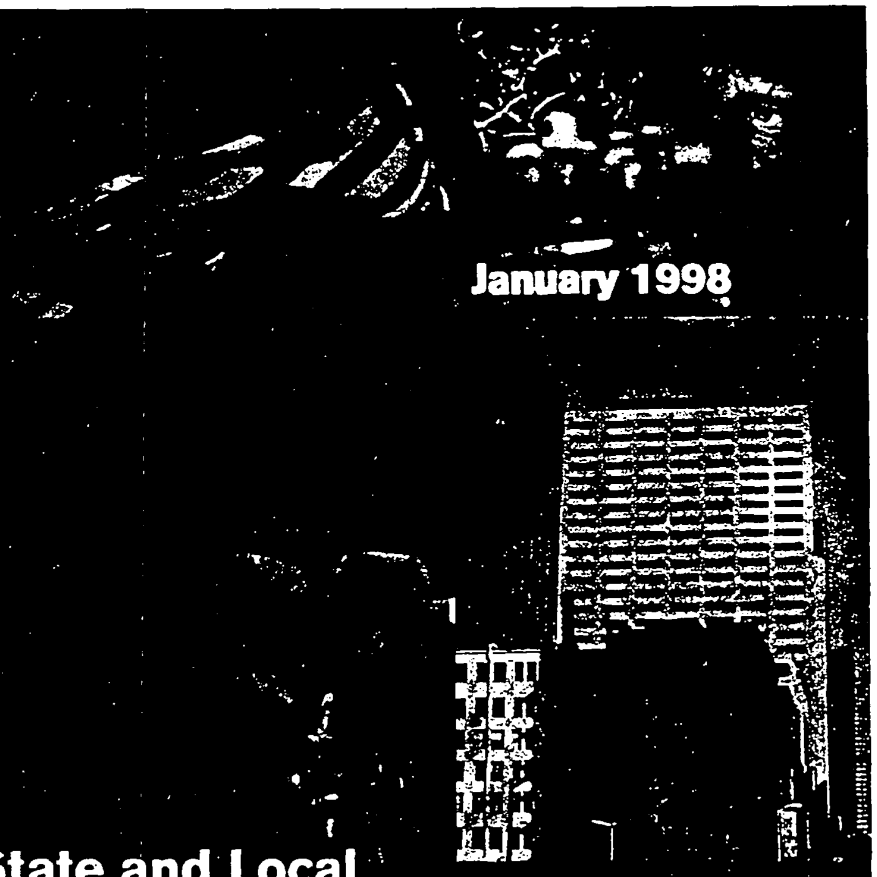


January 1998

Inventory of State and Local Law Enforcement Technology Needs to Combat

Prepared by
TriData Corporation
1000 Wilson Boulevard
Arlington, Virginia 22209-2211
for the
Director, National Institute of Justice
Office of Justice Programs
U.S. Department of Justice

CYBERTERRORISM NEEDS

State and Local Law Enforcement Technology Needs to Combat Terrorism

Volume I - Inventory of Needs

Sponsored by:

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

March 1998

Opinions or points of view expressed in this document are those of the authors and do not necessarily reflect the official position of the U.S. Department of Justice.

Contents

Figures and Tables

Figures

Tables

Preface

"Oklahoma City wounded the entire nation. We felt it up here. The United States is now seen as vulnerable to terrorism, and that scares me."

Police lieutenant, Midwestern city

"We're as prepared to fight terrorism today as [we] were prepared to fight World War II.

Police official, Midwestern city

"The government needs to continue to invest in research and development to keep up with the bad guys....they keep inventing new ways to get around our technology."

Special investigator, sheriff's office, large Western county

"Terrorists may be anti-social, but they're not stupid."

Chief of law enforcement, Midwestern State

"We are starved for intelligence."

Police lieutenant, Eastern State

"Intelligence is the bastard child when it comes to funding for technology."

Police official, large Mountain State city

"There's not enough communications equipment, not good enough equipment, inadequate training on its use, and different [law enforcement] languages that all contribute to a major problem in coordination at a major incident."

Training official, Mountain State emergency management agency

"Few law enforcement departments in [my state] know how to use the variety of technology available. [We need to] simplify the technology... or increase training."

Mountain State law enforcement official

"The bad guys end up having a lot more secured communications devices [than we do]."

Lieutenant, Western State bureau of investigation

"Cyberspace is the battleground of the future because the potential for disruption is so big, and growing daily.

Transit police official, large Northeastern city.

"We need to get crime analysis equipment out of the lab and into the field."

Detective, Western city

"We don't have many of these [technology] items because those who have to approve them don't go out and see what we need...

Police sergeant, Southeastern city

Executive Summary

One of the tasks assigned to the National Institute of Justice (NIJ) by the Anti-Terrorism and Effective Death Penalty Act of 1996 was to assess the technology needs of State and local law enforcement to combat terrorism. NIJ developed a two-phased approach to this task. Phase I, which is documented in this report (Volume I of the assessment), is a nationwide inventory of the technology needs of state and local law enforcement to combat terrorism. Phase II of this assessment, which is now in progress and will be published in Volume II, is the analysis of those needs to determine whether existing or developmental technology can meet them or whether new technology is required.

TriData Corporation of Arlington, Virginia, conducted this inventory under the sponsorship of NIJ's Office of Science and Technology. A subsidiary of System Planning Corporation, TriData is a consulting firm that provides assistance to state and local governments on issues pertaining to public safety. TriData initiated this inventory in March 1997 and delivered an interim report in June 1997.

METHODOLOGY

To identify unmet technology needs, the methodology employed in this inventory used interviews and focus groups involving law officers and a small set of other individuals (e.g., emergency management officials) who coordinate the activities of law enforcement agencies in response to terrorist incidents. There were 108 interview and group discussion sessions, the majority of which were completed the week of May 4, 1997.

NIJ's four regional National Law Enforcement and Corrections Technology Centers (NLECTC's) played a key role in this inventory. They hosted the interviews and focus groups and worked with TriData's project management staff to select participants.

The participating state and local agencies, listed at Appendix A, were notably cooperative, in many instances allowing their leading experts on terrorism to take part on short notice. The goal was to have at least 100 agencies participate. In fact, 138 agencies from all 50 states and the District of Colombia took part. They represented a wide variety of urban and rural jurisdictions and a broad segment of law enforcement entities (e.g., transit police, sheriff's departments, city police, state bureaus of investigation, etc.) Care was taken to ensure representation of those law enforcement disciplines with specific relevance to combating terrorism. These included bomb disposal, SWAT (Special Weapons and Tactics), intelligence, and mass transit security. As much as possible, selection of agencies and in some instances individuals for participation was based on their particular expertise in combating terrorism. Those selected had taken part in large-scale exercises dealing with terrorism, had experienced a terrorist incident, or were assigned a lead role in combating terrorism in their state. One hundred and ninety-five (195) individuals participated in the interview and group discussion sessions.

Experts on combating terrorism were interviewed to gain their insights and advice on research design. Relevant literature was reviewed to derive additional background information on tactics, techniques, and existing technology available to combat terrorism.

Eleven (11) experienced interviewers with relevant backgrounds conducted the interviews and focus group sessions. Interview and discussion protocols were developed and the interviewers were trained on their use to ensure consistency in information collection and documentation. Interviewers asked participants to describe the technology capabilities their agencies lack to combat terrorism in terms of eleven functions suggested by the literature review and the interviews with experts. They were:

1. Intelligence
2. Surveillance (a special subset of intelligence)
3. Command, control, and communications (C3)
4. Site hardening and security
5. Detection, disablement, and containment of explosive devices
6. Defense against cyberterrorism—attacks using or against computers or computer systems (a special subset of site hardening and security)
7. Defense against weapons of mass destruction [specifically nuclear, biological, and chemical (NBC) devices]
8. Apprehension (and neutralization) of terrorists
9. Forensics and investigation
10. Public information
11. Crowd and riot control

A twelfth function, training, was added after it was raised by the participants during the interviews and group discussions. While not involved in combating terrorism, per se, training prepares law officers to combat terrorism. Providing and maintaining training programs poses a significant challenge to law enforcement agencies in terms of time and cost.

FINDINGS

Key Findings and Observations

1. The technology needs of state and local law enforcement are remarkably similar across the nation, with minor regional variations.

2. State and local law enforcement agencies are often less well equipped than the potential terrorists they face.

3. From the perspective of state and local law enforcement, affordability is perhaps the key criterion for new technology. If a technology is not affordable, it might as well not be available.

4. Terrorist acts can expand the scope of what are otherwise routine police functions, thereby creating a need for new technology.

5. However, many if not most of the capabilities needed to combat terrorism are also needed to combat crime in general, with the possible exception of the capability to address the threat of NBC weapons.

6. The majority of the technology needs expressed by participants in this inventory correspond well with the technology development efforts undertaken by NIJ to address law enforcement needs in general. However, the priority assigned to developing specific capabilities may differ, based on the unique aspects of combating terrorism.

7. State and local law enforcement understand that to effectively combat terrorism requires cooperation among state, local and federal agencies, and that cooperation requires improved information and communications technologies —particularly technologies that facilitate access to and sharing of intelligence.

8. State and local law enforcement are particularly concerned about their ability to deal with weapons of mass destruction, especially NBC devices.

9. State and local law enforcement are also concerned about their ability to effectively combat cyberterrorism. This is a capability of growing importance, as documented in *The Report of the President's Commission on Critical Infrastructure Protection* released in October 1997.

Most Frequently Cited Needs

Participants in the interviews and group discussions noted over 100 unmet technology needs. Fifteen needs in particular were most often cited. They are listed in Table l, ordered by the total number of times that they were cited during the 108 individual interview and group discussion sessions. The number of times they were cited by participants as being among their five most important—top five—capability shortfalls in those interviews and group discussions is also shown. That the order of the highest ranking needs differs only slightly in these two ordering schemes suggests that the data is robust.

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. However, needs for more existing equipment, such as need for more patrol cars, were not considered. The assessment of those needs in terms of whether the technology exists to meet them is in progress.

By far the most commonly expressed need was that for ready access to current intelligence. Specifically, participants noted a need for a national terrorism intelligence database resident on a secure information infrastructure that is accessible by state and local law enforcement. It was cited in 58 of the interview and focus group sessions and selected as one of the top five state or local priorities 47 times.

Also mentioned in 58 sessions (but sharply lower in the number of top five designations) was the need for improved means for detecting explosive devices. The most important requirement expressed was to positively determine the presence of an explosive. Analyzing the nature of a device is of secondary importance. Of interest in this regard is the ability to "look into" a device in real time to tell more precisely what it is and how it is constructed. Participants noted that an emerging area of great concern is the threat posed by explosive devices containing chemical or biological agents. They expressed a need to know whether an explosive device contains both types of threats.

Command, control, and communication can be defined as the ability to communicate information and data and to direct and coordinate the activities of individuals and organizations to achieve a common goal. A need for an affordable way to improve communications security, to preclude compromising plans and intelligence, was cited as a capability shortfall in 53 sessions. Participants noted that even in fairly large agencies only a small number of personnel (usually, those involved in counterdrug operations) have secure means of communication. Participants defined this need in terms of secure (mobile) communications to and from first responders involved in combating terrorism.

The need for improved means for detecting nuclear, biological and chemical (NBC) hazards was mentioned in 51 sessions. The emphasis was on detection of chemical and biological agents. Participants expressed a requirement for equipment that was portable (handheld or wearable being preferred), low cost, and responsive to a wide range of hazards. They held that responders needed to be aware of the presence of an NBC hazard in sufficient time to respond to it. Ideally, they also wanted an ability to identify the nature of the hazard (e.g., the type of chemical agent).

A second critical command, control, and communications need (cited in 48 sessions) is for multiagency, multijurisdiction compatibility of communications – enabling different agencies to "talk to each other." Participants noted that this is especially important in large incidents involving multiple agencies, such as the bombing of the Murrah Federal Building.

TABLE 1. MOST FREQUENTLY CITED TECHNOLOGY NEEDS

Need	Function	Total*	Top Five**
National intergovernmental information system with current intelligence on terrorism	Intelligence	58	47
Improved means of explosive detection	Detection, Disablement, and Containment of Explosive Devices	58	21
Improved and/or more readily available, secure communications for the "beat cop"	Command, Control and Communications	53	19
Improved means to detect and categorize NBC threats	Defense Against Weapons of Mass Destruction	51	24
Improved inter agency communications	Command, Control and Communications	48	26
Improved robots for disarmament and disabling of explosive devices	Detection, Disablement, and Containment of Explosive Devices	47	9
Improved, affordable protective	Defense Against Weapons of Mass Destruction	45	16
Improved non-lethal weapons	Apprehension and Riot Control	40	8
Improved "see-through-the-wall" capability	Surveillance	34	18
Improved long-range video monitoring	Surveillance	34	13
Improved detection, forensics, and countermeasures for cyber attacks	Defense 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	Detection and Remediation of Explosive Devices/ Defense Against Weapons of Mass Destruction	31	6
Improved night vision devices	Surveillance	30	15

* Indicates total number of times mentioned as a need.

** Indicates total number of times mentioned as among an agencies top 5 needs.

They further noted that, ideally, incident commanders and others involved in incident management need to communicate with other departments without having to worry about how to get through to them – a communication system that is transparent to the operator. Participants observed that it is important for line officers of different agencies on the scene of an incident (e.g., local SWAT team, FBI, DEA, state and county police) to be able to talk to each other as well. [While not specifically noted, key attributes of such as system would probably include secure, multimedia (e.g., voice, data, video, etc.) communications enabling interagency data-sharing among mobile units and fixed sites.]

Of the next five most frequently mentioned shortfalls, two were cited in between 40 and 50 of the sessions. One of these dealt with explosive detection and remediation. The other dealt with defense against weapons of mass destruction. Three received between 30 and 40 mentions. One dealt with apprehension and neutralization of terrorists and with riot control. Two dealt with surveillance.

Participants noted a need for improved bomb robots for sensing, disrupting, and removing explosive devices. This need received 47 citations. Participants desired robots with a wide range of improved capabilities, including greater dexterity in picking up and handling objects; greater weight-carrying capability; a two-way communications capability (to speak to people at risk); an ability to climb stairs; built-in detectors and disrupters; and lower cost.

A need for better NBC protective gear for first responders received 45 citations. Participants expressed this need principally in terms of affordability. While they wanted protective overgarments and masks offering improved wearability and dexterity, they would settle for functionality equivalent to currently available gear, but at lower cost. Because of the cost, most agencies have too few suits to field more than a token force if there were a significant incident.

A need for a nonlethal capability for use in apprehension of terrorists and in riot control received 37 mentions. Ideally, this capability would enable law officers to incapacitate individuals, as well as groups of individuals, remotely, almost instantaneously, and covertly, and to keep them incapacitated for up to 20 minutes (selectively).

Both the two capability shortfalls that dealt with surveillance received 34 citations. The first was a need to improve the ability to "see through walls." Participants defined it as being able to tell where individuals are in a room, to differentiate between terrorists and any hostages, and, ideally, to determine whether individuals are armed and where those individuals are. Minimally, they expressed a need to "see through the wall" of typical interior residential walls. Ideally, they wanted the ability to remotely "see through" the heavier construction found in exterior residential walls, and both exterior and interior walls of commercial buildings.

The second surveillance shortfall was for improved long-range video monitoring. Higher resolution, "leave behind," remotely operated, unobtrusive devices were of particular interest. In conjunction with this capability shortfall, participants expressed a need for unattended (unobtrusive) air vehicles and/or "stealthy" manned aircraft.

The remaining five of the 15 most cited capability shortfalls all received between 30 and 33 mentions. Two dealt with surveillance. One dealt with defense against cyber terrorism. One dealt with training and another with explosive detection and remediation.

Of the two shortfalls dealing with surveillance, the first, a need for improved electronic listening devices, received 32 citations. Participants noted that a key attribute of such devices, is covertness (ideally, the device would be undetectable) to avoid endangering law enforcement officers and compromising an operation.

The second surveillance shortfall, a need for improved night vision devices, received 30 citations. Among the key attributes desired by the participants were improved affordability, flare resistance (so the wearer is not blinded), broader field of vision, sharper images, telescopic capability, better depth perception, and color resolution.

Defense against cyberterrorism was mentioned 33 times. Needs included ways to detect that cyberterrorism was occurring, ways to defend against it, and ways to track the attack to its point of origin. Most agencies represented had little expertise in this area. Further, many participants held the opinion that the federal government and private sector would take care of this problem, much as the federal government was expected to take care of acts of terrorism in which nuclear weapons were employed.

There were 31 citations of a need for more and better training for law officers on how to combat terrorism. Among the technology needs cited were: (a) computer-based generalized training (virtual/interactive) to reduce the need for, and so the time and cost associated with, live (i.e., real vice virtual) training, (b) computer-based specialized training (e.g., for bomb technicians), and (c) a computer-based capability to realistically rehearse hostage rescue scenarios. Live training often requires specialized sites at some distance from a law officer's office or other work location (e.g., combat marksmanship courses). Ideally, computer-based training, which can be conducted in the office or in a room near the office, could take the place of much of this live training.

Another capability shortfall in the area of explosive device remediation (also cited 31 times) was the need for improved containment vehicles and vessels for explosive devices. Participants felt that these vessels should also prevent release of any chemical and/or biological agents present. Another key attribute of these devices would be the ability to contain the fragments of an exploding device within the vessel for investigative purposes. Affordability was another desired attribute. [One bomb technician noted that his agency's spherical containment vessels cost $100,000 each; as a result, there were too few available, resulting in unacceptable response times.]

FURTHER WORK REQUIRED

This report will be shared with participating state and local law enforcement agencies and other knowledgeable bodies to solicit further details on needs and priorities. Concurrently, the assessment of these needs to determine if existing and developmental technology can meet them or if new technology is required will take place to help NIJ structure its research and development efforts.

Acknowledgments

The authors of this report and its National Institute of Justice (NIJ) sponsors greatly appreciate the contribution made to the inventory by the representatives of the 138 agencies that participated. These representatives, in turn, asked the authors to express their appreciation to the Congress for its support and to NIJ for sponsoring the assessment of their unmet technology needs to combat terrorism.

The authors also greatly appreciate the efforts of the NIJ National Law Enforcement and Corrections Technology Centers, who on short notice helped identify, assemble, and host an outstanding group of participants. Particular appreciation is expressed to the following individuals:

Robert DiCarlo, Northeastern Center , Rome, New York
Fred Demma, Northeastern Center, Rome, New York
Karen Duffala, Rocky Mountain Center, Denver, Colorado
Bill Nettles, Southeastern Center, Charleston, South Carolina
Don Bentzen, Southeastern Center, Charleston, South Carolina
Bill Terwillegar, Western Center, El Segundo, California

This effort was undertaken under the direction of Dr. Peter Nacci, the Deputy Chairman of the Joint (Department of Justice-Department of Defense) Program Steering Group (JPSG), established at the Defense Advanced Research Projects Agency.

The project team was lead by Philip Schaenman and Hollis Stambaugh of TriData Corporation. Interviews in the field were conducted by Ward Caddington, Drew Clark, Richard Crispen, Mac Dorsey, Erik Gaull, Roy Hodges, Bill Malamud and Marv Thordsen. Chris Tillery, Director of Counterterrorism/Force Protection at System Planning Corporation, played a key role in developing the methodology used in this inventory and in reviewing this report. Also contributing were the following experts: Dr. Neil Livingstone, Lawrence B. Sulc, Edward J. Spurlock, and Garry Briese.

Chapter I. Introduction

OVERVIEW

This report describes a national inventory of the unmet technology needs of state and local law enforcement to combat terrorism, conducted under the auspices of the National Institute of Justice (NIJ).

A necessary first step in determining these unmet technology needs is to define "terrorism." The working definition used at the onset of this inventory was that terrorism is a politically or socially motivated criminal act intended to demoralize or intimidate by harming individuals, damaging property, or attacking institutions, whether political, social, or economic. This definition corresponds well to that used by the FBI: "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives."[1]

During the interviews and group discussions involving state and local law enforcement practitioners, consequent to this inventory, many non-federal law enforcement agencies applied a broader interpretation, thereby increasing the number of criminal acts that they consider to be terrorism.

Differences in the definition of terrorism are important because they delimit the extent of terrorist activity and so the magnitude, and the nature of the problem, and hence—indirectly—the technology needed to address it.[2] The federal law enforcement agencies may not define a youth gang randomly firing weapons at cars for "kicks" as a terrorist act, whereas many state and local law enforcement agencies would. While these agencies may not have had much experience in combating international terrorism or terrorism sponsored by domestic hate groups, they have had considerable experience in dealing with these more prevalent acts of terrorism.

In regard to the more traditional definition of terrorism, whether the impetus for a terrorist act originates domestically or outside the United States matters little when it comes to handling the perpetrators and the crime scene or dealing with its effects. The World Trade Center bombing in New York City was committed by international terrorists; the Murrah Federal Building bombing in Oklahoma City, by a domestic terrorist. In both cases local agencies were responsible for the immediate response to the incident. Their roles were and are different from those of federal agencies. Yet the majority of technology development efforts to combat terrorism have been focused on addressing federal needs.

Across the nation, more and more law enforcement agencies are devoting an ever greater share of resources to dealing with terrorism, perhaps most noticeably adding

[1] See the RAND Corporation's report, "Domestic Terrorism - A National Assessment of State and Local Preparedness," published in 1995 under the sponsorship of the National Institute of Justice, p.3

[2] Ibid.

antiterrorism or counterterrorism units. Congress has also responded to this concern. For example, it appropriated $100 million in the Defense Against Weapons of Mass Destruction Act of 1996 (Nunn-Lugar) to combat the threat posed by those weapons. These additional resources—and more—are seriously needed because the impact and severity of terrorist incidents is increasing.

Perhaps the most troubling trend in terrorism in recent years is the increased use of weapons of mass destruction. A noted expert on international terrorism, Dr. Neil Livingstone (an advisor to this project), stated in his most recent book, *Protect Yourself in An Uncertain World* "...acts of terrorism today are more serious and more deadly than in the past."[3] At a U.S. Public Health Services seminar on terrorism in 1995 Ambassador Philip C. Wilcox, Jr., Coordinator for Counterterrorism, Department of State, warned, "...(weapons) of mass destruction can be unleashed on society killing, hundreds of thousands of people."[4] At the same seminar, John P. O'Neill, Chief of the Counterterrorism Section, Federal Bureau of Investigation Headquarters noted, "This is a theme that we see around the world in terrorism. Terrorists are no longer interested in small terrorist activities; they are much more interested in bringing down large numbers of casualties."[5]

Another threat of growing concern is cyberterrorism. Why should a terrorist incur the risks associated with employing a truck bomb if, as *The Report of the President's Commission on Critical Infrastructure Protection* released in October 1997 notes, "...the right command sent over a network to a power generating station's control computer could be just as devastating as a backpack full of explosives."[6]

Obviously, a well-financed group of international terrorists, particularly those with state sponsorship, have access to a wider variety of means to demoralize or intimidate than has the individual domestic terrorist. However, as the bombing of the Murrah Federal Building clearly demonstrated, the ability of individual terrorists or small groups of terrorists to inflict harm is significant.

BACKGROUND

Recognizing the urgency in documenting and responding to unmet state and local needs for better tools to combat terrorism, Congress appropriated $10 million in the Antiterrorism and Effective Death Penalty Act of 1996 (Section 821) for this purpose. Sharing the Congress' concern, President Clinton made available "emergency deficiency act funds" in November 1996 to speed the process. The agency charged with developing these tools is NIJ.

[3] Neil Livingstone, *Protect Yourself in An Uncertain World, (City:* MasterMedia Limited, 1996),xi.

[4]" U. S. Public Health Service, *Proceedings of the Seminar on Responding to the Consequences of Chemical and Biological Terrorism*, (Washington, D.C.: GPO, 1995)

[5] Ibid.

[6] *The Report of the President's Commission on Critical Infrastructure Protection*, October 1997, p. x

Congress charged NIJ to:

(Section 821 (1))	develop technologies that can be used to combat terrorism
(Section 821 (2))	develop standards to ensure the adequacy of products produced and compatibility with relevant national systems
(Section 821 (3))	identify and assess requirements for technologies to assist state and local law enforcement in the national program to combat terrorism.

NIJ developed a comprehensive approach to accomplishing this mandate. It is developing technological solutions for identified needs in the areas of: (1) infrastructure security, (2) hostage rescue, (3) explosive detection and remediation, and (4) information technology. It is also devising technical standards against which new technologies to combat terrorism can be developed and assessed. This is being done, in part, by expanding the existing law enforcement standards and testing program to include technologies and equipment to deal with terrorism. Finally, NIJ is assessing the technology needs of state and local law enforcement to combat terrorism to guide future research and development efforts.

NIJ developed a two-phased approach to this last task: Phase I, which is documented in this report (Volume I of the assessment), is a nationwide inventory of the technology needs of state and local law enforcement to combat terrorism. Phase II, which is now in progress and will be published in Volume II of this assessment, is the analysis of those needs to determine whether existing or developmental technology can meet them or whether new technology is required.

This inventory was undertaken under the sponsorship of NIJ's Office of Science and Technology. It was conducted by TriData Corporation of Arlington, Virginia, under the auspices of the Joint (Department of Justice-Department of Defense) Program Steering Group (JPSG). The JPSG is established at the Defense Advanced Research Projects Agency. Dr. Peter Nacci, the Deputy Chairman of the JPSG, directed this inventory. A subsidiary of System Planning Corporation, TriData is a consulting firm that provides assistance to state and local governments on issues pertaining to public safety. It specializes in the areas of fire protection, emergency medical services, and emergency management. The inventory was begun in March 1997. An interim report was delivered to NIJ in June 1997.

GOALS AND OBJECTIVES

NIJ set three objectives to guide this inventory. These were:

1. Obtain first-hand information from state and local law enforcement practitioners as to their needs.
2. Present a snapshot of field vulnerabilities and requirements at this time.
3. Capture information in sufficient detail to be of use to help evaluate current NIJ technology initiatives for state and local law enforcement.

The goal of this inventory is to define technology needs in enough detail to determine whether existing technologies can meet these needs or whether the development of new, perhaps less expensi·/e technology is required. For example, if there is a need for law officers to "see through walls," what is it they have to "see"? Is it simply being able to tell that there are individuals on the other side of the wall, or is there a need to be able to tell how many individuals there are, where they are located, and which ones are armed? The answers to these questions will dictate the ensuing technological approaches.

This inventory addresses the full spectrum of the technologies needed to combat terrorism from those required to gather intelligence on a potential terrorist incident, to those required to respond to it. Of particular interest is technology associated with coordinating the actions of state and local law enforcement and federal agencies, since that coordination is crucial to effectively combating terrorism. Also of special interest are technologies associated with the ability to deal with weapons of mass destruction (because of the potential magnitude of the effects of such weapons) and explosive devices (because they are perhaps the most common terrorist tool).

ORGANIZATION OF THE REPORT

This report contains three additional chapters. Chapter II, Methodology, describes the approach used to collect information on the unmet technology needs of state and local law enforcement. Chapter III describes these needs. Chapter IV provides a number of observations and conclusions based on both the findings, the process, and some of the interactions with state and local law enforcement agencies during the course of this inventory.

Chapter II. Methodology

OVERVIEW

The approach employed in this inventory involved the use of interviews and focus groups comprised of law officers and a small set of other individuals (e.g., emergency management officials) who coordinate the activities of law enforcement agencies in response to terrorist incidents, and so have some insight into their needs in that regard. NIJ's first inventory objective dictated this approach as the main means of data collection. Input was solicited from 138 agencies, including at least one agency from each of the 50 states and the District of Columbia. The agencies selected were drawn from a broad segment of law enforcement entities (e.g., transit police, sheriff's departments, city police, state bureaus of investigation, etc.). This broad representation is necessary as the tasks that different agencies (and often different units within the same agency) must perform to effectively combat terrorism may differ widely.

