LOCKHEED MARTIN

Law Enforcement Technology Needs Assessment

POLICE EXECUTIVE RESEARCH FORUM

POLICE EXECUTIVE
RESEARCH FORUM

Law Enforcement Technology Needs Assessment: Future Technologies to Address the Operational Needs of Law Enforcement

In partnership with the Lockheed Martin Corporation

By

Christopher S. Koper, Bruce G. Taylor, and Bruce E. Kubu

With contributions by

Eugene Glover, John Anderson, Paul Snabel, Chuck Wexler, Rachael Bambery, Nathan Ballard, Anthony Bellero, David Prothero, Willie Marsh, Mike Schroeder, Mike Taylor, Greg Maultsby, Donnie Gilley and Dave Kier

Police Executive Research Forum
1120 Connecticut Ave., N.W., Suite 930
Washington, D.C. 20036

Jan 16, 2009

Report Outline

Technology and Law Enforcement: Future Technologies to Address the Operational Needs of Law Enforcement

EXECUTIVE SUMMARY

Background

The effects of technology can be seen in almost all aspects of modern life, and law enforcement is no exception. The field of law enforcement has been altered by technology in many important ways. One need only consider that the primary police strategy of the latter part of the 20th Century—motorized preventive patrol and rapid response to calls for service—was developed in response to the invention of the automobile and two-way radio communications. More recent technological developments have also had far-reaching effects on police agencies. Information technology, DNA testing, and bullet-resistant vests, for instance, are now common and critical tools in law enforcement. Contemporary concerns over homeland security and counterterrorism have also created new technological problems and demands for police agencies, as has the growth of computer-related crime.

Given the importance of technology, the Police Executive Research Forum (PERF), a membership organization of police chiefs and sheriffs, has been actively exploring ways to harness technology to help advance the field of law enforcement. This interest has led to a new partnership for PERF. In July 2007, PERF (www.policeforum.org), with support from the Lockheed Martin (LM) Corporation, embarked on a project designed to gain a detailed understanding of law enforcement's perspectives and high-priority technology needs for the next three to five years and beyond. The partnership between PERF and LM's Advanced Concepts Protection Organization (ACPO) in its Law Enforcement Support (LES) group is unique and brings together complementary expertise and skills. LM (www.lockheedmartin.com) brings engineering expertise and extensive experience developing technology for the military. PERF has been working with hundreds of law enforcement agencies across the nation for more than three decades and has expertise in the full range of substantive and operational aspects of law enforcement.

The goal of this joint project was to identify, evaluate, and prioritize cutting-edge, relevant technologies that hold the greatest priority for policing. In doing so, we sought to recognize those technologies that afford the greatest promise in improving the ability of law enforcement to fulfill the security needs of the public in the most efficient manner available. Our project also sought to identify the key stakeholders and supporters within the decision chains of law enforcement, their requirements derivation and acquisition strategies for technology, and opportunities that may emerge from identified gaps between what police need to reduce crime and technologies that might fill those needs.

The project objectives were to explore and document:

- The operational needs of law enforcement agencies
- The law enforcement perspective on technology—including beliefs about its effectiveness
- A prioritized list of technologies to develop for law enforcement
- Barriers to the introduction of technology in the LEA community

Methods

Our general approach was to begin with a broad assessment of prior research in this field. This informed the development of a survey that provided an overall national picture of operational needs, technology uses, and technology needs in law enforcement. We then explored these issues in further depth through a focus group workshop that brought together leading practitioner experts from around the nation. In sum, our team's research methodology included three basic components:

An extensive review of the prior literature on law enforcement technology – Our team wanted to make sure that the project built on prior work in the field, and integrated insights from previous studies into this project.

Survey – PERF wanted to reach out to a large group of law enforcement personnel to assess their operational needs and priorities for technology development, with a special focus on innovative agencies. To this end, we conducted a national survey with approximately 300 agencies affiliated with PERF (over 70% completed the survey).

Focus group / workshop – To explore the results of our survey in more detail, PERF and LM designed a series of integrated focus groups conducted during a two-day workshop with 55 representatives from 29 law enforcement agencies around the country. The focus groups allowed the team to explore the meaning of the survey results, and provide additional context to appropriately interpret the implications of the survey results. The focus groups also allowed the team to explore new issues raised by the survey.

Key Findings

Literature Review

Our state-of-the-field assessment revealed that various forms of technology are being adapted or developed for law enforcement purposes, and there are many specific technologies, both current and emerging, that can benefit law enforcement. Broad points of emphasis from our review of technology uses, impacts, and needs in law enforcement are stated below.

- Police agencies use information technology (IT) extensively, but gaps remain in their IT capabilities. A high priority is the development and enhancement of integrated data systems, including systems and equipment that provide in-field access for officers. Better data systems and access would seem to hold much potential for enhancing the effectiveness of police, particularly when coupled with crime analysis capabilities that

can be used to improve strategy, resource allocation, and managerial control and accountability.

- Communications technology is a high priority for many agencies. Improving the inter-agency interoperability of communications is a particularly important concern. Other issues in communications include improving the ability of police to transmit and receive information from the public and the development/enhancement of locator technologies.

- Improving the ability of police to collect and process DNA evidence has great potential for improving criminal investigation, given both the strong experimental evidence for its effectiveness in clearing cases and the current backlogs that exist in DNA testing. Other technologies to improve suspect identification, including biometric technologies and mobile fingerprint readers, are also spreading in law enforcement and may improve operations.

- Police are increasingly using various forms of camera surveillance, ranging from individual cameras in patrol cars or on officers' uniforms to wireless networks of cameras providing live coverage of numerous areas of a city simultaneously. Some evidence suggests that cameras are effective in reducing some forms of crime; they may become even more effective if coupled with emerging biometric technologies for subject identification. Police are also seeking technologically advanced surveillance equipment that has tactical uses, such as "see through the wall" devices for use in hostage situations.

- Finally, there is a need for more evaluation research to provide police with better evidence on which technologies are most valuable and cost-effective for law enforcement uses. Such studies should seek to determine the types and uses of technology that are most effective and delineate the implementation issues that impact the successful application of technology.

Survey and Focus Group / Workshop Results

In the sections below, we summarize key conclusions from the survey and workshop focusing on three main areas: operational needs in law enforcement, priority technologies for law enforcement, and barriers to technology acquisition and implementation in law enforcement.

Operational Needs in Law Enforcement

Through both the national survey of PERF agencies and the technology workshop, we sought to identify key operational needs that law enforcement agencies will face in the near future. Our intent was to identify these needs so that police practitioners, researchers, and industry can consider if and how technology can be used to address these needs.

The following five operational areas, which emerged as very high priorities in both the survey and workshop, appear to represent the most pressing needs in law enforcement. (They are listed in no particular order.)

- Managing calls for police service
- Crime analysis and information-led policing
- Information technology and database integration
- Prevention and investigation of street crime
- Hiring and retention of police officers

Other operational needs that stood out in the results of the survey and/or the workshop included:

- Freeing officer time for proactive, crime prevention strategies
- Coordination and interoperability with first responders
- Training for police personnel
- Communications and dispatch
- Officer oversight, supervision, and accountability
- Weapons and equipment
- Security for police information systems
- Prevention and investigation of electronic and cyber-crime
- Weapons and equipment

Although technology cannot be the sole solution to these needs (other critical factors, for example, include organizational policies, procedures, structures, manpower, training, and culture), it can play an important role. Here are just a few of the ways that technology is relevant to important operational needs in law enforcement:

- Police increasingly recognize that their deployment and strategies should be guided by information and analysis that helps them focus on the places, persons, times, problems, and situations that contribute most to crime. Information technology can facilitate this orientation by improving the integration, analysis, and dissemination of information both within and across agencies. Information technology can also increase the efficiency of police in ways that ultimately improve their service and performance.

- Responding to calls for service is a central everyday task in policing. Moreover, it is a very resource-intensive task that can greatly limit the ability of agencies to devote resources to crime prevention strategies. Long delays in response can also adversely affect citizen satisfaction with police. Technologies that help agencies better manage calls for service and deploy their resources in more effective ways (e.g., computer-aided dispatching with geographic positioning systems and automated offense reporting) thus have the potential to both improve citizen satisfaction and facilitate crime prevention.

