probably the most common way that terrorists obtain their weapons.

Uncomplicated: Whether a weapon is user-friendly determines how much training is needed to operate it successfully. Even seemingly simple weapons such as handguns require practice and training. Complicated weapons that demand considerable expertise, such as free-flight armor-piercing missiles, will rarely be used. In fact, when such weapons have been used, the attacks have often failed, precisely because the weapons were used incorrectly. In 1972, for example, the Black September movement attempted to bring down an El Al airliner using an RPG-7 grenade launcher; the shot went awry and brought down a Yugoslav Airlines plane instead.

Safe: Bombs are inherently more dangerous than guns. Many members of the Provisional Irish Republican Army were blown up by explosives that detonated prematurely.

We arrived at MURDEROUS by trying to think like terrorists; no doubt the scheme could be refined through empirical research. Such research, however, is unlikely to overturn the basic principle that terrorists favor weapons with specific characteristics that are closely suited to the type of attacks they intend to make. Understanding the nature of these characteristics can help us find ways of preventing attacks and of controlling access to the weapons terrorists favor.

The Lethality of Weapons

The destructive capability of weapons is usually assessed according to the following factors:

- Penetration: how deeply does the weapon penetrate into the target (e.g., armor penetration versus hit-to-kill)
- Generation of fragments, shrapnel, and debris
- Blast and shock: the extent to which the target structure collapses; the ripple effect of the blast
- Production of fire and fumes
- Accuracy: explosions spread their destruction; a high-powered rifle is narrowly focused
- Kill ratio: the number of people who can be killed with one attack.

Consult and follow Department of Defense guidelines on stand-off distances to conventional explosive devices for all buildings that are rated high on your Comparative Risk Analysis (see Brief 31).

Read More: U.S. Department of Defense, *Unified Facilities Criteria (UFC): DoD Minimum Antiterrorism Standards for Buildings*, UFB 4-010-01. Washington, D.C.: U.S. Department of Defense, 2003.

Read More: Clarke, Ronald V. and Graeme R. Newman, *Outsmarting the Terrorists*. Westport, Connecticut: Praeger Security International, 2006.

	Small Arms	Explosive Devices	Biological / Chemical	Nuclear
Penetration	Limited	Limited	Moderate	High
Debris	Limited	High	None	High
Blast	Limited	High	None	High
Fire and Fumes	Limited	High	High	High
Accuracy / Precision	High	Moderate	Low	Low
Kill Ratio	Low	Moderate	Moderate / High	High

Brief 36: Don't Unduly Fear Weapons of Mass Destruction

Many of us live in dread that terrorists will attack with biological, chemical, or nuclear weapons, that is, weapons of mass destruction (WMD). Although this might be your worst nightmare, to date there have been very few attacks using such weapons. In 1995, the Aum Shinrikyo terrorists released Sarin gas in the Tokyo subway, killing 12 people and injuring thousands. In the same year, an unexploded dirty bomb (a device designed to disperse radiological material by means of a conventional explosive) planted by Chechen separatists was discovered in a Moscow park. But these isolated incidents were not forerunners of an outbreak of attacks with weapons of mass destruction, possibly because these weapons fit few of the requirements of MURDEROUS (Multipurpose, Undetectable, Removable, Destructive, Enjoyable, Reliable, Obtainable, Uncomplicated, and Safe; see Brief 35). In fact, WMD are not all that suitable for use by terrorists because they are unpredictable in their effects and often use airborne chemicals or biological agents that might harm terrorists and their sympathizers. Moreover, WMD are not readily available, are complicated to manufacture and use, and are sometimes difficult to transport and conceal. And although they can be very destructive, not every terrorist group wants to wreak destruction on such a wide scale. Eco-terrorists, for example, undertake small but carefully targeted attacks that are narrowly tailored to their political agendas; other groups might prefer to extort concessions by taking hostages or occupying embassies and other official buildings. Use of WMD could even backfire on the terrorists by causing them to lose sympathy.

Terrorists have rarely used unconventional weapons, even those that are relatively easy to obtain, such as ground-to-air missiles, which can bring down airliners. An estimated 700,000 of these missiles, known as man-portable air defense systems (MANPADS), have been produced worldwide since the 1970s. They are not difficult to purchase on the black market and are relatively inexpensive: some estimates put the price as low as a few hundred dollars for the older missiles. Many are believed to be in the hands of terrorists hostile to the United States, but none seem to have been deployed against a U.S. airliner. We can conclude from this that terrorists will likely continue to favor guns and explosives, except in very unusual circumstances or where targets are particularly difficult to reach.

The likelihood of a small city being attacked with WMD is especially low because cities with larger and more concentrated populations offer a much greater potential for destruction—not to mention the ripple effect that such an attack would create. In any event, there is little that can be done at the local level to prevent such an attack from occurring, although you should make sure that you have an emergency response plan in place that addresses such a scenario. We take up these issues in the final section of this manual. You can and should use the expertise of those who are trained to deal with the hazards and intricacies of unconventional weapons. Some of these expert resources are listed below.

Biological and chemical hazards

- U.S. Army Medical Research Institute of Chemical Defense: develops medical countermeasures to chemical warfare agents and trains medical personnel in the medical management of chemical casualties. http://chemdef.apgea.army.mil/
- UCLA Center for Public Health and Disasters: promotes interdisciplinary efforts to reduce the health impact of natural and human-generated disasters. http://www.cphd.ucla.edu
- Environmental Protection Agency: supports the federal counterterrorism program by helping state and local responders plan for emergencies, coordinating with key federal partners, training first responders, and providing resources in the event of a terrorist incident. http://www.epa.gov/ebtpages/emercounter-terrorism.html
- Center for Infectious Disease Research & Policy: dedicated to preventing illness and death from infectious diseases through epidemiologic research and the rapid translation of scientific information into practical applications and solutions. http://www.cidrap.umn.edu/cidrap
- Centers for Disease Control and Prevention (CDC): recognized at home and abroad as the leading federal agency for the protection of the health and safety of the people of the United States, the CDC provides credible information to enhance health decisions and promotes health through strong national and international partnerships. http://www.cdc.gov
- DHS: provides information on hazard mitigation. http://www.dhs.gov/xprepresp

Infrastructure protection

In Brief 34 we provided sources for transportation security experts. Here is a brief list of the major organizations that are involved with infrastructures that might be attacked using unconventional weapons, particularly nuclear or biological agents. Contact them to receive detailed information and sources of help.

Food and agriculture

- United States Department of Agriculture: provides guidelines for disposal of intentionally adulterated products. http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/index.asp
- National Association of State Departments of Agriculture (NASDA): as part of its mission to develop and implement programs designed to support and promote the U.S. agricultural industry, the NASDA web site includes a model food emergency plan for federal and state partnerships. http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Model_Food_Emergency_plan/index.asp
- Center for Food Safety and Applied Nutrition: a division of the U.S. Food and Drug Administration, the Center has created a guidance document to aid retail food stores and food service establishments in implementing basic food security procedures, Retail Food Stores and Food Service Establishments: Food Security Preventive Measures Guidance, http://www.cfsan.fda.gov/~dms/secgui18.html.

Communications

- National Telecommunications System: find directives and manuals at http://www.ncs.gov/.
- Federal Communications Commission: provides guidelines on establishing priorities for the restoration of telecommunications facilities and systems and for the provisioning for replacement systems. http://www.fcc.gov/cgb/consumerfacts/homelandtsp.html
- Information Security and Privacy Board: provides advice to government officials on information security and privacy issues pertaining to Federal Government information systems. http://csrc.nist.gov/ispab
- U.S. Computer Emergency Readiness Team
- National Cyber Security Partnership

Water

The Water Information Sharing and Analysis Center partners with the Environmental Protection Agency and the DHS to offer four contaminant databases, white papers on various water security topics, and access to vulnerability assessment tools. http://www.waterisac.org

Energy

- Energy Information Administration: provides information on refinery disruptions and vulnerability throughout the United States; shipping chokepoints and spills; and protecting oil refineries, storage, and transportation. http://www.eia.doe.gov/emeu/security/Oil/index.html
- U.S. Department of Energy: oversees the Infrastructure Security and Energy Restoration program. Offers training and support at state and local government levels. http://www.oe.energy.gov/our_organization/isei.htm
- Energy and Infrastructure Assurance (Sandia National Laboratories): its primary mission is to enhance the safety, security, and reliability of energy and other critical infrastructures. http://www.sandia.gov/mission/energy

"Terrorists have rarely used unconventional weapons, even those that are relatively easy to obtain."

VI. Be Ready if Attacked


LINE DO NOT CR

“To first responders, it does not matter whether terrorists come from Afghanistan or Alabama. In many respects, terrorist attacks are similar to natural disasters… the effects… are local…”

Brief 37: Know That All Disasters Are Local

To first responders, it does not matter whether terrorists come from Afghanistan or Alabama. In many respects, terrorist attacks are similar to natural disasters such as earthquakes—although there are some obvious and important differences (see Brief 38). Because the effects of such events are local, it is local conditions that must inform you about how to respond to an attack.

For the first few hours of an attack, you are on your own. It takes time—a lot of time—to get help from the government. In the meanwhile, local police must respond to a terrorist disaster as it unfolds. At the onset of an attack, this means using only local resources. If you have done your homework, you will already have established communication channels that allow you to identify and contact the important actors in your own and adjacent communities. You will, of course, notify federal and state authorities that an attack has occurred, but you should not depend on them for immediate support. In fact, they are likely to be most helpful during the recovery phase.

A terrorist attack is a crime scene. As noted in Brief 9, you should think of terrorism as crime. To the extent possible—given that your prime concern will be to mitigate the harm done to victims at the site—you should treat the scene of the attack as a crime scene. Procedures for collecting and preserving evidence should be little different from those used at the scene of any serious crime, although you may need experts to help collect and preserve evidence.

Pursuing the terrorists. Whether the perpetrators are affiliated with a terrorist group is of little relevance to your duties as first responder: your immediate task will be to deal with the destruction and death at the scene. Pursuing the terrorists should be left to the FBI and other federal agencies. You can help them by preserving the crime scene, having available the prevention information you have already collected (Briefs 29, 30 and 31) and systematically collecting relevant information after the attack.

Do what you know best. Local communities are already poised to respond to many potential disasters. Police deal regularly with personal injury and property damage incidents, whether minor fender benders or multicar accidents that threaten to overwhelm the capacity of emergency response units. Most communities have contingency plans for weather-related disasters, such as winter storms, earthquakes, floods, and hurricanes. Since the Columbine school calamity, local communities have begun to prepare for the possibility of violent attacks in their educational institutions; even before Columbine, bomb threats and other forms of violence were not infrequent in many school districts. And in recent years, the fear of flu and other disease epidemics has heightened local awareness of the problems posed by viral and bacterial threats. You probably already know most of those involved in planning the response to these and other types of disasters. One critical role you can play is to develop a plan to coordinate these resources in the event that disaster strikes.

Being ready. In Brief 13 we advised you to counter "what if" with "how likely." Because we were concerned with assessing risk and vulnerability from the point of view of prevention, it made sense to try to identify the targets that were most vulnerable. Disaster preparedness is very different when looked at from the point of view of the first responder. The first responder to a terrorist attack must be prepared for "what if": what will happen if your worst nightmare comes true, regardless of the likelihood of its occurrence. The challenge here is not thwarting the terrorists, but rather mitigating the conditions that the terrorists leave behind: the disaster, injury, and destruction. As the first responders to criminality, the police will be expected to respond immediately when a terrorist attack occurs. You must, therefore, ask yourself the following questions.