NIJ's four regional National Law Enforcement and Corrections Technology Centers (NLECTCs Figure 1) were primarily responsible for identifying the participants in this inventory and inviting them to take part. Each of the centers included among its invitees:

- at least two major cities;
- at least one law enforcement agency from every state;
- several state law enforcement agencies;
- agencies from some smaller communities; and
- at least one expert in each of the disciplines of bomb and ordnance disposal, mass transit, and SWAT (Special Weapons and Tactics).

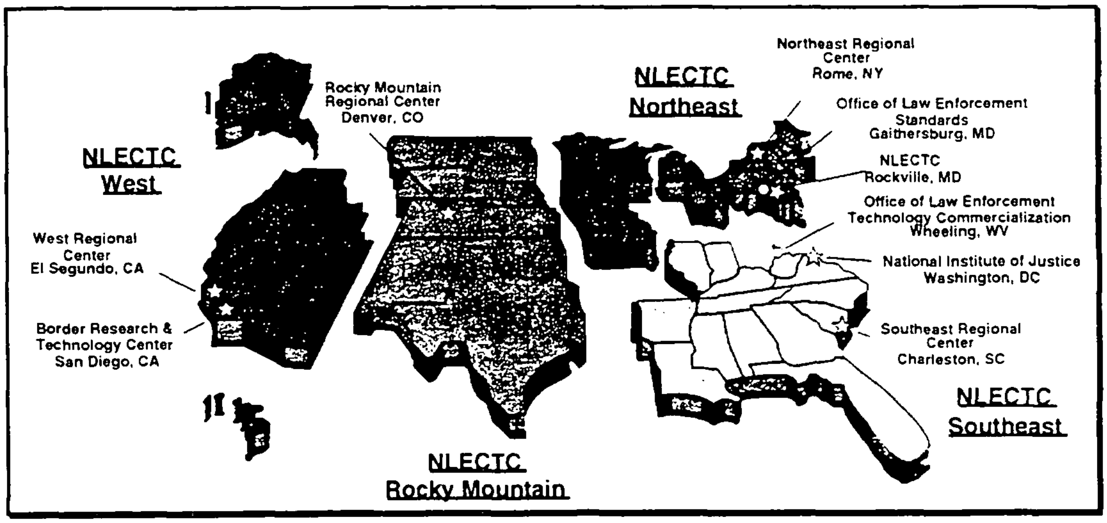

NLECTC West
West Regional Center El Segundo, CA
Border Research & Technology Center San Diego, CA
Rocky Mountain Regional Center Denver, CO
NLECTC Rocky Mountain
NLECTC Northeast
Northeast Regional Center Rome, NY
Office of Law Enforcement Standards Gaithersburg, MD
NLECTC Rockville, MD
Office of Law Enforcement Technology Commercialization Wheeling, WV
National Institute of Justice Washington, DC
Southeast Regional Center Charleston, SC
NLECTC Southeast

FIGURE 1. NIJ TECHNOLOGY CENTERS

The NLECTC's also hosted the individual interviews and focus group discussions at the following locations:

Atlanta, Georgia - Southeastern Region
Rome, New York– Northeastern Region
El Segundo, California – Western Region
Denver, Colorado – Rocky Mountain Region

Most interviews and group discussions were completed the week of May 4, 1997.

Representatives of nine law enforcement agencies in the Washington, D.C. metropolitan area participated in interviews and one group discussion May 1-2, 1997. These sessions provided a mechanism to validate the interview protocol, as well as providing data that is included in this report.

METHODOLOGICAL ISSUES

There were four significant methodological issues identified at the onset of this effort that had to be addressed to ensure its validity. The first three issues (the representativeness, comprehensiveness, and applicability of the findings) were addressed through the criteria applied in selecting participants for the interviews and group discussions. The fourth issue (ensuring that areas of specific concern were addressed without biasing the responses of the individual) was addressed through the interview and discussion procedures.

SELECTION CRITERIA

As mentioned previously, steps were taken to ensure that the findings resulting from this sample of agencies would accurately represent the needs of state and local law enforcement as a whole. As the nature of the terrorist threat may vary from region to region and community to community, a concerted effort was made to ensure nationwide representation across the spectrum of communities. Law enforcement agencies from large, medium, and small communities participated, as well as those representing counties, states, and regions. Representatives of as many of the different types of law enforcement organizations involved in combating terrorism as possible were included. In addition to dedicated anti- or counterterrorism units, particular attention was paid to gaining the participation of representatives from bomb squads, SWAT units, transit police, and intelligence units. These are among the types of organizations most involved in combating terrorist incidents.

The NLECTCs sought individuals with experience in combating terrorism or preparing to combat it, regardless of their rank. However, mid-level managers were preferred, because they tend to have both current, "hands on" experience (which higher level managers, as a rule, do not) and a broader perspective than the ordinary "beat cop." While the specific methods used by each center to select participants differed, each addressed these selection criteria. Participants were asked to present agency positions on needs, in as much as possible, rather than their individual positions.

Inevitably, this sampling approach somewhat overrepresents the larger jurisdictions. We believe this is appropriate because the major potential targets lie in larger jurisdictions, but also recognize that it is important that the inventory not fail to address the needs of smaller departments. Fully 90 percent of U.S. agencies are staffed with fewer than 24 sworn officers and half with fewer than 12. As a consequence, it is likely that the shortfalls identified by this effort are even greater among these agencies.

INTERVIEWERS

The interviews and group discussions were conducted by 11 trained interviewers selected for their interpersonal and interviewing skills, experience in public safety, and in some cases their expertise in combating terrorism. Among these were: a former Deputy Chief of the Washington, D.C., Metropolitan Police Department who is an expert on law enforcement's role in combating terrorism; a decorated military officer who is a graduate of the FBI's Special Air Crimes Course, and has commanded military units involved in combating terrorism as well as serving as the Chief of Security for U.N. Protection Forces in the former Yugoslavia; and a former FBI special agent who is an expert in special weapons and tactics and has advised the U.S. Departments of State and Energy on security and terrorism.

Interviewers participated in a day-long training session for this project. They were briefed on the desired outputs and interview protocols. They were given a common outline for the notes they were to take and background papers on technologies related to combating terrorism. The interviewers worked in pairs to direct the group discussions and individually for the one-on-one interviews.

STRUCTURING THE INTERVIEWS AND GROUP DISCUSSIONS

Literature Review

Work on the inventory began with a review of literature on terrorism. Journal articles, white papers, and speeches were collected from an Internet search. Several expert consultants to this project recommended books and papers on cyberterrorism, intelligence, counterterrorism equipment, weapons of mass destruction, and related topics. These were acquired and reviewed. Also, the Federal Bureau of Investigation, Department of Defense, Department of Health and Human Services, Federal Emergency Management Agency, and other organizations such as the National Governor's Association hosted seminars and conferences on terrorism during the past two years. Reports from published proceedings from these sessions were reviewed as well. Concurrent with the literature review, several experts in combating terrorism were interviewed to obtain their views on state and local technology requirements and on the history of the terrorist threats that law enforcement agencies have been confronting. This ancillary research helped structure the interviews and group discussions and provided the context within which to evaluate the data collected.

Types of Terrorist Scenarios

This ancillary research suggested seven types of terrorist incidents that should be considered because: (1) they represent the incidents in which law enforcement agencies are most likely to be involved, because they result from often-used terrorist tactics (e.g., planting bombs, taking hostages, etc.), and/or (2) their effects are so potentially devastating that they must be considered. The seven types of incidents are:

- bomb threats
- hostage rescue
- nuclear, biological, and chemical attacks
- attacks on mass transit and aircraft
- attacks on infrastructure
- cyber attacks against computer systems
- sniper attacks

Among the sample scenarios used by the interviewers to elicit discussion of these incidents were: hostages held in a building by an armed group; multiple explosive devices planted in a large building; a biological or chemical attack in a subway; a biological or chemical attack on a community; and a report of a nuclear device brought into a community.

Law Enforcement Functions in Combating Terrorism

During the structured portion of the interviews and group discussions, participants were asked to describe the technology capabilities they lack, in the context of these incidents and scenarios, in terms of the functions that they would have to perform to address them. The literature review and the interviews with experts suggested 11 functions. These were:

1. Intelligence
2. Surveillance (a special subset of intelligence)
3. Command, control, and communications (C3)
4. Site hardening and security
5. Detection, disablement, and containment of explosive devices
6. Defense against cyberterrorism (a special subset of site hardening and security)
7. Defense against weapons of mass destruction [specifically nuclear, biological, and chemical (NBC) weapons]
8. Apprehension (and neutralization) of terrorists
9. Forensics and investigation
10. Public information
11. Crowd and riot control

During the course of the interviews and group discussions, participants noted a twelfth function—training. While not involved in combating terrorism, per se, training prepares law officers to combat it. Finding the time and resources (money) to train personnel can be a significant challenge to law enforcement agencies.

Interview Procedures

Three different types of interview and discussion sessions were held. These were:

- Individual interviews, lasting approximately one and one-half hours;
- Group discussions generally involving three or four participants from one large city, and lasting about three hours; and
- Focus group discussions typically involving five or more agencies, from multiple jurisdictions, and lasting three hours.

Table 2 shows the distribution of participants, agencies, and type of session (interviews or focus groups) among the NLECTC regions and the Washington, D.C. metropolitan area. Of the 138 agencies participating in this inventory, all but three took part in the sessions held at the centers. Of the 195 participants, all but four participated in the sessions at the centers.

TABLE 2. PROFILE OF TYPE SESSION HELD BY NLECTC REGION

Number of *AGENCIES* by Type of Session and Region						
Type of Session	**Northeast**	**Southeast**	**Rocky Mountain**	**Western**	**D.C. Metro**	**Total**
Large City or County Interview	2	2	2	3	1	10
Individual Interview	14	16	16	21	8	75
Focus Group	14	17	17	5	0	53
TOTAL	30	35	35	29	9	**138**
Number of *PARTICIPANTS* by Type of Session and Region						
Large City or County Interview	9	5	6	12	3	35
Individual Interview	16	21	17	26	12	92
Focus Group	18	23	21	6	0	68
TOTAL	43	49	44	44	15	**195**
Number of *SESSIONS* by Type of Session and Region						
Large City or County Interview	2	2	2	2	1	9
Individual Interview	16	21	17	26	12	92
Focus Group	2	2	2	1	0	7
TOTAL	20	25	21	29	13	**108**

Individual interviews were handled by single interviewers. Large city and focus group discussions were handled by two interviewers, one serving as the moderator, the other as the recorder. There were a total of 108 sessions.

Interviews and discussions followed the same format. Free-form input was solicited at the beginning of each session, concerning participants' five most important technology priorities with regard to combating terrorism and their operative definitions of terrorism. This was done to obtain unbiased responses on these questions. Prompted responses on needs were then solicited in terms of the scenarios and functions. At the end of each session, participants were asked to further comment on their priority needs.

Confidentiality was assured. Interviewers began sessions by explaining that attribution of quotes or data would not be made to specific participants unless they gave their approval. Further, participants were told that any vulnerabilities of specific local or state institutions to terrorist attack would be protected. That information is treated as a generic finding in this report. For example, if the lack of a particular capability in a department might expose a specific courthouse to a truck-bomb attack, the report only indicates a general potential vulnerability of courthouses arising because that capability is not available to some departments.

Management of Field Work

Field work was closely managed. Interviewers called the main office at mid-day each day during the interviews and group discussions to review progress; discuss challenges; and provide early information on the tenor and results of the sessions. Management personnel were thus able to closely monitor operations and deal with issues as they arose. The project manager also personally directed the group discussions held in Rome, New York, to gain firsthand insight into the efficacy of the protocols.

PROFILE OF PARTICIPANTS

A total of 195 individuals representing 138 agencies participated in this effort. Table 3 profiles represented agencies by type of jurisdiction. Table 4 profiles them by type of agency. Table 5 profiles participants by discipline, while Table 6 profiles them by rank. Appendix A identifies participating agencies by state, while Appendix B identifies participants by type of unit and rank. One federal agency, the U.S. Park Police, was included in this effort because its responsibilities for protecting the Washington, D.C., metropolitan area's national monuments and parks, (and the visitors to them) provide it unique insights

TABLE 3. PROFILE OF REPRESENTED JURISDICTIONS

Jurisdiction	Number
State	**46**
Local	**87**
Cities over 200,000	(33)
Counties over 200,000	(18)
Smaller jurisdictions	(36)
Regional	**4**
U.S. Park Police	**1**

into the problem of combating terrorism. Additionally, its responsibilities are more akin to those of state and local law enforcement than to those of other federal law enforcement agencies. Arizona, California, Colorado, Georgia, Kentucky, Maryland, New York, Oklahoma, Pennsylvania, and Virginia were represented by four or more agencies; the other 40 states, by between one and three agencies. Forty-six (46) state, 87 local, and four regional agencies participated. There were 33 cities and 18 counties with populations over 200,000 represented, as well as 36 cities and counties with populations under 200,000.

TABLE 4. PROFILE OF PARTICIPATING AGENCIES

Agency	Number
Police Department	48
State Police/Highway Patrol/Department of Public Safety/Bureau of Investigation/etc.	37
Sheriff's Department	23
County Police Department	9
State Emergency Management Agency	7
Transit Authority/Airport Police/Port Authority (including one regional entity)	5
Regional Coalitions/Law Enforcement Associations	3
U.S. Park Police	1
State Attorney General	1
State Department of Justice	1
District Attorney	1
City Emergency Management	1
State Department of Communications	1

Types of agencies participating included sheriff's and police departments, state departments of public safety, port authorities, state emergency management offices, transit police, a state attorney general's office, state bureaus of investigation, an association of police chiefs, metropolitan police departments, and state highway patrols.

Table 4 clearly indicates that the majority of agencies participating represented state and local law enforcement. Local law enforcement, including police and sheriff's departments and county police, accounted for 58 percent of participating agencies, while state law enforcement agencies accounted for an additional 27 percent.

Table 5 shows that the largest discipline represented in this inventory was intelligence,

TABLE 5. PROFILE OF PARTICIPANTS BY DISCIPLINE

Discipline	Number
Law Enforcement	**182**
Intelligence	53
Other (including undifferentiated supervisors)	27
SWAT/Special Operations (undifferentiated)	27
Investigation (special investigator, detective, etc.)	27
Anti-Terrorism/Counterterrorism (undifferentiated)	19
Bomb Disposal	15
Emergency Operations/Management	8
Prosecution	2
Communications/Information Technology	2
Mass Transit Security (undifferentiated)	1
Hostage Negotiation	1
U.S. Park Police	**1**
Non Law Enforcement	**12**
Emergency Management	11
Communications	1

accounting for 29 percent of participants. This does not represent an over recruitment of this particular discipline for participation in this inventory. Rather it indicates that a good portion of the expertise on terrorism in state and local law enforcement resides in this discipline. Disciplines that specifically dealt with terrorism accounted for only 10 percent of the participants in this inventory. Disciplines overlap to a certain degree. For example, some intelligence specialists who participated were assigned to mass transit units, while some bomb experts were assigned to SWAT units. Only 6 percent of the participants were not involved in law enforcement.

Table 6 shows that the objective of gaining the participation of mid-level managers was achieved. Fully 42 percent of participants fell into that category.

TABLE 6. PROFILE OF PARTICIPANTS BY RANK

Rank	Number
Senior Law Enforcement Managers (Captains and above)	62
Mid-level Law Enforcement Managers	81
Detective/Trooper/Officer/ Deputy/Investigator, etc.	31
Other	21

Chapter III. Findings

OVERVIEW

This chapter details the findings of the interview and group discussion sessions as to the technology needs of state and local law enforcement to combat terrorism. It is preceded by a brief discussion of issues relating to the documentation of the needs. The findings themselves are organized in two sections: (1) the 15 most frequently cited needs; and (2) in-depth descriptions of all stated needs organized according to the 11 functional areas identified in Chapter II, and the training function identified as a need in interviews and discussions. The functional areas are:

1. Intelligence
2. Surveillance (a special subset of intelligence)
3. Command, control, and communications (C3)
4. Site hardening and security
5. Detection, disablement, and containment of explosive-devices
6. Defense against cyberterrorism (a special subset of site hardening and security)
7. Defense against weapons of mass destruction (e.g., massive explosive devices or nuclear, biological, or chemical weapons)
8. Apprehension (and neutralization) of terrorists
9. Forensics and investigation
10. Public information
11. Crowd and riot control
12. Training and other needs

Appendix C contains tables for each of these functional areas that synthesize the details on these needs. It also shows how many overall citations a particular need received, as well as the number of times it was cited as being among participants' top five priorities.
All needs, even if expressed by only one law enforcement official, are captured in this inventory, with one exception. That is the expressed need for more equipment already possessed by agencies, (e.g., more patrol cars.) Again, the assessment of those needs in terms of a requirement for new technology is in progress.

DOCUMENTING THE NEEDS

The main issue affecting the documentation of the needs was the lack of a common terminology among participants to describe them. At times different participants described the same need in very different ways. The interviewers used their best judgment as to where to fit the participants' comments into the functional categories developed for the project. Management staff reviewed their categorizations. This process resulted in a thorough review of the findings and a clear distinction between the highest and lowest priorities for technology.

Categorization was also made difficult by the fact that some needs fell into more than one functional category. For example, an improved night vision capability could be listed as a need under the surveillance or apprehension functions, or both. Redundancy was avoided whenever possible, by capturing the technology need in one category or the other. However, if the technology required different features according to the function it served, then it was mentioned in each of the applicable categories.

Rank ordering of needs was also difficult. Problems in doing so include the limited sample size and the possible bias from having some specialists and some generalists among the participants. Additionally, it was difficult for many of the participants to prioritize their needs. Specialists tended to focus on their areas of expertise, to the exclusion of other areas. Non-specialists often found it difficult to prioritize among a myriad of competing needs. Participants also faced the dilemma of whether to place a higher priority on technologies needed to deal with a more likely incident (e.g., explosive devices) or a potentially more damaging, but rarer incident (e.g., a nerve gas or biological agent release). As a result, the needs were categorized in two ways. The first was to tally the number of sessions (frequency) in which a need was cited and then to rank order them accordingly, from those receiving the most to those receiving the least number of mentions. The second method of categorization was based on the number of times participants designated the need as being among their agencies' five most important needs. Again the needs were ordered from those receiving the most to those receiving the least number of mentions. As there were 108 sessions (interviews and focus groups), the maximum number of citations for any need is 108.

THE TOP 15 NEEDS

The 15 most often cited needs are listed in Table 7. They are ranked by the total number of times that they were noted in one of the 108 individual interview and group discussion sessions. The number of times they were cited by participants as being among their five most important—top five—capability shortfalls in those interviews and group discussions is also shown. That the order of these needs differs only slightly in these two ranking schemes suggests that the data is robust. The top five needs are the same using either measure; a result that gives greater credibility to their high priority than if there had been significant disagreement between the two approaches. These needs include all needs receiving 30 or more citations, given potential errors of interpretation in placing needs into categories.

TABLE 7. MOST FREQUENTLY CITED TECHNOLOGY NEEDS TABLE

Need	Function	Total*	Top Five**
National intergovernmental information system with current intelligence on terrorism	Intelligence	58	47
Improved means of explosive detection	Detection, Disablement, and Containment of Explosive Devices	58	21
Improved and/or more readily available, secure communications for the "beat cop"	Command, Control, and Communications	53	19
Improved means to detect and categorize NBC threats	Defense Against Weapons of Mass Destruction	51	24
Improved interagency communications	Command, Control, and Communications	48	26
Improved robots for disarmament and disabling of explosive devices	Detection, Disablement, and Containment of Explosive Devices	47	9
Improved, affordable protective suits	Defense Against Weapons of Mass Destruction	45	16
Improved non-lethal weapons	Apprehension and Riot Control	40	8
Improved "see-through-the-wall" capability	Surveillance	34	18
Improved long-range video monitoring	Surveillance	34	13
Improved detection, forensics, and countermeasures for cyber attacks	Defense 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	Detection and Remediation of Explosive Devices/ Defense Against Weapons of Mass Destruction	31	6
Improved night vision devices	Surveillance	30	15

* Indicates total number of times mentioned as a need.

** Indicates total number of times mentioned as among an agencies top 5 needs.

Of these 15 most frequently cited needs, four pertain to surveillance functions, three relate directly to explosive device detection and defense, and two involve capabilities required to combat weapons of mass destruction, i.e., for nuclear, biological, and chemical detection and defense. The functions of intelligence; training; apprehension and riot control; command, control, and communications; training; and cyberterrorism detection and defense each captured one of the 15 highest priority needs. These 15 needs accounted for approximately two-thirds of the possible citations for the top five needs. There were more than 75 other needs expressed.

By far the most commonly expressed need, and also the most frequently mentioned among the top five priorities, is better sharing of intelligence information among local, state, and federal agencies. Improved technology for sharing intelligence was mentioned in 58 of the interview and focus group sessions, and selected as one of the top five state or local priorities in 47 sessions. This need received by far the most top five mentions of any technology need. The vision expressed by participants is for a national terrorism intelligence database, operated by the federal government, with user-friendly software to access it.

Mentioned as frequently as the need for technology to improve intelligence sharing (but sharply lower in top five designation), is the need for improved explosive detection capabilities. The most important capability is to positively determine whether an explosive is present; a secondary capability is to analyze it as exactly as possible. Also expressed was a need for improved means to "look into" a device and ascertain more precisely its contents; this capability would for example, allow an explosive disrupter to be aimed accurately, decreasing the potential for inadvertent detonation. Another desired capability is to determine if an explosive device contains NBC material, an emerging concern in the law enforcement community. (The explosive would be used as a means of disseminating the NBC material.) Portability and affordability are key concerns.

The third most frequently cited need, noted in over half the interview and focus group sessions, dealt with improving communications' security, especially for the "cop on the beat." Only a small number of field officers, even in large departments, have secure, portable radios. Those who do are usually involved in counter narcotics activities.

Fourth in priority is the need to improve the ability to detect NBC threats. The most important capability required is for timely alert of first responders to the presence of an NBC hazard. Better portable detectors are needed. Their most important attributes, beside portability, are low cost and the ability to detect the presence of a wide range of hazards. Ideally, these detectors would be able to identify the precise nature of the hazard as well. A belt-worn detector is most desirable. One mounted on a patrol car would be acceptable.

The fifth need is for multiagency, multijurisdictional communications' compatibility. Although the fifth most often cited need, this is second only to better means of sharing intelligence in the top five needs. Communications interoperability is especially important at a major incident site where multiple law enforcement and other agencies are operating. This is where communications systems are most taxed. Incident commanders and others involved in incident management need to communicate with other departments quickly and easily. It is also important that the line officers from different agencies on the scene to be able to communicate with each other.

The sixth most cited need is for improved means to disable explosive devices. Of particular interest are improved bomb handling robots. These robots would be more dexterous than current robots, and capable of sending more definitive diagnostics (e.g., sharper pictures and x-rays) to the bomb technicians operating them. Reducing the cost of these robots is a key concern.

The seventh most important need is for better means for first responders to protect themselves against NBC hazards. Improved but more affordable protective garments and masks, with protection at least equivalent to that provided by current equipment, are desired. Participants reported that because of cost, most agencies have too few suits to supply more than a token force in the event of an NBC incident.

Eighth is a need for improved non-lethal weapons for use in apprehension and riot control. Participants desired the ability to incapacitate terrorists without imposing an unacceptable risk to hostages or bystanders. They also want to have a range of non-lethal capabilities available to disperse or incapacitate crowds.

Three of the next four needs pertained to surveillance. One, cited in 34 of the sessions, is an improved ability to "see through a wall" and locate terrorists and any hostages. At a minimum, participants noted the need for a capability to see through typical interior residential walls. More desirable is a capability to see through the heavier construction found in exterior residential walls, and both exterior and interior walls of commercial buildings, from a distance. Ideally, this technology would differentiate between terrorists and hostages, as well as locate weapons.

At the same frequency of citation is a need for improved long-range video monitoring. Participants detailed a need for surveillance technology that has higher resolution and longer range than the technology their agencies currently have, and that is unobtrusive and can be remotely operated. A capability to conduct such monitoring from the air as well as the ground is desired.

Participants noted that while cyberterrorism is a growing concern, it is largely unknown territory for most state and local law enforcement agencies. The eleventh most frequently cited need is for improved means of defending against it. Participants noted the need for better capabilities to detect and investigate acts of cyberterrorism and for better countermeasures. Of particular concern was the vulnerability of their agencies' own computer systems.

The need for improved electronic listening devices of various types is the twelfth most frequently cited need. Capabilities desired included: (1) less detectable "body wires" that are smaller, have longer-life batteries, and are more reliable; (2) longer life "bugs"; and (3) a better long-range audio eavesdropping capability that works through windows. Unobtrusiveness is a key desired attribute of these devices, both to avoid endangering law officers using these devices and to avoid alerting terrorists.

Improved training technology is the thirteenth most frequently cited need. The technological capability most desired is virtual reality and interactive computer systems to support training of technical specialists and incident commanders, and to enable "war gaming" of alternate approaches for dealing with terrorist incidents.

Receiving the same number of citations (31) as the need for improved training technology is the need for improved containment vehicles and vessels for explosive devices that could also contain chemical and/or biological agents if present. Another key attribute of these devices would be the ability to contain fragments of an exploding device within the vessel for investigative purposes. Affordability was another desired attribute. (One bomb technician noted that his agency's spherical containment vessels cost $100,000. As a result, there were too few available, resulting sometimes in unacceptable response times.)

The last of the fifteen most frequently cited needs is for improved night vision devices. Besides being more affordable, it was desired that these devices have flare resistance (so the wearer is not blinded by a bright light), broader fields of vision, sharper images, a telescopic capability, better 3-D depth perception, and color images.

INTELLIGENCE NEEDS

Eight principal categories of needs were identified by participants in the area of intelligence. These are detailed in Table C-1. As noted, the most frequently cited need was for technology to assist in improving access to and sharing of intelligence on terrorism. This was a concern of a majority of the participants in this inventory, not simply of the representatives of the intelligence discipline. For example, SWAT commanders noted that they often need better information on the people they confront in hostage and barricade situations.

Participants identified several types of problems associated with accessing and sharing intelligence, that they thought technology could, at least in part, address. Among these were:

- A perceived lack of federal intelligence sharing with state and local officials, in part because of inadequate secure communication channels, and in part because of broader federal concerns about information security.
- A lack of adequate means for state and local governments to efficiently share intelligence data among themselves.
- A lack of agreement on "need-to-know" parameters pertaining to terrorist alerts and warnings.
- A lack of a way to quickly research detailed information about individuals and organizations regarding suspected or actual links to terrorist activities.
- Difficulty local governments have in organizing their own intelligence information.

Information Sharing Technology

Federally Operated Intergovernmental Terrorism Intelligence Data System – The most frequently expressed need for a specific technological capability was the development of a comprehensive terrorism database and associated information system that would collect and provide for sharing of data among all local, state, and federal agencies dealing with terrorism. The system must have user-friendliness and allow rapid access to a hierarchy of detailed information on terrorists and their organizations. It would be established and operated by the federal government.

To implement this system would require effective security, with multi-level access, encryption, and "firewalls" that restrict access to individuals according to their need-to-know. For example, different levels of information might be available to designated local intelligence specialists than to SWAT team leaders, but both would have access.

Participants expressed the need to be able to regulate which pieces of their agency's information would be releasable. The national intelligence system would require "pointers" or tags on information so that law enforcement agencies know where to locate additional information on individuals, methodologies, or other topics, and so that the agencies can regulate who releases the information. This system should have many of the functionalities of the Internet, such as classified chat rooms, bulletin boards on various terrorism topics, ability to send packets of data or information through E-mail, etc.

Participants want a system with "one-stop shopping" capability for intelligence information, including links to criminal databases and to other types of databases, to facilitate analytic processing. Especially noted was the need for this information during terrorist incidents involving hostages. Knowledge of a group's methods of operation, history, and demands would be critical to successfully resolving such an incident.