- The ability to communicate and coordinate actions with other first responders (i.e., fire and rescue and emergency medical personnel) is a need which has received heightened emphasis in recent years due to concerns about responses to potential terrorist attacks and disasters. Communications technology is central to this need.

- Technology has the potential to enhance and economize various forms of police training, such as simulation training in the use of force. At the same time, agencies must ensure that personnel are properly trained in the use of technology.

- Hiring and retention of officers has been a major concern for policing agencies during the last few decades. Technology can be used to market law enforcement (for example, sleek websites) but also can serve as a magnet for younger recruits interested in working with the latest technology. Agencies must attract and retain personnel with skills in the selection, implementation, and use of technology.

- Better technologies for collecting and processing criminal evidence can enhance case clearance rates and potentially reduce crime rates.

Priority Technologies for Law Enforcement

The national survey and workshop identified many technologies that are important to policing. Here, we focus on the top technologies identified by the workshop participants as being particularly critical to addressing high priority needs in law enforcement. Current high impact technologies that workshop participants identified included the following.

<u>High Impact Technologies</u>

- DNA testing equipment
- Integrated databases
- Geographic information system (GIS) software
- Computer-aided dispatch with global positioning system (GPS) tracking of patrol cars
- Video surveillance networks
- Wireless access in patrol cars
- Inter-agency radios
- Use of force computer simulators
- Fingerprint readers
- Conducted energy devices (such as Tasers®)
- Investigative software (such as data mining software)
- Body armor

Workshop participants also identified technologies that, in their view, have high potential for improving policing during the next 3 to 5 years and beyond. (A number of current high-impact technologies also appear on the following list, for reasons that will be discussed on the next page.)

<u>Promising Technologies for the Next 3-5 Years and Beyond</u>

- DNA testing equipment
- Integrated databases
- Computer-aided dispatch with global positioning system (GPS) tracking of patrol cars
- Predictive modeling
- Real-time crime monitoring centers

- Inter-agency radios
- Video surveillance networks
- Geographic information systems (GIS) software
- Investigative software (such as data mining software)
- Patrol car cameras
- Personal audio/video equipment (worn by officers)
- Aerial surveillance equipment (such as drones)
- Computer-based training and simulators
- Software for victimization risk factor analysis
- Next generation 9-1-1 systems (with advanced text and voice capabilities)

As these lists show, workshop participants placed much emphasis on technologies related to IT, crime analysis, and communications. Other priority technologies include non-lethal weapons and equipment for training, surveillance, and the collection and processing of evidence. Overall, most of the high impact and promising technologies listed above ranked highly on the PERF survey—higher percentages of users judged them to be very effective and higher percentages of non-users felt they would fully address important operational needs. Although many of these technologies are fairly common in policing, there is substantial room for expanding their use. This is particularly true for some of the less commonly used technologies like DNA testing equipment and personal audio/video devices.

Several technologies—DNA testing equipment, integrated databases, GIS software, computer-aided dispatch with GPS, video surveillance networks, inter-agency radios, investigative software, and computer-based training equipment—appear in both lists. These technologies thus appear to be high impact technologies with particularly high potential for future expansion and refinement. Indeed, according to the PERF survey, roughly a quarter or more of agencies without the following technologies are very likely to acquire them in the next few years: use of force computer simulators, wireless access in patrol cars, integrated databases, GIS software, inter-agency radios, computer-aided dispatch with GPS, conducted energy devices, and video surveillance networks. Other promising technologies for the future include predictive modeling (a variant of crime analysis and GIS), and real-time crime monitoring systems (which may combine integrated databases, crime analysis, GIS, and video surveillance networks), aerial surveillance equipment (such as small Unmanned Aircraft Systems), audio/video equipment for officers in the field, and enhanced 9-1-1 systems.

We should also note that there are a number of widely used technologies that may need replacement in coming years. Examples include night vision devices, use of force simulators, video surveillance equipment, special purpose vehicles, and mobile command centers. High percentages of agencies use these technologies according to the PERF survey, yet many reported that their equipment is old or outdated. Although these are not all high impact technologies, updating them may be an important issue for many agencies.

Barriers to Technology Acquisition and Use in Law Enforcement

Factors that impede or facilitate the application of technology in law enforcement were explored in both the PERF survey and the PERF-Lockheed workshop. Key issues that emerged include the following:

- Financial Constraints
- Training, Skills, and Project Management
- Partnerships
- Leadership, Mission, and Culture
- Impediments to Information Sharing
- Understanding Best Practices
- Other Political, Economic, and Legal Issues

Future Steps

As noted above, participants in the PERF-Lockheed workshop felt that the workshop was very valuable and that having more such forums would benefit the policing profession in ways such as: 1) identifying important technologies for policing; 2) developing standards for police technology; 3) disseminating best practices in technology implementation and use; and 4) helping agencies find funding and technical assistance for technology. PERF, Lockheed Martin, and others should build on this experience by sponsoring future workshops and conferences on law enforcement technology and by facilitating networking among technology specialists in policing.

Having identified broad technology categories for law enforcement, there is now a need to better understand which specific devices will best meet these technology needs. Further, we must identify best practices for the implementation and use of these technologies. We therefore recommend case studies to examine the implementation and use of these key technologies in agencies that have applied them successfully. Such studies should examine technical and organizational issues involved in planning and implementing these technologies, everyday uses of the technologies, and measurable outcomes associated with the uses of the technologies.

Similarly, there is a need for more evaluation research to provide police with better evidence on which technologies are most valuable and cost effective for law enforcement uses. Researchers, practitioners, and technology developers should collaborate in such work to identify the types and uses of technology that are most efficacious for policing and to delineate the implementation issues that impact the successful application of technology.

Chapter 1: Overview/Introduction

Technology has shaped policing in many important ways. One need only consider that the primary police strategy of the last several decades—motorized preventive patrol and rapid response to calls for service—was developed in response to the invention of the automobile and two-way radio communications. More recent technological developments have also had far-reaching effects on police agencies. Information technology, DNA testing, and bullet-resistant vests, for instance, are now common and critical tools in law enforcement. Contemporary concerns over homeland security and counterterrorism have also created new technological problems and demands for police agencies, as has the growth of computer-related crime.

Technological advances have great potential for enhancing police work. Technology may strengthen crime control by, for example: improving the ability of police to identify and monitor offenders, particularly repeat offenders; facilitating the identification of places and conditions that contribute disproportionately to crime; speeding the detection of and response to crimes; enhancing evidence collection; improving police deployment and strategy; creating organizational efficiencies that put more officers in the field and for longer periods of time; enhancing communication between police and citizens; increasing perceptions of the certainty of punishment; and strengthening the ability of law enforcement to deal with technologically sophisticated forms of crime (e.g., identity theft and cyber crime) and terrorism. Technological advancements in protective gear, weapons, and surveillance capabilities, to provide another illustration, can reduce injuries and deaths to officers, suspects, and bystanders. And to the extent that technology improves police effectiveness, strengthens communication between police and citizens, and reduces negative outcomes from police actions, it may also have the added, indirect benefit of enhancing police legitimacy. Growth in the technological sophistication of policing may even help with recruitment, particularly of younger people.

Given the importance of technology, the Police Executive Research Forum (PERF), a membership organization of police chiefs and sheriffs, has been actively exploring ways to harness technology to help advance the field of law enforcement. This interest has led to a new partnership for PERF. In July 2007, PERF, with support from the Lockheed Martin (LM) Corporation, embarked on a project designed to gain a detailed understanding of law enforcement's perspectives and high priority technology needs for the next three to five years and beyond. The partnership between PERF and LM's Advanced Concepts Protection Organization (ACPO) in its Law Enforcement Support (LES) group is unique and brings together complimentary expertise and skills. LM brings engineering expertise and extensive experience developing technology for the military. PERF has been working with hundreds of law enforcement agencies across the nation for four decades and has expertise in the full range of substantive and operational aspects of law enforcement.