- Is your department prepared for an attack?
- Whose responsibility is it to coordinate the response teams of departments other than the police?
- How does a police department prepare for a major disaster?

Strike a balance. Because first responders are often first in line for blame, it is understandable that a police executive, for example, might be tempted to overreact, either by doing too much or by trying to avoid the first responder role. An example of the former is a small town chief who squanders Department of Homeland Security money on a decontamination chamber without first assessing the risk of a chemical attack. An example of the latter is a police executive who takes the position that the victims, the firefighters, and emergency medical personnel are the true first responders, rather than the police. In this case, the police will take a back seat in the development of first-responder planning; and although this position might be technically accurate, it ignores the likelihood that police will be held publicly accountable because of their traditional role in responding to problems in the community.

Do not let the problem of terrorism overwhelm the other functions of your department. Aim to strike a balance between preparedness and everyday policing, which will help you avoid overreacting. Analyze how preparing for a terrorist attack can benefit day-to-day policing and critically examine options that provide benefits in both areas. Many of the steps in this manual will produce such dual benefits; for example, your department will forge close relationships with businesses and community organizations as you draw up an inventory of vulnerable targets. Partnerships of this kind can also be extremely useful in preventing common and recurring crime. Protecting buildings and business establishments from terrorists also makes them more secure from conventional criminals. Tightening identity authentication procedures at retail stores not only makes the work of terrorists more difficult, it also helps prevent theft. Emergency preparedness drills for natural or accidental disasters will also prepare police to deal with their role as first responder to terrorist incidents.

“Because first responders are often first in line for blame, it is understandable that a police executive might be tempted to overreact.”

Brief 38: Know That Not All Disasters Are Equal

Disasters make exceptional demands on first responders. Terrorist attacks can produce conditions that might resemble disasters, such as the following:

- Kill or injure large numbers of people
- Affect a large geographic area and many jurisdictions
- Require long, drawn out response operations
- Involve many different types of hazards
- Demand resources and capabilities that are beyond the capacity of local response organizations
- Bring in a large influx of volunteers and supplies
- Damage vital transportation, communications, and other infrastructure
- Draw on large numbers of responders from a wide variety of sources, both public and private
- Endanger the lives of responders.

Although few terrorist attacks reach the level of disaster described above, many terrorist response manuals and handbooks are based on manuals for natural disasters;. thus, these manuals advocate an "all hazards" approach to disaster preparedness.

To what extent are major terrorist attacks similar to such disasters? Table 1 uses the criteria listed above to compare the features of a major natural disaster (Hurricane Katrina) and a major terrorist attack (9/11—the World Trade Center).

The lack of warning, which is perhaps the most distinctive characteristic of a terrorist attack, has major planning implications. Apart from this, the duration and the geographic focus of terrorist attacks distinguish them from natural disasters. Conventional terror attacks are narrowly focused: they target either a single location—as was the case in Oklahoma City—or they target several narrowly focused locations, as was the case with the 9/11 attacks. From a local point of view, this focus allows responders to assess quickly the extent of the damage and danger. The 9/11 attack on the World Trade Center was narrowly focused on specific targets. Hurricane Katrina, in contrast, covered a wide swath of territory. First responders who had to address the devastation in the city of New Orleans were also faced with a wide range of problems throughout Louisiana and Mississippi. Furthermore, the hurricane was drawn out over several days, whereas the attacks of 9/11 lasted a mere 102 minutes: it was less than 2 hours from the time the first airplane crashed into the North Tower until both towers collapsed.

Table 1. Comparison of Hurricane Katrina and the 9/11 Attacks.

Disaster characteristic	9/11	Hurricane Katrina
Advance warning	None	Weather advisories for several days warned of the hurricane's approach
People killed	Approx 2,750	1,500 deaths in Louisiana, including approximately 600 in New Orleans; 300 in Mississippi
Geographic area and jurisdictions	At least five jurisdictions, confined geographic area	Many jurisdictions, large geographic area
Duration of disaster	1–2 days	Many days before waters subsided
Recuperation time	Ongoing	Ongoing
Number of hazards	Many health and pollution hazards, others still being discovered	Pollution from refineries and fouled water, but not as serious as first thought
Adequacy of local resources	Local agencies well supplied, but much outside assistance received	Resources totally inadequate; needed outside help, much of which was delayed
Major national media coverage	Yes	Yes
Damage to infrastructure and communications	Yes, at local site, but not citywide, except for some phone disruption	Communications, power, and water wiped out throughout New Orleans
Number and variety of response agencies	Three public agencies, large number of private responders	Initially only the New Orleans Police Department and Coast Guard; later many federal, state, local, city, and private agencies
Threat to the lives of responders	Many responder lives lost	Some danger, but no responder lives lost

Table 2. Terrorism Preparedness Checklist			
Item	Rating Criteria		WTC 9/11 Score
Weapons used (choose weapon types used)	1 - Small arms, guns 2 – Small explosive device 3 – Large explosive device 4 – Very large explosive device 5 – Unconventional weapon		**5**
	Multiply rating by number of weapons =		**10**
Target/locations (check all that apply)	Occupied building High-rise building Open space Multiple targets in different locations Undifferentiated area Densely populated area **Total Checked=**		**5**
Infrastructure damage (3 = most severe)	Power grids Water Transportation routes Communications	1 2 3 1 2 3 1 2 3 1 2 3 **Total=**	**4**
Terrorists	1 – Attackers dead/left scene 2 – Single attacker still at scene 3 – Multiple attackers still at scene **Total=**		**1**
Hazards (use vulnerability survey conducted as part of disaster preparedness)	• Toxicity caused by fire/explosive • Nuclear facility at or close to scene • Chemical factory at or close to scene • Biological facility at or close to scene • Other known hazards at or close to scene **Total Checked=**		**1**
Fire rating (assess using fire department radio codes)	1 – Low 2 – Medium 3 – High **Total=**		**3**
Personnel and equipment needed (check those needed)	• Fire • Medical • Suited biological/chemical personnel • Police – traffic control • Police – scene control • Police – investigators on scene • Police – SWAT team • Communications specialists • Transportation – personnel and equipment **Total Checked=**		**8**
			32

The types of terrorist attack that most resemble a natural disaster are the ones that we most fear: either a weapons of mass destruction (WMD) attack that destroys a large geographic area or a biological attack that spreads poison throughout a large population. Such attacks would not be directed at a specific target, such as the World Trade Center, but at a whole city, just as occurred with Hurricane Katrina. Biological and chemical weapons are difficult to confine to specific targets—and because of their lethality there is little need to so direct them—so they can be used to target very large populations or geographic areas.

With these distinctions in mind, Table 2 presents a checklist that can be used to assess the level of response needed for a terrorist attack. Although it is only a very rough guide, it can be used as an initial assessment of the scope of response that might be needed. The protocol can also be used or developed in conjunction with the vulnerability assessment survey that you should have already completed as part of your terrorism disaster preparedness (see Briefs 29–34).

It is difficult to obtain reliable information in the early phases of a terrorist attack or a natural disaster. As the event unfolds, conditions change constantly, as in the first 17 minutes of the attack on the World Trade Center. Without information, it is impossible to complete a protocol such as the one presented here. It will also need to be revised as new information comes in. As an exercise, we have completed the protocol as it might have been used for the 9/11 attack. In doing so, we have the great advantage of hindsight. If we place ourselves in the shoes of first responders in the first 17 minutes of the World Trade Center attack, we can see that many parts of the protocol would have been difficult to complete. Indeed, it was a lack of reliable information that made for mistakes in management and handling of the disaster scene.

Brief 39: Use the 3-by-3 Approach

Given that local police will be at the center of the response to a major terrorist attack—and will be held accountable as first responders—make sure that you can answer the six questions of SECURE.

1. **S**afe: Have steps been taken to ensure the safety of your officers?
2. **E**ffective: What will your officers do when they get to the scene?
3. **C**apable: Have your officers been well-trained in disaster response?
4. **U**nited: How well is your department coordinated with other first responders?
5. **R**apid: How quickly can your officers get to the scene?
6. **E**fficient: Will policing tasks unrelated to the attack be compromised?

These general questions will serve to keep you on track. You will not be able to answer them all satisfactorily, however, unless you develop a systematic approach to covering all the important issues raised by SECURE. This brief introduces you to the 3-by-3 approach, which is composed of the three phases of the first-responder management cycle and the three phases of a terrorist disaster.

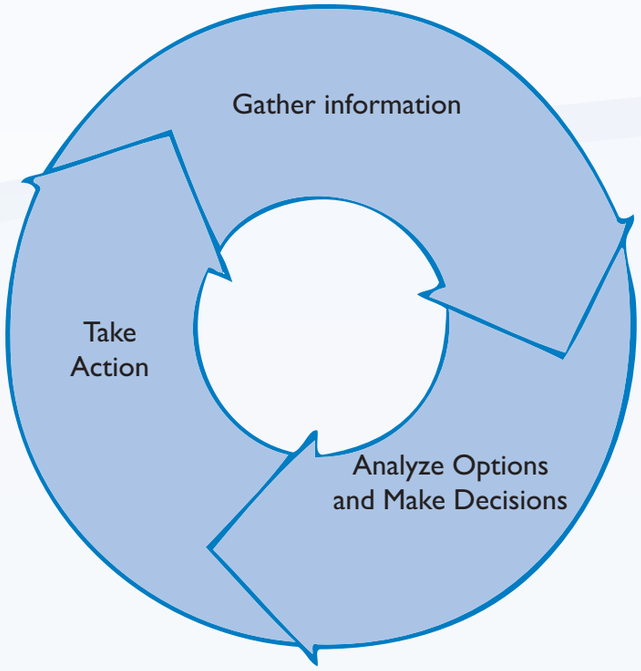
The first-responder management cycle. The first-responder management cycle developed by the RAND Corporation (see Diagram) will help you to act systematically by ensuring that you take three steps in sequence: (1) collect all the information that you need; (2) analyze your options; and (3) take action. By applying this method to each of the three phases of a disaster (see below), you will ensure that your responders know what they are doing and why they are doing it. This, of course, is a continuing process because you will want to reassess the information you have collected after you have taken action. One hopes that you will be able to learn from your mistakes—and your successes. (If you are familiar with problem-oriented policing, you will notice that this process is very similar to the SARA model: Scanning, Analysis, Response and Assessment.)

You should build this information management cycle into the everyday operations of your department. To accomplish this you will need to do the following:

- Make it easy to collect and record information using simple checklists, forms and, above all, electronic tools, such as onsite notebook computers.
- Educate your officers so that they understand the importance of collecting information in solving policing problems.
- Store the information so that it can be easily accessed and updated.
- Create a database that can be used by officers in their daily operations.
- Structure the database so that it can be analyzed to solve persistent policing problems, both large and small.
- Designate and train specific officers to analyze the information.

Information is key to solving all policing problems, including terrorism. The lack of information can have dire consequences. During the attacks of 9/11, the constant updating and replenishing of information vital to rescue operations proved to be crucially lacking, with deadly results.

The First Responder Management Cycle.



Source: Adapted from: RAND Corporation. *Protecting Emergency Responders. Volume 3: Safety Management in Disaster and Terrorism Response*, 2004, p.xvii.