The system should handle all forms of data, including high-resolution images. Access to the system was desired from portable laptops as well as from desktop personal computers, with appropriate security screening.

Users should be able to submit profiles of their information interests—for example, data related to a particular geographic area, type of threat or organization—and then have the software deliver the relevant information.

Intelligence System for State and Local Agencies – Barring establishment of a federal, national system, participants expressed the need for state, if not regional, information sharing systems. Participants offered that while these systems would not provide access to the same level of information, they would be preferable to the current lack of adequate information exchange between any levels of government.[7] The attributes of these State and local systems would be much the same as those described for the national system, except that these systems would be smaller and might be more difficult to develop and govern.

Specialized Intelligence Databases – Barring the establishment of an essentially real-time, collaborative information system, at the national, regional, or state level, or even in the event such systems are created, participants again expressed the need for the federal government to develop databases describing terrorists, terrorist organizations, and terrorist methodologies and incidents. The data could be distributed on CD-ROMs or made otherwise available, with a proper security safeguard. Agencies would use this database off-line, on their own, rather than being connected to a secure interlinked intelligence system. They would not be able to provide inputs to the database in realtime. Nevertheless, this capability would go a long way toward answering questions about terrorists. It would be updated periodically.

[7] A number of State and local law enforcement officials went out of their way to praise individuals in their local FBI offices and other Federal agencies for cooperating in information sharing on terrorism. However, the overall consensus was that intelligence sharing among and between government levels is woefully inadequate.

Information Collection/Data Mining

Mining the Internet for Intelligence – Another major intelligence-related capability shortfall concerns the inability of the state and local law enforcement agencies to glean important terrorist-related material from the Internet. Law enforcement agencies want a specialized "search engine."

There are three major classes of information that law enforcement agencies would like to get from the present Internet. First is intelligence information that could be mined from open sources on the Internet. There is a wealth of information on terrorist incidents, groups, and often individuals, as well as information on technology related to terrorism. There are also ports into Federal data. Although much of the needed information can be collected by an individual skilled at using the net, the participating agencies want software packages or guides to do the search. This would save time and ensure a more complete retrieval of information.

A second, related, more subtle requirement is to be able to view what terrorists themselves are gleaning from the Internet. An example would be instructions for making explosive devices; knowing what is provided on the net would help law enforcement anticipate the most likely forms of explosive devices to expect. Many domestic and some international groups that potentially or already are involved in terrorism have their own Web pages. Some of the home page information is encrypted or in coded terminology, so law enforcement officials need de-encryption technology.

Third, law enforcement agencies need to be aware of the information circulating about themselves on the Internet. Seeing the information that is publicly available could give agencies important insights into needs for counterintelligence and for improving security. This is in fact a counter-intelligence function (see below).

Prepackaged Software to Establish a Law Enforcement Agency's Own Intelligence System – Many law enforcement agencies struggle with organizing their own intelligence data. Some noted that there are excellent models of intelligence databases at the local and regional level for drug enforcement. They would like to have a software package developed that could be used to translate paper files into a computerized intelligence system with many of the same characteristics described earlier for the national system.

Intelligence Information Analysis Software – Whether provided as an element of the national, state, or local intelligence information systems, or as a stand-alone package, several agencies noted the need for software to help analyze their terrorist-related data. The software should predict trends, develop profiles, and pull together in reasonable form the information culled from national systems and other sources. They would like assistance in threat analysis, especially in predicting the types of organizations and types of threats that they are most likely to face. It would be valuable for them to know what similar communities have identified as their threats.

Counterintelligence

Many agencies acknowledged the growing sophistication of the terrorist community in monitoring law enforcement activities and called for improving security of communications as one of the highest priorities. Although only one agency noted some concern about the inability to tell when terrorists are monitoring law enforcement activities, experts interviewed in this research project have written convincingly about this danger.[8]

Other Intelligence Needs

A number of agencies discussed another limitation to intelligence sharing that could be addressed by technology: legal restrictions on what information may be stored or shared with others. Information is restricted for a variety of reasons related to legal, ethical, security, and public safety concerns. Many participants also suggested that current restrictions be reviewed for balance between law enforcement and privacy.

A crucial need is for development by the federal government of a common set of information standards for law enforcement. The absence of such standards will make the establishment of national, regional, and state information systems difficult, if not impossible.

[8] A book by Lawrence B. Sulc, *Law Enforcement Counter Intelligence*, discusses the threat and considerations for dealing with it. He was one of the experts interviewed for this report.

SURVEILLANCE NEEDS

Surveillance needs were assigned to 14 categories, detailed in Table C-2. This functional area included various methods for observing suspects, especially in support of clandestine operations. Surveillance information feeds intelligence and apprehension operations. It encompasses a wide range of technologies – night vision, radar, cameras, infrared, listening devices, and other means.

See Through Walls

The participants mentioned that the ability to "see through walls" better was a high priority in this category (34 sessions mentioned it, with 18 ranking this capability as a top five need). Although there is clearly an ideal of literally seeing through walls, many of the interviewees were able to define requirements that are likely to be more attainable.

In every case the interviewees required that the see-through-the-walls hardware be portable and preferably able to be carried and set up by one individual. Especially for indoor use, the equipment must operate quietly and the set-up process must be quick and quiet. One SWAT team leader envisioned a backpack-mounted technology that might require a technician to operate it. In such a scenario the backpack would carry a flat-screen that would enable all of the members of an entry team to review the situation inside the room before conducting a dynamic entry.

The surveillance device must have the ability, at a minimum, to penetrate various residential interior wall materials including wood, siding, and sheet rock. Preferably, devices would also handle interior block and concrete, and brick or other exterior walls. One state agency saw a need for the device to effectively image a room through 18 inches of stone or reinforced concrete. A Southwestern officer pointed out that adobe walls can often be as thick as 24 inches.

There was considerable debate about the range needed for seeing through walls. The most frequently desired requirement was to observe from "across the street," 100-150 feet away, from behind a defensive perimeter. Clearly, the greater the range, the better.

Many interviewees wanted a device that could differentiate between terrorists, hostages, and undercover agents through interior walls. The device preferably should locate individuals (or body forms) to an accuracy of 1-2 feet. It should show in real time the movement of individuals (e.g., whether they leave the room).

Preferably, the technology should show the presence of weapons and differentiate between unarmed and armed occupants. At a minimum, it should be able to identify metal shapes that may be weapons.

Participants in two sessions specified that the surveillance device should be able to transmit images back to a command post.

Some interviewees see an important side use for see-through-the-wall technology, beyond locating terrorists and hostages. That added utility connects into the general area of explosives and weapons detection capabilities. There are often times when law enforcement agents want to see through a door or wall to check for booby traps or bombs designed to be triggered by their entry. Two interviewees expressed an interest in a "see through walls" device that could indicate whether explosives, chemical agents, or biological agents were present.

Several interviewees want much higher imaging quality than is currently available and in use. They also want to penetrate a wall with fiber optic cameras or other devices. Silent drills, flexible fiber cameras, or other similar devices are desired for stealthy penetration and viewing. Technology that could take advantage of electrical outlets, light fixtures, and other wall penetrations to provide access for miniaturized cameras (and also microphones) is desirable, according to the participants.

Audio Surveillance Tools

Audio surveillance can provide law enforcement with information about a suspect's intentions. The ability to hear a terrorist's threats towards hostages is an important component in the decision to assault. It is becoming progressively more difficult to place covert listening devices without increased officer risk and chance of discovery. A special operations captain stressed the importance of "knowing what is going on inside" while keeping his officers behind a secure perimeter. One rural officer said, "We can't get close. We can be picked off with a high powered rifle."

Distance Listening-Participants in 23 sessions identified a need for improved distance listening-the ability to monitor conversations within a structure from "across the street"-or further. Nine sessions identified this as a top five issue. Interviewees stressed that they need to listen from a distance, without a planted device. They also want to be able to listen through a bug or body wire (covert transmitters). In many of these sessions the participants described parabolic-style microphones operated from a distance or laser beams bounced off windows as their mental image of the technology to fit the need. These would be used instead of or to augment traditional wires and bugs. They are requesting long-range capability with good fidelity.

"Standoff" audio surveillance equipment should be easy to deploy, be operable by one person, and have connectors to allow for recording. It should also allow encrypted radio transmission of the recording. The technology should be covert, operable from at least several hundred feet away, and not place the operating officer in danger.

Covert Transmitters (bugs, wires)-In 14 sessions, participants raised the need for improvements in covert listening devices ("wires" or "bugs"). Requests include miniaturized, less detectable microphones that could fit in a pen, tie clip, or similar small personal item.

An example of the need for less detectable transmissions from "wires" was given in one focus group. A private investigator in one area makes a living revealing undercover agents and conducting surveillance for militia and other groups. A participant told of a situation where undercover officers were meeting with a target group they had infiltrated. The private investigator declared that he would "scan" the group to identify any undercover agents. Though the agents escaped, they were seconds away from being discovered because their body mikes would have triggered his detector.

Another example was that of a compromised undercover sting operation in which an undercover agent wearing a wire entered a store in a shopping mall to arrange for an exchange of material with a suspect. His backup positioned himself across the courtyard in a consumer electronics store. Moments later the backup officer was surprised to hear an echo of the undercover officer's wire through his ear piece. He quickly realized that he was hearing his partner's voice over a scanner located behind the counter of the electronics store. It was tuned to the range of frequencies used by the department for tactical and undercover operations. A later investigation found that an employee of the electronics store was serving as a lookout for the suspects.

There was near unanimity during focus group discussions that practically anyone who has one of the counter surveillance books now available can detect and jam standard bugs. Solutions like encryption of the transmission might hide the nature of the transmission, but if the target group is scanning the frequency they will still be aware they are under surveillance. One focus group, therefore, called for a small recording device that is less electronically detectable. The device might be equipped with an "officer needs help" transmitter that could be activated to "burst" transmit a help signal, or routinely burst transmit recordings to reduce "on-air" exposure time. Another interviewee cited a need for body wires to transmit to a range of 1/2 mile, so the monitors can stand-off further.

Interviewees in three sessions stressed the need for undercover listening devices with longer-life batteries. Requests range from a minimum of eight hours of battery life to upwards of 72 hours on larger devices. Battery failure on wires and bugs can place officers in jeopardy or compromise operations. Returning to replace batteries in bugs adds to the risk of discovery. Two participants requested that the devices include a battery power indicator.

Remote Visual Surveillance

Cameras, Remote Controlled and Leave Behind–Participants in 24 sessions identified a need for improved remote-controlled cameras that can be "left behind" for repeated surveillance. Several interviewees gave positive reviews of pole-mounted cameras and indicated that, except for the cost, they would have additional units in service. Many smaller agencies are aware that pole camera technology was available, but are uncertain of how to acquire it or if they can even afford it.

One interviewee reported a requirement for cameras that can be left in place at high-threat-level targets – around federal buildings, for example. The cameras should have high resolution and transmit a real-time image of the target area. The resolution of the cameras should be high enough to allow for facial recognition of the subjects captured on tape. Ideally the system would "snapshot" a face, digitize it, and compare it to a database of photographs of known or suspected terrorists. One police department investigator related his experience that as the cameras and optics get smaller, the clarity and usefulness of the image diminishes.

There were also requests for repeater technology that could allow for a greater distance between the surveillance camera and the receiving unit.[9] Two interviewees cited a need for non-line-of-sight (NLOS) transmission capabilities for remotely placed audio and video monitoring devices. This is a frequent urban area problem, but rural departments also identified a need for NLOS technology. Several suspect groups have placed their training facilities in remote, hard-to-reach canyons. Another rural officer identified the need for remote cameras with extremely long-range lenses for observing activities as much as a mile or two away.

One intelligence unit supervisor raised the issue of the suspect group having the capability to monitor transmission frequencies in an effort to discover surveillance cameras being operated remotely. He stressed the need for surveillance equipment that was small and self-contained and could be left in place for extended periods of time. The system would need a motion detector that would activate the recording system. The film would be periodically collected from the device. Another interviewee requested that such surveillance devices be equipped with a microwave transmission system or have the ability to "burst transmit" to minimize the chance of discovery.

A captain in charge of surveillance efforts for a state agency requested longer-life batteries for use in surveillance equipment. Batteries should operate for days, not hours. Once remote monitoring devices are in place it can compromise the operation to periodically return and replace spent batteries. A representative of a rural department in the Midwest expressed a need for surveillance devices that do not freeze in severe cold.

There were several requests that surveillance cameras that digitize images be more available and affordable. These cameras provide the ability to store the digitized images with other information in an intelligence database system (also discussed under Intelligence needs).

[9] The requesting agencies may not be familiar with the several repeaters available to meet that need.

Satellite Based Surveillance Systems–Participants in eight sessions suggested that satellite imagery be used to support and augment surveillance capabilities. They desire access to satellite imagery for the following purposes:

- Observing remote structures and training camps, where direct observation is difficult and dangerous.
- Hiding surveillance operations such that an approaching aircraft or helicopter could avoid early detection by the terrorists.
- Monitoring large areas of uninhabited land for changes in use. Rural departments indicated that there are often many square miles of nearly uninhabited land within their jurisdictions that are rarely if ever visited by law enforcement.

Unmanned Aerial Vehicles (Drones)–Those involved in five sessions identified a need for discrete aerial observation, which they believe could be met with an unmanned aerial vehicle (UAV) that is smaller, less observable, and quieter than aircraft. Interviewees want UAVs for aerial observation because of experience with larger manned aircraft and helicopters being detected. One rural agency interviewee indicated that planes other than high flying passenger jets in their jurisdiction were a rarity; helicopters, even more so. He needed to observe events at a suspected terrorist training facility where a group was practicing bomb detonation. Surveillance was difficult because people at the suspected encampment had an unobstructed view of incoming people and vehicles. When approached, suspects had time to hide their materials and avoid discovery. A UAV at a sufficient altitude would probably have been able to give him the information he needed for a warrant and further investigation.

One agency wants UAVs also to be equipped with infrared imaging systems to assist in nighttime tracking of suspects. Interviewees acknowledged that UAV observation equipment exists, but believe it is significantly more expensive than most law enforcement agencies can afford.

Night Vision

"Night vision" technology is an important law enforcement surveillance tool. It allows observation in extremely low light conditions. The need for improvements in night vision was raised in 30 of the 108 sessions, with 15 agencies listing the need among their top five.

Participants repeatedly mentioned cost when discussing night vision technology. Several agencies have night vision devices, but only for a few officers. Others are well aware of the benefits of the technology, but find it altogether beyond their budgets.

Several sessions raised a need for a more effective defense against the temporary blindness that occurs when night vision technology is exposed to bright lights–car headlights, for example. One department reported that their night vision equipment takes as long as 15 minutes to recover from bright-light exposure.

Nine agencies identified a need for night vision technologies with longer range capabilities (100-1000 yards).

Seven agencies identified a need to videotape the image captured in the field by night vision technology. They envision incorporating video output jacks on the night vision device.

There was a strongly voiced need for night vision cameras to operate effectively across a range of moderate, low, and nearly non-existent light. In surveillance situations, suspects often move through different light levels. Night vision technology should function effectively in light conditions ranging from cloudy, moonless nights to bright, full-moon nights where additional artificial light shines on the subjects.

A sergeant with a sheriff's department identified as one of his top three priorities the need for small, easy-to-operate cameras that have a zoom capability and are able to record regardless of the available light.

Hand-held and helicopter-mounted infrared imaging devices were often mentioned. One agency realized its need for a hand-held infrared imaging system after they had an officer shot while tracking a fugitive in heavy brush, a situation where an infrared imaging system would have been ideal. They were unable to utilize their helicopter because of bad weather. They have difficulty tracking suspects in a network of parks and rivers. A hand-held infrared imaging system could be deployed much more quickly than the helicopter. Another agency has access to a helicopter, but it is not equipped with an infrared imaging system. They need an infrared imaging system that can be quickly and easily mounted onto a helicopter.

Ease of use was raised by one interviewee. Night vision equipment is operated in darkness, often from a clandestine, possibly prone position that does not allow the operator much freedom to manipulate the controls. Frequently the operator is wearing gloves or other cold weather gear. In the case of rifle sights that utilize night vision technology, ease of use is of even greater importance.

A police department tactical team commander described a need for helmet-mounted, night vision goggles that can be flipped up and away from the tactical officer's line of sight, like a baseball player's cap with built-in sunglasses. This would allow the officer to use the night vision capability while approaching the target building at night or inside during low light, while still having the freedom to switch quickly to normal sight if lighting conditions suddenly change.

Participants in three sessions identified the need for improved depth perception in night vision equipment. Current monocular systems do not provide the level of depth differentiation that field users would like. One session identified a need for greater peripheral vision than the systems currently have. The ideal technology would allow pilots, tactical team members, and other users to operate without diminished sight to either side.

Members of one focus group pointed out that many potential domestic terrorist groups are equipped with the latest night vision technologies, and law enforcement agencies must have technological parity. This same focus group desired the ability to combine infrared sensing capabilities and available light enhancement in one lightweight, easy to operate device.

Although some military night vision technology is currently available to law enforcement agencies, there were complaints that the "handed-down" technology is older generation, while potential terrorist organizations are purchasing current military technology. Spokespeople from one large city were incensed that they were not permitted to attend military auctions and purchase newer technology. Laws limit civilian law enforcement use of military technology; however, terrorists are "immune" from such restrictions.

One interviewee identified a need for a night vision technology that can easily differentiate between "friend or foe." Such a system would distinguish between officers and others on the viewing screen. Authorized officers could wear a device that is not visible to the naked eye, but which appears clearly when viewed through the system.

Sniper rifle scopes with enhanced night vision also were desired. The risk of "blossoming" when exposed to light is of great concern when night vision technology is used by snipers. Exposure to sudden bright light effectively takes the sniper out of the scenario for the length of time that it takes to adjust the sights to the sudden bright light. At least one agency raised the concern that the night vision sights they currently use must be removed and replaced at dawn and reattached at dusk. During dawn and dusk neither sight is optimally effective, and the sniper is unavailable while he or she is changing sights. This problem led some departments to call for a combination day/night scope that would change modes through a single switch. This issue also arose under the discussion of apprehension technology.

Vehicle Tracking

Twenty-six sessions raised the need for more effective tracking of suspect vehicles. This often arose in discussions of the interjurisdictional challenges associated with terrorist activities–the desire to track a suspect vehicle beyond one's city, county, or even state. Current tracking technology is sometimes defeated when suspects "shake" the following vehicle, or move onto country roads where the tracking vehicle becomes obvious and must fall back. Current technology provides the relative bearing, motion status and range of the suspect vehicle. The requesting agencies presented the following requirements:

- A tracking system that utilizes Global Positioning System technology or another technology that provides the suspect vehicle's coordinates.
- A tracking system that takes the vehicle's coordinates and shows its location on an electronic map. As the vehicle "moves down the road", its course of travel is indicated on the map.
- A tracking system that transmits its information to satellite (or other technology) and removes the need for a tracking vehicle.

- A tracking system built to a common standard so that one agency can easily "pass over" the tracking of the vehicle to another.
- The transmission of the transmitter should be such that standard detection methods will not readily detect its presence.

One focus group identified a need for a spray-on material that can illuminate or paint the suspect vehicle and that is invisible to the naked eye. By applying the material officers could easily track vehicles (or people). Ideally, the reading device that would be used to identify the marking would be discrete so as not to reveal the tracking officer or his vehicle.

One interviewee defined a need for a GPS tracking system that could be used to track individuals, especially officers conducting undercover operations away from immediate backup.

Cellular Phone Monitoring Capability

The growing use of cellular phones prompted 12 sessions to identify a need to "tap" cellular phone conversations. Three of the 12 ranked this need among their top five. They wanted to be able to monitor cellular conversation from a central location. At present, some monitoring of cellular frequencies is possible, but as the calling phone moves from cell to cell it is difficult to track. With the advent of digital cellular systems and encryption, there is the added need to decipher the transmission.

The desire to pinpoint the location of a cellular phone in a structure was expressed in four sessions. Current technology can identify a cellular phone location within a few square block cells or less in major cities. During a hostage or barricade situation, as one officer put it, one knows where at least one of the perpetrators is if you can get him on a fixed phone. But with portable and cellular phones, location is harder to pinpoint. Ideally a cellular triangulation device would allow the operator to pinpoint the location of a cellular transmission to the level of a specific room within a structure, preferably within two feet.

Real-Time Video Feed to Command Post

Participants in nine sessions identified a need to have real-time video transmitted from an incident scene, a surveillance outpost, or a circling helicopter back to a command post, and for the command post to be able to send images back (e.g., of a suspect or vehicle). In many cases this need was associated with the desire for the remote-controlled surveillance cameras with night vision capability.

The technology needed to meet this need should have the following characteristics:

- Provide real-time, color video feed from helicopters, tops of buildings, or discrete locations.
- Operate non-line-of-sight (NLOS), especially in rural areas, and be ground-to-ground capable in an urban environment.
- Allow for remote control (for placement in discrete locations, on top of buildings, or in hazardous locations).
- Portable and easy-to-set-up receiving units at the command post, whether that is a vehicle, a roadside tent, or an abandoned building. The receiver should be transportable in the trunk or back seat of a patrol car.
- A minimum 1/2 mile transmission range between the camera and the receiver. One state-level agency would like the system integrated into a satellite uplink so there is the option of transmitting it anywhere in the country.
- Ability to capture images in computer databases.
- Ability to transmit images via phone lines.
- Encrypted transmission of images.

A representative from a mid-size police department defined affordability at the $10,000 - $20,000 range for a system with hand-held transmitter and small portable receiver. Smaller departments might pay as much as $5,000 for a version with fewer features.

One large city currently addresses this need by videotaping the incident scene and then transporting the tape to the command post for review. In a rapidly evolving situation this approach is insufficient.

Computer Transmission Tapping

It is clear in every region of the country that the majority of law enforcement agencies expect terrorist groups to become more computer savvy. Many emerging terrorist groups already use the Internet for communication, information dissemination, and even recruitment. In addition to the needs described in the later section on cyberterrorism, there is a growing need to monitor computer use. Participants in six sessions identified the need to intercept data transmissions over the Internet, with two agencies including it among their top five priorities. A state agency intelligence officer described the need to "follow" someone on the Internet without them knowing they were being followed. Another intelligence officer described the need to "trap and trace" electronic communication including e-mail, fax, and cellular phones.

Weapon Detection at a Distance

Officers want to identify individuals **in a group** who are carrying a weapon, without having to pat them down. Five sessions mentioned this. The desired weapons detector would detect small weapons, handguns, and knives under clothing. It must be patrol car portable and able to detect weapons on an individual from a distance of 30 feet. It must be simple to use and affordable. A minimum capability is to know that weapons are present; conventional means can be used once danger is evident.

Subsurface Imaging (Earth-Penetrating Sonar/Radar)

Increasingly, terrorist groups are burying their weapons and equipment or keeping stockpiles in hidden underground storerooms. It would be desirable to have a system that can define shapes that are buried, identify disturbed earth, identify metal objects, and, ideally, indicate the location of buried bodies. A Western state police department also identified the need to detect buried booby traps. (The department has recently discovered buried booby traps.) Officers are not currently equipped to effectively scan the ground for buried devices.

Telephone Number Dialed Logging System

Speakers in two sessions desired a technology that can log telephone numbers dialed on a targeted phone. They have an interest in knowing the dialed numbers almost instantaneously after they are dialed, rather than sometime later when they can ascertain the number through phone company records.

Underwater Search Capability

A large coastal city with an extensive harbor has a need to perform channel and harbor sweeps to check for possible devices, or "unexpected objects," and to locate forensic evidence. The current technology used by the agency is too slow and provides only a murky picture of what is happening below the surface. They need a system that would indicate the presence of an object like a handgun at a distance of 150 feet. Ideally the equipment would produce a sonar map of the channel bottom, and provide GPS coordinates overlaid on a map of items found.

Seismic Sensors

One interviewee identified a need for "leave behind" seismic sensors that would indicate the passage of a vehicle or person. Such technology would be used in rural surveillance situations to augment perimeter definition around a target structure. The interviewee represents a department protecting over 5,000 square miles with less than 20 officers. Such a technology would allow them to monitor activity in suspected hideouts, laboratories, and training facilities.[10]

[10] Existing seismic intrusion detectors, magnetic detectors, passive infrared detectors, and break beam detectors might fit this need.

Fiber Optics Monitoring

One agency wants the ability to tap fiber optics communications channels. Several of the agencies have had their transmissions monitored by non-law-enforcement groups. In several of the agencies, tactical operations have been compromised by suspects monitoring tactical frequencies.

COMMAND, CONTROL, AND COMMUNICATIONS (C^3) NEEDS

This section addresses C^3 needs, primarily in connection with field operations at an incident. Needs for improving law enforcement command and communication are closely linked to intelligence needs; one of the larger state and local law enforcement problems is secure communication of intelligence information dealing with terrorists. These needs have been organized into 15 categories, ranging from effective interagency crisis management system to telephone encryption. These are detailed in Table C-3.

Radio Encryption

Participants in about half (53) of the interview sessions raised radio transmission encryption as a need, with 19 of those identifying it as one of their top five. The majority of agencies interviewed experienced having their transmissions monitored by non-law enforcement groups. Several had first-hand experience of tactical operations being compromised by suspects who monitored tactical frequencies. For example, one agency reported that witnesses in a bank robbery saw one of the robbers carrying a scanner and updating the others as to the impending arrival of the police.

Several agencies knew of suspected terrorist groups that were monitoring their transmissions. A state attorney general's office investigator put it succinctly: "The bad guys are listening to us."

Current encryption methods for police radios were described as extremely limited in terms of the distance the radios can transmit, and the need for line-of-sight use. The requirement is for encryption of transmissions from hand-held radios without decreasing effective radio range. Affordability of encryption systems was also raised as an issue.

Interagency Communications (Interoperability)

Major incidents like terrorist attacks require a coordinated response by several agencies and jurisdictions. Often the responding agencies come from beyond the immediate area and may have little experience working with the coordinating agency on a major incident. The main technological issue these situations present, according to the interviewees, is the inability to communicate because the agencies do not share a common radio frequency. A significant number of sessions (48) identified this as a primary need, with over half (26) including it in their top five priorities.

Most of the agencies identifying this need had first-hand experience with interagency communication problems. One state agency told of a situation where their helicopter was pursuing a suspect in a car but was unable to communicate with the local patrol cars in pursuit or with the incident commander. A high-ranking police official raised the issue of effective communication between agencies from different states. Even though one state may have a standard car-to-car frequency, agencies in a neighboring state, which may be only minutes away, will not necessarily share the same frequency.

A state law enforcement agency reported that, to communicate with its local law enforcement agencies, it must be able to broadcast and receive on over 280 authorized frequencies. Another interviewee described a multiple-agency emergency that created a bizarre situation in the command center. The incident commander surrounded himself with six or seven "radio men," each holding a radio compatible with one of the participating agencies. Important information was constantly lost in the confusion this set-up created.

Another agency had six months to prepare for a large multiple-agency event, but interagency communication still proved to be a challenge. Their solution was to establish a large command center with dispatchers from each agency in cubicles along the wall. Other interviewees told of setting up adjacent command posts in parking lots, with runners used to take written notes back and forth between the command posts.

One interviewee only semi-facetiously said that he handles interagency communications with his counterpart in a neighboring department by driving up next to his car, rolling down his window, and asking the other person what is going on.

Five interviewees felt strongly enough about this issue to suggest the creation of federal guidelines regarding interjurisdictional communication, with two of those rating it as among their top five priorities. Two of the five suggested that Federal funds be withheld from those agencies that do "not meet the standard for public safety communications."