The goal of this joint project was to identify, evaluate, and prioritize cutting-edge, relevant technologies that hold the greatest priority for policing. In doing so, we sought to recognize those technologies that afford the greatest promise in improving the ability of law enforcement to fulfill the security needs of the public in the most efficient manner available. Our project also sought to identify the key stakeholders and supporters within the decision chains of law enforcement, their requirements derivation and acquisition strategies for technology, and

opportunities that may emerge from the capability gaps in the form of technology products and/or services needs. By more effectively addressing the high priority technology needs, capability needs can be better defined, leading to a more refined solution, and that the "problem to solution cycle time" could be compressed, providing the law enforcement end-user a *"better, cheaper, faster"* solution (perhaps even skipping a generation in the technology development and/or acquisition periods).

The project objectives were to explore and document:

- The operational needs of law enforcement agencies
- The law enforcement perspective on technology—including beliefs about its effectiveness
- A prioritized list of technologies to develop for law enforcement
- Barriers to the introduction of technology in the LEA community
- Insights into the technology acquisition process for LEA of different sizes
- The uniqueness of the law enforcement context and implications for technology applications (e.g., officer use of discretion, political context, differences from military context)

Our team's research methodology included three basic components:

- An extensive review of the prior literature on law enforcement technology – Our team wanted to make sure that the project built on prior work in the field, and integrated insights from previous studies into this project. The results of this review are presented in the next chapter.

- Survey – PERF wanted to reach out to a large group of law enforcement personnel to assess their operational needs and priorities for technology development, with a special focus on innovative agencies. One of the most efficient approaches to meet this aim is to conduct a survey. The results of our survey are presented after the literature review.

- Focus group – To explore the results of our survey in more detail, PERF and LM designed a series of integrated focus groups conducted within a two-day workshop. The focus groups allowed the team to explore the meaning of the survey results, and provide additional context to appropriately interpret the implications of the survey results. The focus groups also allowed the team to explore new issues raised by the survey.

This document is organized into three main substantive chapters covering, in order, the following areas: the literature review, the survey findings, the focus group/workshop findings, and then a concluding chapter that brings all of the results together and discusses the implications of the results.

Chapter 2: Technology and Law Enforcement: An Overview of Applications, Impacts, and Needs[1]

2.1. Introduction

This chapter provides a comprehensive review of what is known about contemporary uses of technology by police agencies, the impact of technology on police effectiveness and outcomes, and the technological needs that police agencies are likely to face in the near future. Our discussion focuses on the following broad categories of technology, which are not mutually exclusive:[2]

- Information Technology
- Communications and Dispatch
- Identification and Investigation
- Sensors and Surveillance
- Weapons and Tactical Equipment

In the process, we attempt to identify the types of technology that may be most needed and useful to law enforcement in coming years.

2.2. Current Applications of Technology in Law Enforcement

In this section, we examine uses of technology by state and local police agencies, drawing largely upon national surveys and anecdotal reports.[3] Some of the most extensive information about the use of technology in policing comes from the Law Enforcement Management and Administrative Statistics (LEMAS) survey, a periodic survey conducted by the federal Bureau of Justice Statistics with a nationally representative sample of over 3,000 state and local law enforcement agencies that includes all agencies with 100 or more sworn officers. The most recent LEMAS data that are publicly available were collected in 2003 (Hickman and Reaves, 2006a; 2006b).[4]

2.2.1. Information Technology

Information technology (IT) has upgraded records management, data sharing, crime analysis, and performance management in police agencies in many ways over the last few

---

[1] A modified version of this chapter was disseminated as a discussion paper at the Law Enforcement Future Technologies Workshop discussed in Chapter 4. The authors thank Kristin Kappelman for research assistance in the preparation of this chapter.

[2] Our focus is generally on what some refer to as "high technology," defined as "scientific technology involving the production or use of advanced or sophisticated devices especially in the fields of electronics and computers" (www.merriam-webster.com/dictionary/high%20technology). However, our discussion extends beyond electronics to include advanced technologies such as DNA testing and sophisticated weapons systems.

[3] Our purpose here is to highlight the use of selected technologies rather than to provide an exhaustive inventory of all technology used by police.

[4] The 2003 LEMAS survey was administered by PERF for the Bureau of Justice Statistics. As of this writing, PERF is completing data collection for the newest version of LEMAS.

decades. According to the LEMAS survey, police agencies now commonly use computers to maintain a wide array of data. As of 2003, the majority of police agencies maintained electronic data on incident reports, arrests, calls for service, stolen property, and traffic citations (Hickman and Reaves, 2006a: 31; 2006b: 31). Other data that agencies often maintained in electronic form included warrants, criminal histories, traffic accidents, and summonses. Roughly 40% of agencies used electronic methods (including computers, data devices, telephone lines, and wireless transmission) as their primary method of transmitting incident reports (Hickman and Reaves, 2006a: 34; 2006b: 34). Furthermore, police use their IT capabilities to support a variety of functions including records management, crime analysis, criminal investigations, dispatch, and personnel management. Indeed, computers are now used to support many of these functions in a majority of all but the smallest police agencies (Hickman and Reaves, 2006a: 30; 2006b:30).

Many agencies also equip their officers with mobile computers or mobile computer terminals (collectively referred to as in-field computers) that afford direct access to many data systems from the field. The percentage of police agencies using in-field computers increased from around 5% in 1990 to roughly 55% in 2003; by the latter date, they were used by more than 90% of municipal and county agencies serving a population of 50,000 or more (Hickman and Reaves, 2006a: 32) and by more than two-thirds of sheriffs' offices serving similar size populations (Hickman and Reaves, 2006b: 32). In-field computers include a variety of vehicle-mounted and portable computers and terminals (e.g., laptops, digital data terminals, digital data computers, and personal digital assistants). In-field computers are often used to access information about vehicle and driving records, warrants, and criminal histories, among other items. In addition, between 27% and 33% of all agencies used in-field computers for writing field reports as of 2003 (Hickman and Reaves, 2006a: 33; 2006b: 33).

Nonetheless, significant gaps remain in the IT capabilities of law enforcement. As of 2003, only a minority of agencies maintained computerized files on potentially useful data such as criminal histories, use-of-force incidents, terrorism-related intelligence, and fingerprints (Hickman and Reaves, 2006a: 31; 2006b: 31). Less than one-third used computers for crucial functions such as crime analysis and dispatch (Hickman and Reaves, 2006a: 30; 2006b: 30). And most did not have in-field access to data systems on vehicles, driving records, warrants, and other information (Hickman and Reaves, 2006a: 33; 2006b: 33).

IT capabilities tend to be much more limited in very small agencies, notably those serving populations of 10,000 or less. Among agencies serving a population of 50,000 or more, for example, over 90% of municipal and county agencies and over two-thirds of sheriffs' offices had deployed in-field computers or terminals as of 2003; in contrast, fewer than half of the agencies serving 10,000 or fewer people had done so (calculated from Hickman and Reaves, 2006a: 3, 32; 2006b: 32).[5]

There were also substantial deficits in the capabilities of large agencies as of 2003. For example, even among the nation's largest agencies—those serving a population of 500,000 or more—many, and in some cases most, did not use computers for key functions like interagency information sharing, resource allocation, identification of crime "hot spots," and automated

[5] For additional discussion of IT uses in agencies serving a population of 50,000 or fewer persons, see Justice and Safety Center (2002).

booking (Hickman and Reaves, 2006a: 30; 2006b: 30). At least one in five also appeared to make limited use of computers for functions like crime analysis, intelligence gathering, criminal investigation, and dispatch. And many still lacked computerized files on items including criminal histories, use of force incidents, fingerprints, and biometric data (Hickman and Reaves, 2006a: 31; 2006b: 31).

The development of systems for sharing data within and across agencies is an IT issue that has received substantial emphasis in recent years. Due in part to recent concerns over terrorism, a number of systems and software packages have been designed to facilitate the sharing and analysis of data across agencies. Examples include regional data sharing systems and the 58 state and local fusion centers that have been established around the country by the Department of Homeland Security (DHS) to share information and intelligence (see http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm.