Understand the three phases of a major terrorist attack. A major disaster or terrorist attack has three phases: before, during, and after the attack. Careful preparation for each phase will incrementally mitigate the problems faced in each subsequent phase. Thus, if you put a lot of effort into the pre-attack phase, you will face fewer problems in responding to the attack itself. And if you pay careful attention to the scene of the attack, you will mitigate the effects of the attack, thereby reducing the problems faced after the attack. First responders and the media tend to pay most attention to the middle stage, the attack, because of the obvious trauma and destruction that it brings; however, a major terrorist attack is a very brief moment in time, which accounts for just a small portion of the overall effects of the disaster and the responses that are needed to mitigate it.

Although it may seem obvious that the moment of attack is different from the periods before or after, there is much controversy among disaster specialists as to when each phase of a disaster begins and ends. It can be argued, for example, that the worst effects of Hurricane Katrina were not felt in New Orleans until some days after the hurricane hit because of the inadequacy of the official response. The situation in the Louisiana Superdome, where people had been told to congregate, created its own type of disaster. There is considerable overlap of each phase, depending on the type of disaster and type of response. As we stated, the work you do in each phase will mitigate the effects of each subsequent phase. It is obvious that different government agencies play different roles of differing importance at different times as a disaster unfolds. For an example of this, see the Figure in Brief 49, which illustrates how the roles of first responders change over time in a small natural disaster.

The Table below summarizes the 3-by-3 approach. It depicts the three stages in the first-responder management cycle as they apply to the three phases of a terrorist disaster. In the next several briefs we will look more closely at each phase of a terrorist disaster.

The 3-by-3 Approach to Terrorist Disaster Management.

	1. Collect information.	2. Analyze options.	3. Take action.
Before	Make lists	Draw maps	Develop response plans
During	Have efficient communications	Coordinate efforts	Deploy personnel and equipment
After	Monitor hazards and the health of victims and first responders	Assess treatment needs; assess preventive needs	Sustain recovery; revise disaster plans

Brief 40: Be Ready Before an Attack

Make lists and plenty of them. To be prepared for a terrorist attack you will need to assess your overall response capabilities. To assist in this endeavor, make lists of the following:

- Response organizations and their affiliations, whether federal, state, or local; the number of personnel in each organization; and their skills, areas of expertise, and level of training.
- Businesses that might be involved as first responders, such as hospitals and transportation and telecommunications companies.
- Equipment that is available to your department and other responders, such as suits, masks, weapons, and vehicles.
- Money available to support your response, including possible sources of long-range funding, such as state and federal homeland security grants (see Brief 20).
- Stocks of equipment and supplies.
- Essential items to equip your officers in the face of emergency (see below concerning hazards). For this you will need expert advice. A good place to start is the RAND knowledgebase for first responders (see Brief 39).

Learn about hazards. Once you have conducted a vulnerability survey (Briefs 29–31), you will have a good idea of the risks that your community faces. Major terrorist attacks can take many forms: chemical, biological, nuclear, high explosives, and so forth. Depending on the type and location of the attack, you might be faced with secondary hazards; for example, particular locations might contain products that can cause additional danger if damaged by explosion, heat, fire, or water. You should, therefore, make a list of all the hazards that lie hidden in local businesses, manufacturing plants, and warehouses. You will probably need expert help in assessing the risk that these hazards present, including whether any chemical, biological, or radiological agents are so lethal that they will pose an immediate danger to first responders. There might be ways of minimizing potential hazards for first responders and victims, including the use of protective gear for corrosive chemicals or the use of antidotes in the case of biological hazards. You should seek expert advice regarding the feasibility and necessity of purchasing such materials, given the possible hazards.

Map it out. Once you have collected all the relevant information, proceed to Stage 2 of first-responder management: analyze your options. You will have an enormous amount of information on your lists. It is time to transform this information into a form that will help you to assess your options. A useful way to visualize your options is to make a map that includes the following information;

- Location of hazards and their levels of toxicity and vulnerability
- Location of potential targets and their levels of vulnerability
- Location of responder organizations; if your community is small, the actual residences of personnel
- Availability of volunteers, their levels of expertise, and how they can be contacted
- Transportation routes, including those that first responders might take to potential targets
- Location of specialized equipment needed by first responders
- Location of hospitals and other treatment centers to which victims can be transported
- Location of transportation resources, such as buses and trains.

From this map you will be able to identify the following:

- Preferred meeting points for first responders
- Preferred routes to be taken to particular targets and from targets to treatment centers
- Routes for mass evacuation
- Problem locations that require more pre-incident attention to mitigate the consequences of an attack
- Potential difficulties in transporting multiple responders to and from the disaster scene.

Develop an emergency response plan. To develop an effective plan you will need to work with major first-responder organizations, both in your own jurisdiction and in adjoining ones. Armed with the information that you have collected in the first two stages of the responder management cycle, create a plan for coordinating all the various first-responder groups. This will require working closely with other responder organizations because holding frequent meetings can be important to establishing trust and to working out the roles and responsibilities of each organization. A critical incident response plan should include the following:

- A Critical Incident Response Team (CIRT) composed of representatives of first-responder organizations, businesses, and public service agencies likely to be affected by an attack.
- An agreement among the first-responder organizations concerning roles and responsibilities, including details on how their special expertise and equipment will be used.
- A clear description of the command structure in the event of a major attack or disaster, including the appointment of an overall commanding officer (see Brief 45).
- A timetable of disaster preparedness activities.
- A plan for activating first responders in the event of an attack.
- A plan for evacuation if it is deemed necessary.
- A protocol that measures the seriousness of a disaster or attack so that the level of response can be adjusted accordingly. As noted in Brief 38, not all disasters are equal: the extent of casualties and of destruction to infrastructure can vary from attack to attack. Experts in biological warfare, for example, might not be needed if a site is attacked with conventional explosives.
- Criteria for deciding whether and when to call for federal or state assistance (National Guard, U.S. Army Corps of Engineers, etc.) and a description of how these entities will fit into the CIRT command structure.
- A communications protocol that allows for communication across jurisdictions and first-responder organizations.
- A schedule for pre-incident training of first responders and testing of command structure and communications.
- Designation of contacts and the establishment of formal agreements with federal, state, and regional authorities that might be necessary for legal or operational procedures.
- Assessment of supplies and services necessary for coping with a disaster (e.g., medical supplies, emergency facilities); if needed supplies are not immediately available, a plan for procuring and transporting such materials.
- A plan for enabling first responders to meet their family needs in addition to their official duties.

You have a lot of control over what you can do in the predisaster phase. If you are diligent, the work you do in this phase will pay off in the next phase, because getting information and interpreting it correctly is by far the most difficult challenge that faces the first-responder management team in the face of an unfolding terrorist attack.

“...getting information and interpreting it correctly is by far the most difficult challenge that faces the first-responder management team.”

Brief 41: Invest in Training

Police training is essential, especially for dealing with the nightmare of a massive terrorist attack. Before you even consider counterterrorism training, however, you should first review the training your officers have already had in the course of their regular policing duties.

Basic training. All your officers should be trained in data collection and management. Although some might see data management as irrelevant to their daily police work, it should be abundantly clear by now that your department cannot be prepared to deal with a terrorist attack without having collected a massive amount of information about terrorism prevention (targets, terrorist opportunities, and hazards) and terrorism response (sources of community support, equipment, and supplies).

Ideally, your data-collection course would be taught in house so that it could be linked directly to the system your department uses to record daily events, calls for service, and situations and information concerning terrorism prevention and response. Not all officers need to be trained in the finer points of vulnerability assessment, but they all need to understand the significant impact data collection practices will have on how your department responds to a terrorist attack—and indeed, to any type of crime or disorder problem. In-house training on departmental data-collection procedures and systems, therefore, is essential. Although this minimal training will be sufficient for most of your officers, recognizing the importance of collecting data is only the first step. To take full advantage of your intelligence gathering, you must also have individuals who are trained to analyze and interpret the information so that you can use it to make sensible decisions. For this you will need a crime analyst. Courses on crime analysis are available at many universities. If such a course is not available in your area, approach your local university social science or criminal justice department and see if they are amenable to offering one. The manual *Crime Analysis for Problem Solvers in 60 Small Steps* will help experienced crime analysts expand their knowledge and their role into that of a key member of a problem-solving team. http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=47.

Beyond training in the basics, how can you make sure that your officers are ready to become first responders in the event of a terrorist attack? For this, you will need to decide the following:

- Which topics will be covered?
- What form will the training take (lectures, videos, workshops, field exercises)?
- Which officers will take which courses?
- Who will do the training?
- How will the training be paid for?

Which topics? The Federal Emergency Management Agency (FEMA, now part of the Department of Homeland Security [DHS]) provides many helpful courses online, the most relevant of which are listed in the Table below. All your officers should take the introductory and general courses; there might also be others that are relevant to your particular needs or responsibilities. Clearly, the breadth of topics to cover will depend on your role in the National Incident Management System (NIMS) structure (see Brief 45) and the extent to which you and your officers participate in NIMS activities. Not surprisingly, the most popular course is NIMS compliance, which is required for all agencies receiving money from the DHS. Online courses are probably the most convenient alternative, especially if your officers can take them at designated times on department computers. Certificates of achievement are issued once the courses are completed.

Scenario-based drills. Although reality-based drills are necessary, they can be demanding of time and resources. Real-life scenarios—where trainers stage a mock emergency and all the relevant agencies respond—require a great deal of preparation and coordination. They also require trained staff or consultants to develop the scenarios and to supervise the operation. Basic scenarios might include the following:

- Dirty bomb attack in populated location
- Bombing of a chemical plant or nuclear installation
- Truck bombing of a shopping mall
- Bombing of a power grid
- Release of a biological weapon in the subway system.

In deciding whether to expend resources on such training operations you should consider how likely such attacks are to occur in your region. The criteria outlined in Briefs 8 and 29–31 can be helpful. Although such operations might needlessly raise local fears, there is no better way of ensuring that all emergency management agencies are prepared for an attack. Indeed, such exercises might be the only sure way to uncover errors and blind spots in multiagency and multijurisdictional operations. FEMA offers scenario training courses online, which provide virtual or simulated scenarios to which NIMS staff and other agencies respond.

Who will train them? Some of your officers might already have received emergency response training. These officers can be an important resource and with some additional train-the-trainer training, they might be able to conduct scenario-based training sessions for the rest of your officers. Train-the-trainer courses are available at the Emergency Management Institute (EMI), a division of FEMA. EMI also provides more intensive courses on most of these topics. Finally, make use of the Community Emergency Response Team (CERT) accessed at https://www.citizencorps.gov/cert. This site runs programs in every state and will tell you how to set up a local CERT program.

Who Pays? Online training courses are free: all you need is a computer with a good Internet connection. EMI courses are free, too; in addition, limited travel stipends are available. Depending on your location and circumstances, you might not have to pay for the training at all. The main cost will be in manpower because training will take up time that your officers would have spent performing routine policing tasks. To increase the efficiency of such operations, try combining this specialized training with instruction that can aid your officers in carrying out their routine departmental duties.

A selection of FEMA certification courses available online. See the latest list at http://training.fema.gov/IS/crslist.asp.