Several agencies provided the following more detailed description of their interagency communication needs. They desired:

- A "mixer" or "black box" that was no larger than table-top size and easy to set up. As arriving agencies check into the command post, they would report to the communications chief the number of radios they have and what frequencies they are using. The chief could then assign them a designator and register the agency's radio frequency into the black box. From that point on, the incident command staff could talk and listen on that frequency selectively or as part of a group call. Transmissions from officers in the field could be patched over to other frequencies at the discretion of the communications chief. This is more complicated than having every agency patched to one frequency, but it avoids the problems of overlapping transmissions and channel overload.

- A simpler, and less expensive version of the above "mixer" allows the Incident Commander (IC) to group broadcast across all frequencies without the patching capability. The IC will be dealing with more than just law enforcement agencies during a major terrorist incident. He or she may wish to broadcast instructions to the fire department, EMS, the hospitals, the sanitation department, the city buses, all city employees, or the media. For example, the broadcast might request that "all city buses report to the main compound parking lot for evacuation preparation. The primary triage area for walking wounded is Smith Hospital. All major trauma should be routed elsewhere....."

- The capability for officer-to-officer communications access for officers responding from different agencies.

- Regionally available caches of common frequency radios and repeaters, upwards of 250 radios, that could be quickly dispatched to a terrorist incident and distributed to responding agencies. One state agency has a case of 50 radios and a portable repeater that can be mounted in an aircraft. With the aircraft repeater the system provides nearly statewide radio coverage.

Improved Handheld Radio Performance

Sixteen agencies identified a need for improved handheld radio performance. The most commonly noted problem was operating in structures, especially large commercial structures. Tunnels, subways, and other underground locations also present a problem for radio transmission. The agencies need their portable radios to work as well from inside a building as they do outside. Officer risk increases when he or she is unable to communicate effectively.

Three sessions identified a need to equip portable radios with GPS transponder technology. One of the three considers it a top five priority. These three agencies all have vast areas to patrol, often with infrequent radio contact. In the event that an officer fails to respond to a radio message, the agency can only backtrack to his or her last known location. In some cases their information might be an hour old and 50 miles from where the officer had been last. Ideally the command center would be able to connect to the portable radio and receive an automatic reading of its GPS coordinates. Alternatively, the system might regularly report each radio's location.

Three sessions requested the integration of cell phone technology with portable radios. They would like officers in the field to be able to place cellular phone calls directly from their radios. This capability was especially needed during crises, when officers are handling a variety of duties not all of which can be effectively conducted via radio. Additionally, in the event that local phone lines are rendered useless, there is the chance the cell phone system would still be operational.

Two sessions reported a need for improved performance of the hands-free microphones used with portable radios. This need is especially acute for entry teams that must operate weapons and equipment, yet still be able to transmit and receive on the radio. They want a system that is more reliable, has more clarity, and is easier to use than the current system that employs an ear microphone attached by an arm to the voice transmitter.

Secure Data Networks

Participants in ten sessions raised the need for secure data-sharing among law enforcement agencies. Of these, six identified the need for secure data sharing as a top five issue. Agencies require the ability to transmit graphic images, data files, sound files, and even video across interoffice and interagency networks. One officer observed that as long as there is the perception that networks are not secure, they will not be used effectively. This requirement is tightly coupled to the requests for improved intelligence databases and software discussed under Intelligence.

Management Information System to Assist the Incident Commander and Staff

Ten sessions described the need for assistance in organizing the command function at major incidents. They envisioned some sort of "intelligent" software system that would help the incident commander organize resources, track assignments, and most importantly, prompt the IC for critical decisions. Interviewees told anecdotes about the challenges of tracking arriving resources, where they are dispatched, and when they need relief. They also need to keep track of what decision-making chain is in place for the crisis. Participants in three of the ten sessions envision software that comes with pre-defined scenarios. Two expressed a desire for the software to be fully integrated with a mapping function so that as units are dispatched their location is represented on a map.

Further details of the desired capability were described as follows:

- Computer software that establishes a common command language across agencies and that prompts the user to establish the necessary functions under an incident command system (ICS). The software would track the assignment of personnel and resources. It should be able to track resources as they arrive, document what their qualifications are and where they are assigned, and monitor when the resources need to be relieved, etc.

- The software should include a "savvy checklist" or system of checklists that prompts the user throughout the crisis. These prompts might be along the line of, "Have you arranged for scene lighting? It will be dark in four hours." Or, "With your dispatch of Medic 5 from staging you have only two medic units left in staging."

- The system should archive decisions as they are made, for later recall and review after the incident. One officer stressed that incident commanders often need this for post-incident reviews.

- The system should be expandable to handle information for events that may last for weeks or months, and involve large numbers of responding agencies.

- The system should be designed so that training scenarios are consistent with what the user will encounter from the system during an actual emergency.

- An integrated map function should indicate by icon the location of all resources dispatched on the crisis and those awaiting dispatch in a staging area. By "clicking" on a unit's icon the command staff can view, in an expanded screen, the unit's characteristics, its status, the time since it was assigned the task, resources it has requested, and so forth.

Field Laptop Computers with Communication Links to Various Databases

Nine agencies requested help in creating a law enforcement laptop computer capability that would have the following features:

- Rugged
- Secure, with encrypted transmission
- Operable from a squad car or surveillance position
- Able to connect to agency fingerprint, information, and other databases
- Easy to use
- Software to assist the officer in his or her duties
- Databases about suspicious objects, explosive devices, etc.
- Maps, addresses, and related information

The agencies envision the laptop as an important tool to get relevant intelligence, warrants, and other information quickly to officers in the field.

Improved Radio Coverage and Performance

The interviewees in nine sessions described problems with radio performance in remote areas–specifically where they know that a violent hate group or militia cell is based. There are large areas with no radio coverage and areas where the terrain interferes with radio transmission. Four agencies identified problems associated with non-line-of- sight (NLOS) transmissions and the need for a radio system unhampered by mountains and terrain. In seven of the nine sessions, participants rated remote radio coverage as a top five issue, especially in Western states and Alaska. The agencies described dead zones in their radio coverage that in some cases were miles wide. There was a great deal of concern for officer safety when operating in these dead zones. The cost associated with potential solutions was cited as the main reason for not having adequate coverage today.

Two potential solutions were offered, both in the context of remote area radio coverage and in the broader context of law enforcement needs in general. These were terrestrial-based radio repeaters and satellites. Five participants suggested the need for radio systems that can be switched to a satellite or long-range repeater when the user ventures into an area where normal transmissions are not possible. Three agencies expressed a need for affordable, portable, easy-to-set-up repeaters to increase communications range during surveillance and during response and recovery from terrorist incidents, not necessarily in the context of remote areas. These repeaters would be placed so that blocked or weakened transmission could be boosted. They would also serve as temporary replacement repeaters in the event that a permanent system was disabled. Another need identified was for more affordable satellite phones for use in remote areas and during extended surveillance. Affordable satellite phones would allow surveillance officers to communicate with the command center without being dependent on local phone service. Satellite-connected phones can also thwart radio scanners.

Advanced Command Post/Communication Vehicle

Eight sessions identified the need for more affordable and effective command post vehicles. The command vehicle should be able to fully utilize the resources of modern-day law enforcement. One participant noted that the converted bread truck of the past poorly meets the needs of today's surveillance and terrorist response requirements.

The command post vehicle must be equipped with secure communications equipment, maps, secure radios and faxes, high-resolution photo faxes, personal computers connected to intelligence databases, resource contact lists, and other information. It should be designed in a way that allows agencies to customize the vehicle.

Priority Usage of Cellular Telephone System

Six sessions noted the importance of the cellular phone system as a resource during an emergency and the necessity of law enforcement to be able to override the system's normal transmission priority. One of the six identified this need as a top five issue.

Two agencies that had recently experienced major events described system access problems with the cellular phone system. The excessive demands on the cellular systems often effectively shuts them down during the peak hours of a crisis.

In addition to technology that can give law enforcement and other emergency personnel telephone priority, there must be agreements with the cellular service regarding when and how such priority will be activated. The priority must apply to both incoming and outgoing calls.

Secure Video Conference Capability

Three interviewees identified a need for secure intra-agency and interagency video conferencing. They emphasized the advantage of bringing key personnel together electronically to present evidence, discuss scenarios, talk to sources, and share information. For law enforcement to take advantage of the technology, it must be encrypted and secure from interception.

Blackout of Terrorists' Communications

It is important in a major terrorist hostage or barricade situation to isolate the primary participants from lookouts and allies located beyond the police security perimeter. Three sessions expressed a need for the ability to effectively cut off all communications by terrorists during a barricade or hostage situation. No longer is cutting the phone lines enough. More than likely, terrorists will be equipped with radios, cellular phones, pagers, and possibly televisions. At a minimum the agencies would like to "blanket" the building with an electronic blackout that would scramble the perpetrators' cellular phones. Ideally, the agencies said they would like a communications scrambling device or system that could be placed around a structure without significant spill-over into the surrounding area. The goal would be to enable controlled communications with the terrorists.

Ability to Deactivate a Stolen or Lost Law Enforcement Radio

Two interviewees articulated the need for low-cost technology to deactivate lost or stolen law enforcement radios. One of the two specified it as a top five requirement. Stolen or lost radios provide access to law enforcement frequencies. This is especially dangerous when the radio is equipped with an encryption/decoding capability for tactical or surveillance channels.

Establishment of a Common Radio Language Standard (or Translators)

Many law enforcement agencies use their own radio codes, often called 10-codes, which cause great confusion when several departments with different codes are thrown together on major incidents. Some departments have switched to a system of "plain English." Either a single national (or at least regional) standard is needed, or the ability to automatically translate from one 10-code "language" to another.

Telephone Encryption

One interviewee voiced a need for affordable and effective telephone encryption. There is a concern that as terrorist groups become more sophisticated they will monitor not only police radio communication but telephone conversations as well.

SITE HARDENING AND SECURITY NEEDS

Site hardening and security refers to the need to protect buildings, facilities, and major, on occasion, outdoor events, from terrorist attack. It also includes ways to reduce site vulnerability from attack and damage. Most of the expressed concern was for protecting target buildings such as federal and state government buildings, law enforcement offices, and private sector structures with high occupancy or high economic value. There was also considerable concern for protecting outdoor locations, infrastructure, and mass transit, including airports.

More than half of those interviewed cited a need to improve or make affordable site hardening technology. This was brought up in 52 of 108 interviews and focus group sessions.

Interviewees from state and local law enforcement agencies that had experienced attacks tended to be especially sensitive to the need for site hardening technology for police and other facilities. Identified needs were organized in nine categories, detailed in Table C-4.

Fixed Intrusion Detection Systems

The most frequently expressed need for site hardening was for better devices to detect unauthorized entry (13 sessions). They include sound and motion detectors, heartbeat detectors, thermal detection and imaging equipment, seismic detectors, low-light vision observation devices, laser beam or other "electric eyes," and remote cameras. Participants want affordable systems that can withstand extreme temperatures (e.g., in Alaska). Some further specialized needs:

Remote Cameras–Seven sessions identified the need to improve remote camera technology specifically for site security (many more wanted improvements for surveillance, as discussed earlier). Two agencies put it among their top five needs. The desired capabilities included high-resolution digital camera technology, videotape compression capability (for fast review and for storage), color cameras capable of zooming and freezing frames, and cameras with night vision capability.

Underwater Perimeter Security–One session identified a need to better detect underwater intruders. (This also arose under the surveillance discussion.) Systems such as sonar, underwater hydrophones, underwater cameras, or other devices would help establish a secure perimeter around structures that have an underwater component and that may be vulnerable to attack or sabotage from sub-marine sources.

Tunnel Detection Device–Two Western law enforcement agencies raised the need to detect the presence of tunnels that have been constructed to gain covert access.

Improved Passive Site Hardening and Architecture (Built-in Physical Security)

Passive, built-in site hardening includes ways to make entry more difficult and make buildings more survivable from attack. Concrete barriers, bars, razor wire, bullet proof/shatter proof glass and improved lighting are examples of this technology. Participants in ten sessions identified a need for improved physical security technology.

Anti-Vehicle Technology–Several sessions called for improved access to vehicle barrier technology. One Southern agency identified a need for technology to improve parking lot safety.

Computer Bomb Blast Modeling Software–Several sessions, including one which named it a top five concern, called for computer software that can model potential blast damage on particular structures and use that information to either make changes in the building architecture or the security measures.

Personnel Access Controls

Personnel access controls have several purposes: to restrict access to buildings or events to authorized people; to keep track of who and possibly how many enter a specified area; and to provide a record of activities or whereabouts of both authorized and unauthorized persons. These controls can be either automated (such as computerized entry controls) or manual (e.g., a security guard checking identification cards). Nine law enforcement agencies identified needs for improvements here, especially for more affordable systems and systems providing better access control. This seemed to be an area where existing technology is not well known.

Computerized Entry Controls–Several interview sessions identified a need for improved or less expensive systems to restrict access by use of alphanumeric codes, passwords, fingerprint scanning, or other means. Technology such as Advanced ID cards with computer chips carrying detailed authorization information are desired.

Personnel Access/Status and Tracking Log Technology–Several participants noted the need for a technology to better control and record the access, whereabouts, and activities of those who enter controlled areas. They were particularly interested in restricting and recording access to computers, databases, files, etc. Two Southern agencies also suggested the need to track the position of guards and site patrol units, perhaps using GPS tracking technology.

Metal and Explosive Detectors for People and Vehicles

Seven agencies called for improved technology for detecting metal or explosives that are carried or driven into a structure or site. Devices could be either handheld or large and free-standing. They would detect even small amounts of metal, possibly from weapons or other materials such as bomb components.

Several Mountain and Western region sessions identified a need for *discrete* (surreptitious) metal detectors, which could be hidden or blended into existing structures.

Portable Perimeter Security

Portable perimeter security refers to site hardening technology that can be moved and deployed as needed. Portable perimeter security items include portable barricades, bullet-proof shields, metal detectors, x-ray screening machines, and others. Seven agencies felt this was important technology to have, especially to secure large public assembly areas. It also is needed to protect VIPs inside or outside structures, in areas that do not normally require high security. One session identified a need for a portable baggage screening machine as a top five concern.

Improved Letter/Package Scanners

Five sessions called for improved, higher speed letter and package scanners.

Intruder Countermeasures Technology

One focus group raised the need for systems that not only detect intruders, but that incapacitate intruders or actively deny entry (e.g., by sound waves that increase in intensity as one gets closer to the protected area). Some officials called for an ability to automatically seal or increase the hardening of a structure in the event of a terrorist attack.

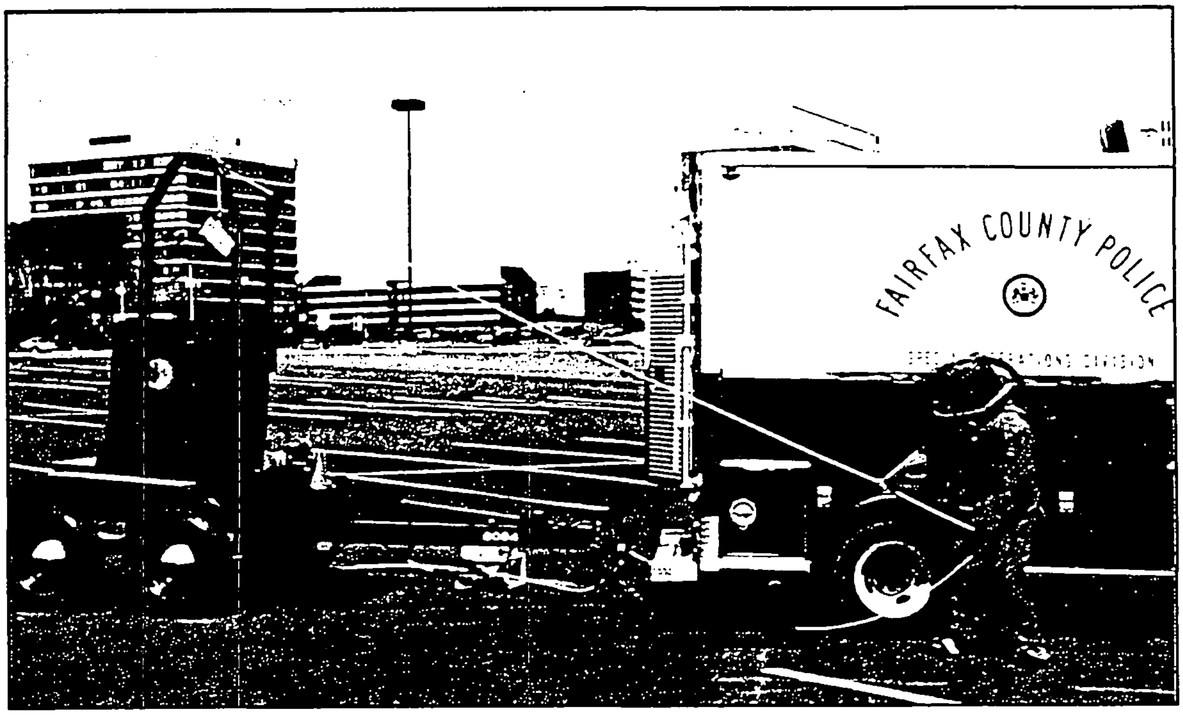
Site Patrol Boats

Boats equipped with sophisticated surveillance and dive and rescue equipment are needed for river and harbor patrol.

Computer-Aided Site Design

In addition to the previously mentioned blast simulation software, one Western focus group called for computer software to model and assess site security for particular structures. Others felt that computer-aided design could be used to improve traffic flow around buildings and reduce vehicle bomb threats.

DETECTION, DISABLEMENT, AND CONTAINMENT OF EXPLOSIVE DEVICES NEEDS



One of the key needs for combating terrorism is improving the ability to detect explosives and then to disable or contain them. This was the second most frequently mentioned capability, just after intelligence capabilities. The needs have been categorized into five areas: improved detection; improved explosive disarmament or disablement technology; blast containment; information management technology; and improved maintenance. These are detailed in Table C-5.

State and local law enforcement agencies are keenly aware of the threat posed by common mail and pipe bombs as well as the explosive devices used in the high-profile bombings at the World Trade Center, the Alfred Murrah building in Oklahoma City, and the Olympic Centennial Park. Over three-quarters of the law enforcement agencies interviewed identified a need for improvements in dealing with explosives, and over one-third of the agencies interviewed identified that need as one of their top five concerns.

Improved Detection Technology

The highest priority in dealing with explosives is to have a greater capability to detect them. Interviewees raised that need during 58 of the sessions. Clearly, this is a high priority. While automated explosive detection technology is available, most state and local agencies use bomb dogs.

Interview and focus group participants routinely praised the explosive-sensing dogs. Many identified a need for obtaining more dogs. However, it was repeatedly stated that the dogs have certain shortcomings, such as cost and time-on-target (dogs can become distracted after 20-30 minutes on the job). It can cost $20,000 for training and more for routine housing, care, and feeding. The leading technology request here was for a portable, preferably handheld explosive detector that was at least as accurate as a canine and less expensive. Thirty-six agencies requested this, with 18 placing it among their top five needs.

A number of participants identified a need for more sensitive detection devices, with a broader range of explosive-sensing capabilities. This broader spectrum capability was the second most desired improvement in detection (after portability); it was mentioned in 10 sessions, and flagged as one of the top five priorities by five. Participants called for devices that can test for more than the nine scents for which bomb dogs are trained.

Increased distance of detection for explosive detectors, as well as the capacity for a detector to function in a wide-open area such as a stadium or arena, were cited as important detection attributes in at least four sessions each.

Another critical need is to detect the presence of any additional explosive devices following detonation of the first–something dogs cannot do well. The detonation of the initial device scatters explosive residue that overloads and confuses the dogs' olfactory senses. A series of bombings in Atlanta, in which second devices were employed with the specific intent of injuring law enforcement officers and other first responders, has heightened the concern about this threat. Ten agencies explicitly called for the capability to detect additional devices at a bomb scene. Several voiced the need for related technology that, after a first explosion, could detect the presence of the triggering device for a remote control (radio frequency) detonator in a crowd.

Merging bomb detection technology with bomb mechanism imaging technology is seen as highly desirable. Participants desire the type of imaging technology that alerts a first responder to a sound-based or motion-sensitive arming or firing mechanism. Officials felt that allowing officers to both quickly locate an explosive device and determine a bomb's firing or arming mechanism are essential first steps to assist officials in determining the appropriate response measures.

Some participants called for a device that combined explosive sensing with chemical and biological sensing capabilities. One of the great concerns is for devices that have chemical or biological agents dispersed by an explosive device.

Several officials called for explosive detectors that could quickly and discretely interrogate a slow moving car. One official envisioned merging this scanning technology with a device that can disable or trap a vehicle if it is transporting explosives.

As noted under site security, a portable explosive scanner for packages and baggage is desired (and repeated here for completeness). One agency identified the need for detection technology that could locate buried explosives as well as detect explosives at longer ranges.

Affordability concerns were evident throughout the interviews. Many participants stressed a need for less expensive detection devices. Participants stressed that new detection technology must be reliable, with very low false alarm rates. Participants, especially those from areas that experience harsh environmental conditions, pointed out that new devices must withstand a wide variety of environmental stresses. Another concern was that new technology should require little maintenance. Participants called for devices that could be left inactive for long periods of time – in a patrol car trunk, for example – but which would provide accurate results if needed.

Many responders requested technology that was simple enough for officers to use without extensive training.

One focus group noted the need for a detector that could identify diesel fuel and ammonium nitrate when mixed or in close proximity. They cited the massive bombs at the World Trade Center and in Oklahoma City as evidence that the capability is extremely necessary.

Disarmament and Disablement Technology Capabilities

Improved EOD Robots

Disarming or disabling a device usually requires an explosive specialist to view and understand a bomb's arming or firing mechanism, and then disable it, either by delicate manual techniques, remote controlled Explosive Ordnance Disablement (EOD) robots, stand-off disrupters, or combinations of approaches. The most frequently identified need in disarmament/disablement was for an improved generation of EOD robots, to reduce human exposure to risk. Almost half of the interviews and focus groups raised this need. Many state and local explosive ordnance specialists use robots. Current robot technology incorporates a number of rudimentary EOD procedures, such as object imaging and disruption capabilities. However, the robots are viewed as too expensive, with prices above $100,000. Also, they often are unable to enter certain environments or perform necessary procedures.

The prospect of acquiring EOD robots commanded a great deal of interest in all regions, but especially in the Southern region. The general need expressed is for a robot capable of performing the majority of EOD procedures, and having these features:

> ***Remote Control Capabilities***–Several officials requested better wireless communication with their robot, an increased range, and safeguards so that control is not blocked by common building materials. Several said that a one-quarter mile range would be desirable. Any new robot communication system should be designed to prevent activation of radio-triggered explosive devices. Another troubling issue, discussed further under EOD (bomb) suits, was that the current intercom communications system of bomb suits interferes with some EOD robot controls.
>
> ***Remote Detection, Viewing, and Disruption Capacity***–Several interviewees called for robot-mounted explosive detection equipment, which would reduce hazard exposure time for bomb detection. One focus group listed this detection capability as a top five need. One agency felt that EOD robots should be mounted with chemical and biological detection equipment. Fifteen agencies identified the need for a robot to remotely view suspicious objects. Several requested that robots be outfitted with x-ray or other imaging technology. One complained about the quality of current images transmitted by robot mounted cameras, and felt that real-time digital color cameras could improve coverage and depth perception. Ten interviewees identified a need for robots to provide more effective disruption capabilities. Current models frequently incorporate either a shotgun or water-type disrupter, but they wanted something even better.
>
> ***Robot Mechanical Operations***–A number of users were frustrated that robots are frequently unable to enter certain buildings or areas. The capacity to climb stairs (even spiral stair cages), was identified as an essential design characteristic. A top five concern of one focus group was to develop a robot capable of opening doors. A number of respondents called for a robot capable of lifting and manipulating packages.

Several participants felt that a robot should be able to lift a 100-pound package, or more.

Lower Maintenance–Many interviewees called for a robot that requires less maintenance than current models. Several larger city respondents reflected that it was particularly frustrating to purchase an expensive robot that was frequently out of service for repair. Another recurring concern was that any new technology should be user friendly and simple to operate.

Affordability–One of the most common desires was the need for a more affordable robot. As noted above, a third of all comments about robot technology were calls for a more affordable robot. Respondents felt that the $100,000 price for current models was prohibitively expensive. A side effect was a reluctance to risk a highly expensive robot on an unstable EOD. Several of the interview sessions in the Mountain states therefore called for a low-cost "sacrificial lamb" robot that could easily be replaced if it was damaged or destroyed while manipulating explosive devices. It would be sent in first to handle and assess the suspect package before risking the more sophisticated robots.

EOD (Bomb) Suits

EOD suits are personal protective outerwear that provide bomb technicians a measure of protection from the effects of the detonation of an explosive device, e.g., blast, shrapnel, etc. A variety of suit models are available. Most protect the head, chest, abdominal area, and the major artery areas of the arms and legs, but they are bulky and restrict movement. Although EOD suits often make hand protection available, it is commonly not used since it restricts the fine finger movements necessary for EOD operations.

Improvement in EOD suit technology was identified in 22 sessions, and was a 'top five' priority of seven agencies. The following are some of the EOD suit technology needs identified:

Lighter and Cooler–The new generation of suits needs to be lighter and have a built-in cooling system. A number of Southern participants felt the lighter suits should weigh less than 65 pounds. This was the single most needed modification they mentioned. Also common, especially among Southern and Eastern participants, was a desire for suits that are suitable for working in the presence of chemical/biological risks and are environmentally sealed, with a self-contained breathing apparatus housed within the suit to provide an air supply.

Improved Intercom Communications–As noted above, participants frequently voiced their frustrations over EOD suit intercom systems that interfere with the operation of EOD robots.

Improved Blast Protection–Although there is a desire for lighter suits, there also was an expressed need for blast protection to combat more powerful explosive devices.

Several interviewers identified a need for suits to withstand explosions of one pound of C4, two to ten pounds of "generic explosive," or seven to ten sticks of dynamite from four to five feet away. Participants called for improved hand protection that allowed fine finger movements. One Southern police official expressed a need for improved knee and spinal protection as well as for protection from blast over-pressurization effects.

Improved Visibility–Several participants felt that current EOD helmets did not provide adequate visibility for bomb technicians. One called for helmets that provide a 180° field of vision.

Improved Diagnostics

State and local explosive ordnance disposal technicians routinely rely on field-proven x-ray technology to view the inner workings of an explosive device. Although x-ray technology already is a powerful tool, participants in 19 sessions called for improvements. Specific needs include the following:

Portable Imagers–Participants feel that current devices are too bulky and unwieldy. They prefer smaller, lighter, more portable devices. Several participants noted the need for x-ray imagers that can be quickly set up and operated by one individual.

Standoff X-Ray Equipment–Participants called for x-ray technology that would allow real-time imaging of an EOD from a safe distance, without a technician having to approach it or encircle it with x-ray receivers and transmitters. A sizable number of participants believe that EOD robots might effectively perform this function. A member of a state explosive ordnance team summed up by saying that the team needs technology to reduce a technician's exposure time, one way or another.

Image Quality and Production–Some participants are disappointed with x-ray image quality. Several participants noted that the current state-of-the-art computer software should allow for 3-D color imaging of explosive devices. Several participants addressed x-ray film technology needs, noting that x-ray film is expensive and "archaic." X-Ray imaging devices that do not use physical film plates should be made available.

There was a call for developing technologies other than use of x-rays for examining explosives, because of the problems discussed above.

Disrupter Technology

Disrupters are devices that use kinetic energy to physically disrupt a bomb's firing or arming mechanism. Shotguns, disrupters that fire a slug of water, and disrupters that fire coin-like munitions are examples of current technology. Several participants identified the need for better disruption technology as a top five concern. The disruption technology needs included the ability to utilize disrupters from a greater range; percussion activated non-electric (PAN) disrupters; and "cloaking" technology to defeat explosive devices that incorporate passive infrared receivers in their firing mechanisms. It was noted that the military already employed some of this technology.