At the national level, the Federal Bureau of Investigation recently launched the Law Enforcement National Data Exchange, or N-DEx. N-DEx is a national information-sharing system available through a secure Internet site for law enforcement and criminal justice agencies (http://www.fbi.gov/page2/april08/ndex_042108.html). N-DEx allows agencies to search and analyze data using powerful automated capabilities designed to identify links between people, places, and events. The system includes several basic but vital capabilities, including searching and correlating incident/case report information and arrest data to help resolve identities (i.e., determining a person's true identity despite different aliases, addresses, etc.). N-DEx will also create link analysis charts to assist in criminal investigations and identify potential terrorist activity.

Furthermore, new software for crime analysis is enhancing the ability of police to use these data systems. For example, new software called COPLINK®, which has been characterized as "a super Google for police officers," has been designed to perform complex data searches and uncover hidden relationships and associations across multiple databases (http://www.COPLINK.com/overview.htm; also see Chen et al., 2002). Standard crime analysis capabilities are also becoming more sophisticated with respect to predicting crime patterns and tracking offenders through techniques like geographic profiling. Indeed, advances in IT hardware and software have spurred the advance of crime analysis as a new field that has great potential for increasing the efficiency and effectiveness of police work.

2.2.2. Communications and Dispatch

Virtually all of the nation's police agencies participate in 9-1-1 emergency telephone report systems (Hickman and Reaves, 2006a: 14; 2006b: 14). As of 2003, moreover, over 70% of police agencies, including 80% to 90% of those serving a population of 50,000 or more, utilized enhanced 9-1-1 systems, which display information such as a caller's phone number, address, and special needs. The majority of agencies serving a population of at least 10,000 persons also use computer-aided dispatch systems to help manage calls and minimize response times (Hickman and Reaves, 2006a: 30; 2006b: 30).

Enhancements to 9-1-1 systems that are being tried in some places include vehicle tracking systems that can identify the specific locations of patrol cars in real-time,[6] speech translation systems to provide immediate translation of calls, and the development of complementary 3-1-1 systems designed specifically to handle routine, non-emergency requests and queries (regarding the latter, see Mazerolle et al., 2002; Office of Community Oriented Policing Services, 2008). In the next decade, moreover, 9-1-1 call centers throughout the country may upgrade to a new system called Next Generation 9-1-1 (Daneman, 2008). Some of the capabilities designed into this system, which is being tested in a small number of jurisdictions, include the ability to take calls via text message or through voice over the Internet, as well as the ability to receive information about traffic accidents through navigation services like OnStar®.

Police are also upgrading their communications systems in various ways. One current priority is the development or improvement of communications systems that provide interoperability between police and other emergency first responders such as fire-rescue and medical units. To improve communications with the general public, police are also adopting or experimenting with technologies such as Internet notification (e.g., to inform the public about crimes, missing persons, community issues, alerts, etc.), text message alerts and tips, and handheld language translation devices.

2.2.3. Identification and Investigation

New technological tools are also aiding in criminal investigation. In 2003, about 60% of police agencies, employing nearly 90% of all officers, had access to an Automated Fingerprint Identification System (AFIS) that included a file of digitized fingerprints (Hickman and Reaves, 2006a: 34; 2006b: 34). Between 5% and 17% of agencies owned an AFIS system (this is more common among larger agencies), while the remainder shared an AFIS system[7] or accessed one through another agency. Between one quarter and one half of agencies, including two-thirds or more of those serving jurisdictions of 50,000 or more, had digital imaging technology for fingerprints. Also, between 9% and 21% of agencies had computerized files on fingerprints, including the majority of agencies serving jurisdictions of 500,000 or more people (Hickman and Reaves, 2006a: 31; 2006b: 31).

Though not yet in widespread use, new mobile fingerprint scanners allow officers in the field to conduct rapid checks of fingerprints. In addition, new chemical techniques for identifying fingerprints may also soon permit officers to identify substances handled or secreted by suspects (The Economist, 2008: 77).

However, DNA testing, which is based on the identification of unique individual genetic codes from biological evidence (such as blood, semen, hair, and saliva), now represents the state of the art in offender identification. Over the last few decades, DNA testing has become a

[6] Vehicle tracking systems can have the added benefit of increasing officer safety by quickly pinpointing the location of officers who are injured or in danger.

[7] AFIS was built by the Lockheed Martin Corporation for the FBI and later updated building the Integrated Automated Fingerprint Identification System (IAFIS). In 2008 the FBI awarded Lockheed Martin the Next Generation Identification (NGI) contract to update IAFIS adding facial recognition features, iris scan and advanced palmer surface search capabilities beyond the standard FBI “ten-print” scan.

common method of identification, particularly for sex crimes and other violent offenses. The DNA Identification Act of 1994 authorized the FBI to establish a national DNA database with indexes for persons convicted of crimes, missing persons (and relatives of missing persons), samples recovered from crime scenes, and samples recovered from unidentified human remains (Roman et al., 2008: 13-14). This national database is combined with state and local DNA databases in a system named CODIS (for the Combined DNA Index System). By the late 1990s, all 50 states had passed legislation requiring convicted offenders to provide DNA samples (Scwabe, 1999). Twelve states also require the collection of DNA samples from all or selected felony arrestees, though most of these laws require the samples to be destroyed if the suspect is released or acquitted (Johnson, 2008).

According to a recent survey, only 12% of local agencies have their own lab to conduct DNA testing; 80% send evidence to state labs for testing, while the remaining agencies use federal, private, or other types of labs (Lovrich et al., 2003: 15). Nationally, there is a substantial backlog of cases with biological evidence that has not been tested (Lovrich et al. 2003**).** Although they do not yet appear to be in common use, portable devices for the collection and testing of DNA evidence have been developed that may alleviate backlogs in DNA testing and greatly reduce the cost of such tests (Nunn, 2001: 263).

Turning to other means of identification, one-half to three-fourths of agencies had digital imaging technology for mug shots as of 2003 (Hickman and Reaves, 2006a: 29; 2006b: 29). Nearly a quarter of all agencies, and roughly 50% to 60% of those serving jurisdictions of 50,000 or more, had digital imaging technology for suspect composites. However, it is still fairly rare for agencies to have digital imaging technology for facial recognition or computerized files with biometric data for facial recognition (Hickman and Reaves, 2006: 29,31; 2006b: 29,31).[8]

Digital imaging is also commonly used to investigate gun crimes. Through its National Integrated Ballistic Information Network (NIBIN) Program, the federal Bureau of Alcohol, Tobacco, Firearms and Explosives deploys Integrated Ballistic Identification System (IBIS) equipment to federal, state and local law enforcement agencies for their use in imaging and comparing ballistics evidence (http://www.nibin.gov/documents/081208atf-nibin-program.pdf).[9] The NIBIN Program currently has 203 sites that have received IBIS equipment. There are 174 agencies participating in the program, and every major population center has access to ballistic imaging technology.

Criminal investigation has also been improved by various other forms of technology. The IT advances noted above—including automation of criminal records, integration of

[8] To illustrate the use of such technology, researchers in the United Kingdom have used facial and voice recognition systems to build a database of violent criminals and sex offenders (Reed, 2008). The Pinellas County (FL) Sheriff's Office, to provide another illustration, uses facial recognition software to identify prisoners booked into the county jail (Reed, 2008). These images are stored in a database along with other identifiers (name, date of birth, address, etc.) that can be searched in order to find a match. Finally, the National Law Enforcement and Corrections Technology Centers (NLECTC) can enhance audio tapes and videotapes to assist in investigations, and have also developed an integrated facial identification system that can screen over one million mug shots in less than two seconds (Scwabe, 1999).

[9] This equipment allows firearms technicians to acquire digital images of the markings made by a firearm on bullets and cartridge casings; the images then undergo automated initial comparison.

databases, in-field computer access, and sophisticated crime analysis and investigative software—have undoubtedly facilitated the identification and apprehension of suspects. To provide other examples, the use of GPS devices to track stolen vehicles is becoming more common, particularly in the largest police agencies (Hickman and Reaves, 2006a: 29; 2006b: 29). Further, about half of police agencies reported conducting cyber crime investigations as of 2003 (Hickman and Reaves, 2006a: 15; 2006b: 15), thus making technologies for such investigations another priority area.