Introductory and General

- Emergency Manager: An Orientation to the Position
- Introduction to the Incident Command System for Law Enforcement
- Disaster Basics
- An Introduction to Hazardous Materials
- Animals in Disaster: Community Planning
- Developing and Managing Volunteers
- An Orientation to Community Disaster Exercises
- Introduction to Continuity of Operations
- Introduction to the Public Assistance Process
- A Special Events Contingency Planning for Public Safety Agencies.

Emergency and Disaster Management

- Introduction to Incident Command System (ICS)
- Introduction to the Incident Command System, I-100, for Public Works Personnel
- National Incident Management System (NIMS), An Introduction

Emergency and Disaster Management (cont.)

- National Incident Management System (NIMS) Public Information Systems
- NIMS Resource Management
- Introduction to Mitigation
- National Response Plan (NRP), An Introduction
- Single Resources and Initial Action Incidents
- State Disaster Management
- Principles of Emergency Management
- Emergency Planning
- Multi-Hazard Emergency Planning for Schools
- Introduction to Debris Operations
- Public Assistance Operations.

Special Skills

- Leadership and Influence
- Decision Making and Problem Solving
- Effective Communication
- Building Partnerships with Tribal Governments.

Specialty Areas

- Radiological Emergency Management
- Radiological Emergency Response
- Emergency Radiological Response Transportation Training
- Building for the Earthquakes of Tomorrow: Complying with Executive Order 12699
- Livestock in Disasters
- Coordinating Environmental and Historic Preservation Compliance
- Anticipating Hazardous Weather & Community Risk
- The EOC's (Emergency Operations Center) Role in Community Preparedness, Response and Recovery Activities
- Engineering Principles and Practices for Flood-Prone Residential Structures
- An Orientation to Hazardous Materials for Medical Personnel
- Introduction to Residential Coastal Construction .

Brief 42: Know About Disaster Scenes

Research shows that the victims of sudden disasters generally do not panic—and if they do, the panic is short-lived. Rather, victims generally try to help each other. The chaos and panic that is so often portrayed in the wake of a disaster is largely a creation of the media. Neither do widespread looting and lawlessness generally follow a disaster, despite media coverage to the contrary, such as the ubiquitous scenes of depravity depicted by the media in New Orleans in the wake of Hurricane Katrina. In fact, the great majority of individuals in New Orleans managed for themselves. And it can be argued that at least some of the initial chaos and pandemonium that followed in the hurricane's wake (such as the scene at the Louisiana Superdome) was caused by the incompetence of state and local officials, rather than by the citizenry.

Although definitive studies are not available, crime rates generally do not seem to increase during major disasters. In fact, there is good reason to expect a cooperative and helpful public at the scene of a disaster. In the aftermath of a disaster, however, there is sometimes a spike in certain types of fraud (housing construction fraud, loan sharking, insurance fraud).

Let's examine the process of managing a disaster scene, using the attacks of 9/11 as an example.

Getting information. The events of 9/11 were extremely complex: there were multiple events in multiple places, each unfolding according to its own timetable. As the 9/11 Commission concluded, it was the failure to (a) get accurate information; (b) interpret the data correctly; and (c) impart the information to those whose role it was to manage the disaster scenes that contributed to the chaotic first-response operations. There were several reasons for this.

- A number of competing first-responder organizations transmitted information and issued orders, including the North American Aerospace Defense Command (NORAD), the Federal Aviation Administration (FAA) and its subsidiaries, the federal counterterrorism task force, the U.S. Secret Service, various military departments, local police, fire departments and medical emergency personnel, and various federal actors, including the office of the vice president.
- There was no actual disaster team or plan in place to manage the attack—or if there was it was not followed—even though several of the first responders had recently undergone terrorist attack training, including a reality-based scenario wherein a commercial airplane crashed into a building.
- The complexity of the attack was overwhelming. One timeline of the 9/11 attack counted 425 separate communication events on that day—and this is surely an underestimate, considering the thousands of 911 calls that were likely made by the public in response to the attacks.

At the local level, the inability to communicate clearly and efficiently severely affected actions on the ground, as can be seen in the Box, which summarizes the communications that affected the 9/11 first responders in New York City for the first 17 minutes of the attack against the World Trade Center.

Interpreting information. We can see from the Box that it was extremely difficult for responders to comprehend the enormity of the 9/11 calamity. This might be the greatest challenge to a first-responder team: to assess the severity of the attack. Without some knowledge of the seriousness of the disaster, it will be difficult to deploy personnel and equipment effectively and to assess the danger involved for the first responders themselves. The response time of the New York City Police Department (NYPD) and the Fire Department of New York (FDNY) to the attack on the World Trade Center was extremely rapid—some Port Authority Police Department (PAPD) personnel were already on the scene when the incident occurred—but there is little use in getting to the scene of a disaster quickly if there is no means of properly assessing the nature and extent of the damage and the numbers of rescue personnel required. A triage protocol is needed so that the first-responder management team has some criteria to apply to the information it receives to gauge the seriousness of the event.

Both the NYPD and the FDNY, in fact, did have different levels of alarm call-up, but these proved too general and, particularly in the case of the FDNY, this resulted in the congregation of many personnel at the scene, without a sense of how to deploy them efficiently. Many simply walked up the towers as the occupants were walking down. The result was that many first responders, having achieved little, became exhausted from climbing and were trapped when the towers collapsed.

9/11 First-Responder Timeline for the World Trade Center Attack: The First 17 Minutes.

(Account compiled from the 9/11 Commission Report)

In hindsight, it is easy to pinpoint the failures. This detailed accounting of the first 17 minutes of the attack accentuates the failures in response that were identified by the 9/11 Commission and others. Overall, it took just 17 minutes for first responders to understand that this was a rescue mission, not a fire-fighting mission. Thirty-nine minutes later the South Tower collapsed and 29 minutes later the North Tower collapsed. Note that the New York City Office of Emergency Management (OEM) is omitted from the timeline: it played a limited role in directing the operations, even though coordinating the first-responder agencies was an explicit part of its mission. Initially, OEM did make calls to FEMA requesting rescue teams, and to the Greater Hospital Association. Fatefully, its headquarters was on the 23rd floor of World Trade Center Building 7.

Time	Event	The Fire Department of New York	New York City Police Department	Port Authority Police Department
8:46 a.m. to 9:03 a.m	Flight 11 crashed into North Tower. 911 swamped with calls; 911 operators advised occupants of North Tower to stay put and wait for rescue workers, i.e., standard operating procedure. Most occupants began evacuating regardless of instructions.	FDNY arrived at site by 8:52 a.m. Dispatchers have no information about location or magnitude of the impact zone. FDNY chiefs in lobby determined that all occupants should evacuate. This information not conveyed to 911 operators or FDNY dispatchers. Units ordered to climb tower to impact zone. FDNY advised that building not likely to collapse. Chiefs spoke with PAPD and OEM.	At 8:50 a.m., NYPD dispatched helicopters to survey damages. No FDNY officers in helicopters per standard operational procedures. NYPD determined rooftop rescue impossible. Information not conveyed to FDNY. NYPD officers on scene by 9:00 a.m.	PAPD advised FDNY that full evacuation orders had been issued through public address system, but that the system was not fully functional. PAPD officers on scene help in rescue operations on lower floors, but not all officers had World Trade Center command radios.
8:49 a.m. to 8:57 a.m.	South Tower deputy fire director informed occupants that building was safe and urged them to remain in their offices.	FDNY issued evacuation order for South Tower. Unable to keep track of various rescue operations and personnel deployment.	NYPD cleared major thoroughfares and worked with PAPD to evacuate World Trade Center plaza.	At 9:00 a.m., PAPD commanding officer ordered evacuation of all civilians from World Trade Center complex.
9:03 a.m.	Flight 175 hit South Tower. 911 operators overwhelmed with calls, advised occupants to stay put.	FDNY analog radios functioned poorly because WTC repeater system not switched on.	NYPD sent small rescue teams up towers. Combined NYPD and PAPD rescue operations.	PAPD officers responded individually; PAPD did not know how many officers were responding or where they were going.

Brief 43: Take Charge—Intelligently

When faced with a disaster or terrorist attack, the major task of local police is quite simply to maintain order. Police are more likely to be called on to manage the scene of a terrorist attack than are any other emergency response agencies simply because it is the traditional role of police to maintain order. It is important, however, to recognize that there are other first-responder agencies, such as the National Guard and various military units (e.g., the U.S. Army Corps of Engineers) whose roles also involve maintaining order; therefore, in developing a terrorism or disaster preparedness plan, it is crucial to delineate the role that each agency has in maintaining the social order. During the aftermath of Hurricane Katrina, the failure of police and military organizations to work together in maintaining order was widely seen as a serious breakdown in control; local police were largely blamed. Because local police are often first to be blamed, you should make sure that you are ready to do the following:

1. **Manage ingress to and egress from the attack site.** Once an attack occurs, one of your primary concerns should be keeping major thoroughfares clear so that emergency vehicles can get to and from the scene and so that victims can be evacuated from the disaster area. Even if the attack is completed quickly, its worst effects might be yet to come, as was the case in the collapse of the World Trade Center. The responsibility for assessing whether such dangers are likely usually rests with the fire department or municipal engineer.
2. **Stay with community policing when it is needed most.** When a community is hit by a major disaster, expect to find almost ideal conditions for community policing. One of the consistent (and heartening) revelations regarding major disasters is that the victims tend to band together for mutual aid and comfort. Your community policing officers can take the lead in coordinating these efforts and can help avoid vigilantism, such as occurred after Hurricane Andrew, when some localities posted signs announcing "If you loot we shoot."
3. **Watch out for fraud.** Only a few days after Hurricane Andrew, unscrupulous individuals came into the afflicted area from neighboring localities to offer their services as contractors and to sell items such as generators and ice at outrageous prices. Contractor fraud and price-gouging emerged as major crime problems.
4. **Manage information and give accurate instructions.** As a result of inadequate information and poor communications, faulty evacuation instructions were issued to the occupants of both towers of the World Trade Center during the 9/11 attacks. Fortunately, many of the occupants, especially those in the second tower, decided on their own to evacuate, which resulted in far fewer casualties than might have otherwise occurred. The key to overcoming such errors is to have efficient communications technology and a clear system for sharing information among the four types of first-responder agencies—police, fire, military, and medical—that are usually found at a disaster scene (see Brief 47).
5. **Issue warnings to victims and potential victims.** Predicting the path of a hurricane is possible with a known degree of error (approximately 150 miles); its arrival time can be predicted with even more accuracy. Predicting exactly when or where a terrorist attack will occur is extremely difficult—and probably impossible—although it is possible to identify particular targets that are more likely to be attacked. The daily threat level that was instituted after the 9/11 attacks, therefore, is almost useless. Because surprise is the hallmark of any terrorist attack, any vague warnings or instructions given prior to an actual attack are only likely to generate panic. If you have a protocol (developed in your planning stage) that you can follow in deciding which conditions require warnings and what levels of urgency should accompany these warnings, your decision-making will be much easier.

6. **Move equipment and supplies.** The terrorism disaster response plan will have identified the suppliers and routes that will be needed to transport equipment that might be needed to deal with an attack, as well as supplies to support the needs of first responders and victims. Police will need to keep those supply routes clear lest a lack of equipment and supplies aggravate the situation. Furthermore, if the response preparedness team has done its job properly, the supplies and equipment provided will be critical in mitigating the long-term damage to both victims and first responders.