Blast Containment

Blast containment technology refers to devices designed to contain or minimize the energy and products released by an explosive device. Bomb trailers, bomb blankets, and hardening foam are examples. Bomb transport trailers are either spherical containment or cylindrical blast deflectors. The spherical units are designed to evenly distribute explosive forces. The cylindrical deflective units direct the explosive upward to avoid ground level destruction. The trailers often incorporate fire suppression equipment. Most bomb trailers, however, can only contain small amounts of explosives (less than ten pounds), and even spherical containment units are not designed to seal in the gases released during the explosion. Several law enforcement agencies expressed the need to contain the explosive effects and all of the gases of 10 to 30 pounds of explosives. Bomb blankets are temporary covers that provide limited protection from explosive forces, but cannot contain explosive gases. Hardening foam is designed to be sprayed around an object and harden to provide an insulating protection barrier.

Improved bomb blast containment technology was identified as a need in 31 sessions, and was a top five need of at least six agencies.

Access to bomb trailers was a top five concern for five agencies. Many state and local agencies do not have rapid access to their own bomb trailer and are forced to borrow them from other departments or the military. Several participants noted that this often causes delays of several hours. The principal access problem is having too few containment vessels because of their high price tag (over $100,000 for new spherical containers). Lower cost devices are necessary.

Several interviewees called for improved bomb blankets or other fast-to-use containment technology to combat more powerful explosives. The blankets would be quickly placed over a small-to-medium-sized bomb to provide blast protection. Another participant identified a need for a vehicle-sized bomb blanket that could be rapidly deployed.

Several participants, mostly from the Western Region, requested access to hardening foam technology to contain explosions. Several bomb squad participants reflected how military EOD teams had access to that technology, but civilian law enforcement use of these foams has not been authorized.

Information Management

Computerized information management systems can provide bomb technicians with a means to quickly access technical information or explosives. Participants in eighteen sessions raised a need for improved information.

Officers stressed the importance of having current information on the most current bomb making techniques. Nine agencies wanted a CD-ROM with the latest information on a bomb's internal features (e.g., schematic drawings). Officials stressed that access to this information needs to be restricted. One officer lamented that the Internet provides an assortment of bomb making information and that it would be very helpful for law enforcement to have convenient access to similar information on site in the field.

One participant identified a top five need for computer software that could model and predict blast effects upon specific types of construction. The technology would allow officers to perform more accurate risk assessments. It would provide the officers better information about potential consequences when confronted with a decision about how best to handle the explosive device (disarm, disable, or explode in place). This is needed both for site design and for real-time decision making when an EOD is discovered.

Several participants called for increased access to reports and bulletins from the FBI Bomb Data Center. Others identified a need for officers in the field to have laptop computers capable of providing a secure real-time connection to the FBI Bomb Data Center.

Improved Maintenance

As noted in part in the discussion of robots, there was strong feeling (expressed by eight agencies) that reliability of the above technology, especially robots, needs to be improved so that there are lower maintenance costs and higher availability.

CYBERTERRORISM NEEDS

"Cyberterrorism," as it has come to be known, generally refers to using computers or computer networks to harm or threaten. It includes attacking computer databases and processes controlled by computers, as well as the computers themselves. State and local law enforcement's needs to combat cyberterrorism were organized in five categories, detailed in Table C-6.

A key finding of this inventory, based on participants' input, is that there is not enough information or expertise in most law enforcement agencies to articulate the threat specifically, let alone to combat it. About two-thirds of the interviews and focus groups included reference to cyberterrorism, but most often only in general terms. In over one-third of the interview sessions, the interviewees indicated that they or their agency recognizes the threat posed by cyberterrorism. Most of these respondents related that their agency is unable to address the issue, either because the agency views cyberterrorism as the domain of federal law enforcement, is not prepared for this function, or has not yet instituted an agency initiative because the threat is so new.

Training to Counter Cyberterrorism

In 10 sessions, the participants indicated that training on cyberterrorism is an important need, starting with basic training. Two respondents (both in the Western region) included training on cyberterrorism in their top five lists.

Intrusion Prevention

Twelve agencies expressed a need for technologies to prevent intrusion into critical computer systems. They specifically mentioned the need for improved "firewalls" or user authentication.

Four agencies called for better technology to detect and report intrusion attempts on computer systems. This need echoed recommendations about intrusion detection in a 1996 GAO report on computer security, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (AIMD-96-84):

> [We] recommend that at a minimum the Secretary of Defense strengthen the Department's information systems security program by developing department-wide policies for preventing, *detecting,* and responding to attacks on Defense information systems (emphasis added).[11]

Two respondents (both from the Western region) requested better forms of user authentication. Both specifically mentioned improved biometric capabilities (i.e., the ability to read and validate physiological traits of a user, such as retinal patterns, fingerprints, etc.).

[11] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (AIMD-96-84), 1996, Chapter 4:2.

These interviewees believe that current authentication technologies can be defeated, allowing unauthorized users access to sensitive systems.

Forensic Capabilities

Forensic capabilities are needed to identify who gains entry to computer systems unlawfully, who attacks them, and who uses them to convey threats. At least 15 agencies noted the need for forensic capabilities related to computers. By far the most interest was in the area of de-encryption technology. These interviewees stated that many criminals (and presumably many cyberterrorists) have encoded the data stored on their computers. Data encryption programs such as PGP (Pretty Good Privacy) are widely available (either commercially or as free software that can be downloaded from the Internet). Use of these programs renders the encrypted data unintelligible without the privacy key. Obviously, such a capability cripples the investigative capabilities of law enforcement. To the extent that terrorists have access to or can make use of encryption technologies, these respondents contend that law enforcement must have access to technology that will allow them to de-encrypt data so that they can read what is on the disk drives of computers that are seized or read remotely.

Three respondents noted that some computers are "booby trapped" and will self-destruct the data stored on them when an unauthorized user (in this case a law enforcement officer) attempts to examine the data. Linked closely with this idea is the notion of a virus that attacks the computer that reads the booby-trapped floppy disk (or other removable medium). These three indicated that along with virus protection software that is commercially available, there needs to be some device or program to detect the presence of a booby trap or virus and neutralize it.

Two respondents indicated that the biggest need in this area is skilled computer investigators. The sense is that state and local law enforcement agencies need to train computer forensics specialists, or need to have such experts available to assist.

One participant of the Western region focus group mentioned that he would like to have the capability to access the computer of a suspect remotely. Presumably, this would necessitate the target computer being connected to the Internet, a network, or some other accessible point from "the outside." (It also presumes that an agency has obtained the required warrant to do so.)

Other Needs

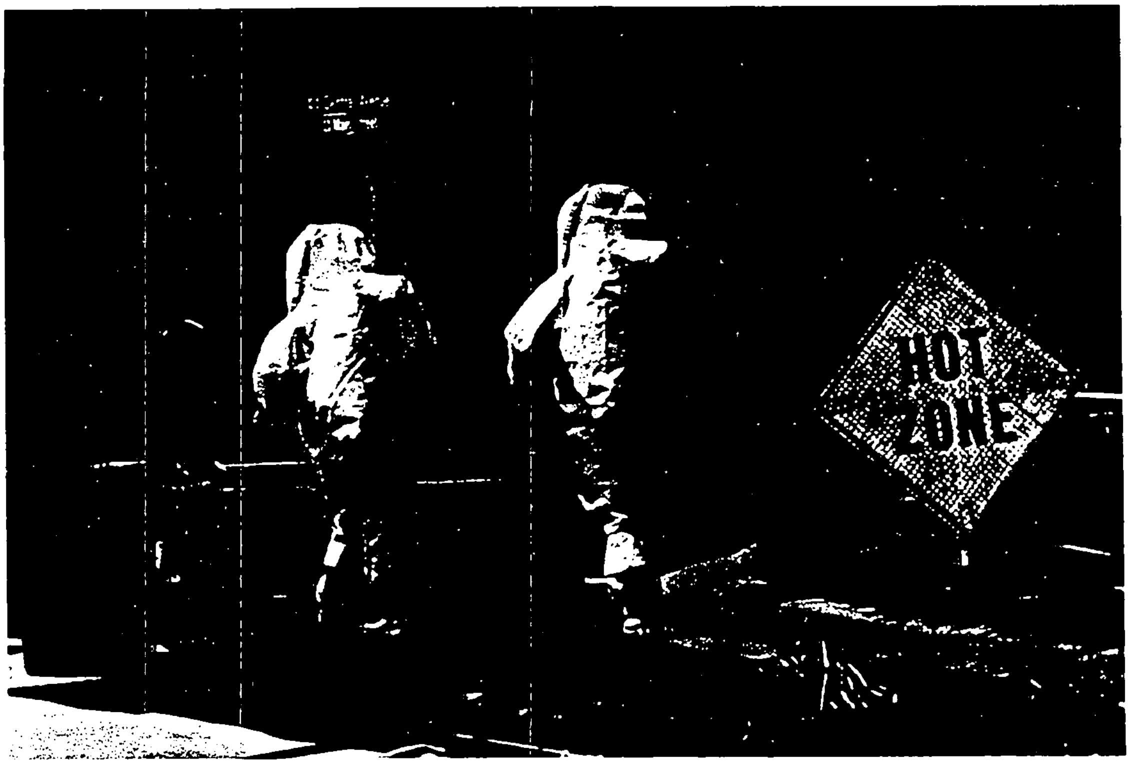
A variety of other ideas surfaced regarding cyberterrorism or computer-related issues:

System Monitoring Log–One member of a focus group indicated that he would like to have some means of identifying what the **authorized** users were doing on his agency's computers. He felt it was important to know who had modified a database, or what types of searches were being performed on accessible databases. Such a capability would help ensure the integrity of the computer and data collection operations of the department, deter illegitimate usage by authorized users, and help serve as a basis of comparison for detecting use by unauthorized users who had obtained passwords.

Security Self-Assessments–One respondent thought that a systematized technique is needed for conducting computer security surveys.

Better Back-up Systems–Two respondents indicated a need for better back-up systems for their computers. This was to prevent vulnerability of their computer operations in case their information systems (or power grid) were the object of an attack. One respondent focused on back-up power for the computers. The other focused on having alternate computers to use.

DEFENSE AGAINST WEAPONS OF MASS DESTRUCTION NEEDS



This section discusses the detection of and response to weapons of mass destruction, focusing on nuclear, biological, and chemical threats. The technology needs for dealing with the other major type of such weapons, massive explosive devices, were addressed in the section addressing detection, disablement, and containment of explosive devices. Of all the areas of technology identified in this inventory, this was seen by the law enforcement interviewees as one of the most important areas of need and yet the one for which they were least prepared.

Nuclear, biological, and chemical weapons are often thought of as the responsibility of the federal government. The Sarin attack on the Tokyo subway reminded local law enforcement in America that regardless of the lines of responsibility, it will be their officers who arrive first at the scene of an NBC incident. They will be forced to make life-and-death decisions about the citizens at risk–and themselves.

An experienced officer from a major city police department said, "We are just in the early stages of talking about NBC. We can handle everything else on your list pretty well, but not this. On all the other categories we adapt, improvise, and overcome...but on NBC we would honestly be in real trouble." His statement was echoed by many participants who agreed that of all the threats, terrorist use of NBC agents is perceived as having the lowest probability of occurring, but is also the most feared. A state police commander noted that, "We currently have no way to detect the presence of a chemical or biological substance at an incident area. We need technology for the first responder to detect the presence of a chemical threat and to warn the public."

Several officers explained that they considered their primary responsibility to be identifying the agent. They then can define the perimeter in which the agent is contained, secure that perimeter, provide what aid they can to the injured without spreading the agent, and wait for federal reinforcements.

Unlike other technology categories where participants were able to offer specific desired improvements, the interviewees acknowledged that their lack of experience with NBC technology made it difficult to define their needs precisely.

The technology needs in this area have been placed into the following three categories: detection, protection, and decontamination and containment. They are detailed in Table C-7.

Detection

In 51 out of 108 sessions, participants stressed the criticality of being able to better detect and categorize hazardous, life-threatening NBC agents; 24 listed it in their top five needs. The chief concern was to be warned of the presence of the danger; a secondary concern was to know what type of hazard existed.

Law enforcement officials worry that first-responders may unknowingly walk into a deadly environment. The most commonly stated need here was for a portable, preferably belt-wearable, affordable chemical and biological hazard detector. This was requested in 32 sessions, of which 16 identified it as a top five need.

The detector should indicate the presence of an agent from as great a distance as possible. If the detector sounded, the officer would either retreat from the area or don an NBC suit. One interviewed agency has begun issuing detector strips to their patrol officers. If the strips come into contact with a liquid agent, they change color to indicate whether the agent is chemical, nerve gas, or biological–but the officer is already at risk.

In 10 sessions, respondents stipulated that the detection technology be mountable on a vehicle, allowing officers to monitor the air for hazardous substances without leaving their patrol car. This feature also would allow officers to quickly assess other locations, something that could not be done efficiently on foot. The sensor should be relatively unobtrusive, to avoid alarming the public. The ability to quickly characterize a detected agent, across at least broad categories, was also desired.

There are belt-worn detectors already available that detect several classes of chemical agents. The need is to expand the range of the chemical agents detected, and to include a capability to detect biological and, ideally, radioactive hazards in the same device. Ease of operation is also important, especially because detectors will be used very infrequently and the operators will not necessarily be familiar with the devices. Moreover, there will not be enough time to read through an instruction manual. None of the participants believe their agency has any biological detectors.

Other improvements participants would like to see include:

- high sensitivity
- clear alarm signals
- low false alarm rate
- short detection response time
- long-lasting battery
- affordable enough for multiple units

A need for a small, badge-like detector was also identified in two sessions. "We want our officers to know if they are threatened; we don't want them to be "blue canaries," bluntly stated one East Coast police official. ["Blue canaries" refers to the small birds employed as chemical agent detectors by the military during the First World War. When the birds died (they were more sensitive than humans to the agents used at the time) the soldiers knew it was time to don their gas masks.]

Transit police attending the focus groups voiced the need for a fixed detection system that could continuously monitor subway systems-a matter of great sensitivity to them considering the Tokyo Sarin attack. They would like a series of detectors placed throughout a subway system that periodically (e.g., every 15 minutes) sampled the air for a variety of NBC agents and transmitted the results to a command post. The system needs to be highly accurate, with very low false alarm rates.

A similar technology was desired to detect and identify agents in large public, high-risk locations, such as stadiums and arenas. At a minimum, respondents want to be able to monitor the presence of a chemical or biological risk, and then quickly to characterize the risk by at least the class of agents (e.g., nerve gases).

Two police officials described need for the ability to detect the presence of substances used to manufacture chemical and biological weapons, such as Sarin or Ricin. The ability to determine where such substances are stored or manufactured was considered highly desirable. A related capability that was mentioned was to be able to monitor ingress and egress from sites where potentially dangerous biological substances are stored or manufactured for legitimate use. Such monitoring (presumably by the private sector) would help defend against the theft and criminal use of these raw materials.

An officer of a rural police agency stressed the importance of being able to detect the components for manufacturing NBC weapons. While NBC attacks on his population are unlikely, attacks on large urban centers might be planned from locations in his jurisdiction and the weapons used in the attacks assembled there. He currently does not have the technology to recognize components of chemical or biological agents even if they were seized during a search by his officers. His fear is that a Tokyo Sarin-style attack will occur and that when the perpetrators are identified they will be tracked back to an abandoned farm where they could have been stopped had local law enforcement known what to look for and how to identify it.

One agency identified a need for an expert system with a query capability to assist local law enforcement in identifying what threat they were facing. They would like to be able to enter what they know about a possible NBC threat situation and have the expert system help them identify the agent and suggest an appropriate response. For example, if the victims presented symptoms such as difficulty breathing, drooling, nausea, twitching and pinpointing of the pupils, the system would suggest that a nerve agent had been present. The expert system would suggest testing for the nerve agent; recommend application of nerve agent antidotes; and recommend ventilating the building to dissipate the gas.

Somewhat surprising was the relatively infrequent mention of the need to detect NBC problems in water supplies, and also the infrequent discussion of nuclear/radiological threats, considering their enormous potential for mass casualties. Almost all of the interview discussions dealt with only the airborne chemical and biological agents aspects of the NBC threat. Only two agencies raised the need for NBC detectors in water supplies. This could be because recent threats involved airborne agents and these are the situations that come to mind most quickly. It is also possible that terrorist threats against water supplies simply were not scenarios that occurred to the participants at the time of their session.

Regarding the few mentions of nuclear/radiological threats, detection and defense against nuclear materials are just becoming topics of concern in most agencies. Some of the participants noted that this is considered a federal problem beyond local capabilities. Only four agencies noted the need for increased availability of radiation detectors, and the desirability of smaller, hand-held, reliable radiation detectors that were affordable and widely distributed.

Protection

Close behind detection capabilities was the expressed need to have better protection against NBC agents for law enforcement personnel.

In 45 sessions participants spoke of their unmet needs for protective suits. Forty-two of these sessions stressed the need to protect both first responders and the personnel assigned to special teams that would deal directly with NBC situations. For the specialists, a high level of protection was desired; six interviewees suggested that self-contained breathing apparatus (SCBA) be part of the NBC protective equipment. Three agencies requested suits that fit over standard SCBAs. Work underway at Sandia National Laboratory to create a "chemical lab on a [computer] chip" was discussed in one large city interview as allowing development of "smart" protective ensembles that could alert the wearer to an NBC agent and even administer an antidote or prophylaxes.

A more affordable, widely available, basic NBC protective suit for first responders was cited as a need in five sessions (as distinguished from the more comprehensive protection outfits for NBC specialists). One participant expressed the opposite view: that first responders should not be issued protective clothing and equipment so they would not proceed into areas that should be reserved for the local hazardous materials (HAZMAT) or bomb team. A common theme in the interviews was that the standard operating procedures for law enforcement officers was not to handle an NBC situation themselves, but rather to call in other local or federal agencies. Others felt that local law enforcement has no choice but to become better prepared and protected because, at best, "it will take 6-12 hours or more for the feds to be able to get here."

Four sessions added a specific need for better NBC masks. The masks must be easy to operate, allow the wearer to perform his or her duties, be affordable, not require extensive training in their use, and have a long "shelf life."

Positive pressure SCBA's used by fire departments have been identified as effective against many agents. However, they have a limited applicability as they hold only enough air for about 20 minutes of use and are not usually available to law enforcement. Participants in six sessions identified a need for the development of a law enforcement SCBA that would allow SWAT teams and bomb technicians to operate in contaminated environments.

Participants in one session identified a need for more readily accessible vaccines, antidotes, and prophylaxes. It was unclear to them where these would come from or how they would be deployed in the event of an attack.

NBC Decontamination and Containment

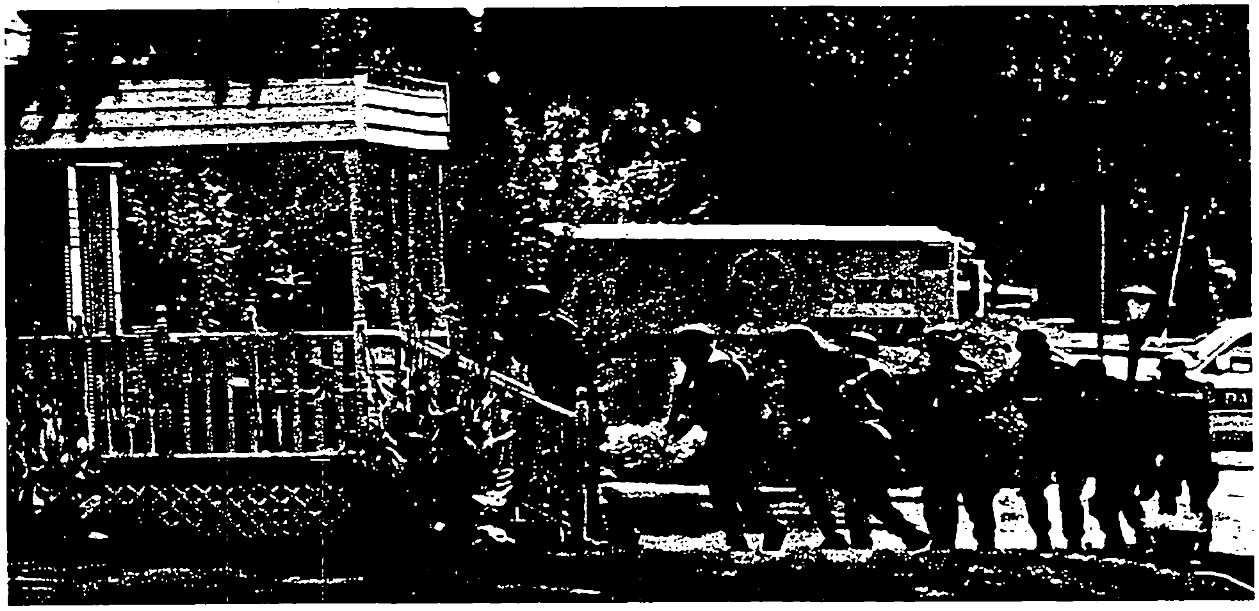
Participants in eight sessions identified needs for NBC decontamination and containment. Decontamination is generally not a law enforcement responsibility, but these interviewees recognized that it is an integral part of the response to an NBC attack. There is a concern that planners are not clearly visualizing the need to care for hundreds, thousands, or even tens of thousands of people who may be exposed to chemical or biological agents. Further, the first responders may spread the contaminate as they attempt to rescue the initial victims. The contaminate may be transferred to ambulances, hospitals, and health workers if decontamination technology is not available quickly.

There is a need for mobile, easy to operate, decontamination systems that can be set up at the perimeter of an attack for decontamination of victims and rescue workers. It is important that the system decontaminate victims quickly. There were suggestions for mobile units (at least the size of buses) that could be brought to a scene to effect decontamination. Large numbers of vehicles may need decontamination. In eight sessions, interviewees stated that the speed of the operation is important, with four sessions identifying it as a top five need.

Containment of the people exposed to NBC, to minimize further exposures, was another major concern. One capability mentioned was for an emergency vehicle or bus with containment capability, to transport victims to decontamination sites. Another capability mentioned was the need for sturdier NBC protective garments for law enforcement officials that could withstand the pulling and pushing of a mob, and allow mobility when wearing the suit. This would allow law enforcement officials to help handle crowds and perform other functions.

A handful of respondents cited the need to be able to contain suspected explosive devices with NBC components. This was discussed in the section dealing with the detection, disablement, and containment of explosive devices. Most explosive containment vessels are designed to "vent" the force of the blast up and away from people. Unfortunately, such a system would "vent" the NBC agent into the surrounding atmosphere.

APPREHENSION AND NEUTRALIZATION NEEDS



Although police officers perform generally similar work on a daily basis, apprehending terrorists presents some unique needs. Terrorists tend to be more heavily armed than the "common" criminal. They also tend to me more motivated. As such they tend to be less concerned with their own lives, if not the lives of others. This makes them more difficult to negotiate with and so to apprehend and neutralize.

More than two-thirds of the participants cited a need for improvement in their apprehension technology. Nearly one in every four sessions considered an apprehension technology one of their top five concerns. The apprehension technology needs identified by participants were grouped into six categories, described in the following paragraphs. They are cataloged in Table C-8.

Nonlethal Weapons

Nonlethal weapons refer to technology intended to neutralize a suspect without causing serious bodily harm. Nonlethal weapons technology identified by the participants included chemical agents, stun devices, vehicle-disabling technology, nets, sticky foams, and frangible ammunition.[12]

Participants identified a need for nonlethal apprehension technology in almost one-third of the interview and focus group sessions (27); six considered nonlethal apprehension technology a top five need. Significantly more agencies in the Western region mentioned a need in this area versus other regions, but all regions were represented.

Chemical Agents–Eight agencies identified a desire for improved chemical agents and dispensers. One specific need was for a portable, high-volume tear gas dispenser about the size of a fire extinguisher and capable of delivering a medium amount of gas. A high priority was an odorless, non-flammable sleeping gas. Several members requested a "sleeping gas" that would be effective on crowds or small groups of people (this was mentioned frequently for riot control, too).

Stunning Weapons–Eight interview sessions identified the need for various stun-type weapon improvements. One participant considered a wireless Taser-like device to be a top five concern. Other members felt that they needed a longer range Taser-like device, one that could penetrate clothing. Yet others said that a beam-based Taser-like weapon whose power setting could be altered would be very useful. One participant felt that an "acoustical stunning weapon" was a top five technology need.

Vehicle Ignition Disabling Device–Vehicle ignition disabling technology was cited as an apprehension technology need in 10 interview and focus group sessions. Two participants identified this technology as a top five concern.

"Net Guns" and "Glue Guns"–A number of interviewees identified a need for "net guns" and "glue guns." These are developmental technologies designed to effectively

[12] Non-lethal weapons are also used for riot control, and are further discussed below.

immobilize criminal suspects. "Glue guns" project a sticky foam that prevents targets from moving. "Net guns" are deployed from projectiles fired from standard grenade launchers. These "guns" have not been field tested or deployed for civilian law enforcement use, primarily due to very real safety/lethality concerns. One Washington, D.C. area agency considered net guns to be a top five concern. However, in one of the few negatives voiced about any technology, one Western region participant was adamantly opposed to glue guns, demanding to know what an agency was expected to do with a suspect after he had been "glued."

Frangible Ammunition–One Western region participant called for more non-lethal ammunition to be made available. This ammunition would be similar to current ceramic ammunition that can break apart and stun a person without killing or ricocheting.

Conventional Weapons Technology

A variety of conventional weapons and weapons-related technology is needed to apprehend or neutralize terrorist suspects. Lethal weapons technology needs were identified by 15 agencies from all regions, with several agencies mentioning better weapons among their top five concerns. Most of the needs expressed here were for technologies that are currently available, but not available to the represented agencies.

Sighting Systems–Eight law enforcement agencies identified a need for improved gun sights. Included were longer-range scopes, night vision scopes, more affordable sighting technology, and laser-assisted sighting systems. (The latter was mentioned by five agencies.)

Weapon Security–One official identified a top five need for a palm print recognition system or other way to provide a safety mechanism should officers lose control of their sidearms. The official felt that current electronic chip technology was probably fast enough to develop this type of scan without adversely impacting officer response times.

Ammunition–One focus group felt the need for either development or identification of a better multipurpose round of ammunition.

Firearms–One participant requested a weapon or technique for highly accurate sniper shooting through glass (e.g., through a house or storefront window). Another participant identified a top five need for silenced and suppressed long-range weapons, in order to prevent officers from revealing their positions while engaging targets. Other participants in several sessions identified needs for firearms that are currently available, but that their agencies do not have. Among the needs they identified were weapons in the .223 caliber range, larger caliber handguns, MP5 submachine guns, and .50 caliber machine guns for armored vehicles. One survey participant considered the need for more MP5 submachine guns or their equivalent a top five concern.

Assault (Armored) Vehicles

The need for specially tailored armored assault vehicles was identified in 12 sessions. The capabilities that were described for such a vehicle are for the most part available today or could be made available with some modification of existing vehicles. One participant noted the need for an affordable armored vehicle. Another participant noted the requirement for making patrol cars usable in this role. Among the other capabilities desired in armored assault vehicles were:

- Several survey members called for armored vehicles with an appearance like an armored Suburban, similar to those used by the Secret Service. They felt that the less attention the vehicle attracted, the better their chances for a successful operation.

- One Washington, D.C. area respondent considered the need for an amphibious armored vehicle a top five concern. Other sessions, notably Western areas, wanted vehicles able to carry and protect an assault team over open terrain. Several sessions called for armored vehicles to be all-terrain, armored to withstand at least assault-rifle-caliber rounds if not more, have "run flat" tires, and be able to move quickly. A common view was that vehicles should be able to safely deliver entry teams, perform rescue operations, and carry lethal and nonlethal weapons.

- Several agencies felt that the armored vehicle's function was to deliver entry teams of approximately 10 people into hazardous conditions. Several sessions called for vehicles with rear-facing exit ramps. Some interviewees want the vehicles to carry hazardous environment detectors to sample the air before officers exit.