2.2.4. Surveillance and Sensors

Stand-alone and networked video cameras provide police with the ability to monitor high-risk locations, roadways, and interactions between officers and the public. In 2003, roughly two-thirds of state and local police agencies used video cameras on a regular basis (Hickman and Reaves, 2006a: 28; 2006b: 28). More than half used video cameras in cars, where, as experts have noted (Schultz, 2008), they can be a valuable tool not only for recording suspects' behavior but also for monitoring officer professionalism in traffic stops, criminal investigations, arrests, and training. To a lesser extent, agencies also used video cameras for fixed-site surveillance, traffic enforcement, and mobile surveillance. Some agencies are also attaching small cameras to their officers' uniforms.

Surveillance systems are growing rapidly in size and sophistication. Though systematic data are not yet available, cities are increasingly deploying networked, wireless surveillance systems that monitor many locations simultaneously (sometimes from cars as well as from fixed locations), thus facilitating rapid response to crimes and providing a tool for follow-up investigation (e.g., see Police Executive Research Forum, 2007: 22-24). In Washington, D.C., New York City, Chicago, and London, for example, police have access to systems with thousands of cameras (Hohmann, 2008). Some new systems have the ability to recognize sounds that signify potential trouble, and cameras may move in synchronization with sounds. Soon, video monitoring systems may also be augmented with facial and behavioral recognition systems (Nunn, 2001: 264-265).

It also appears that more police agencies are deploying gunshot detection systems (e.g., Mazerolle et al., 1999; Police Executive Research Forum, 2007: 30). These systems, which consist of sensors placed on buildings or other locations, are designed to recognize gunfire and instantaneously pinpoint its location using GPS technology. On a related note, there have also been efforts to develop portable devices that can detect the carrying of concealed weapons (e.g., see National Institute of Justice, 1996). Such devices have not yet been widely deployed, due perhaps to both technical and legal complications (on the latter, see Jacobs, 2002: 201-205). A national survey conducted in 2000 revealed that nearly two-thirds of police agencies felt that concealed weapon detection devices would be valuable but were not available to them (Schwabe et al., 2001).

Other new developments with respect to sensors and surveillance systems include the use of GPS devices to track suspects and stolen vehicles (on the latter point, see Hickman and Reaves, 2006a: 29; 2006b: 29); the deployment of license plate readers (in cars or in fixed locations) that automatically scan the license plates of motor vehicles and check them against databases on stolen cars and other vehicle records; and the use of various night-vision, electro-

optic, and "see through walls" devices. According to the 2003 LEMAS survey, roughly a quarter to a third of all police agencies, and a majority of those serving a population of 50,000 or more, used infrared (thermal) imagers, and between 10% and 13% used image intensifiers (Hickman and Reaves, 2006a: 29; 2006b: 29).[10]

Various fixed and portable sensor devices are also becoming more available for the detection of drugs, contraband, and hazardous materials of a chemical, biological, or nuclear nature. Sandia National Laboratories, for example, are developing a handheld drug detection device (the MicroHound®) that will have an estimated commercial cost of $5,000 to $10,000, making it far less expensive than earlier versions that were priced at $74,000 (Falcon, 2005: 22-24). To provide another illustration, the federal Counter Drug Technology Assessment Center (a center within the Office of National Drug Control Policy) has been developing non-intrusive cargo inspection devices, as well as devices for detecting hidden compartments in automobiles. A prominent application of new sensor devices will occur in New York City, which has announced plans to establish an extensive system of surveillance cameras and hazardous substance detectors throughout the city. Other places at high risk of terrorist activity may follow suit.

2.2.5. Weapons and Tactical Equipment

Besides weaponry, there are numerous technologies that have tactical uses for police, some of which have been mentioned above. Examples include special surveillance equipment (i.e., night vision/electro-optic devices), engine disruption devices, aerial surveillance equipment, and robots for disposal of explosives and hazardous materials, to name a few. Our discussion below, however, focuses on technology related to weaponry and protective gear.

In recent years, police have increasingly sought technologically advanced non-lethal weapons to replace or complement traditional weapons such as batons, firearms, tear gas, and chemical agents. The most common of these are conducted energy devices that incapacitate subjects through pain compliance or electro-muscular disruption (i.e., stun guns or the well-known Taser®). Such devices were used by 23% to 30% of police agencies as of 2003 (Hickman and Reaves, 2006a: 26; 2006b: 26).[11]

Other newly emerging devices for controlling individuals or crowds include high intensity light weapons, currently used by only 1% of police agencies (Hickman and Reaves 2006a: 26; 2006b: 26), and sound wave devices. An illustration of a non-lethal light weapon is the "LED Incapacitator" recently developed for the Department of Homeland Security (Allen, 2008). This device causes "flash blindness," nausea, and disorientation by flashing lights at several randomly changing frequencies. In contrast, long range acoustic devices, which can be used to amplify police orders over a long distance, can also be used as a non-lethal weapon that

[10] Thermal imaging devices produce images of radiated or reflected surface energy in the thermal portion of the electromagnetic spectrum through the use of a non-intrusive electronic device (Schultz, 2008). Applications of thermal imagers include searches for missing or fleeing individuals, collection of physical evidence, and marijuana investigations. Image intensifiers are devices used to enhance night vision.

[11] The U.S. Government Accountability Office (GAO) recently reported that more than 7,000 police agencies in the United States use conducted energy devices (GAO, 2005).

causes pain, nausea, disorientation, and possibly hearing damage. Reportedly, about a dozen public safety agencies nationally have purchased such equipment (Webby, 2008).

On a related note, new technology is also providing better means by which to train officers in the use of force and to monitor use of force by officers. Computer-driven, interactive simulation training systems are now available that require officers to make use of force decisions using hundreds of scenarios that police trainers can customize in various ways (e.g., see McCarron, 2008; also see www.ies-usa.com/products/range_pro). A few agencies are also reportedly considering or testing pistol cams, small video-audio recorders attached to firearms that can capture important contextual details about the circumstances in which officers use firearms (Washington Times, 2008).

Turning to protective gear, lightweight body armor has been widely available to law enforcement for more than two decades. As of 2003, about 70% of police agencies required officers to wear body armor in at least some circumstances, with between 55% and 60% requiring officers to wear it all the time (Hickman and Reaves, 2006a: 25; 2006b: 25). Agencies are also now seeking gear to protect officers from other hazards, notably nuclear, biological, and chemical hazards (hereafter, we use the term CBRNE for chemical, biological, radiological/nuclear, and explosive). Such gear may not yet be widely deployed among police agencies; as of 2000, at least 79% of local police agencies reported that blister/nerve agent protective clothing was not available to them (Schwabe et al. 2001: xvii).

Looking ahead, researchers at the U.S. Department of Defense are designing the LEAP system uniform, which will offer ballistic, chemical, and biological protection for special operations officers (Reed, 2008). This state-of-the-art equipment will also have features that include a helmet that has a GPS, radio antenna, and visor with a heads-up display.

2.3. Technology and Police Effectiveness

Having reviewed many of the technologies in use by police, we now consider the available evidence on how technology has impacted the outcomes and effectiveness of policing. In principle, many forms of technology would seem to have the potential to improve police efficiency and effectiveness. Yet the impact of any given technology on police effectiveness may be limited by several factors, including: technical (i.e., engineering) problems; difficulty in using the technology; ancillary costs associated with using the technology (e.g., costs associated with training, technical assistance, and maintenance); unanticipated effects on organizations, officers, or citizens; the prevalence of the problem(s) the technology is intended to address; or a misunderstanding of the problem(s) the technology is intended to address. For any of these reasons, some technologies will perform better than others, and some may not perform as intended at all. Some technologies may also create economic and political liabilities for police. Understanding which technologies are most useful to police and why has obvious value to agencies allocating scarce resources.