7. **Be adaptable.** Although the disaster response plan is there to be followed, recognize that it is just a plan, and we all know that the best-laid plans can go astray. When there is a fire in a high-rise office building, for example, the standard procedure is for the occupants to remain at their desks and await instructions from authorities, whether fire, police, or their own security officers. Had all individuals in the World Trade Center done that, few would have survived. Consider: did it make sense for first responders to begin climbing the towers with the view to reaching the fire zone to assess the damage? This certainly was heroic, but in hindsight it also seems foolhardy—although climbing the stairs to aid those in need of help was not. Many of these decisions were made on the assumption that the towers would not or could not collapse. Experience with the World Trade Center scene suggests that it can be difficult to adapt to new situations during the course of a disaster unless there is someone who can step back and comprehend the entire scene. One can be adaptable only if there are several options to take. Information concerning the fire zone was critical; NYPD helicopter pilots were probably the only ones who could make such an assessment. Unfortunately, their primary mission appears to have been to assess the possibility of a rooftop rescue. They were not instructed to assess the severity of the fire and did not have fire department officers on board to help them do so.

"Because local police are often first to be blamed, you should make sure that you are ready..."

Brief 44: Mitigate Harm, but Don't Overreact

The process of mitigation begins during the preparedness and anticipation phases of counterterrorism. The more prepared a community is for an attack, the greater the chance of mitigating the harm done. The better the protection of attractive targets, for example, the better the chances of reducing the effects of the attack. If backup generators and communications equipment have been installed, secondary attack effects can be minimized. If first responders have been well-trained and an efficient emergency disaster plan is in place, the greater the chances of mitigating the harm done by an attack. On 9/11, better communication among the first-responder agencies would most likely have helped even more individuals to evacuate the Twin Towers. The untold story—perhaps the biggest mystery of the World Trade Center disaster—is why relatively so few people were killed, given the confusing and conflicting instructions they received during the first 17 minutes of the disaster. The initial estimates, based on the known occupancy of the towers, were around 12,000 dead. As we noted in the previous brief, managing the disaster scene intelligently will help mitigate harm, because it increases the chances of victims escaping from the disaster scene and makes the scene more accessible to emergency workers. It is, however, possible to overreact in managing a disaster scene and its aftermath.

Don't overreact. All airplane traffic was halted far too late in the 9/11 attack, probably when it was no longer necessary, thereby contributing to the crisis rather than mitigating it. There appears to have been no assessment of the effect this action would have on travelers or on the airline industry as a whole. Many of the security responses that occurred in the aftermath of the 9/11 attack had all the earmarks of panic. A police or fire chief might be strongly tempted to overreact to an incident because he or she is likely to be held accountable should something go wrong; however, overreaction can invoke panic and magnify the effects of a terrorist incident. When something bad happens, your best defense against criticism is to be able to show that you were as well-prepared as possible, that you approached the situation in a systematic and rational manner, and that you obtained and followed the best available expert advice. Some of the overreactions that have occurred in the aftermath of the 9/11 attack are reported in the Table.

"The better the protection of attractive targets... the better the chances of reducing the effects of the attack."

Overreacting?	
Incident	**Considerations**
Benamar Benatta, an Algerian national and a Moslem, was arrested on 9/11 and held in U.S. custody for more than 3 years "without [the government] actually taking any procedural action on the offense with which he [was] accused." He was held in maximum security prisons and eventually cleared of all charges against him brought by the FBI and the INS. He was eventually released in Canada in July 2006 where he is seeking political asylum..	The overemphasis on intelligence as a means for taking out a supposed terrorist network can lead to overly zealous responses. The Benatta case is one of many examples in which particular arms of the criminal justice system—law enforcement, prosecution, INS agents—target individuals based on inadequate or incomplete information on the assumption that further incriminating information (that is, giving up names of associates) can be squeezed out of them while they are in custody. In this case, scarce resources were wasted on an unproductive task.
On October 17, 2001, fire trucks, police, and an Orange County hazmat unit dispatched to South Junior High School based on a report of a suspicious white powder. The school was subsequently locked down.	Was this really necessary? Wouldn't one expect to find white powder at a school where chalk is used daily? But what if it were anthrax? Perhaps if local first responders had done an all-hazards survey and developed an emergency response plan based on their assessments of target vulnerability and the probability of a biological attack at a school, a more restrained response would have been implemented.
On August 12, 2005, the discovery of a suspicious oral cleaning device in a dentist's luggage resulted in a 3-hour lockdown at Kinston Regional Jetport in North Carolina.	Did airport security management have an incident response plan? Whose responsibility was it to order a lockdown? Were consultations required with other first responders before making a drastic decision that affected thousands of passengers throughout the United States? On what information was this decision based? Did the critical incident response plan include graded responses to different types of attacks or incidents?
On May 26, 2006, Washington, D.C., police briefly sealed off the Capitol Building and launched a floor-by-floor search of the largest office structure on Capitol Hill after an unidentified caller reported gunfire. More than 4 hours later, police reopened the building.	Did the emergency response team have a protocol for responding to bomb threats or reports of other kinds of violent incidents? Did the first responders assess the type of report and select the appropriate level of response? Was a lockdown necessary? If gunshots were heard, what were the officers searching for during the lockdown?
On November 16, 2001, the Hartsfield Atlanta International Airport was shut down for four hours, severely affecting travel throughout the United States. The cause? A young man ran the wrong way through a security checkpoint after having retrieved a forgotten camera bag.	What assumptions underlay the decision to shut down the airport? Were other contingencies considered—especially the effects on other travelers? Were other less onerous options available? Does better safe than sorry apply here? This was ultimately the safest choice, but it ignored the disruption to the lives of other passengers—which is just what terrorists want. Did the airport security critical incident team have a protocol for assessing the severity or criticality of breaches of security?

Brief 45: Know Who's in Charge: Conquer NIMS

Perhaps the most important component of the disaster plan laid out in Brief 40 is the Critical Incident Response Team (CIRT). Its first duty is to delineate the chain of command and the specific roles and functions of the various first-responder agencies. Voluminous amounts have been written about chains of command in disaster situations, much of which is encapsulated in the National Incident Management System (NIMS). This model, shown below, is widely used throughout the United States to impose a uniform and cooperative approach on first responders. The NIMS arose in the wake of a series of wildfires in the 1970s, which required cooperation from multiple agencies in multiple jurisdictions. There were several factors that made fighting these fires difficult:

- Unclear command structures
- Misunderstandings and poor communication
- No method for coordinating roles and responsibilities
- Lack of a clear leader
- Competition for, and scarcity of, resources.

The sensible way to overcome these difficulties is to establish a clearly structured organizational plan to ensure that everyone knows who is supposed to do what. This is what NIMS does. There are many variations of the plan; the most recent incarnation, HPD5, was developed by the DHS in an attempt to impose a degree of uniformity on various disaster preparedness agencies. You will need to decide (a) where you and your deputies should be located in the chart and (b) whether this plan will work in the face of a terrorist attack.

Who goes where? Where should you and your deputies be located in the NIMS chart? The temptation is to have someone everywhere, but that might stretch the limits of your available manpower. It might also blur the roles and responsibilities of yourself and your officers because each would be different depending on the type of attack and the other agencies involved. For example, it is quite possible that as a disaster unfolds, different agencies will play a greater or smaller role, so the chiefs of those agencies, therefore, would assume greater or lesser leadership responsibility.

Commander or leader? On 9/11, Mayor Rudolph Giuliani's emergency management staff remained in the background. As far as can be gleaned from the 9/11 report, Giuliani did not take control of the operation. He did, however, appear as the leader of the city's response to the attack on that day and the days that followed. And in fact, it has generally been acknowledged that Giuliani's public appearances and actions played a major role, both in helping people to comprehend the magnitude of the disaster and to cope with the loss and disturbances to their everyday lives caused by the attack. Mayor Giuliani was the clear leader of the city's response, but he was not the operational commander; perhaps there should have been one. It certainly can be argued that the mayor's emergency management staff should have played a larger role in coordinating the first responders, although it is possible that any increased efforts still would have been hampered by the incompatible communications technologies used by the different agencies. A single operational commander might have been able to mitigate some of the competition and lack of coordination between the fire and police departments, but given the circumstances on the ground, especially in the first 17 minutes, it is unlikely. The problems that hampered rescue activities on 9/11 probably could not have been overcome by a single commander. It is possible, however, that at least some of the problems that arose that day might have been discovered by preparedness training that should have been conducted long before any disaster occurred. What role would you want? Leader? Commander? Both? Before you answer, understand that Mayor Giuliani could not have assumed the leadership role he did without media support (Brief 46).

The command staff. The disaster plan should include a command staff appropriate to the disaster faced. For example, if there is no evidence of chemical or biological hazards, there would be no need to include individuals from agencies that deal with such hazards. In addition to municipal agencies, the entities and authorities represented on the command staff might include the following:

- Business associations
- Major local businesses
- School districts
- Hospitals associations
- Volunteer associations
- Hazmat specialists
- Private security personnel
- Transportation officials
- Major media groups
- Homeland security representatives
- Telecommunication and utility companies.

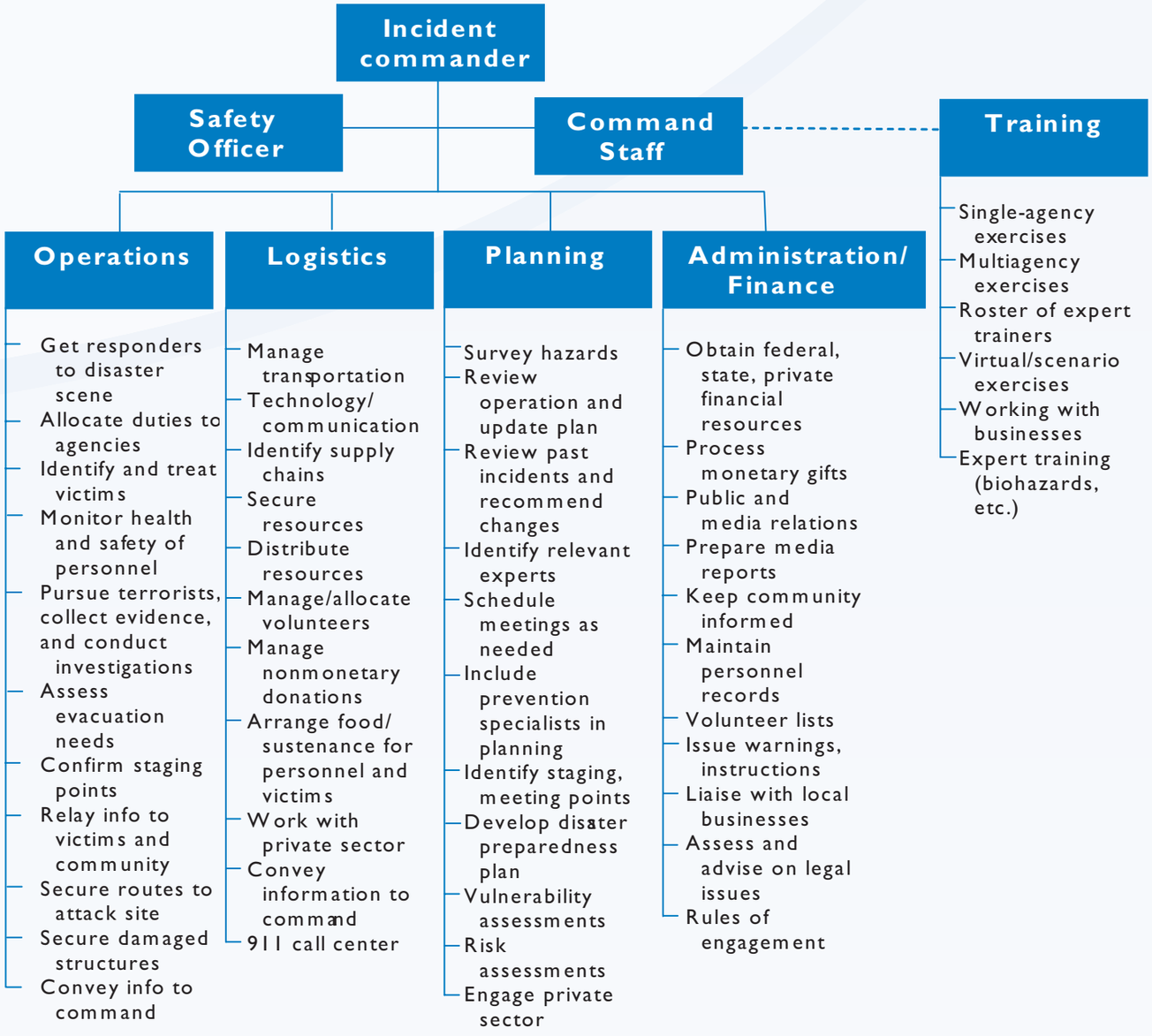
Not every entity mentioned above would necessarily be included in each operation, but they should be included in training exercises. Because a large command staff becomes unwieldy, especially if quick decisions are needed, many in the list above could be retained on call, should their special knowledge be needed (for example, locations of power grids, underground gas lines, etc.)