- Several sessions identified a need for armored vehicles capable of rescuing downed officers via a chute-like entry or other appropriate mechanism, and hatches in the bottom of the vehicle, to collect a wounded person.

- Several sessions called for vehicles armed with heavy-caliber automatic weapons. Others identified a need for multiple firing ports. Several called for vehicles capable of delivering nonlethal chemical or other agents. One session felt that an armored car should carry approximately an hour's worth of pepper spray-type material or the equivalent. One Washington, D.C. area session called for armored vehicles mounted with net-guns.

- Several agencies called for vehicles to be equipped with sophisticated imaging and communications technology, night vision, and thermal imaging cameras. One agency felt that the vehicle should have the capability of a mobile command post, carrying fax, cell phone, and digital communications links to intelligence systems and to communications and other tactical units. One felt that electronic controls should be installed to allow for remote operation of armored vehicles.

Personal Protective Equipment (PPE)

Law enforcement officers are routinely issued various forms of PPE, such as bulletproof vests. Apprehending terrorist subjects, however, can involve higher threat levels than are found in routine police work, and 11 interview or focus group sessions raised the need for improvements, including the following:

Better Body Armor–Nine interviewees identified the need for stronger, lighter, and more flexible body armor. Several noted that their PPE must be capable of withstanding military assault weapons. One participant complained that his body armor was so rigid he felt like a turtle on its back when knocked down. Several participants, including one who called it a top five concern, identified a need for tactical body armor with pockets. The respondents envisioned armor that also includes a tactical assault harness and vest.

Weapons Retention Holster–In addition to the previously mentioned palm print identification safety lock for sidearms, another session identified a need for a more advanced weapon retention holster. The survey participants felt that current technology still did not do enough to prevent a criminal from gaining access to officers' sidearms.

Wall Breaching Technology

Breaching technology refers to devices used by law enforcement officers to gain access by physical or mechanical force into structures. Breaching technology is used to open doors or walls in dynamic entry situations where officers must seize the element of surprise. A particular problem associated with performing this operation is locating the best access location.

A need for better breaching technology was identified by 10 law enforcement agencies interviewed. Three considered it a top five need. The following represent some of the desired areas of improvement:

Door and Wall Breaching Tools–Several participants identified a need for improved tools to breach doors and walls faster and more successfully. One respondent described the need for a "six-foot long, hole punch-like" device to breach through walls. Another participant visualized a high-powered water cannon to breach doors.

Silent Penetration Technology–Several sessions, including one that identified it as a top five concern, called for development of silent or clandestine breaching capability. Silent wall penetration and door opening technology would preserve the element of surprise.

Sensing and Modeling of Entry Points–Several participants, including one who identified it as a top five concern, called for computer-based sensing technology that can scan a wall's structure and identify the best entry point. The envisioned technology would display the results of the scan on a computer monitor of some form to allow officers to "see" the weakest or easiest access point.

Shaped Explosive Charges–Two agencies wanted greater understanding of and capability for shaped explosive charges, which direct a controlled explosive force to breach a target. Shaped explosives can be problematic if the person placing them is not aware of the amount needed to breach a wall or door. Using too much explosive can injure or kill suspects and hostages. One participant felt that the previously mentioned scanning technology would assist in determining how much explosive should be used. Another survey participant said he could not use shaped charges because of state law.

Helicopters and Boats

Several sessions called for improvements to their helicopters involving existing technologies, including bulletproof shields, hoisting systems, and infrared image systems. However, one Western state official said that they had received surplus military helicopters, but had been forced to return them because of the stigma attached to helicopters by some Western residents. He noted that some local community law enforcement agencies did not want a state law enforcement helicopter flying over their jurisdictions without warning or permission.

One Southern official identified a need for patrol boats capable of "running with whatever terrorists might be using," as was discussed in the section on site security.

Other Apprehension Technologies

A wide variety of other needs were raised for assisting in apprehension, including the following (See Table C-8 for the full list.):

Night Vision Goggles–Improved night vision goggles were discussed as part of surveillance equipment above. Ten sessions raised the need for improved or more affordable night vision for both assaults and apprehension. Virtually all of the other technologies discussed under surveillance are applicable to apprehension, too.

Computerized Terrorist Database–Session participants identified a need for access to an updated terrorist database for use in apprehending suspects as well as gathering intelligence. The data would reveal whether a suspect was indeed linked to terrorist activities. Also desired was a means for identifying a suspect (e.g., through automated fingerprint search). These ideas are expanded upon under the intelligence and forensics subsections, respectively.

Officer Tracking Technology–Several sessions called for technology that can track the status and locations of law enforcement officials moving about the scene of an incident for situation awareness, safety, and tactics.

Standoff Weapons Detector –Participants in several sessions, including one that considered it a top five concern, cited a need for technology that, from a safe distance, can determine whether a suspect is armed. (This is a more specialized and easier to fulfill version of the need to detect the presence of any weapons among a group of people.)

Hostage Communication Technology–Several sessions called for technology that would allow them to better communicate with hostages. One session suggested the possible use of a device that could use a laser beam to write or display messages. Another called for secure wireless communication technology that can be slipped to hostages.

FORENSICS AND INVESTIGATION NEEDS

Detailed investigation of a crime scene and careful examination of the evidence associated with that crime are crucial to successful prosecution, whether that crime is a common criminal act or an act of terrorism. This is particularly difficult with respect to incidents involving weapons of mass destruction, where the crime scene may extend over a large area (a city block or more). The devastation associated with a massive explosive device can be expected to make collection difficult in the extreme. Evidence may simply be destroyed, or massive amounts of rubble might have to be moved to get at it. Evidence collection may have to occur concurrently with rescue operations, which would take priority. Gathering potentially contaminated evidence at the site of an NBC attack would be even more difficult, if not impossible. Investigators would have to wear protective garments. Exposure to radiation would have to be closely monitored and strictly limited.

The forensics and investigation needs identified by participants have been captured in eleven categories, detailed in Table C-9.

Detection and Analysis of Materials at the Scene

It is desirable to perform as much analysis of materials at the scene as possible, for faster results and quicker identification of suspects. Fifteen agencies identified speedier detection and analysis of materials at the scene as among the capabilities needed, with three of them listing it as one of their top five priorities.

A variety of specific portable analysis needs were identified, most frequently the ability to analyze explosive evidence on the scene. This requires the ability to identify a broad range of chemicals and explosives and to identify components of the explosives as well as the explosives themselves.

Participants specified the need to quickly detect and identify metal and other substances, including shell casings and metal fragments. They also want a mass spectral analysis database on a CD-ROM in the field, to help in identifying unknown materials, including signatures of substances that might reveal the manufacturer and place of sale.

It also is necessary to be able to gather evidence in a hazardous environment, such as would result from the use of an NBC device. Flexible protective garments that allow dexterous manipulation of evidence by forensic analysts on the scene would help, as would having portable analysis equipment.

Explosives Tracing

To improve tracing of explosives, whether using field or laboratory techniques, participants want to have a computerized database on explosives. Ideally, this would be a national directory of bomb components, cross-referenced to known or convicted bombers to help identify likely perpetrators. Adding taggants to explosives and other materials used to make explosives would assist in tracing them.

Rapid Suspect and Victim Identification

Six of the law enforcement agencies interviewed pointed out the desirability for more rapidly identifying suspects. One specific need is for a portable scanner for fingerprints and palm prints, which could be used on the scene to identify suspects and transmit prints to other agencies. The same technology could be used for identifying victims (see below). Some form of portable DNA technology and associated database was also suggested. These methods would be used to identify a suspect in custody on the scene, or a print left behind. Also needed is a faster method of identifying the existence of fingerprints, such as by rapidly disseminating fingerprint dusting powder in a room via a "bug bomb" type of device, to quickly bring out all the prints in the room.

Other Forensic Reference Databases

A number of departments proposed databases other than for explosives to assist in their investigations: a database on purchasers of government surplus military supplies (frequently made by militias); a database on purchasers of unusual quantities of chemicals or fuels used for explosives; reference materials used by terrorists (e.g., Internet descriptions of common components of bombs), and a database on local technological resources (e.g., special analysis tools) available to aid in investigations. By far the database most in demand is one that would track terrorists and their activities as well as methods employed. This type of data also is discussed under the intelligence section.

De-encryption

It is becoming more frequent to find that the data seized from the computers of terrorists and other criminals have been encrypted, mostly at what is known as the "Pretty Good Privacy" (PGP) level. Agencies need tools to de-encrypt the seized data rapidly. (See this subject discussed under the section on Cyberterrorism.)

Gun and Bullet Analysis

Another forensic need is to identify bullet shells found at a crime scene. One agency proposed an online, nationwide ballistics comparison system, with readily accessible relational databases. If one can immediately determine the kind of gun that fired a round, investigations can proceed more quickly. One agency noted the need to match ballistics from high-caliber rounds, something that is difficult today.

Rapid Identification of Mass Fatalities

Major terrorist incidents can result in mass casualties. It is both humane and forensically useful to identify the fatalities quickly and to preserve their remains. The former could be done with the previously mentioned portable palm or fingerprint scanning device. Portable morgues with cooling can help preserve the remains and any evidence associated with them. It is also good police work to separate the remains of the suspects from those of the victims.

Lie Detectors

Participants talked about needing more accurate, portable, easier to use, and affordable lie detectors. One agency suggested the desirability of a hybrid voice-stress analyzer/lie detector device.

Photo Recording of Evidence

It is helpful to be able to quickly transmit high-resolution video and/or photos from the field (e.g., with digital cameras). The same capability can be useful for surveillance and intelligence.

One agency suggested that to record evidence, a wireless video camera attached to bomb search dogs would be very useful.

Laboratory Equipment

A continued theme was reducing the costs of existing forensics laboratory equipment such as scanning electron microscopes.

Other Needs

Four other needs received at least one citation. These were: computer modeling tools to recreate and analyze a crime scene; better technology to identify fraudulent documents; better ways to prevent evidence contamination; and a need for some means of positive position location (GPS was cited) to mark and identify crime scenes in rural areas.

PUBLIC INFORMATION NEEDS

State and local law enforcement have four primary concerns regarding public information. The first is ensuring that accurate information is provided to the public to promote safety. The extent of the affected area, evacuation routes, and appropriate actions to take are all elements of information the release of which must be quickly and accurately broadcast. At the same time, law enforcement needs to protect key information the release of which may compromise evidence or ongoing or planned operations. It also needs to minimize the physical impact of media coverage on operations. Finally, law enforcement needs to communicate information to the public that will elicit its support in preventing or solving terrorist incidents. An example of this is the nationwide distribution of the composite drawings of the suspects in the Murrah Federal Building bombing.

The public information needs expressed by the participants have been captured in four categories: methods of getting accurate, consistent information to the public; protecting preparations and tactics; minimizing the adverse impact of media actions on operations; and soliciting public assistance in resolving terrorist acts. These needs are detailed in Table C-10. It is worth noting that, other than communications technology for the most part already addressed in the section on Command, Control, and Communications (C^3), the needs expressed in this section should be addressable with existing technology.

Disseminating Information to the Public

Twelve law enforcement agencies expressed the need for new or enhanced technology to get accurate, consistent information to the public. These needs include both new and existing technology. Among the needs expressed were:

- improved emergency broadcast capability;
- a local version of the emergency broadcast network (with the ability to break into local media programs);
- video-teleconferencing with the media;
- incident site-to-media communications;
- improved communication links between the public information officers of different agencies;
- mobile faxes for public information officers (PIOs); and
- frequently updated Web pages to which the public could refer for information.

One agency suggested the need for on-the-scene public service announcements (PSAs)

Another idea that originated in one of the interviews was for electronic billboards that could be carried in and deployed externally on squad cars. The billboard would provide information and directions to the public on a sign that repeated the information.

In case of an evacuation, one law enforcement agency suggested the desirability of a "leave behind" public information booth with evacuation information. It could feature a repeating audio output and the ability to answer citizens' queries via computer.

Many police departments use local volunteers to help spread information to their communities during emergencies. Simple technological aids to the volunteers to help them identify themselves and provide information to the public were suggested.

Protecting Preparations and Tactics

When television broadcasts police operations live during a major incident, terrorists under siege can be forewarned of the plans to capture them. At least eight law enforcement agencies suggested the need to screen their preparations for handling terrorists from the media. Their requirements include passive, portable screens or curtains to shield movements (the U.K. police use curtains), limiting broadcasts from the scene, and encrypting police and PIO communications [also addressed in the section on Command, Control, and Communications (C^3).[13] Clearly, this is a difficult issue because law enforcement must consider First Amendment concerns as well.

Minimizing the Adverse Impact of Media Presence on Operations

Several participants expressed concern about how media operations sometimes interfere with radio or other communications of law enforcement agencies. They want to have non-jammable communications capabilities. Electromagnetic radiation from the media may also interfere with remote control robots, set off bombs that use triggering transmitters, and interfere with other equipment. There is a need to ensure this does not happen. There also is concern about media aircraft violations of airspace. Many of these issues of media interference can be dealt with simply by negotiation. However, interviewees also are calling for technological safeguards, especially when security and clandestine preparations are being made.

Eliciting Information from the Public

Participants noted needing not only better ways for disseminating information *to* the public, but also improved methods for obtaining information *from* the public. Technology can help, they suggest, by enabling a Web site to be established so they can both provide and collect information on the terrorists.

[13] As noted earlier in the section on Command, Control, and Communications (C^3), another alternative is to cut off communications to the terrorists under siege. Police sometimes simply cut the TV cable going into a building, but it may not be readily accessible or may be in the line of fire. That also still permits through-the-airreception.

CROWD AND RIOT CONTROL NEEDS

Terrorist incidents tend to generate panic and/or a high degree of interest, and can so cause crowds or riots. Dealing with crowds and riots is a particularly vexing law enforcement challenge, especially in regard to minimizing potential injuries. Technology needs in this area were organized into six categories (Nonlethal Crowd Control, Personal Protective Gear for Law Officers, Language Translation Capability, Barricades, Predicting Crowd Dynamics, and Direct Video Transmission). They are detailed in Table C-11.

Nonlethal Crowd Control

A capability desired by 24 law enforcement agencies is to improve nonlethal agents that either disperse or incapacitate a threatening crowd. The same agents often might be used on terrorists themselves, as discussed in the apprehension section above.

Current nonlethal agents include, among other things, gases, pepper spray, Taser-like devices, beanbags, rubber bullets, slippery materials, and water. Sixteen agencies want further refinements in non-lethal technologies, and three consider this need among their top five priorities.

Certain interviewees want to be able to selectively apply agents that are non-painful and immediately effective. They need the agents to either temporarily stun, paralyze, or otherwise incapacitate crowds for between one to twenty minutes—the duration to be chosen by law enforcement. They would like to have the ability to covertly deliver materials, and they call for portable, nonlethal agents that can be used by a single officer. Some respondents want to be able to target the agents to an individual or a group and to a specific part of the body. The "dose" needs to be adjustable for the size of the space. For gases or other agents that affect the body, it is desired to have antidotes immediately available. Nonlethal stun agents should be able to penetrate clothing (unlike some existing Taser-like devices), according to the participants.

In some sessions interviewees mentioned that they would like to be able to apply nonlethal agents to stationary or moving targets and to select the range from 20 to 100 yards (rock-throwing distance). If a gas or other agent affects the body, it should be nonlethal for children and adults, including individuals with asthma or other ailments. The launcher or application device needs to be instantly rechargeable. Finally, law officers want the agent removable quickly after the event.

Personal Protective Gear for Law Enforcers

Various participants noted that police officers need better riot control shields, gas masks, and in some cases, bullet-resistant barriers to protect themselves from crowds and the effects of agents they apply for dispersing or incapacitating crowds.

Four law enforcement agencies expressed the need for improved riot control shields that are lighter and stronger than the current ones, and ballistically "more sound." The shields need to be shatterproof.

Gas masks used by law enforcement to work in the presence of tear gas or other agents need to be lighter and most importantly, "actually work." "Many current ones do not filter well, or they leak," said one police official.

Some participants also want an improved barrier that can stand up on its own and allow officers to operate safely behind it. Preferably the barriers will deflect a rifle shot and have viewing ports. These protective masks, because they only need to deal with nonlethal incapacitating agents, may be less expensive and utilize different technology than protective masks designed to address lethal chemical threats.

A police official pointed out that officers who wear protective outfits and try to deal with unprotected crowds fleeing from a chemical attack (or any NBC agent) would not have normal flexibility and mobility because of the suit. They also might be in danger of people trying to seize the suit–another reason for developing flexible, strong suits. Having to stock several types of protective suits poses a logistics problem and is expensive, but consideration is needed to providing stronger, crowd-resistant suits.

Language Translation Capability

Police need to communicate with non-English speaking crowds and require an automatic translation capability that allows an official to speak in English and deliver a message in any one of a variety of selected languages common in the community. A less complicated option is to have the capability to broadcast pre-recorded or even on-scene recorded messages in foreign languages, using stock phrases appropriate to the specific emergency. The languages needed run a wide gamut corresponding to the populations in the United States, from widely-used languages like Spanish to more unusual languages such as Hmong or Farsi.

Crowd Barricades

Police need improved, lightweight barricades to hold back and channel crowds. These barricades, it was suggested, could be carried in a patrol car and inflated when needed. Several participants suggested that the barricades come equipped with remote audio capability and small cameras to help communicate with and observe the crowd.

Predicting Crowd Dynamics

One law enforcement agency suggested developing a computer model that could predict likely crowd reactions given inputs on the circumstances of the situation, the weather, the nature of the space, and crowd size. The output would be the consequences in the event of a required evacuation or the insertion of riot control substances, to predict which way the crowd might respond.

Direct Video Transmission

One agency considered it very important to be able to transmit live video pictures from the field to police headquarters so that senior police officials could monitor the progress of a riot or potential crowd problem and give advice to the incident. It was suggested that the capability to transmit video directly from a patrol car to headquarters would be desirable.[14]

[14] Many traffic -assigned patrol cars can videotape but not transmit. Helicopters are often used for getting an overview, but are not always available to police agencies, especially in the smaller and more rural areas.

TRAINING AND OTHER NEEDS

During the course of the interviews, participants sometimes mentioned needs or presented ideas that did fall neatly into the categories discussed before. Following is a collection of miscellaneous other topics, especially training needs, they wanted to have aired. These needs are listed in Table C-12.

Training to Combat Terrorism

By far the most often cited "other need" was training. Fully 31 interview sessions identified the need for more training, with nine of the statements being among the top five priorities of the agencies that commented. Eight law enforcement agencies said that there must be training to accompany any new technology. Too often, they said, technologies are sent to the field without adequate training being provided, leaving many sophisticated technical solutions unused. Lack of training also leads to maintenance problems.

There was a very strong desire for computer-based training tools, preferably virtual reality systems that allow hands-on training for specialist tasks and interactive training for war gaming terrorist situations. Computerized training modules are desired for Explosive Ordnance Device (EOD) detection, EOD disarmament, NBC defense, dynamic entry (explosive) breaching, collapse rescue, and command strategies. It was considered especially desirable to be able to practice disabling explosive devices using virtual reality. Another potential application of virtual reality is as an enhancement for marksmanship and rules of engagement ("shoot"/"no - shoot") training. Several police agencies pointed out the high expense associated with sending specialists out of the area to train, and said that much money could be saved with realistic training at home. Second best would be to establish regional centers with virtual reality simulators.

If realistic simulations of terrorist events can be created on the computer, they could be used for training multiple agencies simultaneously at their home positions. The same tools might also be used during an actual event to explore different strategies or look up what had been tried before. This technology would incorporate such information as potential targets such as abortion clinics and other lesser known targets; traffic loading for various likely evacuation routes; evacuation plans; and layout and alternate points of entry at primary targets.

Information on Available Technology to Combat Terrorism

Participants in 12 sessions also described a need for a searchable database or an "information clearinghouse" to quickly identify the available technological resources and how to obtain them. The agencies sometimes want to know where to obtain a particular technology (e.g., NBC protective suits, explosives containment vessels) and sometimes what technology is appropriate or available for a particular situation. Some of the interviewees described the concept as a Web page or national information source they could log onto from their computers. Others described a "clearinghouse" that they could call or e-mail.

Standards and Testing

Several law enforcement agencies raised the need for standards for the development and testing of new technology. There was a strong desire that feedback be collected from the initial field use of new technology, so that it could be refined or withdrawn if need be. There was criticism for not being prepared to produce second or third generations of technologies based on field experience. One agency suggested the desirability of a "Consumer Reports" periodical on new technology for combating terrorism.

Chapter IV. Conclusions

SALIENT FINDINGS

There appear to be five salient observations that can be drawn from this inventory. These are:

Similarity of Needs Across Regions

The technology needs expressed by the participants in the individual interviews and group discussion sessions were remarkably similar across the nation, with minor regional differences. For example, some agencies in communities in mountainous areas have problems with communications connectivity. On the other hand, agencies in jurisdictions with large, flat, open terrain have difficulty undertaking surveillance operations.

Issue of Affordability

Affordability appears to be perhaps the overarching concern of state and local law enforcement agencies. If a technology is not affordable, it might as well not exist. Many participants stated that they lacked critical equipment and material because their agencies cannot afford it. As a result, state and local law enforcement are often less well-equipped than the potential terrorists they face. State and local officials may only have 286- and 386-class personal computers, while their adversaries are equipped with the latest Pentium-based models. It appears, at this point, that many, if not most, of the needs captured in this document could be met by existing technology. For example, improved night vision devices, improved armored vehicles, and mobile facsimile machines are all available. The question is one of affordability. Many participants suggested a reassessment of the architecture of the law enforcement system, specifically in regard to sharing the technology needed to combat terrorism, as one means to get at the issue of affordability.

Critical Deficiencies

State and local law enforcement are particularly concerned about their ability to deal with weapons of mass destruction, specifically NBC devices. Part of the problem, again, is the issue of affordability. Many participants commented that they find it hard to defend budgets for equipment that might only rarely, if ever, be used, even if it could help avert catastrophe if purchased. Many observed that to deal with NBC threats they would have to rely on the federal government. Yet another part of the problem appears to be a lack of understanding of the nature of the threat and the training needed to deal with it. The federally-sponsored initiatives to help state and local governments prepare to deal with the use of a weapon of mass destruction by terrorists have focused on emergency services personnel and senior managers.

Another troubling concern is that state and local law enforcement on the whole appear to lack the ability to effectively combat cyberterrorism. As the President's Commission on Critical Infrastructure Protection noted in its report of October 1997:

> 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 cyber threats before they materialize and produce major system damage.[15]

There are a number of dimensions to this problem, including a lack of appropriate equipment and software (as a result of funding constraints), and a lack of trained personnel. This is also a relatively new threat that 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 can expand the scope of what are routine police functions, thereby creating a need for new technology. A crime scene covering several city blocks or a traffic jam caused by a mass evacuation pose unique technology-linked challenges in the area of forensics and traffic management.

While state and local law enforcement generally can deal with common criminal acts using their own resources, they understand that combating organized terrorism requires cooperation among state, local and Federal law enforcement agencies, as well as with other types of agencies (emergency management, etc.). This cooperation requires improved information and communications technologies—particularly technologies that facilitate access to and sharing of intelligence among disparate agencies. Organized terrorism in general is interjurisdictional, interstate and international in nature. To combat it, state and local law enforcement must cooperate with each other and with federal agencies.

Commonality of Law Enforcement Technology Needs

Many of the capabilities needed to combat terrorism are capabilities that also are needed to combat crime in general, with the possible exception of the capability to address the threat posed by weapons of mass destruction. As a result, the technology needs expressed by participants in this inventory appear to correspond well with the technology development efforts NIJ has undertaken to address law enforcement needs in general. Differences in the priority assigned to the development of technologies by the Law Enforcement and Corrections Technology Advisory Council (LECTAC), which is based on generic law enforcement needs, and the priority assigned to them by participants in this inventory can be attributed to the unique aspects of the problem of combating terrorism. None of the top five priorities identified in this research falls into the top five technology

[15] *The Report of the President's Commission on Critical Infrastructure Protection*, p. 5

development areas established by LECTAC. However, four of the five (except for improved means to detect chemical and biological agents) fall within LECTAC's top 10 areas. The LECTAC is comprised of senior law enforcement and corrections officials from throughout the United States.

FURTHER WORK REQUIRED

This draft report will be shared with participating state and local law enforcement agencies and other knowledgeable bodies to solicit further details on needs and priorities. Concurrently, the assessment of these needs to determine if existing and developmental technology can meet them or if new technology is required will take place to help NIJ structure its research and development efforts. This will be the subject of a separate report that will be distributed as Volume II.

