U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

National Institute of Justice

Research in Brief

Jeremy Travis, Director

January 1999

Issues and Findings

Discussed in this Brief: An inventory of State and local law enforcement agencies from the 50 States and the District of Columbia that is being used to determine the technologies needed by these agencies to combat terrorism. The inventory, conducted through interviews and focus groups involving State and local law enforcement officers and others who coordinate agency responses to terrorist incidents, is the first phase in a two-phase project sponsored by the National Institute of Justice (NIJ) under the Anti-Terrorism and Effective Death Penalty Act of 1996.

Key issues: Terrorist acts and the ability of the United States both to prevent incidents and to deal with them effectively when they occur are issues of increasing concern in the country today. Recent incidents have shown that the United States is at risk from parties and individuals abroad and within its borders. Recognizing the need to identify, document, and respond to shortfalls in State and local capabilities to combat terrorism, Congress, through the Act, charged NIJ with determining State and local law enforcement technology needs for handling terrorist activities and with developing technological solutions to respond to those needs.

Key findings: Participants in the project provided researchers with a firsthand perspective of the

continued…

Inventory of State and Local Law Enforcement Technology Needs to Combat Terrorism

Recent acts of terrorism within the United States, such as the bombings of the World Trade Center in New York City and Centennial Olympic Park in Atlanta, have focused attention on the ability of law enforcement to manage these incidents and investigate individuals and groups suspected of planning or executing terrorist acts. Of particular concern is the gap between technologies available to and used by law enforcement—especially State and local agencies—and the advanced technologies used by persons and groups planning terrorist acts.

To improve the ability of law enforcement agencies to fight terrorism, Congress enacted the Anti-Terrorism and Effective Death Penalty Act of 1996. The Act charged the National Institute of Justice (NIJ) with the task of determining what technologies are needed by State and local law enforcement agencies to combat terrorism. To fulfill this task, NIJ sponsored a survey of State and local law enforcement officials and representatives of other groups that could be involved in preventing and managing terrorist attacks. The project was to be carried out in two phases: Phase I involved an inventory of the technology needs of State and local law enforcement, with respondents from all 50 States and the District of Columbia, while Phase II will involve analyses of those needs to determine whether existing or developing technology can fulfill them or whether new technologies are required. This Research in Brief presents findings from Phase I of the project, identifying the most frequently mentioned needs as well as issues related to fulfilling them.

Methodology

In 1997, to identify unmet technology needs, researchers conducted interviews and formed focus groups involving State and local law enforcement officers and a small number of other individuals (e.g., emergency management officials) who coordinate agency responses to terrorist incidents—108 interviews and group discussion sessions altogether. A total of 195 individuals representing 138 agencies from 50 States and the District of Columbia took part. They represented a wide variety of urban and rural jurisdictions and a broad segment of State and local law enforcement entities, including transit police, sheriffs' departments, city police, and State bureaus of investigation. (See exhibits 1 and 2.)

Issues and Findings

continued…

technology tools required by law enforcement agencies to combat terrorism. On the basis of participants' statements, researchers made the following observations:

- The counterterrorism needs of State and local law enforcement agencies across the country are similar, with minor regional variations.

- In terms of technologies available, law enforcement agencies often are not as well equipped as the terrorists they may face.

- A key issue for State and local law enforcement agencies is the affordability of new and existing technologies.

- Terrorist acts can expand the scope of routine police functions, creating a need for new technologies.

- Many of the capabilities used to combat terrorism also are needed to combat crime in general.

- State and local law enforcement agencies are aware that entities at all levels must cooperate to combat terrorism effectively, requiring improved information and communications technologies.

- Of particular concern to State and local law enforcement agencies is their ability to deal with weapons of mass destruction, especially those involving nuclear, biological, or chemical hazards.

- An issue of growing importance to law enforcement agencies is their ability to combat cyberterrorism.

Target audience: Federal, State, and local policymakers; law enforcement officers and administrators; emergency management officials; and technology development specialists.

Research staff, with the assistance of the four regional offices of NIJ's National Law Enforcement and Corrections Technology Center (NLECTC) system, selected potential participants. Care was taken to ensure representation of law enforcement disciplines specifically relevant to counterterrorism efforts, such as bomb disposal, SWAT (special weapons and tactics), intelligence, and mass transit security units. To the extent possible, selection of agencies and, in some instances, individuals was based on their particular expertise in combating terrorism—those that had taken part in large-scale exercises dealing with terrorism, had experienced a terrorist incident, or were assigned a leading role in combating terrorism. In addition, researchers interviewed experts on combating terrorism to gain their insights and advice on research design and reviewed relevant literature to derive additional background information on tactics, techniques, and existing technology available.