NIMS is a paper solution. NIMS is an organization chart and only that. It is useful in developing training exercises that teach individuals their roles and responsibilities. Although it

might sometimes be necessary to contravene the command structure in the face of a disaster, training should make clear that this can have serious consequences, particularly for communications among the many first-responder agencies. When an attack is in progress, quick decisions have to be made, often based on flimsy information. We saw in the first 17 minutes of the 9/11 attack how difficult it was for information to travel from one agency leader to another (see Brief 42), and even from one chief to another within the same department. There must, therefore, be a way for this management structure to change dynamically in response to how things change on the ground. This change cannot occur effectively without efficient communications systems and technologies—because the crucial part of any command structure is the collection and movement of information from the ground to the commander and back again. The NIMS chart shows nothing of this dynamic need for operational efficiency. What we need is an understanding of how and where information should flow, which unavoidably cuts across the lines of our organization chart. We address this issue in the next brief.

Read More: Jackson, Brian A. et al., *Protecting Emergency Responders, Vol. 3, Safety Management in Disaster and Terrorism Response*. RAND Corporation, 2004.

NIMS Chart for Police Executives



Brief 46: Know That Information Is Key

Although the National Incident Management System (NIMS) organization chart shown in the previous brief has no arrows to show the flow of information, in charts such as this it usually is assumed that the information flows from the top down. That is, orders originate from the commander and are conveyed by intermediaries to the front lines. So in a sense, the NIMS chart is more a picture of authority than a design for solving problems. In fact, the biggest problem in this organizational arrangement is the commander, because without the proper information he or she can give the wrong orders. Any efficient command system must have a way of collecting information, analyzing it, and transmitting it to those who make the decisions, in this case, the incident commander. To create such an efficient flow of information, you must integrate the First Responder Management System (FRMS) into the NIMS in the following manner:

- Identify all sources of information at the disaster scene
- Identify ways to control the flow of information
- Overcome barriers to the efficient movement of information.

Sources of information. All first responders at the disaster scene are potential sources of information, but it should not be assumed that the information they retrieve will provide an accurate or complete picture of events on the ground. For example, the first responders who rushed into the Twin Towers had little idea of what the actual disaster scene was like. Their actions were limited to sending people up to the fire zone to assess the disaster. The New York City Police Department (NYPD) helicopter pilots had more accurate information about the fire zone, although they did not have the expertise to interpret what they saw. The 911 dispatchers— whose job it was, in theory, to advise callers on what to do—lacked clear and consistent information about the disaster scene, gave conflicting advice, and unwittingly helped spread misinformation. There was no direct flow of information from the 911 call center to police or fire responders (see Diagram). The 911 system was devised to increase efficiency in response to calls for help; ironically, its very efficiency helped spread misinformation more quickly during the World Trade Center attack.

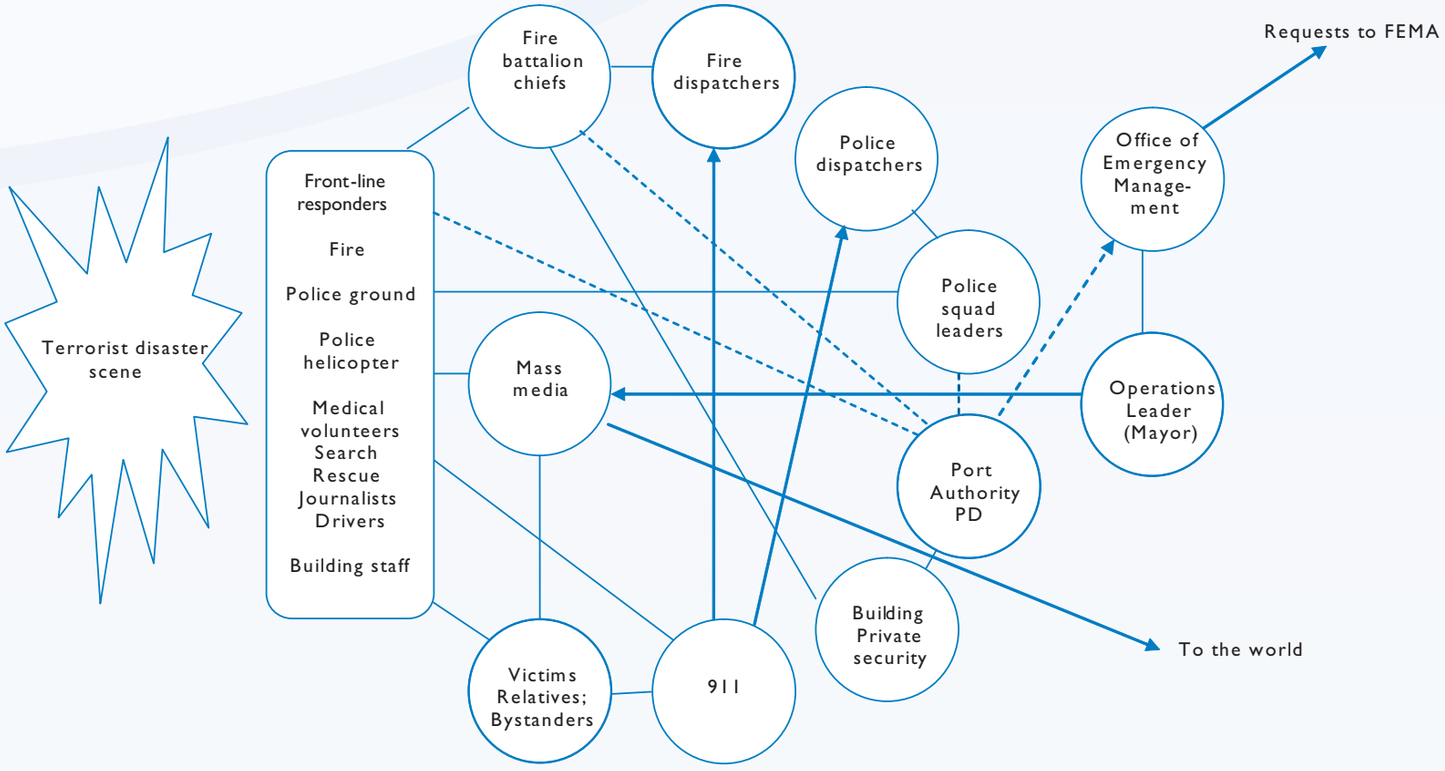
Offsite experts were also needed to help interpret events at the disaster scene. Could the towers collapse? What systems were in place to prevent the spread of the fire? Should the operation be viewed as a firefighting operation or a rescue operation? It is unknown how long it took to track down the needed experts during the 9/11 attack. The lesson is clear, however: information and expertise that will be needed in the event of a disaster must be located before the disaster occurs.

Control the flow of information. Advanced communications technologies such as cell phones, enhanced 911, various radio band technologies, and mass media radio and TV have increased our ability to communicate beyond our wildest dreams. One of the problems inherent in this communications bonanza is that there is no way of knowing whether the information is true or false. This is why major disaster-management centers maintain close links with the media: to make sure that the coverage is accurate, that it does not exaggerate the disaster, and that it does not add to the problems faced by first responders. It often is possible for disaster management teams to take advantage of the media's obvious expertise; for example, the major network news reports during Hurricane Katrina seem to have portrayed a more accurate picture of conditions in New Orleans than did the information passing between the Federal Emergency Management Agency (FEMA) and local government officials.

In the case of the World Trade Center attack, the media played an additional role by functioning as the conduit by which Mayor Giuliani reassured and encouraged the community. As the flowchart illustrates, the mayor's role in the flow of information was essentially linked to the mass media, and secondarily to the New York City Office of Emergency Management (OEM). As it happened, OEM had been established many months before 9/11 precisely to overcome the communications and logistical difficulties that had historically existed between the city's various emergency response agencies and was intended to coordinate the city's disaster-response operations. This was NIMS by the book. As the 9/11 report clearly shows, however, the NYPD and the FDNY continued to operate as independent agencies. (This is highlighted in the Chart.) Their radios did not talk to each other—and their users wanted it that way. Neither did either agency want to be subservient to the OEM, which played a very minor role in the operations on 9/11. Its only function appears to have been to request assistance from FEMA. So be cautioned: NIMS is a chart on a piece of paper. It will take effort to make sure that interoperability occurs in practice.

Note that the Chart is a simplified representation of information flow and communications. On 9/11 there was a multiplicity of information sources; we have confined the snapshot to the first 17 minutes of the World Trade Center attack. As can be seen from the Chart, the direct links between the 911 call center and victims and agency dispatchers were crucial. The 911 operators were perhaps the most important source of information because they could both receive information from victims at the scene and convey information to the victims and subsequent callers. They could also convey this information to the emergency command center—in this case OEM—which, if it were functioning properly, would have then collated the information from other sources and made sure that accurate information was transmitted down the chain of command (i.e., to the NYPD and the FDNY) and back to the 911 call center. The Chart also reveals where links were missing between agencies. These links failed because of barriers that made it difficult for information to move across them.

Disaster Scene Information Flow, First 17 Minutes, 9/11 WTC Operation



* All lines are bidirectional unless otherwise indicated
* Broken line indicates sporadic information flow because of poor communications technology.

Brief 47: Establish Interoperability

Overcome barriers. There are two major barriers to the efficient movement of information: (1) newfangled technology and (2) old fashioned groupthink.