Appendix A - Participating Agencies

PARTICIPATING AGENCIES

Interview Code	*State*	*City (Location)*	*Agency*
W080I	AK	Anchorage	Alaska State Troopers
S027F	AL	Gadsden	Gadsden, Police Department
S026I	AL	Montgomery	Alabama Department of Public Safety
S040I	AR	Little Rock	Arkansas State Police
S027F	AR	Little Rock	Little Rock Police Department
W064I	AZ	Phoenix	Arizona Department of Public Safety
W075I	AZ	Phoenix	State of Arizona Department of Emergency And Military Affairs
W069F	AZ	Phoenix	Phoenix Police Department
W069F	AZ	Tucson	Pima County Sheriff's Department
W060I	CA	City of Commerce	California Department of Justice
W060I	CA	Sacramento	California Department of Justice, Intelligence Branch
W063I	CA	City of Commerce	Los Angeles Police Chief Association
W073I	CA	El Centro	Imperial County Sheriff's Office
W066I	CA	Hemet	Riverside Sheriff's Department
W077I	CA	Los Angeles	Los Angeles Airport Police
W015B	CA	Los Angeles	Los Angeles Police Department
W057B	CA	Los Angeles	Los Angeles Sheriff's Office
W076I	CA	Sacramento	Western States Information Network
W078I	CA	San Bernardino	San Bernardino Sheriff's Department
W069F	CA	San Diego	San Diego Police Department
W069F	CA	San Pedro	Los Angeles Port Department
W072I	CA	Santa Ana	Orange County Sheriff's Department
M038F	CO	Arvada	Arvada Police Department
M038F	CO	Aurora	Aurora Police Department
M038F	CO	Denver	Colorado Department of Public Safety
M029I	CO	Denver	Colorado State Attorney General's Office
M038F	CO	Denver	Colorado State Bureau of Investigation
M038F	CO	Denver	Denver Office of Emergency Management
M081B	CO	Denver	Denver Police Department
M038F	CO	Golden	Colorado State Office of Emergency Management
M037F	CO	Littleton	Arapahoe County Sheriff's Office
M035I	CO	Lakewood	Colorado State Department
E011I	CT	Colchester	Connecticut State Police
C089I	DC	Washington	Metro Transit Police Department
C092B	DC	Washington	Metropolitan Police Department
C0951	DC	Washington	U.S. Park Police
E004F	DE	Wilmington	Wilmington Police Department
S039B	FL	N. Miami Beach	Metro Dade Police Department
S022I	FL	Tallahassee	Florida Department of Law Enforcement
S049F	FL	Tallahassee	Florida Division of Emergency Management

S019B	GA	Atlanta	Atlanta Police Department
S049F	GA	Atlanta	Fulton County Sheriff's Department
S049F	GA	Atlanta	Georgia Emergency Management Agency
S049F	GA	Atlanta	Metropolitan Atlanta Regional Transit Authority
S027F	GA	Decatur	Dekalb County
S041I	GA	Decatur	Georgia Bureau of Investigation
W069F	HI	Honolulu	Honolulu Police Department
E016I	IA	Des Moines	Des Moines Police Department
E009I	IA	Des Moines	Iowa Department of Public Safety
W065I	ID	Coeur D'Alene	North Idaho Antiterrorist Program
S049F	IL	Chicago	Chicago Police Department
S020I	IL	Chicago	Illinois Division of Investigation
S049F	IN	Fort Wayne	Allen County Sheriff's Office
S042I	IN	Indianapolis	Indiana State Police
M083I	KS	Lawrence	Lawrence Police Department
M006I	KS	Leavenworth	Leavenworth Police Department
M031I	KS	Lenexa	Lenexa Police Department
S021I	KY	Columbia	Kentucky State Police
S049F	KY	Frankfort	Kentucky Disaster and Emergency Services
S049F	KY	Lexington	Lexington Police Department
S043I	KY	Louisville	Jefferson County Police Department
S018I	KY	Louisville	Louisville Police Department
S044I	LA	Baton Rouge	Louisiana State Police
S027F	LA	New Orleans	New Orleans Police Department
E001B	MA	Boston	Boston Police Department
C091I	MD		Montgomery County Police Department
E005F	MD	Baltimore	Baltimore Police Department
E004F	MD	Jessup	Maryland State Police
C093I	MD	La Plata	Charles County Sheriff's Department
C094I	MD	Riverdale	Prince George's County Police Department
E023I	ME	Augusta	Kennebeck Co. Sheriff Department, ME
E013I	ME	Sanford	Sanford Police Department
E005F	MI	Detroit	Detroit Police Department
E008I	MI	Lansing	Michigan State Police
E007I	MN	St. Paul	Minnesota Division of Emergency Response
S045I	MO	Jefferson City	Missouri State Highway Patrol
S056I	MS	Jackson	Mississippi Department of Public Safety
S027F	MS	Ocean Springs	Ocean Springs Police Department

M038F	MT	Helena	Lewis & Clark County Sheriff's Office
M051I	MT	Helena	Montana Criminal Investigation Bureau
M034I	MT	Jordan	Garfield County Sheriff's Office
S046I	NC	Charleston	Charleston Police Department
S027F	NC	Greensboro	Greensboro Police Department
S027F	NC	Raleigh	North Carolina Highway Patrol
M079I	ND	Bismarck	Burleigh County Sheriff's Office
M033I	ND	Bismarck	North Dakota Bureau of Criminal Investigation
M038F	ND	Sioux Falls	Sioux Falls Police Department
M028I	NE	Omaha	Omaha Police Department
E096I	NH	Concord	New Hampshire State Police
E005F	NJ	Newark	Newark Police Department
E010I	NJ	West Trenton	New Jersey State Police
M052I	NM	Albuquerque	Albuquerque Police Department
M036I	NM	Santa Fe	New Mexico State Police Department
W068I	NV	Carson City	Nevada Division of Investigations
W059I	NV	Reno	Reno Police Department
E012I	NY	Albany	New York State Police
E005F	NY	Brooklyn	New York City Transit Police Department
E003B	NY	Brooklyn	New York Police Department
E017I	NY	Orchard Park	Erie Co. New York Sheriff's Office
E014I	NY	Yaphank	Suffolk County Police Department
E005F	OH	Cleveland	Cleveland Police Department
E005F	OH	Columbus	Columbus Police Department
E004F	OH	Dayton	Montgomery County Sheriff's Department
M037F	OK	Chickasha	Grady County Sheriff's Office
M037F	OK	El Reno	Canadian County Sheriff's Office
M037F	OK	Norman	Cleveland County Sheriff's Office
M037F	OK	Oklahoma City	7th Judicial District - District Attorney's Office
M037F	OK	Oklahoma City	Oklahoma City Police Department
M037F	OK	Oklahoma City	Oklahoma County Sheriff's Office
M037F	OK	Shawnee	Pottawatomie County Sheriff's Office
M037F	OK	Shawnee	Shawnee Police Department
W058B	OR	Portland	Portland Metro Police Department
W061I	OR	Salem	Oregon State Police
E004F	PA	Hershey	Pennsylvania State Police
E005F	PA	Philadelphia	Philadelphia Police Department
E004F	PA	Pittsburgh	Allegheny County Police Department
E004F	PA	Pittsburgh	Pittsburgh Police Department
E004F	RI	Providence	Providence Police Department

S024I	SC	Columbia	South Carolina State Law Enforcement Division
M082I	SD	Pierre	SD State Department of Radio Communications
S027F	TN	Morristown	Morristown Police Department
S055I	TN	Nashville	Tennessee Bureau of Investigation
M054B	TX	Dallas	Dallas Police Department
W062I	UT	Kearns	Utah Department of Public Safety
W074I	UT	Taylorsville	Utah State Patrol
C087I	VA	Alexandria	Alexandria Police Department
C090I	VA	Annandale	Fairfax County Police Department
C088I	VA	Arlington	Arlington County Police Department
S049F	VA	Norfolk	Norfolk Police Department
S047I	VA	Richmond	Virginia State Police
E097I	VT	Williston	Vermont State Police
W067I	WA	Colfax	Whitman County Sheriff's Office
W071I	WA	Olympia	Washington State Patrol
W084I	WA	Spokane	Spokane Police Department
E002I	WI	Milwaukee	Milwaukee Police Department
S025I	WV	Parkersburg	West Virginia State Police
S048I	WV	South Charleston	West Virginia State Police
M032I	WY	Cheyenne	Cheyenne Police Department
M085I	WY	Cheyenne	State of Wyoming Emergency Management Agency
M050I	WY	Cody	Park County Sheriff's Department

Appendix B - Participants

PARTICIPANTS

ID #	*Rank/Title*	*Specialties*	*Agency*	*City*	*State*
W080I	Sergeant	Coordinator for WSIN	Alaska State Troopers	Anchorage	AK
S026I	Captain	Intelligence	Alabama Department of Public Safety	Montgomery	AL
S026I	Analyst	Intelligence	Alabama Department of Public Safety	Montgomery	AL
S027F	Lieutenant	Planning Officer	Gadsden Police Department	Gadsden	AL
S040I	Lieutenant	Special Investigator	Arkansas State Police	Little Rock	AR
S027F	Captain	Special Investigations Div.	Little Rock Police Department	Little Rock	AR
W069F	Detective	Intelligence	Phoenix Police Department	Phoenix	AZ
W075I	Assistant Director	Response, Recovery and Mitigation	State of Arizona, Department of Emergency and Military Affairs	Phoenix	AZ
W069F	Lieutenant	Intelligence	Pima County Sheriffs Department	Tucson	AZ
W064I	Major	Antiterrorist	Arizona Department of Public Safety	Phoenix	AZ
W057B	Lieutenant	Judicial Protection District Commander	Los Angeles Sheriffs Office	Los Angeles	CA
W057B	Sergeant	Special Investigations	Los Angeles Sheriffs Office	Whittier	CA
W057B	Sergeant	Special Investigations	Los Angeles Sheriffs Office	Whittier	CA
W063I	Executive Director	Executive Director	Los Angeles Police Chief Association	City of Commerce	CA
W076I	Criminal Intel. Analyst	Intelligence	Western States Information Network	Sacramento	CA
W078I	Sheriff Dep. Chief	Intelligence	San Bernardino Sheriffs Department	San Bernardino	CA
W015B	Captain	Antiterrorist	Los Angeles Police Department	Los Angeles	CA
W073I	Chief Deputy	Special Investigations	Imperial County Sheriffs Office	El Centro	CA
W078I	Sheriffs Sergeant	Intelligence	San Bernardino Sheriffs Department	San Bernardino	CA
W057B	Deputy	Special Investigations	Los Angeles Sheriffs Office	Whittier	CA
W069F	Lieutenant	Intelligence	Los Angeles Port Department	San Pedro	CA
W069F	Detective	Intelligence	San Diego Police Department	San Diego	CA
W077I	Lieutenant	Intelligence	Los Angeles Airport Police	Los Angeles	CA
W066I	Lieutenant	SWAT	Riverside Sheriffs Department	Hemet	CA
W072I	Investigator	Special Investigations	Orange County Sheriffs Department	Santa Ana	CA
W060I	Supervisor	Intelligence	State of California Department of Justice, Intelligence Branch	Sacramento	CA
W060I	Research Analyst	Intelligence	State of California Department of Justice, Intelligence Branch	Sacramento	CA
W015B	Commander	Commander, Uniformed Services Group Op.	Los Angeles Police Department	Los Angeles	CA
W057B	Deputy	Emergency Operations	Los Angeles Sheriffs Office	Los Angeles	CA
W057B	Lieutenant	Emergency Operations	Los Angeles Sheriffs Office	Los Angeles	CA
W069F	Detective	Intelligence	San Diego Police Department	San Diego	CA
W060I	Special Agent	Intelligence	California Department of Justice	City of Commerce	CA
W015B	Detective	Antiterrorist Division	Los Angeles Police Department	Los Angeles	CA
W060I	Special Agent	Intelligence	California Department of Justice	City of Commerce	CA

W063I	Criminal Intelligence	Intelligence	Los Angeles Police Chief's Association	City of Commerce	CA
M081B	Lieutenant	Intelligence	Denver Police Department	Denver	CO
M038F	Director	Explosion Emergency Operations	Denver Office of Emergency Management	Denver	CO
M038F	Lieutenant	General Criminal Investigator	Arvada, Colorado Police Department	Arvada	CO
M037F	Sheriff		Arapahoe County Sheriff's Office	Littleton	CO
M029I	Special Investigator	Special Prosecution Unit	Colorado State Attorney General's Office	Denver	CO
M081B	Detective	Bomb Squad	Denver Police Department	Denver	CO
M038F	Captain	Intelligence	Aurora Police Department	Aurora	CO
M038F	Officer	Intelligence	Aurora Police Department	Aurora	CO
M038F	Director	Criminal Investigator	Colorado State Bureau of Investigation	Denver	CO
M035I	Detective	Intelligence	Colorado State Department	Lakewood	CO
M081B	Lieutenant	SWAT	Denver Police Department	Denver	CO
M038F	Director	Antiterrorist Preparations	Colorado Department of Public Safety	Denver	CO
M038F	Director	-	Colorado State Office of Emergency Management	Golden	CO
M081B	Sergeant	Bomb Squad	Denver Police Department	Denver	CO
E011I	Trooper 1st Class	Bomb Technician	Connecticut State Police	Colchester	CT
E011I	Lieutenant	Commanding Officer	Connecticut State Police	Colchester	CT
C092B	Lieutenant	Hostage Negotiator	Metropolitan Police Department	Washington	DC
C095I	Lieutenant	Special Operations Division	U.S. Park Police	Washington	DC
C089I	Sergeant	-	Metro Transit Police Department	Washington	DC
C092B	Captain	SWAT (Emergency Response Team)	Metropolitan Police Department	Washington	DC
C092B	Lieutenant	Intelligence	Metropolitan Police Department	Washington	DC
C089I	Chief	Antiterrorist	Metro Transit Police Department	Washington	DC
E004F	Lieutenant	SWAT, Bomb Unit	Wilmington Police Department	Wilmington	DE
S039B	Officer	Bomb Technician	Metro Dade Police Department	N. Miami Beach	FL
S039B	Sergeant	SWAT	Metro Dade Police Department	N. Miami Beach	FL
S039B	Detective	Investigator	Metro Dade Police Department	N. Miami Beach	FL
S049F	Chief	-	Florida Division of Emergency Management	Tallahassee	FL
S022I	SAC	Intelligence	Florida Department of Law Enforcement	Tallahassee	FL
S019B	Sergeant	SWAT	Atlanta Police Department	Atlanta	GA
S019B	Police Officer	Bomb Technician	Atlanta Police Department	Atlanta	GA
S049F	State Director	-	Georgia Emergency Management Agency	Atlanta	GA
S049F		-	Georgia Emergency Management Agency	Lilburn	GA

S049F	Lieutenant	Consequence Mgt. Coordinator	Georgia Emergency Management Agency	Atlanta	GA
S049F	Director	Dir. Spec. Projects	Georgia Emergency Management Agency	Atlanta	GA
S041I	Special Agent	Bomb Technician	Georgia Bureau of Investigation	Decatur	GA
S041I	Principal Investigator	Special Investigator	Georgia Bureau of Investigation	Decatur	GA
S049F	Chief		Metropolitan Atlanta Regional Transit Authority Police	Atlanta	GA
S027F	Investigator	Investigator	Dekalb County Georgia	Decatur	GA
S049F	Lieutenant	-	Fulton County Sheriffs Department	Atlanta	GA
S049F	Sergeant	-	Fulton County Sheriffs Department	Atlanta	GA
W069F	Lieutenant	Intelligence	Honolulu Police Department	Honolulu	HI
E016I	Sergeant	Tactical Supervisor (SWAT)	Des Moines Police Department	Des Moines	IA
E009I	SAC	Intelligence	Iowa Department of Public Safety	Des Moines	IA
W065I	Coordinator	Intelligence	North Idaho Antiterrorist Program	Coeur D'Alene	ID
S049F	Detective	-	Chicago Police Department	Chicago	IL
S049F	Lieutenant	Intelligence	Chicago Police Department	Chicago	IL
S020I	Chief	Special Investigator	Illinois Division of Investigation	Chicago	IL
S049F	Captain	-	Allen County Sheriffs Office	Fort Wayne	IN
S042I	Lieutenant	Intelligence	Indiana State Police	Indianapolis	IN
S042I	Investigator	Bomb Squad	Indiana State Police	Pendelton	IN
M031I	Captain	SWAT	Lenexa Police Department	Lenexa	KS
M006I	Officer	Bomb Technician	Leavenworth Police Department	Leavenworth	KS
M006I	Lieutenant	Bomb Technician	Leavenworth Police Department	Leavenworth	KS
M083I	Chief of Police	-	Lawrence Police Department	Lawrence	KS
S049F	Manager	Operations	Kentucky Disaster and Emergency Services	Frankfort	KY
S043I	Major	Investigator	Jefferson County Police Department	Louisville	KY
S018I	Lieutenant	Intelligence	Louisville Police Department	Louisville	KY
S021I	Lieutenant	SWAT	Kentucky State Police	Columbia	KY
S049F	Detective	-	Lexington-Fayette County Police Department	Lexington	KY
S027F	Lieutenant	SWAT team	New Orleans Police Department	New Orleans	LA
S044I	Major	Bureau of Investigation	Louisiana State Police	Baton Rouge	LA
S027F	Lieutenant	Intelligence	New Orleans Police Department	New Orleans	LA
E001B	Lt. Detective	Intelligence	Boston Police Department	Boston	MA
E001B	Deputy Supt.	Information Technology	Boston Police Department	Boston	MA
E001B	Dep. Superintendent	Field Services	Boston Police Department	Boston	MA
E001B	Lieutenant	Environmental Safety Group/Special Op.	Boston Police Department	Boston	MA
E001B	Sergeant	Tactical Team Coordinator for SWAT	Boston Police Department	Boston	MA

E004F	Lieutenant	SWAT	Maryland State Police	Jessup	MD
C094I	Captain	Special Operations	Prince George's County Police Department	Riverdale	MD
C093I	Lieutenant	Intelligence	Charles County Sheriff's Department	La Plata	MD
E004F	1st. Sergeant	-	Maryland State Police	Jessup	MD
C091I	Sergeant	-	Montgomery County Police Department		MD
C093I	Corporal	Intelligence	Charles County Sheriff's Department	La Plata	MD
E005F	Lieutenant	SWAT	Baltimore Police Department	Baltimore	MD
E013I	Major	Administration	Sanford Police Department	Sanford	ME
E023I	Sergeant	Operations	Kennebeck Co. Sheriff Department	Augusta	ME
E008I	Inspector	Intelligence	Michigan State Police	Lansing	MI
E005F	Dep. Chief	SWAT	Detroit Police Department	Detroit	MI
E008I	Lieutenant	-	Michigan State Police	Lansing	MI
E007I	SAC	Counterterrorism Task Force	Minnesota Division of Emergency Response	St. Paul	MN
S045I	Captain	Antiterrorist	Missouri State Highway Patrol	Jefferson City	.MO
S056I	Captain	Special Operations	Mississippi Department of Public Safety	Jackson	MS
S027F	Chief	-	Ocean Springs Police Department	Ocean Springs	MS
M051I	Bureau Chief	Special Investigations	Montana Criminal Investigation Bureau	Helena	MT
M034I	Sheriff	Terrorist Control	Garfield County Sheriff's Office	Jordan	MT
M038F	Deputy	Antiterrorist Activities	Lewis & Clark County Sheriff's Office	Helena	MT
S027F	Detective	Special Investigations	Greensboro Police Department	Greensboro	NC
S027F	Major	Director of Research and Planning	North Carolina Highway Patrol	Raleigh	NC
M033I	Chief Agent	Criminal Investigator	North Dakota State Bureau of Criminal Investigation	Bismarck	ND
M079I	Major	Administration/Investigations	Burleigh County Sheriff's Office	Bismarck	ND
M028I	Lieutenant	Bomb Squad	Omaha Police Department	Omaha	NE
E096I	Lieutenant	Special Investigations Unit Coordinator	New Hampshire State Police	Concord	NH
E010I	Captain	Intelligence	New Jersey State Police	West Trenton	NJ
E005F	Lieutenant	SWAT (Emergency Response Team)	Newark Police Department	Newark	NJ
M036I	Captain	SWAT	New Mexico State Police Department	Santa Fe	NM
M052I	Captain	SWAT	Albuquerque Police Department	Albuquerque	NM
W059I	Detective Sergeant	Antiterrorist	Reno Nevada Police Department	Reno	NV
W068I	Lieutenant	Intelligence	Nevada Division of Investigations	Carson City	NV
E014I	Inspector	Executive Officer	Suffolk County Police Department	Yaphank	NY
E003B	Captain	Emergency Service Unit	New York Police Department	Brooklyn	NY
E005F	Dep. Inspector	Operations Commander	New York City Transit Police Department	Brooklyn	NY
E012I	Chief	Bomb Technician	New York State Police	Albany	NY
E003B	Sergeant	ESU HAZMAT Coordinator	New York Police Department	Brooklyn	NY
E003B	Captain	Disorder Control Unit	New York Police Department	Brooklyn	NY

E003B	Sergeant	Intelligence	New York Police Department	Brooklyn	NY
E017I	Tech. Sergeant	SWAT (Weapons and Ordnance Unit)	Erie County Sheriff	Orchard Park	NY
E005F	Lieutenant	Intelligence	Cleveland Police Department	Cleveland	OH
E004F	Lieutenant	Special Investigations	Montgomery County Sheriff's Department	Dayton	OH
E005F	Sergeant	Intelligence/Int'l. Terrorist Issues	Columbus Police Department	Columbus	OH
M037F	Undersheriff	Antiterrorist Investigator	Canadian County Sheriff's Office	El Reno	OK
M037F	Sheriff	Antiterrorist Activities	Grady County Sheriff's Office	Chickasha	OK
M037F	Major	Antiterrorist Activities	Oklahoma City Police Department	Oklahoma City	OK
M037F	Investigator	Antiterrorist Activities	Pottawatomie County Sheriff's Office	Shawnee	OK
M037F	Sheriff	Antiterrorist Activities	Cleveland County Sheriff's Office	Norman	OK
M037F	Deputy Sheriff	Antiterrorist Activities	Canadian County Sheriff's Office	El Reno	OK
M037F	Lieutenant	Antiterrorist Activities	Oklahoma County Sheriff's Office	Oklahoma City	OK
M037F	1st. Assistant DA	Criminal Prosecutions	7th Judicial District - District Attorney's Office	Oklahoma City	OK
M037F	Captain	Command Officer	Oklahoma City Police Department	Oklahoma City	OK
M037F	Lieutenant	Antiterrorist Investigations	Shawnee Police Department	Shawnee	OK
W061I	Captain	Special Operations	Oregon State Police	Salem	OR
W061I	Sergeant	Criminal Investigation Services	Oregon State Police	Salem	OR
W058B	Officer	Intelligence Unit	Portland Metro Police Department	Portland	OR
W058B	Lieutenant	Intelligence Unit	Portland Metro Police Department	Portland	OR
W058B	Sergeant	Intelligence Unit	Portland Metro Police Department	Portland	OR
E004F	Captain	Intelligence	Pennsylvania State Police	Hershey	PA
E004F	Captain	Command, Emergency Operations Ctr.	Pennsylvania State Police	Hershey	PA
E005F	Detective	Headquarters Investigation Unit	Philadelphia Police Department	Philadelphia	PA
E005F	Lieutenant	SWAT	Philadelphia Police Department	Philadelphia	PA
E005F	Sergeant	Intelligence	Philadelphia Police Department	Philadelphia	PA
E004F	Lieutenant	SWAT Team, Bomb Unit	Allegheny County Police Department	Pittsburgh	PA
E004F	Lieutenant	Tactical Commander of SWAT	Pittsburgh Police Department	Pittsburgh	PA
E004F	Sergeant	Bomb Technician	Providence Police Department	Providence	RI
S024I	Captain	Antiterrorist	South Carolina Law Enforcement Division	Columbia	SC
S046I	Major	Investigation	Charleston Police Department	Charleston	SC
M082I	Director	Communications Administration	South Dakota Department of Radio Communications	Pierre	SD
M038F	Captain	Intelligence	Sioux Falls Police Department	Sioux Falls	SD
M038F	Captain	Intelligence	Sioux Falls Police Department	Sioux Falls	SD
S055I		Intelligence	Tennessee Bureau of Investigation	Nashville	TN
S027F	Lieutenant	Investigator	Morristown Police Department	Morristown	TN
M054B	Captain	Intelligence	Dallas Police Department	Dallas	TX
M054B	Lieutenant	Intelligence	Dallas Police Department	Dallas	TX

W062I	Sergeant	Intelligence	Utah Department of Public Safety	Kearns	UT
W074I	Commissioner	Senior Research Associate	Utah State Patrol	Taylorsville	UT
C088I	Sergeant	Special Operations Division	Arlington County Police Department	Arlington	VA
C090I	Captain	SWAT	Fairfax County Police Department	Annandale	VA
C088I	Lieutenant	Special Operations Division	Arlington County Police Department	Arlington	VA
C087I	Lieutenant	SWAT	Alexandria Police Department	Alexandria	VA
S049F	Investigator	Intelligence	Norfolk Police	Norfolk	VA
C086I	Asst. Special Agent	Bomb Unit	Virginia State Police		VA
S047I	Captain	Commander, Patrolman	Virginia State Police	Richmond	VA
E097I	Captain	Special Investigations	Vermont State Police	Williston	VT
W084I	Captain	Antiterrorist	Spokane Police Department	Spokane	WA
W071I	Sergeant	Intelligence	Washington State Patrol	Olympia	WA
W071I	Sergeant	Intelligence	Washington State Patrol	Olympia	WA
W067I	Sheriff	Law Enforcement	Whitman County Sheriff's Office	Colfax	WA
E002I	Captain	Intelligence	Milwaukee Police Department	Milwaukee	WI
S025I	Lieutenant	Community Relations and Training Officer	West Virginia Division of Police	Parkersburg	WV
S048I	Investigator	Bureau of Criminal Investigation	West Virginia State Police	South Charleston	WV
M032I	Lieutenant	SWAT	Cheyenne Police Department	Cheyenne	WY
M050I	Lieutenant	-	Park County Sheriff's Department	Cody	WY
M085I	Training Manager	Coordinator of Training/Counter Terrorism	Wyoming Emergency Management Agency	Cheyenne	WY

Appendix C - Needs Tables

Table C-1. INTELLIGENCE NEEDS

NEEDS	Number of Times Cited (out of 108 sessions)	
	Total	Top Five
1) ***Federally Operated Intergovernmental Terrorism Intelligence Data System***	58	47
• text or data on terrorism to be queried/searched by any law enforcement agency		
• timely, real-time access		
• local/state/federal inputs		
• affordable	26	19
• Internet-like features, including secure "chat rooms," compartments with data on specific topics or regions, bulletin boards, etc.	8	7
• multi-media (especially ability to store and forward graphics)	8	5
• pointer index (tagged information) to names/phone numbers of law enforcement officials associated with various data to get further information directly/or get authorized access to more information in the database	8	5
• multi-level security/access control	7	1
⇒ selective encryption		
⇒ individual agency control of access to their inputs		
⇒ firewalls		
• "flash" messages sent proactively to departments that need to know about activities/individuals that might affect them	2	2
• other features:		
⇒ user-friendly		
⇒ integrated vertically (hierarchical) and horizontally (indexed)		
⇒ links to other databases (NCIC, liens, license plates, lawsuits, subpoenas, others)		
⇒ ability to access by laptop from remote location (with security guarantees)		
⇒ individual agency control of access to their inputs		
⇒ use of intelligent agent software to automatically collect information on specified topics		

Table C-1. INTELLIGENCE NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
2) Specialized Intelligence Databases [see also Forensics, and Communications and Command Sections] ● databases, profiles, and information on known terrorists and terrorist groups ● databases that track thefts/losses of explosives, weapons, lethal substances ● disseminated on CD-ROMs or equivalent ● assembled and updated by federal agencies	Several*	Several*
3) Intelligence System for State and Local Agencies ● linkage of intelligence databases maintained by individual states	Several*	Several*
4) Mining the Internet for Intelligence ● specialized search software (or training) to collect information ⇒ monitor data on the net of use to terrorists (e.g., how to make explosive devices) ⇒ monitor information on terrorism (terrorist events, data on NBC, new technology, etc.) ⇒ break into (tap) suspected terrorist databases, and decrypt if necessary (also noted under surveillance) ⇒ conveniently access open sources on potential terrorists (e.g., home pages of militia groups) ⇒ identify "hidden" user groups with potential terrorist interest ⇒ monitor what is being disseminated about one's own law enforcement agency and its intelligence assets	Several*	Several*
5) Prepackaged Software to Establish a Law Enforcement Agency's Own Intelligence System ● allow rapid conversion of manually accessed data into automated system ● databases of names, incidents ● connections to command databases with encryption capability	4	3

*Participants described this need capability in a myriad of ways--each with a different feature. Thus, it was difficult to obtain a precise count.

Table C-1. INTELLIGENCE NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
6) Intelligence Information Analysis Software	5	3
• general need for developing useful information from masses of available data to produce terrorist profiles, prediction of activity, most likely targets, etc.		
• ideally linked to a national or regional database(s) or able to use their data products		
• software to analyze phone call patterns (links between people), but with purging of information beyond the warrant authority		
7) Specialized Intelligence Databases [see also Forensics, and Communications and Command Sections]	Several*	--
• e.g., databases that track thefts/losses of explosives, weapons, lethal substances		
• technology available to law enforcement (classified if necessary)		
8) Method for Notifying Key Individuals and Agencies when a Terrorist Incident Occurs	Several*	--
• automatic, computer-based		
• function of the nature and location of the incident		
• "auto dial" or conceptual equivalent		
9) Other Intelligence Needs	4	3
• addressing legal issues affecting intelligence sharing	4	3
• standards for data and information sharing on terrorism	3	3
• ability to access raw media feeds	1	1
• better communication of intelligence data to operations personnel in the field	1	1
• capability to ascertain when a law enforcement agency or its personnel are under surveillance	1	--

*Participants described this needed capability in a myriad of ways—each with a different feature. Thus, it was difficult to obtain a precise count.