Exhibit 1: ***Profile of Represented Jurisdictions***

Jurisdiction	Number *n*=138
U.S. Park Police	**1**
Regional	**4**
State	**46**
Local	**87**
Cities with populations of more than 200,000	(33)
Counties with populations of more than 200,000	(18)
Smaller jurisdictions	(36)

In the sessions, interviewers asked participants to describe the technology capabilities needed to combat terrorism that their agencies lacked, in terms of 11 functions drawn from the interviews with terrorism experts and the literature review:

- Intelligence.

- Surveillance (a special subset of intelligence).

- Command, control, and communications (C^3).

- Site hardening and security (protecting buildings, facilities, and outdoor events from terrorist attacks and reducing site vulnerability to attack and damage).

- Detecting, disabling, and containing explosive devices.

- Defending against cyberterrorism—attacks using computers or computer networks (a special subset of site hardening and security).

- Defending against weapons of mass destruction—specifically, nuclear, biological, and chemical (NBC) devices.

- Apprehending and disarming terrorists.

- Forensics and investigations.

- Public information.

- Crowd and riot control.

A 12th function—training—was added because many participants mentioned its importance during the interviews and group discussions.

Most Frequently Cited Needs

Participants in the interviews and group discussions noted more than 100 unmet technology needs; the 15 most cited are listed in Exhibit 3. Needs are ordered by the number of times they were cited during the interviews and group discussions; the number of times they were cited by participants as among their five most important needs also is shown.[1]

By far, the most commonly expressed need was for ready access to current intelligence. Participants specifically noted the need for a national terrorism intelligence database housed on a secure information

Exhibit 2: **Profile of Participating Agencies**

Agency	Number *n*=138
Police departments	48
State police, highway patrols, departments of public safety, bureaus of investigation, etc.	37
Sheriffs' departments	23
County police departments	9
State emergency management agencies	7
Transit authorities, airport police, port authorities (including one regional entity)	5
Regional coalitions, law enforcement associations	3
City emergency management	1
District attorney	1
State attorney general	1
State department of communications	1
State department of justice	1
U.S. Park Police	1

infrastructure. Such a database must be accessible to all State and local law enforcement officials.

Improved means to detect and analyze explosive devices was also mentioned as a major need. The most important requirement expressed was the ability to verify the presence of an explosive; analyzing the nature of a device was of secondary importance. In addition, the ability to "look into" a device more accurately to determine what it is and how it was constructed was of major interest.

Of emerging concern was the threat posed by explosive devices possibly containing chemical or biological agents; improved means for detecting NBC hazards was frequently mentioned by participants. Requirements for equipment included portability (preferably handheld or wearable equipment), affordability, and responsiveness to a wide range of hazards. Such tools could allow additional time for responding to NBC hazards. In addition, participants wanted the ability to identify the nature of the hazard (e.g., the type of chemical agent) more precisely.

Also cited was the need for better NBC protective gear (including masks, gloves, and suits) for first responders; the key issue involved affordability. While participants wanted protective outerwear and masks offering improved wearability and dexterity, they remarked that they would settle for functionality equivalent to that of currently available gear, but only if it cost less. Because of the high cost of currently available gear, most agencies would not have enough suits to field more than a token force if a significant incident were to occur.

Command, control, and communications (C^3), another area frequently mentioned by participants, involves the ability to communicate information and data and to direct and coordinate the activities of individuals and organizations (particularly first responders) to achieve a common goal. The cost of improving communications security so that plans and intelligence are not compromised was considered a major shortfall. Participants noted that, even in fairly large agencies, only a small number of personnel—usually those involved in counterdrug operations—have access to secure communications.

A second C^3 need cited was for multiagency, multijurisdictional compatibility of communications equipment, enabling agencies to remain in contact at an incident scene. Incident commanders, line officers, and others from various agencies (e.g., the local SWAT team, Federal Bureau of Investigation, Drug Enforcement Administration, and State and county police) at an incident scene must be able to communicate with other departments without worrying about how to contact them, which would require an operator-friendly communications system.[2]

Other technology needs mentioned dealt with disarming and disabling explosives, defending against weapons of mass destruction, apprehending and disarming terrorists, crowd and riot control, and surveillance.