Departments that need to work together in the event of a disaster sometimes choose competing and incompatible communications technologies. This was one of the many problems that faced the first responders in New York City on 9/11. The NYPD and FDNY radios were not compatible with each other. The FDNY radios were compatible with the communications equipment used by Twin Towers personnel, but only if the repeater within the towers was switched on—which it was not. The Port Authority Police Department (PAPD) radios were of such poor quality that PAPD officers were barely able to communicate with anyone at all. And although tower occupants were able to call 911 dispatchers to provide them with information from the scene, the information was not passed on to all the dispatchers; consequently, much of this vital on-scene observation was never transmitted to the first responders.

The obvious question is: why were incompatible radios purchased for the NYPD and the FDNY? The answer is old-fashioned groupthink. These two departments have a long tradition of competition and it seems likely that they had incompatible technologies precisely because they did not want to talk to each other. Thus, the problem of barriers to information flow cannot be solved by technology alone. (Lest it be thought that this could happen only in New York, during the London Underground bombing in July 2005, police radios did not work in the subways, so officers could not communicate with each other underground.) The National Incident Management System (NIMS) command staff should treat this issue as its top and perhaps most important challenge. The problem cannot be solved by directive. Long before the 9/11 attack on the World Trade Center, Mayor Giuliani had issued an order requiring interoperability between departments; in fact, that directive had been precipitated by the first attack on the World Trade Center, some 8 years earlier. Not only that, Giuliani had established an entire office (OEM) whose mission it was to make sure that interoperability was achieved. As a lesson learned, you would do well to ensure that all the departments and agencies that might respond to an attack in your jurisdiction have interoperable communications equipment.

Create bridges. Although there are a number of techniques that can be helpful in developing effective interagency relationships, perhaps the most important factor is the historical relationships between the departments in your community that make up your first-responder team.

1. Find your place. What is your role as police executive in fostering closer relationships with other agencies? Do you have the authority? Unless you are the designated NIMS commander, you might not have the power to enlist the cooperation of competing departments, including your own. In New York City, the mayor—who seemingly had the authority to do so—attempted to impose interoperability from the top down; clearly, this attempt failed.

> **"... barriers to information flow cannot be solved by technology alone."**

2. Do not depend entirely on training. Training and drills are extremely important, but they cannot fix everything. Although they can improve specific operational skills, they will do little to counteract years of interdepartmental competition. No amount of training will counteract the natural antagonisms that arise when two departments are competing for the same budget. Certainly New York City's OEM supervised many training exercises prior to 9/11; but these were not enough to countervail the longstanding enmity between the NYPD and the FDNY. It is clear that training alone is not enough to overcome historical or cultural divisions and competition between departments. To overcome this competition, departmental chiefs must change departmental attitudes. If change is to last, it cannot be imposed from above, although a canny mayor might devise incentives to help his chiefs pull it off.

3. Try mutual aid. Approximately half of individuals who work in law enforcement, fire, rescue, emergency medical, and related fields hold a second job in another similar emergency response agency. The most seriously affected are small fire departments that depend heavily on volunteer fire fighters. Many police departments also experience this "two-hat syndrome." In addition, many public safety and emergency personnel are also members of the National Guard; if a number of them are called up at one time, the pool of manpower available to respond to a disaster will be reduced drastically. Obviously, this is more of a concern in small towns and villages than it is in heavily populated cities such as Chicago or Los Angeles. It makes sense for small departments in adjacent municipalities to formalize arrangements whereby each agrees to help the other if a terrorist strike or natural disaster makes unusual demands on manpower or other departmental resources. Recognizing the unusual challenges that can face small or rural jurisdictions, the Department of Homeland Security encourages emergency responders in such locales to file joint applications for homeland security grants. Finally, conduct an inventory of equipment and resources in neighboring jurisdictions, so that the Critical Incident Response Team knows what supplies are on hand, where they are located, and whether any critical materials are unavailable or outdated.

4. Foster other partnerships. If a number of your officers are in the National Guard, it might be helpful to develop a mutual aid package with the Guard for training facilities, drills, and equipment. Public and private partnerships can also be important in developing an efficient response strategy because businesses are most often the primary or subsidiary targets of terrorist attacks. Cultivate relationships with the owners and occupants of possible targets and keep their contact details close at hand. In addition, private businesses have significant resources that can be of use in a disaster, such as communications equipment, food, bedding, and transportation. They might also have access to specialized equipment, such as demolition materials, construction equipment, and so forth.

Read More: Hawkins, Dan M. *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects*. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2006.
http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=238

Brief 48: Keep On Going After the Attack

Coping with volunteers. One of your problems in the aftermath of an attack will be dealing with the many offers of help that you will receive. Expect an influx of volunteers, but be careful because among the many legitimate offers there will undoubtedly be a few that are not quite pure. Obviously, if your jurisdiction is small, the fact that you know many of your constituents personally will help reduce this problem. In larger jurisdictions, however, you will need to work with public records agencies to develop a system of keeping track of the movement of persons in and out of the disaster area. This should be done before an attack, as part of your preparedness planning. In addition, it is likely that many volunteers will simply show up, not knowing where to go, who to help, or how to go about doing so. The easiest solution might be to channel untrained volunteers to organizations such as the Red Cross. In fact, you can use such organizations as part of your preparedness planning. The Red Cross, for example, has developed a series of courses, including some on the Internet, to train people in how to work as volunteers after a disaster (http://www.redcross.org/). Some church organizations have developed similar disaster training courses for volunteers. Your own logistics team should take such courses so that they are prepared to take best advantage of volunteers and their skills. In addition, make sure that other volunteer organizations in your community are aware of the opportunities for volunteer training.

The most important volunteers will be health care professionals. After the 9/11 attack in New York City, many doctors and nurses simply showed up at area hospitals offering their help; however, many of them could not be accommodated because their credentials could not be verified. This is a complex problem that involves a number of legal and technical issues. Fortunately, in 2002 Congress authorized the development of an Emergency System for the Advanced Registration of Volunteer Health Professionals. As part of your emergency response planning, make sure that local hospitals and clinics are apprised of this advanced registration procedure so that they will be able to accommodate volunteer health professionals if a disaster occurs. For more information, visit the Health Resources and Human Services Administration web site at http://www.hrsa.gov/esarvhp.

Assessing the fallout of the attack. After an attack it is crucial that you assess the extent of the damage and injury done to your community by collecting and analyzing relevant information. Without this information, a recovery plan cannot be implemented. The information you have assembled concerning hazards and vulnerability prior to the attack will be very useful at this stage. Were hazards or vulnerabilities exacerbated by the attack? What critical facilities were affected? You will need to have experts evaluate the attack site and its periphery to determine whether the attack introduced any new hazards and, if so, what long- and short-term health effects these hazards might have. For example, the enormous amount of dust that spewed forth during the World Trade Center attack included a wide variety of toxins, including lead, mercury, and asbestos and exposure to the dust has given rise to debilitating and chronic illnesses that can require extended treatment and leave individuals unable to work to support their families. The opposite Table gives a brief summary of the actual economic and personal effects of the attack on the World Trade Center.

Damage and Injury Resulting from the World Trade Center Attack.

Persons Killed	
Total	Approx. 2,750
Firefighters and paramedics	343
NYPD officers	23
PAPD officers	37
Personal loss	
People who lost a spouse or partner in the attacks	1,609
Children who lost a parent	3,051
Business losses	
WTC companies that lost employees	60
Economic loss to New York in month after attack	$105 bill
Jobs lost in New York owing to the attacks	146,100
Days the New York Stock Exchange was closed	6
Damage	
FDNY vehicles destroyed	98
Tons of debris removed from site	1,506,124
Estimated cost of cleanup	$600 mill
Help	
Units of blood donated to the New York Blood Center	36,000
Units of donated blood actually used	258
Amount donated to 9/11 charities	$1.4 bill
Money raised for NYPD and FDNY families	$500 mill
Total FEMA money spent on the emergency	$970 mill

Source: Adapted from "9/11 by the numbers," *New York Magazine*. http://www.newyorkmetro.com/news/articles/wtc/1year/numbers.htm

Taking stock of your response. The transition from mitigation at the disaster scene to the longer process of recovery requires perseverance and stamina. Not only will you have to deal with the effects of the disaster itself, but this transition phase is almost always accompanied by a painful assessment of the disaster and the performance of first-responder agencies. What went wrong? What went right? Who gets the blame? Who gets the credit? The answers to these questions will not only require an assessment of how your officers performed at the disaster scene, but also of the preparations that your department made in anticipation of a terrorist attack.

You will undoubtedly be held responsible for the performance of your department and your officers. If you have followed the steps outlined in this manual, you will have plenty of information on which to base a review because you will be able to demonstrate that you took the following 10 steps:

1. Systematically assessed the dangers of terrorism to your community.
2. Took all necessary steps to protect likely targets in your community.
3. Engaged experts to assist when you needed help.
4. Obtained the necessary training for your officers.
5. Worked closely with the combined emergency response team.
6. Participated fully in training exercises.
7. Shared resources with other agencies.
8. Ensured interoperability with other agencies and jurisdictions.
9. Prepared proposals for homeland security funding.
10. Protected the health and safety of your officers at the disaster scene.

The power of these 10 points will rest on the extent to which you have implemented the Terrorism Disaster Management Cycle. By building data collection into your regular policing activities—details of criminal events, calls for service, and recurring disorder problems; inventories of vulnerable targets, hazards, and at-risk populations; deployment and training of officers; procurement of equipment and supplies—you will have at your fingertips the information needed to demonstrate that your department did everything possible to prevent and mitigate the attack. Of course, there will be mistakes, particularly in the face of the chaos that occurs in the first moments of a disastrous attack. And in fact, a review should unearth those mistakes so that you can learn from them. If you can demonstrate that your department did everything possible, it will be easier for you to admit your mistakes and easier for others to forgive you for them.

Brief 49: Sustain the Recovery

It is said that time heals all. To the extent that we forget the terrible events of the past, this might be true. Rebuilding or regenerating the site of a disaster helps us recover from the trauma, but it also helps us forget. Many victims—families who lost loved ones and those who must live with their injuries—cannot forget because they must live with the results of the disaster every day of their lives. The significant change that occurs after the attack, or any disaster, is the transition from on-scene mitigation to sustainable long-term recovery. The timeline for this transition will vary with the nature of the event. The Table shows the recovery period for a 1-square-mile area devastated by a small cyclone. As can be seen, the transition from mitigation to recovery occurred between 4 and 5 days after the event. The timeline for transition will depend on the specific type of disaster. In the case of the World Trade Center attack, the timeline extended over days, months, and years: fires continued to burn at the site for 99 days after the attack; cleanup crews worked for many months to remove the debris. Much of this work continued among rubble and toxic dust. Although the 9/11 scene was smaller than the 1-square-mile affected by the cyclone disaster described below, there obviously was much more packed into the World Trade Center site.

NIMS and sustaining recovery. It is the task of the National Incident Management System (NIMS) command staff and its ancillary bodies to arrange assistance through requests to federal, state, and local government agencies. What community help is available? What financial assistance do families need? Of special interest will be the welfare of police who served as first responders, either as members of the department or as liaisons to other agencies. The long-term effects of an attack on your officers and their families might be one of the more difficult aspects to manage.