Table C-2. SURVEILLANCE NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
1) ***See Through Walls (Interior and Exterior)***	34	18
• operable from a distance of at least 100 feet	14	--
• differentiate between individuals	11	--
• capability for obtaining optical-quality image	9	1
• one-person portability	8	--
• quiet set-up if indoors	8	--
• see weapons (or at least metal objects)	6	--
• see "booby traps"	3	--
• acoustic coupled	2	--
⇒ integrated with sound detection system		
• ability to transmit image from device to command post	2	--
• ability to distinguish friend vs. foe (e.g., undercover officers seen in the image)	2	--
• combined with ability to identify chemical or biological hazards	1	--
⇒ integrated display to allow multiple users to view image		
• remote control operable	1	--
⇒ "leave behind" ability, such that the system can be assembled, aimed, and then controlled remotely		
• ability to identify explosive device	1	--
2) ***Audio Surveillance Tools***	33	15
• systems that allow surveillance officer to listen to conversations and activities within a targeted structure from behind a secure perimeter or covert listening location.	23	9
⇒ easy to deploy		
⇒ operable by one person		
⇒ with connectors to allow recording		
⇒ encryption of recording when desired		
⇒ increased range (several hundred feet) for safety and covertness		
⇒ covert		
• covert transmitters (bugs, wires)	14	8
⇒ smaller, more reliable, less detectable wires and bugs	2	2
⇒ longer-life batteries (minimum of 8 hours)	3	1

Table C-2. SURVEILLANCE NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
⇒ transmit capability 1/4 mile or more	2	--
⇒ transmission of battery failing signal	1	--
• ability to monitor transmission from a suspect's plane		
3) Remote Long Range Video Monitoring	34	13
• remote control cameras	24	--
⇒ leave behind, operate remotely		
⇒ higher resolution videotape for facial identification/ ID of suspects		
⇒ increased video camera clarity and reduced cost		
⇒ longer range (1-2 miles)		
⇒ digital cameras that record images in a digital format for easy storage in databases and transfer to other systems		
⇒ non-line-of-sight transmission repeaters		
⇒ longer-life batteries		
⇒ burst transmission capability		
⇒ all weather (especially cold)		
• satellite based observation	8	2
⇒ for clandestine observation, observation of remote areas, and observation of large rural areas		
• unmanned aerial vehicles	5	1
⇒ carry surveillance cameras discretely over targets		
⇒ small, quiet, and fly at a sufficient altitude not to attract attention		
⇒ with forward looking infrared (FLIR) capability for nighttime observation		
4) Night Vision	30	15
• general purpose night vision devices	30	15
⇒ improved affordability	12	2
⇒ longer range (100-1000 yards)	9	2
⇒ recordable output	7	2
⇒ bright-light "flash" protection	7	1
⇒ less costly, handheld forward looking infrared (FLIR) devices	7	--
⇒ improved depth perception (binocular)	3	--
⇒ ability to operate at different and changing light levels	3	--
⇒ image quality sufficient to identify individuals	1	--

Table C-2. SURVEILLANCE NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
⇒ easier use at night, in cold, from field surveillance positions	1	--
⇒ increase magnification for long range surveillance	1	--
⇒ expand peripheral vision	3	--
• convertible night vision rifle scopes	1	--
⇒ scopes that convert from day to night with one switch rather than removing the scope		
• friend or foe identifier		
⇒ small device that would indicate which of the bodies seen through night vision is a law enforcement officer		
5) Vehicle Tracking	26	4
⇒ use of GPS technology or equivalent to pinpoint location	24	3
⇒ track vehicles over time and across jurisdictions	3	--
⇒ technology to "paint" vehicle with non-visible, but easy to track substance		
⇒ integrated with map display showing vehicle location	1	--
⇒ discrete device for undetected tracking	1	--
⇒ ability to track individuals (e.g., field officers)	1	--
6) Cellular Phone Monitoring Capability	12	3
⇒ monitor and record a specific cellular phone as it moves from cell to cell	8	3
⇒ triangulate location of a cellular phone within a structure, within 2 feet	4	--
7) Real-Time Video Feed to Command Post	9	--
⇒ handheld, easily portable video camera that transmits image and sound to a command post for real-time viewing by commanders		
⇒ quiet, discrete, and non-line-of-sight transmission		
8) Computer Transmission Tapping	6	2
⇒ tapping and "tailing" of individuals as they send e-mail, converse in chat rooms, view web pages, and download files		
9) Weapons Detection at a Distance	5	2
⇒ detect concealed weapons on individuals from 30 feet or greater		

Table C-2. SURVEILLANCE NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
10) Subsurface Imaging (Earth-Pentrating Sonar/Radar) ⇒ a tool to image subsurface booby traps, tunnels, buried arms caches, and human remains	2	1
11) Telephone Number Dialed Logging System ⇒ log and transmit numbers dialed from a specific phone in real time	2	--
12) Underwater Search Capability ⇒ provide a detailed image of the area being searched	1	--
13) Seismic Sensors ⇒ sensors that can be left in the field to indicate the passing of people or vehicles, a valuable adjunct when surveillance is being conducted of a large area or a remote structure	1	--
14) Fiber Optics Monitoring ⇒ ability to tap fiber optics	1	--

Table C-3. COMMAND, CONTROL, AND COMMUNICATIONS NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	Top Five
1) *Encryption for Law Enforcement Radios* (especially handheld)	53	19
• for surveillance teams, field officers, tactical teams		
• affordable		
• maintain radio range or clarity		
2) *Interagency Communications (Interoperability)*	48	26
• communicate with multiple agencies during incidents when many jurisdictions respond		
• ability to simultaneously broadcast from Incident Commander and his/her staff to participating agencies (on their own frequencies)		
• officer-to-officer communication across responding agencies		
• federal guidelines for compatibility	5	2
3) *Handheld Radio Performance*	16	2
• better quality from within structures (especially large, commercial buildings)	6	0
• better quality from tunnels or other underground structures	2	0
• GPS tracking capability	3	1
⇒ GPS receiver integrated into the radio; can be queried for officer location		
• cell phone capability	3	1
⇒ Radios equipped with an integrated telephone pad and cellular system		
• more dependable hands-free microphones	2	0
• smaller, more reliable, more durable radios	1	1
4) *Secure Data Networks*	10	6
• an intra-agency and interagency data communications system that is extremely secure		
5) *Management Information System to Assist the Incident Commander and Staff*	10	--
• usable in real-time during incident		
• prompting on what to be thinking about, where they are on the incident time line		
• ability to track units, resources, location of assigned units		

Table C-3. COMMAND, CONTROL, AND COMMUNICATIONS NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	Top Five
• savvy electronic checklist system		
• scenario software	3	--
⇒ series of preset scenarios on which to build the real scenario facing the command staff		
• integrated mapping system	2	--
⇒ unit locations superimposed on map of the incident area		
⇒ ability to click on the unit icon and call up information about the unit, its skills, status, agency affiliation, etc.		
• ability to track all resources for multiple day incidents	3	--
⇒ up to hundreds of responding agencies		
⇒ time frame of days to weeks to months		
• archiving capability	1	--
⇒ record and archive steps taken by the command staff and the status of the "incident world" at the time those decisions were made		
6) Field Laptop Computers with Communication Links to Various Databases	9	--
• link laptop computers available on scene to information such as AFIDS (fingerprints) and intelligence databases quickly		
• transmit and receive information in encrypted form		
7) Improved Radio Coverage and Performance	9	7
• long range	5	--
⇒ satellite or long-range repeater-capable radios usable anywhere in a 200-mile radius		
• non-line-of-sight	4	--
⇒ not hampered by mountains and other barriers		
8) Incident Command System (ICS) (Especially for Multiple Agency Response)	8	2
• technologies and training that support the use of ICS		
9) Advanced Command Post/Communication Vehicle	8	1
• equipped with digital radios, secure faxes, photo faxes, PC, incident software, etc.		

Table C-3. COMMAND, CONTROL, AND COMMUNICATIONS NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	Top Five
10) Priority Usage of Cellular Telephone System • capability to prioritize cellular phone infrastructure for law enforcement and emergency services use in crisis	6	1
11) Secure Video Conference Capability • between offices within one agency or between agencies	3	--
12) Blackout of Terrorists' Communications • ability to jam cellular phone usage by terrorists during hostage/barricade situations • ideally, directional system set up around a structure that negates radio, television, and pager transmissions as well as cellular transmissions	3	--
13) Ability to Deactivate a Stolen or Lost Law Enforcement Radio • need to deactivate stolen analog radios that might compromise tactical or other operations	2	1
14) Establishment of a Common Radio Language Standard (or Translators) • the use of 10-codes with different meanings leads to confusion during multiple agency incidents	1	1
15) Telephone Encryption • secure conversation capability for phones within and between agencies	1	--

Table C-4. SITE HARDENING AND SECURITY NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	Top Five
1) Fixed Intrusion Detection Systems	13	2
• more affordable		
• special concern for federal buildings		
• withstand extreme temperatures		
⇒ remote cameras high-resolution digital cameras color cameras that can zoom and freeze frames night vision technology for cameras videotape compression technology	7	2
• laser or electric eye beam technology	2	--
• sound detection	2	--
• underwater perimeter security technology	1	--
• motion detection	3	--
• thermal detection	2	--
• human heartbeat presence indicator	1	--
• tunneling detection	1	--
2) Improved Passive Site Hardening and Architecture (Built-in Physical Security)	10	1
• non-shattering window glass ⇒ used to minimize injuries from flying glass caused by explosions	1	--
• vehicle barriers	1	--
• prevent/minimize threat of unattended or unauthorized vehicles	1	--
• secure parking areas	1	--
• minimize threat of unattended or unauthorized vehicles		
• computer blast modeling software	4	1
3) Personnel Access Controls	9	--
• computerized entry controls (including ID cards with computer chips)	3	--
• personnel access/status and tracking technology	4	--

Table C-4. SITE HARDENING AND SECURITY NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
4) ***Metal and Explosive Detectors for People and Vehicles***	7	3
• fixed facility explosive detectors	3	1
• vehicle explosive screening device	3	3
• airplane cargo hold explosive detectors	1	
5) ***Portable Perimeter Security***	7	1
• portable explosive screening devices	2	1
• portable bullet-proof barriers	2	--
⇒ erected for ceremonies, used to protect VIPs, etc.		
• technology to set up perimeter security for large events	1	--
⇒ outdoors, special events, etc.		
6) ***Mail and Package Scanners***	5	--
• improved airport-type scanners	1	--
• improved letter/package scanners	3	--
• high volume mail scanners	2	--
7) ***Intruder Countermeasures Technology***	2	--
• site lock-down technology	2	--
⇒ ability to seal building; either manually or electronically		
• intruder incapacitation system	1	--
8) ***Site Patrol Boats***	2	--
⇒ equipped to handle rescues and function as dive platforms. Outfitted with surveillance equipment to include night vision goggles, video recorders and sonar equipment	1	--
9) ***Computer-Aided Site Design***	3	--
⇒ improved traffic flow modeling, to prevent traffic from backing up around high threat targets		
⇒ computer model to assess site security		
⇒ individual agency control of access to their inputs		

Table C-5. NEEDS FOR THE DETECTION, DISABLEMENT, AND CONTAINMENT OF EXPLOSIVE DEVICES

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
1) Improved Detection Technology	58	21
• portable, preferably handheld detectors	36	18
⇒ as sensitive as dogs		
⇒ affordable		
⇒ all weather		
⇒ simple to operate		
⇒ rugged, low maintenance		
• detect wider spectrum of explosives than canines can detect	10	5
• detect second device after initial explosion	10	1
⇒ detect remote control devices in a crowd		
• characterize bomb mechanism (as well as explosive)	1	--
• combine with chemical and biological detection capability	7	2
• detect in wide area (e.g., stadium, arena, outside area)	6	2
• detect at longer range	4	1
• detect more reliably (few false alarms)	4	--
• detect explosives in vehicles (from outside)	4	2
• detect more sensitively than canines (smaller quantity of explosives)	4	3
• high-volume, portable package scanner	3	--
• detect fuel and fertilizer when mixed	1	1
• detect buried explosive	1	1
2) Disarmament/ and Disablement Technology Capability	57	18
• improved Explosive Ordnance Disablement (EOD) robots	47	9
⇒ with remote viewing, preferably in color	15	4
⇒ more affordable	15	1
⇒ do most EOD procedures	10	1
⇒ with disrupter capability	10	1
⇒ climb stairs	9	5
⇒ manipulate packages, lift 100 lb.	8	--
⇒ x-ray, detect, and characterize device	6	--
⇒ lightweight (<200 lb.)	5	--

Table C-5. NEEDS FOR THE DETECTION, DISABLEMENT, AND CONTAINMENT OF EXPLOSIVE DEVICES

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
⇒ up to 1/4 mile range communication	3	--
⇒ ability to open doors	2	--
⇒ with chemical and biological detection	1	--
⇒ lower maintenance	Many	--
• "sacrificial lamb," low-cost robot to scout before using highly sophisticated, expensive robot	4	--
• improved EOD (bomb) suits	23	7
⇒ lighter (<65 lb.)	4	--
⇒ lighter, with cooling option	13	7
⇒ with chemical and biological protection, SCBA	10	1
⇒ built-in intercom/communication system, non-interfering with robot control	6	3
⇒ with hand protection that allows finger movement	4	2
⇒ improved visibility, 180° field of vision	2	--
⇒ better blast protection (at least 2-10 lb. generic explosive; seven to ten sticks of dynamite @ 4 ft.; 1 lb. C4)	7	1
⇒ spinal and knee protection	1	--
• improved x-ray equipment	19	--
⇒ more portable	12	--
⇒ standoff (remote operation)	11	3
⇒ 3-D imaging	2	1
⇒ color	2	1
⇒ less expensive films	2	--
⇒ combined x-ray and sniffer	1	--
⇒ non-film device	1	--
• other than x-ray imaging technology	19	--
⇒ portable EOD imaging other than x-ray		
⇒ digital images		
• disrupters	10	5
⇒ cloaking technology (to defeat passive IR receiver as initiator)	2	2
⇒ stand-off disarmament, disruption, capability (> 100 feet away)	1	1
⇒ beam technology for disruption	3	--

Table C-5. NEEDS FOR THE DETECTION, DISABLEMENT, AND CONTAINMENT OF EXPLOSIVE DEVICES

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	Top Five
⇒ percussion activated non-electric (PAN) disrupters		
• other		
⇒ electric current presence detectors		
⇒ device to jam radio remote controlled device		
3) ***Improved Blast Containment***	31	6
• improved bomb transport vehicles, trailers and containment vessels	22	5
⇒ contain 10-30 lb. of explosive and all released gases	17	4
⇒ built-in foam system to disarm	2	--
⇒ hardening foam to contain	4	--
⇒ more affordable containers (much less than $100K)	6	--
• bomb "blankets"/other fast-to-use containment technology	2	1
⇒ fast deployment over small to medium bomb		
⇒ transport kit sample of the explosive		
⇒ blanket large enough to place over a vehicle		
⇒ ability to "contain" evidence		
4) ***EOD Information Management***	18	3
• database/CD-ROM with latest bomb schematics	9	1
⇒ access FBI bomb data by laptop	1	--
• digital information link to bomb experts	1	--
• increased timeliness and scope of FBI Bomb Data Center publications and advisories	1	--
• computer model to assist bomb technicians to predict blast effects upon specific types of construction (for detonate-in-place decision)	1	1
5) ***EOD Maintenance***	8	1
• lower maintenance for all EOD technology		

Table C-6. NEEDS FOR DEFENSE AGAINST CYBERTERRORISM

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
1) ***General Improvement in Countering Cyberterrorism***	33	3
2) ***Training to Counter Cyberterrorism***	10	2
3) ***Intrusion Prevention***	12	1
• intrusion detection	4	1
• better firewalls	8	--
4) ***Forensic Capabilities (for Cyberterrorism)***	15	--
• de-encryption technologies	9	--
• ability to trace a hacker and/or the entry point	5	--
• ability to gain remote access to suspect computers	1	--
• ability to detect "booby trapped" data/viruses	3	--
• better human expertise - skilled computer investigators	2	--
5) ***Other Needs***	1	1
• system monitoring log	1	--
• techniques to conduct system security self-assessments	1	--
• better back-up systems	1	--

TABLE C-7. NEEDS FOR DEFENSE AGAINST WEAPONS OF MASS DESTRUCTION

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
1) Ability to Detect and Categorize Wide Range of NBC Threats	51	24
• portable, sensor/monitor to alert first responder of presence of NBC threat	32	16
⇒ detect at safe distance 12-20 ft. minimum, preferably with ability to detect traces from 5 miles away		
⇒ able to mount on vehicle	10	--
⇒ preferably wearable and unobtrusive looking		
⇒ clear alarm signal	10	6
⇒ preferably with identification of substance as accurate as possible	4	3
⇒ affordable		
⇒ quick responding		
⇒ long life battery		
⇒ sensitive; detect small quantities (e.g. residual traces on outside of packages)		
⇒ badge-type monitor	2	--
• fixed system for large public areas (subways, arenas, etc.)	2	1
⇒ continuous monitoring	2	2
⇒ rapid detection and identification		
⇒ transmit output to central command post		
⇒ highly accurate (few false alarms)		
⇒ ability to characterize "cloud" in a large space: quickly determine whether Chemical or Biological hazard is present; second, identify what type of agent it is		
• detection of NBC material in water systems	2	--
• database with NBC characteristics	2	--
• capability to detect components of NBC weapons (especially in rural areas)	2	--
⇒ detect presence of components of Ricin, Sarin, etc.		
• radiation detectors	4	--
⇒ handheld, small, durable Geiger counters		
⇒ greater supply (more affordable for widespread use)		

TABLE C-7. NEEDS FOR DEFENSE AGAINST WEAPONS OF MASS DESTRUCTION

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
2) *NBC Protection*	45	16
• better protective suits (outerwear)	42	10
⇒ more affordable	11	5
⇒ lightweight	7	5
⇒ choice of three levels of protection		
⇒ suits for tactical specialists:	14	4
total encapsulated, high level of protection	2	--
with SCBA for 15-30 minutes	6	1
built-in NBC detection/identification capability (“on a chip”)	1	--
built-in capability to administer antidotes or prophylaxes	1	--
compatible (worn over) bomb suits	3	--
• suits for SWAT and first responders:	6	2
• basic protection	5	1
• inexpensive	2	--
• suits for civilians:		
provide some protection for at least short duration		
inexpensive		
• better protective masks	4	3
⇒ affordable for all first responders	1	3
⇒ incorporate throw-away mask in blast protection of bomb suit	1	1
• Accessible vaccines, antidotes and prophylaxes	1	--
3) *NBC Decontamination and Containment*	8	4
• portable decontamination equipment	5	3
• rapid, mobile, high volume decontamination facility transported to the site	8	4
• emergency vehicles with containment capability, to transport victims to decontamination site	1	1
• atmospheric plume modeling		
⇒ ability to predict paths of plume, especially in an urban environment	1	--
⇒ “knockdown” capability for chemical-biological airborne cloud	1	--

Table C-8 NEEDS FOR APPREHENSION (AND NEUTRALIZATION) OF TERRORISTS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
1) ***Non-lethal Weapons***	27	6
• chemical agents	8	1
⇒ high-volume, portable (fire extinguisher-sized) CS dispensers	2	--
⇒ pepper sprays	1	--
⇒ odorless non-flammable sleeping gas	6	1
• stunning weapons	8	1
⇒ beam based stunning weapon	1	--
⇒ more effective stun grenades	1	--
⇒ better stun gun equipment	3	1
⇒ improved "Tasers" wireless long-range	4	1
• acoustical weapons	1	1
• net guns	3	1
• glue guns	3	--
• frangible ammunition	1	--
• vehicle ignition disabling devices	10	2
2) ***Conventional Weapons***	15	3
• improved sighting	8	--
⇒ longer range scopes	2	--
⇒ night vision scopes	1	--
⇒ affordable optics for long-guns and hand guns	1	--
⇒ laser-assisted sight system	5	--
• improved ammunition	1	--
⇒ better multi-purpose round		
• gun security	1	1
⇒ palm print recognition safety lock		

Table C-8 NEEDS FOR APPREHENSION (AND NEUTRALIZATION) OF TERRORISTS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
● sniper weapons	1	1
⇒ weapon that can accurately shoot through glass	1	--
⇒ silenced sniper weapons	1	1
⇒ more readily available, specialized weapons		
3) Assault (Armored) Vehicles	12	4
● affordable armored personnel carrier (APC)	1	--
● amphibious APC	1	--
● unobtrusive (non-military looking) APC	1	--
4) Personal Protective Equipment	11	6
● body armor	9	--
⇒ lighter, stronger and more flexible body armor	7	1
⇒ tactical load bearing body armor able to defeat 30-06, 308, caliber rounds	2	--
● special weapons holster to protect weapon during apprehensions	1	--
5) Wall Breaching	10	3
● faster, better breaching	5	1
⇒ 6 ft. hole punch to breach walls, doors, etc.	1	--
⇒ better door opening technology	2	--
⇒ high-powered water cannon to breach doors	1	--
● silent wall penetration technology	2	1
● sensing technology to determine structure of wall and identify best entry point	2	1
● improved shaped charge devices	2	--
6) Enhanced Helicopters	3	--
● FLIRS for helicopters	2	--
● armor	1	--
● hoist system to pull people out of buildings	1	--
7) Other Apprehension Needs	10	--
● night vision devices	10	--
● computerized terrorist database	9	--

Table C-8 NEEDS FOR APPREHENSION (AND NEUTRALIZATION) OF TERRORISTS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
• fingerprint/palm scanning device (also noted as a forensics need)	6	--
• location tracking of police tactical personnel	2	--
• language translator device (more frequently cited as a crowd control or public information need)	1	--
• robot to deliver items in hostage situations	1	--
• database of building layouts	1	--
• standoff weapons detector	4	--
• hostage communications devices	2	--
⇒ covert communication (e.g. laser beam messages on walls) with hostages	2	--

TABLE C-9. FORENSICS AND INVESTIGATION NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
1) Detection and Analysis of Materials at the Scene • portable (ideally belt clip-on) kit • explosive evidence analysis ⇒ more accurate ⇒ broader range of chemicals and explosives (like chromatography) ⇒ ID components or explosives • pick up minute particles/traces • mass spectral database on CD-ROM help identify unknowns, where manufactured, where sold • metal and other object detection for shell casings, metal fragments • capability to gather evidence in a hazardous environment • capability to preserve and collect evidence from a large crime scene area ⇒ firewalls	15	3
2) Rapid Suspect Victim Identification • fingerprint/palm print field scanner, with ability to transmit to other agencies • portable DNA technology and database • faster locating of fingerprints (e.g., “bug bomb” of fingerprint dusting powder in a room, to bring out all prints.)	6	2
3) Explosives Tracing • database on explosives • taggants on explosives	9	1
4) Forensic Reference Databases • searchable, on web or CDs • national directory of bomb components, ideally cross-referenced to known or convicted bombers • databases for tracking terrorist activities and terrorists [also for intelligence] • database on purchasers of government surplus supplies	9	--

TABLE C-9. FORENSICS AND INVESTIGATION NEEDS

NEEDS	Number of Times Cited (out of 108 sessions)	
	Total	**Top Five**
• database on purchases of unusual quantities of chemicals or fuels		
• database on MOs of terrorists		
• database of reference materials used by terrorists (e.g., what **they** find on the web)		
• database on local technological resources available		
• "smart" check of driver's license, with link to other databases		
• facilitate collecting impression of foot or tire print		
• better, unique identification of bloodstains		
5) ***De-encryption of Seized Data***	5	--
• most at PGP (Pretty Good Privacy) level		
6) ***Gun/Bullet Analysis***	5	--
• nationwide ballistics comparison system	2	--
⇒ one national standard		
⇒ interconnectivity to all agencies, services		
⇒ real-time (get matching responses back immediately)		
⇒ have a database search mechanism		
• means to link bullet to specific gun other than by rifling markings	2	--
• gunshot residue collector	1	--
⇒ handled to identify suspects		
7) ***Rapid Identification of Mass Fatalities***	3	--
• palm or fingerprint scan		
• portable morgue with cooling, to preserve evidence		
8) ***Lie Detector***	3	--
• more accurate, portable, easier to use, and affordable (less than $12K), with automated voice stress analysis		
9) ***Photo Recording of Evidence***	4	--
• transmit and receive high resolution video and/or photos from the field	3	--
• wireless video camera attached to bomb search dogs	1	--
10) ***Less Expensive Laboratory Equipment***	1	--
• lower cost but equally reliable equipment, e.g., scanning electron microscope		

TABLE C-9. FORENSICS AND INVESTIGATION NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	Top Five
11) Other Needs • computerization of crime scene analysis and its recreation • equipment to identify fraudulent documents • ways to prevent evidence contamination • GPS to mark and identify crime scenes in rural areas	1	--

TABLE C-10. PUBLIC INFORMATION NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
1) ***Methods for Getting Accurate, Consistent Information to the Public*** ● emergency broadcast capability (break into local media) ● video teleconferencing with media ⇒ incident site-to-media communications ⇒ communications links between Public Information Officers (PIOs) of different agencies ⇒ mobile faxes for PIOs ⇒ Web sites ⇒ capability to make public service announcements (PSAs) on the scene ⇒ portable "message boards" attachable to squad cars ⇒ "leave behind" public information booth for evacuation (portable, updated remotely by radio) ⇒ technology to help volunteers better disseminate information to the public	12	--
2) ***Protecting Preparations and Tactics*** ● use of portable screens, curtains (as in U.K.)	8	--
3) ***Minimizing the Adverse Impact of Media Presence on Operations*** ● reduce radio interference; non-jammable communication ● reduce interference with remote control robots or other equipment ● stop violations of airspace or rescuers on scene	4	--
4) ***Eliciting Information from the Public on Terrorists*** ● to get help in identifying and locating terrorists (e.g., with Web page)	1	--

Table C-11 CROWD AND RIOT CONTROL NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
1) Nonlethal Crowd Control Agents	24	4
• noninjuring, preferably nonpainful		
• nondetectable or covert delivery, if desired		
• choice of duration of effect, from temporary stun or instantaneous paralysis incapacitation for a short time		
• portable, usable by single officer, preferably handheld		
• antidote available (for gas or spray)		
• targetable to specific area of person(s)		
• adjustable "dose" for size of space (from a room to a riot out-of-doors)		
• effective on stationary or moving target		
• launcher/application device instantly rechargeable		
• "one-way doses" to reduce possibility of being thrown back or redirected against police (e.g., a tear gas canister can be thrown back).		
• penetrate clothing		
• increased range of 20-100 yards (rock-throwing distance)		
⇒ if gas, nonlethal for children, people with asthma, others		
⇒ capable of being cleaned up or disposed		
2) Personal Protective Gear for Law Enforcers	9	1
• improved riot control shields	5	1
⇒ stronger, lighter	1	--
⇒ more bullet resistant (shatterproof)		
• bullet-resistant barriers	1	--
⇒ portable in patrol cars		
⇒ stop NATO-type round		
⇒ weigh <30 lb.		
⇒ stand up on own		
⇒ with "see through" window/port		
• means of reducing officer vulnerability to a crowd	1	--
⇒ shock or force-field like protection database		
• incapacitant agent resistant gas mask		

Table C-11 CROWD AND RIOT CONTROL NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
3) ***Language Translation Capability*** ● automatic real-time translation of announcements to crowds, in selected language(s) ⇒ ability to use pre-recorded or on-scene recorded stock phrases	6	--
4) ***Crowd Barricades*** ● portable ● inflatable ● equipped with remote audio speaking and listening capability	5	--
5) ***Computer Model for Predicting Crowd Dynamics***	1	1
6) ***Direct Video Transmission to Headquarters*** ● to allow police officials to monitor the scene from patrol car or other means ⇒ individual agency control of access to their inputs	1	--

Table C-12 TRAINING AND OTHER NEEDS

NEEDS	*Number of Times Cited (out of 108 sessions)*	
	Total	**Top Five**
1) ***Training to Combat Counterterrorism***	31	9
• training on new technology	8	1
• computer-based virtual reality or interactive training, including:	15	6
⇒ specialist training modules: explosive containment explosive detection NBC defense other HAZMAT operation dynamic entry/explosive breaching collapse rescue command strategies		
⇒ "war gaming" terrorist event scenarios, preferably with multiple agencies or involved at same time		
⇒ laptop version with mission planning and rehearsal capability	2	2
⇒ weapons trainer	1	--
• training on cyberterrorism	2	-
2) ***Information on Available Anti-terrorism Technology***	12	4
• nationally accessible database, Web page or "information clearinghouse"		
• query about available technological tools and how to obtain them		
3) ***Standards and Testing for Technology***	2	--
• "Consumer Reports" on technology		