However, demonstrating impact and cost-effectiveness is more straightforward for some technologies than for others. Technologies that improve everyday operations and crime reduction, for instance, are easier to assess in this regard than technologies designed to address low-probability, high-impact events (such as CBRNE attacks). Another complication is that the

effectiveness of one technology may be dependent on the availability of other complementary technologies within an agency. As one expert has noted with respect to surveillance and biometric technologies (Nunn, 2001: 262):

> "Grabbing video images of apparent lawbreakers is less valuable if there is not also in place a compendium of faces against which to compare the video still. Biometric measurements are less useful without an ancillary database of templates against which comparisons for identity can be made. In this sense, many law enforcement technology systems are sequential and highly dependent on other systems."

In our assessment below, we focus on scientific evaluations rather than descriptive accounts.[12] Further, we emphasize social science process and impact evaluations of technology, as opposed to engineering reports on the design and testing of technologies. We also generally limit our attention to studies from the mid-1990s onward.

We note at the outset that there has been relatively little scientific study of technology's impact on policing and few carefully controlled before-and-after evaluations of technology implementation. Much of the available evidence, moreover, fails to show that technology has brought about clear and quantifiable improvements in policing. Although the evidence on these matters is very limited both in quantity and in scientific quality,[13] it does suggest, nevertheless, that there is a need for scientists and police to think carefully about the uses and efficacy of technology in policing. For instance, will a given technology enhance proven crime control strategies? Does it fit with known facts about crime? What other organizational changes—in terms of policies, procedures, equipment, systems, culture, and/or management style—might be necessary to optimize the use of a new technology? And what implementation issues and unintended consequences (both internally and externally) might arise?

2.3.1. Computers and Information Technology

As discussed in section 1, computers and IT more generally have become quite common in policing. In many respects, IT would seem to be the category of technology that has the most potential to enhance the effectiveness of police in reducing crime. By improving the ability of police to collect, manage, and analyze data, IT can enhance the administrative efficiency of police organizations and help them target the people, places, and problems that contribute most to crime. With respect to the latter point, promising policing innovations such as hot spots policing (e.g., see Braga, 2007; National Research Council, 2004; Police Executive Research Forum, 2008) and Compstat (e.g., see Bratton, 1998; Weisburd et al., 2004) have been spurred largely by advances in IT.

At the same time, however, there are many costs associated with IT, including costs for hardware, software, training, support staff, and maintenance. These costs may drain resources from other important functions. Complications in using IT may also limit its effectiveness.

[12] Note, however, that we generally do not discuss the technical aspects of these studies (i.e., research methods and statistical approaches).

[13] Our discussion focuses on general conclusions from the available literature; we do not discuss and critique studies in detail.

Finally, the impact of IT on police performance is likely to be mediated by the ways in which officers and resources are managed, a point to which we return below.

Global assessments of IT's impact on policing have yielded mixed and ambiguous results. For example, some research indicates that police departments with higher levels of computerization and IT tend to have higher expenditures, a larger share of employees in technical positions, and fewer officers per capita (Nunn, 2001). Whether this affects their ability to reduce crime has not been studied. While these patterns suggest that agencies with more IT have fewer officers on the street (due perhaps to the resources required to operate and to maintain IT), it is also possible that agencies with more IT make better use of their officers, thus offsetting their smaller deployments.

Some of the broadest assessments of IT's impact on policing have come from evaluations of the Community Oriented Policing Services program, a federal initiative launched in 1994. Commonly known as the COPS program, this initiative provided hundreds of millions of dollars in grants to state and local agencies for technology acquisition (as well as billions for hiring new officers). These grants were intended to assist agencies in acquiring technology that, by creating time savings and other efficiencies, would enable the grantees to put more of their officers into the field and to keep them there for longer periods of time. It was also expected that agencies would use these additional officer-hours to implement various forms of community policing.

COPS grantees used much of their funding to obtain various forms of IT. Common forms of IT acquired by COPS grantees as of 1998 included mobile and desktop computers (acquired by 79% and 45% of grantees, respectively), computer-aided dispatch systems (acquired by 12% of grantees), booking and arraignment technologies (acquired by 12% of grantees) and telephone reporting systems (acquired by 6% of grantees) (Roth et al., 2000). Although grantees often reported unexpected costs and complications associated with technology implementation (Roth et al., 2000), it appears that the grants enabled agencies to achieve substantial officer redeployments. As of 2000, grantees reported that they had or soon expected to redeploy the equivalent of between 29,000 and 30,000 officers through their technology grants, though some uncertainty remains about the validity of these estimates (Koper et al., 2002; also see Koper and Roth, 2000).[14]

Studies of the COPS program's effects on crime have yielded contradictory findings with respect to technology grants. One analysis of COPS grants and crime from 1995 to 1999 suggested that the technology funding did not improve the ability of grantees to control crime (Zhao et al., 2001). In contrast, a later study by the United States Government Accountability Office (GAO) concluded that each $1 spent per person on technology grants reduced the index crime rate by approximately 17 per 100,000 persons (GAO, 2005).[15] However, both studies

[14] To make these projections, agencies' estimates of time savings attributable to technology were converted into full-time officer equivalents (FTEs). Each FTE is equivalent to 1,824 hours, which is the federal estimate of the average time that a police officer works each year (excluding overtime). FTEs redeployed or expected as of 2000 represented 92% to 93% of the redeployment levels that grantees had originally projected when they applied for their grants (Koper et al., 2002). For other studies of time savings (or the lack thereof) associated with the use of mobile data terminals and mobile computers, see Colvin (2001) and Frank et al. (1997).

[15] Index crimes, as defined by the Federal Bureau of Investigation, include murder, rape, robbery, aggravated assault, burglary, larceny, auto theft, and arson. Also note that the technology grants discussed above were made

indicated that grants for hiring officers and supporting innovative programs had larger impacts on crime than did technology grants. And neither study aimed to identify the types or uses of technology that were most effective in reducing crime.

Case studies of IT in policing have also yielded mixed findings. While some research suggests, for example, that the use of mobile data terminals by patrol officers improves the recovery of stolen autos (Nunn, 1994), other research suggests that enhanced wireless communication technology has relatively little impact on officer productivity and does little to enhance problem-oriented policing (Nunn and Quinet, 2002). Similarly, other evidence casts doubt on whether access to regional information sharing systems improves clearance rates, though officers with access to such systems believe that information sharing makes them more productive and contributes to solving crimes (Zaworski, 2004).

At the same time, it is worth reiterating that IT-related advances in geographic information systems (GIS), records management, and crime analysis software, for instance, have been very important to the spread of innovations like geographically-focused, "hot spots" policing—an approach that has proven effective in a number of rigorous evaluations (Braga, 2007). Yet such technologies will have less impact if organizations fail to make other changes that are necessary to fully capitalize on new technologies. Technologies that facilitate hot spots policing, for example, will have less impact if police managers fail to focus adequate resources on crime hot spots or if the results of crime analysis are not adequately disseminated throughout the agency. Hence, the impact of IT (and other technologies) will depend in many cases on other organizational changes, such as the adoption of Compstat, a managerial approach that takes advantage of IT by combining state-of-the-art management principles with crime analysis and GIS (e.g., see Willis et al., 2004; Weisburd et al., 2003).[16]

2.3.2. Communications and Dispatch

Studies of communications-dispatch systems illustrate how new technology may have unanticipated side effects or may fail to achieve desired outcomes. Today's standard 9-1-1 emergency phone and response systems, for example, were a technological innovation intended in large part to improve offender apprehension by reducing police response times to reported crimes. As some observers have noted, "Emergency 9-1-1 call systems comprise the single most important technological innovation that has shaped and defined police practices over the last three decades" (Mazerolle et al., 2002a). Police agencies continue to put vast sums of money into upgrading and improving their computer-aided dispatch 9-1-1 systems.

However, 9-1-1 systems do not appear to have enhanced police effectiveness; on the contrary, it is often argued that 9-1-1 limits police effectiveness. To begin with, the notion that 9-1-1 systems improve offender apprehension has been undermined by studies showing that

---

through the COPS MORE program (MORE is an acronym for Making Officer Redeployment Effective). Although MORE funding was primarily awarded for technology acquisition, some MORE funds were also used for hiring civilians and for officer overtime.