The need for improved bomb robots for sensing, disrupting, and removing explosive devices was cited frequently. Participants sought a wide range of improvements, such as greater dexterity in picking up and handling objects, the ability to carry more weight, two-way communications to speak to people at risk, the ability to climb stairs, built-in detectors and disrupters, and a lower cost.

Nonlethal capabilities for apprehending terrorists and for crowd and riot control also were cited by participants. Ideally, this capability would enable State and local law enforcement officers at a remote location to incapacitate individuals and groups covertly and almost instantaneously, for up to 20 minutes.

One of the surveillance needs involved the ability to "see through walls"—being able, from a remote location, to locate individuals in a room, to differentiate between terrorists and hostages, and to determine whether individuals are armed and where armed individuals are. While participants expressed a need to see through standard interior residential walls, they ideally wanted the ability to see through the heavier construction found in exterior residential walls and the exterior and interior walls of commercial buildings.

Another surveillance need was for improved long-range video monitoring. High-resolution, unobtrusive remote devices that could be left in place were of particular interest. Related to this capability, participants saw a need for unattended, unobtrusive aerial vehicles (UAVs) and stealthy manned aircraft and helicopters to carry such equipment.

In addition, participants noted a need for improved electronic listening devices. Such devices should be covert—ideally, undetectable—to avoid endangering State and local law enforcement officers and compromising an operation.

Also mentioned was the need for improved night vision devices. Among the key attributes desired were improved affordability, resistance to light flares, a broader field of vision, sharper images, telescopic capability, and better depth perception and color resolution.

Defense against cyberterrorism was another area addressed: Needs included tools for preventing intrusion, detecting and defending against it, and tracking attacks to their points of origin. Most agencies represented in the project had little expertise with cyberterrorism, and many participants believed the Federal Government and private sector would handle this problem, much as the Federal Government is expected to manage acts of terrorism involving nuclear weapons.

Exhibit 3: ***Most Frequently Cited Technology Needs***

Need	Function	Total Times Mentioned	Top Five*
National intergovernmental information system with current intelligence on terrorism	Intelligence	58	47
Improved means of detecting explosives	Detecting, disabling, and containing explosive devices	58	21
Improved and more readily available secure communications	Command, control, and communications	53	19
Improved means of detecting and categorizing nuclear, biological, and chemical threats	Defending against weapons of mass destruction	51	24
Improved interagency communications	Command, control, and communications	48	26
Improved robots for disarming and disabling explosive devices	Detecting, disabling, and containing explosive devices	47	9
Improved affordable protective gear	Defending against weapons of mass destruction	45	16
Improved nonlethal weapons	Apprehending terrorists; crowd and riot control	40	8
Improved "see-through-the-wall" capability	Surveillance	34	18
Improved long-range video monitoring	Surveillance	34	13
Improved detection and tracing mechanisms and countermeasures for cyberattacks	Defending against cyberterrorism	33	4
Improved electronic listening devices	Surveillance	32	15
Improved training to combat terrorism	Training	31	18
Improved containment vessels and vehicles for explosive devices	Detecting, disabling, and containing explosive devices; defending against weapons of mass destruction	31	6
Improved night vision devices	Surveillance	30	15

* Indicates the total number of times mentioned as being among an agency's top five needs.

In explosive device remediation, the need for improved containment vehicles and vessels was cited. Participants felt that these vessels also should be designed to prevent the release of any chemical or biological agents present. For investigative purposes, they also wanted devices capable of containing the fragments of an exploding device within a vessel and more affordable devices. (One bomb technician noted that his agency's containment vessels cost $100,000 each; as a result, too few were available, resulting in unacceptable response times.)

The need for more available and higher quality training for State and local law enforcement officers on how to combat terrorism was discussed. Among the technology training needs cited were the following:

- Computer-based general training (to reduce the need for, and thus the time and costs associated with, live training).
- Computer-based specialized training (e.g., for bomb technicians).
- Computer-based models to rehearse realistic hostage rescue scenarios.

Live training (e.g., combat marksmanship courses) often requires specialized sites far from an agency's office or other work location. Ideally, computer-based training, which can be conducted in an individual's office or in a nearby room, could replace much live training.

Conclusion

On the basis of the findings of the inventory, researchers made the following observations on the current status of what State and local law enforcement agencies need to investigate and manage terrorist acts and the individuals and groups who cause them.

Similarity across regions

The technology needs expressed were remarkably similar across the country, with minor regional differences. For instance, some agencies in mountainous areas have problems with communications line of sight, while agencies in jurisdictions with flat, open terrain experience difficulty undertaking covert surveillance operations.