Depending on your role in the NIMS command organization, you might want to take a front seat in activities that are designed to sustain recovery. In particular, you will need to do the following:

1. After completing an internal review of your department's performance (see Brief 48), participate in reviews of other agencies and prepare an after-action report.
2. Identify the needs of your own and other agencies in the light of the disaster and its consequences. Pay particular attention to the health and welfare of your officers, the replenishment of supplies and equipment, and the identification of training and equipment that was lacking.
3. Compare mistakes in operations and devise ways to overcome them, including improved training.
4. Set up a plan to monitor the long-term health and welfare of your officers, those of other agencies, and other victims of the disaster.
5. Partner with other agencies to seek external financial aid for victims.
6. Using the partnerships you established as part of your disaster preparedness, engage the commercial sector in providing financial support to ensure the long-term sustainability of the recovery process.
7. Use your ties to businesses to facilitate the economic redevelopment of areas hit by the disaster.

Changing roles of police. A large attack will place immediate demands on any police department; coping with the permanent changes that follow the attack can be equally demanding. At the World Trade Center disaster, police were called on for search and rescue operations. During the mitigation phase, police directed traffic, managed roadblocks, and supervised increased security in tunnels and bridges. Still others recorded and classified body parts recovered from the site, a job that went on for months. The aftereffects of the attack were so substantial that they necessitated the permanent redeployment of many police. The traffic flow in downtown Manhattan has been redesigned to cope with cleanup, reconstruction, and sightseeing. Deployment of police to maintain surveillance of possible targets (bridges, tunnels, subways, train stations, etc.) has changed the way the New York Police Department operates, probably permanently. For the World Trade Center, the recovery phase continues and will continue until the new World Trade Center is completed.

Changing faces of crime. As noted earlier, immediately after a major disaster people bond together to help each other overcome the enormous difficulties they face. Depending on the nature of the disaster, new opportunities will arise for criminals such as contractor fraud, price gouging, insurance fraud, and public assistance fraud. One of the more serious problems that can arise in the wake of a disaster is the destruction of records, both personal and public. When this occurs, an important impediment to committing fraud and many other types of crime is removed.

Recovery Timeline
Source: Adapted from Neal, David M. *Transition from Response to Recovery: A Look at the Lancaster, Texas Tornado.* Quick Response Report #79. Denton, Texas: University of North Texas, 1995. http://www.colorado.edu/hazards/qr/qr79.html

Brief 50: Keep the Public Informed

A road accident involving deaths and serious injury will certainly find its way onto the local evening news, but police and emergency personnel usually have time to deal with the incident before the media arrive. Major disasters and terrorist attacks are very different: the media often are on site at the same time as the first responders. In the wakes of Hurricane Katrina and the 9/11 attack, the media played a significant role in disseminating information about the disaster scenes. Depending on your role within the National Incident Management System (NIMS) command structure, you might be responsible for dealing with the media and the public. Careful management and communication with the media and the public is essential, lest a media disaster occur on top of the terrorist disaster.

Before the attack

Help the media to tell your story. There is much to tell the public about your efforts to assess vulnerability and to develop partnerships that increase security. Obviously, you should be circumspect in releasing the exact details of the steps you have taken to secure the most likely targets. Although you do not want terrorists to know the specifics of the preventive actions you have taken, you should want them to know that you have taken steps to make their job harder, and that might be enough to deter them from attacking targets in your city. In addition, the more the public knows of the steps you have taken to protect them, the more you will be insulated from recriminations after an attack.

Include media representatives in the NIMS planning. Get the media on board as early as possible and allow them a role in the NIMS planning. By ensuring that you have some control over the information the media disseminate to the public, you will avoid misconceptions and misunderstandings about what the NIMS is trying to accomplish. This can be done by embedding the media in the work of the NIMS.

Designate a public information officer. Designating a public information officer and making sure that the officer has a close, positive relationship with the media will allow you to avoid negative publicity. For example, on August 28, 1992, a scant 6 days after Hurricane Andrew, a *Miami Herald* story headlined "Swamped Metro officers only handling emergencies" told readers: "House burgled while you were away from home? Don't call Metro-Dade Police. They can't come." Although it is important for the media to convey information to the public—even the information that police and everyone else are overwhelmed by search and rescue operations—a positive relationship with the media will ensure that the information is conveyed in a fair and balanced way.

Set up a volunteer communications network. A volunteer communications network can effectively communicate information to local community organizations and volunteers. Amateur radio operators have played a significant part in coping with many disasters. Church groups and other volunteer organizations often have communication networks that can reach individuals of whom you are unaware, such as the sick, the aged, and the disabled. Beyond reassurance and support, these individuals will need to be identified and located in case of an evacuation.

Set up a police department web site. The mass media is a very powerful presence in a disaster, but the Internet is fast overtaking traditional media as a major information resource. If you have not already done so, create a web site and treat it as your department storefront. Establish a special section on terrorism and disaster preparedness and include advice on how to prepare for a disaster and what to do if one occurs. In addition, delineate the steps your department will take in the event of a disaster, up to and including the criteria that will be used in assessing the need for evacuation. As one of many excellent examples, check out the Sacramento Police Department web site, which offers downloads of the Sacramento Region Citizen Corps Council publication *Are You Prepared?* (available in seven languages). Another approach is to offer answers to frequently asked questions (FAQ) concerning what might happen in the event of a terrorist attack. The Table shows the FAQ from the City of Mountain View (California) Police Department web site. As a best practice, your department web site can serve a dual purpose: it can help in your response to terrorism and also serve as an aid to your department's regular policing work.

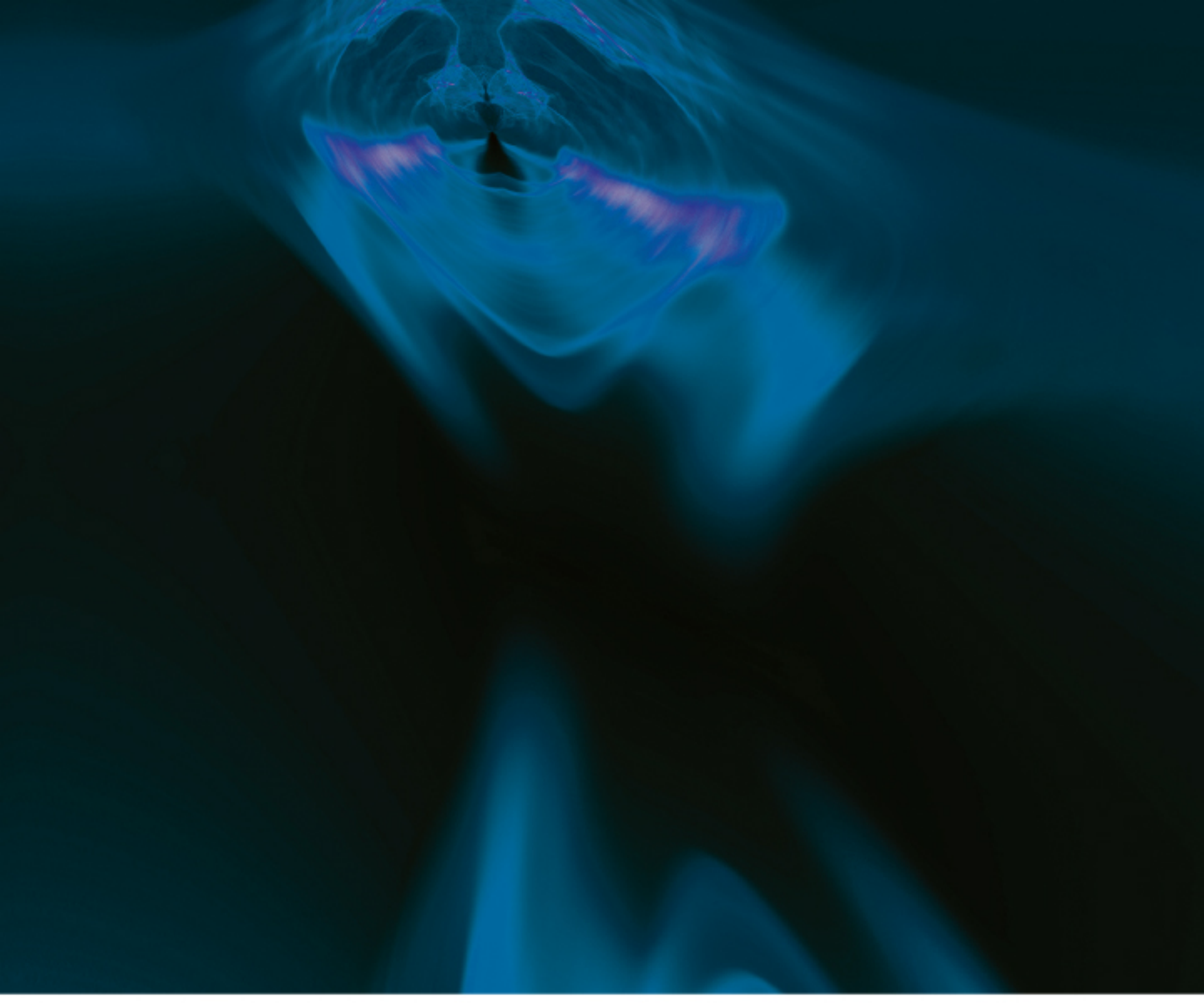
"The mass media is a very powerful presence in a disaster."

Terrorism FAQ Web Site of Mountain View, California, Police Department	
What can I expect from the police and fire departments in the event of a disaster?	What is anthrax?
How can I prepare for a disaster?	What should I do if I receive mail containing a white powdery substance?
How will I be notified of a disaster?	What is smallpox?
What should I do if a disaster occurs?	How contagious is smallpox and how is smallpox treated?
What should I do if I see suspicious behavior in my neighborhood?	Can my children or I be vaccinated against smallpox?
How should I avoid being in the middle of an act of terrorism?	Will sealing windows with duct tape and plastic sheeting help protect me against an incident of bioterrorism?
What can I do about the stress I'm feeling? And how do I explain this to my children?	Should I get a gas mask?
How likely is it that an act of terrorism will happen in Mountain View?	
How can I help my community if an attack occurs?	More Information/Helpful Links

During the attack, do the following.

1. Make sure that the media are on board as early as possible through your public information officer.
2. Ensure that information you convey to the public is consistent with what the media release.
3. Enlist media assistance in issuing warnings and evacuation orders.
4. Use the media to communicate to volunteers and to control requests for assistance, equipment, and donations.
5. Designate a media-savvy individual on the command staff to issue press releases and to give interviews to the media.
6. Make sure that your web site is updated constantly with changes in conditions and new instructions for residents.
7. Make sure that consistent and timely information is provided to 911 call operators so that they have a means to keep callers up to date. In addition, make sure that there is a process for recording and corroborating information that is received from callers so that it can be included in the information flow. Providing monitors that display the web site and local news stations can also help keep media sources up to date.

After the attack. The media can play an important role in the recovery phase of a terrorist disaster, especially if donations and volunteer assistance are needed. The recovery timeline in Brief 49 shows that only the Federal Emergency Management Agency remained active in the recovery phase of the disaster despite its late arrival on the scene. The local media provided only intermittent coverage, although donations requests were publicized daily. Of course, in a disaster of major proportions, such as 9/11, the recovery will take years, not months. There is probably little that police can do in this phase, except perhaps to feed stories to the media that keep the recovery fresh in the mind of the public. Nonetheless, you must continue to remain prepared in the event of another attack.



For More Information

U.S. Department of Justice
Office of Community Oriented Policing Services
1100 Vermont Avenue, N.W.
Washington, DC 20530

To obtain details about COPS programs, call the
COPS Office Response Center at 800.421.6770

Visit COPS Online at www.cops.usdoj.gov.

e080828168