[16] As described by Willis et al. (2004), the core elements of Compstat include: mission clarification; internal accountability; geographic organization of command; organizational flexibility; data-driven identification of problems and assessment of the department's problem-solving efforts; innovative problem-solving tactics; and external information exchange.

response times have little effect on arrests due to typical delays in the reporting of crime (Sherman and Eck, 2002: 304-306).[17] Further, the burden of answering 9-1-1 calls, roughly half or more of which are not urgent (Mazerolle et al., 2002a: 98), tends to leave police with less time to engage in proactive or community-oriented policing. Indeed, the 9-1-1 system is commonly viewed as an obstacle to innovative policing (e.g., see Sparrow et al., 1990).

More recently, some police agencies have established alternative 3-1-1 systems for non-emergency calls as a technological approach to reforming their 9-1-1 systems. Limited research on 3-1-1 systems suggests that they can help police agencies to better manage calls and reduce burdens on 9-1-1 systems (Mazerolle et al., 2002a). They may also improve response times to true emergency calls and improve citizen satisfaction with the handling of calls. However, 3-1-1 systems do not create much more time for officers to engage in proactive activities, absent other organizational and policy changes to manage call loads. Hence, it is not clear whether the development of 3-1-1 systems will improve the ability of police to reduce crime.

2.3.3. Sensors and Surveillance

Several studies, conducted mostly in the United Kingdom, have examined the effects of closed-circuit television (CCTV) on crime. In principle, CCTV should reduce crime by raising offenders' perceptions of risk. Some have also speculated that the presence of CCTV may strengthen informal social control in an area by improving residents' and workers' perceptions of the area and increasing their sense of territorial ownership (Welsh and Farrington, 2004).

A recent review of 19 high-quality studies of CCTV found that CCTV generally reduces crime by about 21% (Welsh and Farrington, 2004: 509). However, this overall effect was largely attributable to studies focusing on parking lots and garages in the United Kingdom. CCTV has not been as effective in reducing crime in center city areas or in residential/public housing settings. Further, the few tests of CCTV that have been done in the U.S. have not shown strong effects on crime (Mazerolle et al. 2002b; Musheno et al., 1978). This has led some to speculate that the relative ineffectiveness of CCTV in the U.S. may be linked to greater public wariness of, and political resistance to, public surveillance in the U.S. (Welsh and Farrington, 2004: 515-517).[18] On the other hand, a study in Cincinnati suggests that CCTV has short-term effects on anti-social behavior that might be optimized by rotating CCTV across crime and disorder hot spots every one to two months (Mazerolle et al., 2002b). Further, the effectiveness of CCTV in reducing crime may be enhanced by the incorporation of biometrics technology for facial and behavioral recognition into surveillance systems (e.g., see Nunn, 2001) and by the emerging use of widespread CCTV networks that facilitate live monitoring. Assessing such systems will require careful examination of exactly how they are used for both rapid response and follow-up investigation.

Gunshot detection systems are another form of surveillance technology that has been tested in the United States. Field tests conducted in Redwood City, California and Dallas, Texas

[17] These include delays in the victim's discovery of the offense (e.g., discovering that one's car has been stolen) as well as delays in victim reporting after offenses involving direct contact with offenders.

[18] As noted by Welsh and Farrington (2004: 516), this could result in, among other possibilities, cuts in program funding or police assigning a low priority to the camera systems.

suggest that the deployment of these devices is unlikely to increase arrests of shooters because police will not arrive at gunshot locations quickly enough to apprehend offenders (Mazerolle et al., 1999). (This finding is consistent with the research findings discussed above on rapid response to calls for service.) Whether newer systems can improve upon the performance of earlier systems remains to be seen. Even if not, some argue that gunshot detection devices can still be a valuable tool for studying and responding to gun crime (Mazerolle et al., 1999).[19]

2.3.4. Identification and Investigation

Two ways in which technological advancements can improve the identification and apprehension of offenders are by improving the collection, preservation, and testing of physical evidence and by integrating data systems within and across agencies. Part of the value of these technologies lies in the fact that they can facilitate the identification of repeat offenders who contribute disproportionately to crime.

One of the most notable advancements in this area has been the use of DNA evidence to identify criminal suspects. As discussed in section 1, the use of DNA evidence by law enforcement has expanded greatly during the last several years. In the U.S., DNA testing is mostly used in violent crime cases due to its expense, and evidence on its effectiveness is largely anecdotal (Roman et al., 2008).

However, a recent randomized experiment involving five jurisdictions found that DNA evidence greatly enhances outcomes in property crime cases, namely, residential and commercial burglaries and thefts from automobiles (Roman et al., 2008). Compared to traditional investigations, cases involving the use of DNA evidence resulted in twice as many suspects being identified, twice as many suspects being arrested, and more than twice as many cases being accepted for prosecution. Compared to the use of fingerprints, the use of DNA was also at least five times more likely to result in the identification of a suspect. Moreover, suspects identified through DNA evidence tended to be more serious offenders; overall, they had at least twice as many felony arrests and convictions as did suspects identified in other cases.

These findings are also consistent with evidence from the United Kingdom, where there has been a national program to expand the use of DNA evidence in property crimes. Research from the UK indicates that the suspect identification rate in burglary cases with DNA evidence is 41% as compared to 16% in other cases (Home Office, 2005, cited in Roman et al., 2008: 7).

As stated earlier, data systems that better integrate information, both across units within an agency and across multiple agencies, constitute another form of technology that should improve the ability of police to identify and apprehend offenders. The impact of IT on policing was discussed above, but it is worth noting here that early research on IT and policing suggests

[19] To our knowledge, other forms of surveillance technology have not been tested in a rigorous manner. However, PERF and the Mesa, Arizona Police Department are currently conducting a field test of portable license plate scanners using a rigorous, randomized experimental design. This study is assessing whether the use of license plate scanners improves the recovery of stolen automobiles and the apprehension of auto thieves in auto theft hot spots.

that access to computerized systems such as national and state databases on criminal histories and warrants has improved the productivity of detectives (Danziger and Kraemer, 1985).

Current state-of-the-art systems provide many agencies with sophisticated capabilities for linking and querying databases within and across agencies. For example, officers may query things like nicknames or see linkages of offenders, suspects, victims, and associates across multiple databases within an agency. Agencies are also increasingly linking databases with other agencies in regional data sharing systems. There has been little study of the impact of these advanced systems on case clearances and crime rates. One comparative study of two agencies, one with access to a regional data sharing system and one without, found that officers with access to regional data systems view IT more favorably, but it did not find evidence that these systems enhance clearance rates, due in part to the mediating influence of management style on performance (Zaworski, 2004).

Indeed, a general caveat to this discussion is that the spread of advanced technology in policing does not seem to have been accompanied by higher clearance rates for criminal investigations. Clearance rates for violent and property crimes in 2007—44.5% and 16.5%, respectively—were no better than those in 1995—45.4% and 17.1%, respectively (see the Federal Bureau of Investigation's Uniform Crime Reports at (http://www.fbi.gov/ucr/ucr.htm#cius).

2.3.5. Weapons and Tactical Equipment

Recent research on police weaponry and tactical equipment has focused on the deployment of conducted energy devices, commonly known by the trade name Tasers™. These devices were developed to provide an effective, non-lethal method of incapacitating suspects, thereby reducing injuries and deaths of both officers and suspects. Testing data from Taser® International, the developer of the Taser® device, and data reported to Taser® International voluntarily by a number of police agencies suggest that the devices have reduced injuries and deaths to officers and civilians (Jenkinson et al., 2006).[20] Further, some of these data suggest that despite a relatively small number of deaths associated with Taser® use, the devices have saved 70 lives for every one lost (Jenkinson et al., 2006).