Affordability

Affordability appears to be an overarching concern of State and local law enforcement agencies. Many participants stated that they lacked critical equipment and materials because their agencies cannot afford them; as a result State and local law enforcement often are not as well equipped as the terrorists they may face. For instance, State and local officials may have only 286- or 386-processor personal computers, while their adversaries are equipped with the latest Pentium®-based models.

It appears, at this point, that many of the needs participants mentioned could be met using existing technologies. For example, improved night vision devices, improved armored vehicles, and mobile fax machines all are available now; the question is whether agencies can afford them. Many participants suggested that technology-sharing be more frequently employed as one means of making equipment more affordable.

Critical deficiencies

State and local law enforcement are particularly concerned about their ability to handle nuclear, biological, and chemical (NBC) devices and other weapons of mass destruction. Again, affordability is a barrier; many participants mentioned the difficulty of defending expenditures for equipment that might rarely, if ever, be used. A large number observed that they must rely on the Federal Government to manage NBC threats. Another problem is that agencies often do not fully understand the nature of NBC threats and the training required to deal with them. For instance, federally sponsored initiatives to help State and local governments prepare to deal with a weapon of mass destruction have focused on emergency services and fire personnel and senior managers rather than law enforcement line officers.

Another concern is that State and local law enforcement generally lack the ability to combat cyberterrorism effectively. As the President's Commission on Critical Infrastructure Protection noted:

> Physical means to exploit physical vulnerabilities probably remain the most worrisome threat to our infrastructure today. But almost every group we met voiced concerns about cyber vulnerabilities and threats. They emphasized the importance of developing approaches to protecting our infrastructures against cyberthreats before they materialize and produce major system damage.[3]

This is a multidimensional issue involving a lack of appropriate equipment and software (often the result of funding constraints) and a lack of trained personnel. Also, this threat is relatively new to State and local law enforcement and has been viewed previously as mainly a private and commercial problem rather than a major law enforcement concern.

Unique aspects of combating terrorism

Terrorist acts are unique in that they often expand the scope of routine police functions, thereby creating a need for new technologies. A crime scene covering several city blocks or a traffic jam caused by a mass evacuation would pose unique technology-related challenges in forensics and traffic management, respectively.

While State and local law enforcement generally are able to manage more common criminal acts using their own resources, they realize that combating terrorism requires cooperation among Federal, State, and local law enforcement agencies as well as cooperation between law enforcement and other agencies, such as emergency management offices. This cooperation requires improved information and communications technologies, particularly those that facilitate access to and sharing of intelligence among agencies.

For Further Study

The State and local law enforcement and emergency response practitioners involved in this project identified many areas in which funding and research efforts can be focused. Phase II of the project will address how the capability needs mentioned by participants can be met by either existing technologies or technologies yet to be developed.

This Research in Brief is derived from a full report written by Hollis Stambaugh, Chris Tillery, and Philip Schaenman. Hollis Stambaugh is Director, Investigation and Public Protection Programs, TriData Corporation; Chris Tillery is Director, Counterterrorism/Force Protection, System Planning Corporation; and Philip Schaenman is President of TriData Corporation.

This study was sponsored by the Joint [Justice-Defense] Program Steering Group, for NIJ, under contract number MDA 972–93–C–0016 between System Planning Corporation (of which TriData Corporation is a wholly owned subsidiary) and the Defense Advanced Research Projects Agency.

This Research in Brief (NCJ 173384) is available online through the Justice Information Center Web site (http://www.ncjrs.org) or the NIJ Web site (http://www.ojp.usdoj.gov/nij). Copies of this document are available free from the National Criminal Justice Reference Service (NCJRS), at 800–851–3420, Box 6000, Rockville, MD 20849–6000. Copies of the full report are also available from NCJRS through interlibrary loan or for a small photocopying cost.

Notes

[1] The fact that, in many cases, the technology to meet these needs already exists was not a consideration in compiling categories. All expressed needs for new technology were captured, but needs for additional existing equipment, such as more patrol cars, were not considered.

[2] While not specifically noted, key attributes of such a system would probably include secure multimedia communications (e.g., voice, data, video) enabling interagency datasharing among mobile units and fixed sites.

[3] *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*, Washington, D.C.: The President's Commission on Critical Infrastructure Protection, October 1997: 5.

Findings and conclusions of the research reported here are those of the authors and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

NCJ 173384

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Washington, DC 20531

Official Business
Penalty for Private Use $300