However, an independent study of Taser® use in two police agencies found that use of the devices reduced officer and suspect injuries in only one of the two agencies (Smith et al., 2007). In the other agency, Taser® use had no association with officer or suspect injury; further, the use of pepper spray appeared to be more effective in reducing suspect injuries.[21] It is also not yet clear how Tasers® affect the likelihood that officers will choose or need to use force.[22]

Body armor, which began to be deployed in police agencies in the mid- to late-1970s (National Institute of Justice, 2001), has also been effective in reducing officer fatalities. To

[20] Similarly, some police agencies have reported reductions in firearms discharges after deploying Tasers® (Jenkinson et al., 2006).
[21] However, evidence from both agencies indicated that Tasers® and other intermediate level weapons were preferable to the use of hands-on force.
[22] With funding from the National Institute of Justice, PERF is currently studying the impact of Taser® adoption on deaths and injuries to suspects and officers in several cities.

date, there have been more than 3,000 lives reportedly saved by the use of personal body armor (National Law Enforcement and Corrections Technology Center, 2006). Data compiled by the Federal Bureau of Investigation on officers killed and assaulted indicate that officers are 14 times more likely to sustain a fatal injury when not wearing body armor (FBI, 1994). Indeed, the growing use of body armor by police is believed to have contributed to a decline of more than 50% in felonious killings of police from the early 1980s to 1999 (Fridell and Pate, 2001).[23]

2.4. Technology Needs in Law Enforcement

The research evidence discussed in the preceding sections provides insight into the technology needs of law enforcement by showing which technologies are most widely used (and presumably valued) in policing, which technology applications are underdeveloped or underutilized, and which technologies are most effective in practice. Additional evidence on technology needs in policing comes from the opinions of law enforcement practitioners and other experts, which we explore below.

2.4.1. Research on Technology Needs in Law Enforcement

The most systematic information available on technology needs in policing is based on a number of survey and focus group projects that were conducted in the late 1990s and early 2000s. The most comprehensive of these projects were conducted during or before 2000**,** thus underscoring the need for an updated assessment of this issue.

In 1997, the National Institute of Justice (the research and development agency within the U.S. Department of Justice) sponsored a review of law enforcement technology needs to combat terrorism (National Institute of Justice, 1999; TriData, 1998). Some of the key conclusions from this project, which involved more than 100 interviews and group discussions with nearly 200 practitioners representing 138 state and local agencies throughout the nation, included the following:

- The technology needs of state and local law enforcement are remarkably similar across the nation, with minor regional variations;
- Affordability is a key criterion for new technology;
- Many, if not most, of the capabilities needed to combat terrorism are also needed to combat crime in general;
- State and local agencies are particularly concerned about their ability to deal with weapons of mass destruction; and
- Combating cyber-terrorism is a growing concern.

The report also highlighted several more specific technological needs that practitioners cited most frequently:

[23] During this time, the number of police officers feloniously killed in the line of duty decreased from over 90 in the years preceding 1983 to 42 in 1999 (Fridell and Pate, 2001).

- Improved capabilities for sharing information among local, state, and federal agencies. Participants suggested that a national terrorism intelligence database, operated by the federal government, would be the best method for them to share intelligence information.
- Technology to detect explosives, including the means to "look into" a device, ascertain its contents, and determine if it contains chemical, biological, radiological/nuclear, or explosive (CBRNE) material.
- Secure communications. Only a small number of field officers, even in large departments, have secure portable radios, and those who do have radios are typically involved in counter-narcotics activities.
- Improved means of detecting and categorizing CBRNE threats. Needs cited here included portable detectors that can detect a wide range of hazards.
- Multi-agency, multi-jurisdictional communications systems (i.e., interagency communications systems), especially for use in responding to major incidents that could involve multiple law enforcement agencies and other government agencies.
- Robots for disarming and disabling explosive devices. Reducing the cost of these robots was considered key, along with dexterity and the ability to send more definitive diagnostics (such as sharper pictures and X-rays) to technicians.
- Improved and affordable protective gear against CBRNE hazards.
- Less-lethal weapons for suspect apprehension and riot control.
- "See through the wall" capability to locate terrorists and hostages, especially through typical interior residential walls.
- Long-range video monitoring equipment with higher resolution, longer range, unobtrusiveness, and remote operation capability.
- Improved means to detect, investigate, and defend against cyber-terrorism. Of particular concern was the vulnerability of agencies' computer systems.
- Improved electronic listening devices with, for instance, less detectable body wires, longer life "bugs," and better long-range audio eavesdropping capability that works through windows.
- Improved technology for training, including capabilities for virtual reality and interactive computer systems that support training of technical specialists and incident commanders.
- Improved containment vehicles and vessels for explosive devices that could also contain chemical and/or biological agents if present; and
- Improved night vision devices.

In 2000, the RAND Corporation conducted a more general examination of technology needs in law enforcement (Schwabe et al., 2001). In a national survey, RAND found that the majority of agencies reported that the following technologies were both not available and "not unnecessary" (the percentage of agencies citing each technology is listed in parentheses):

- Detection and analysis of cyber attacks (79 percent)
- Blister/nerve agent protective clothing (79 percent)
- Video conferencing equipment (75 percent)
- Kinetic energy projectiles (75 percent)
- Chemical agent detection (71 percent)
- Long-range video monitoring (69 percent)

- Stun devices/projectiles (68 percent)
- Radioactive agent detection (66 percent)
- Explosive detection (64 percent)
- Fleeing vehicle interdiction equipment (63 percent)
- Concealed weapon detection devices (62 percent)
- Bomb containment/disablement equipment (60 percent)
- In-field (in car) computers (58%)
- Electronic listening devices (57%)
- Night vision devices (57%)

Other technologies commonly cited included, among others, special purpose vehicles, technology for crowd and riot control, equipment for computer-based training, computer-assisted dispatching, and integrated databases (2001: xvii). However, the findings above should be qualified by noting that the agencies did not indicate how strongly these technologies were needed.

The study also examined technology in need of replacement. Roughly half of the agencies reported that their radio equipment, training equipment, or administrative accounting systems were either old or obsolete (2001: xix). Other technologies described as old or obsolete by a quarter of more the responding agencies included workspace computers, audio-visual equipment to obtain evidence, crowd or riot control equipment, body armor, computer-based training, integrated databases, cell phones, and others.

Other leading technology-related needs identified by state and local police agencies included training (both technology to improve training, and training to use newly acquired technology); technology to improve command, control, and accountability; information and standards for judging technology and improving technology-related planning; and technology for interoperability with other agencies (2001: xxix). Finally, the study also drew attention to the inability of forensic labs to keep up with demand, due in part to the lack of automated technology that could increase productivity (2001: xxx).[24]

Another NIJ-sponsored survey conducted in 2000 looked specifically at technology use and needs in smaller police agencies, defined as those having no more than 19 officers and serving a jurisdiction of 50,000 or less (Justice and Safety Center, 2002; National Institute of Justice, 2004). Technologies that small agencies perceived to be most important included communications technology (e.g., mobile, portable, and base station radios), personal and mainframe computers, and video cameras in patrol cars (Justice and Safety Center, 2002: 16). To varying degrees, small agencies placed less emphasis on, and tended to have less experience with, a number of more sophisticated technologies, including in-field computers, digital imaging, GPS, and night vision/electro-optic devices. It was also apparent that small agencies would need a great deal of training to adopt many advanced technologies. (However, two-thirds of the agencies surveyed said they received technology assistance through inter-agency cooperation.)

[24] On a related note, backlogs in DNA testing were also explored in an NIJ-sponsored study by Washington State University and Smith Alling Lane (Lovrich et al., 2003). As of 2001, they estimated that there were more than a half- million criminal cases with possible biological evidence that either had not been submitted for DNA testing or that were backlogged at forensic laboratories (p.3).

The report concluded that small agencies may be underutilizing advanced technologies and that this tendency is largely driven by resource limitations, a belief that advanced technologies are not strongly needed in small jurisdictions, and unawareness of many new technologies and their benefits (NIJ, 2004: ii).

Finally, the International Association of Chiefs of Police (IACP) conducted an online survey for NIJ in 2005 to identify technology needs in law enforcement (IACP, 2005). Because only 47 agencies answered the survey, the results must be viewed cautiously. However, the participants represented a range of large and small agencies.

Among 12 technology categories that participants were asked to rank in priority, the top five were those related to communications, patrol cars, management, forensics, and video cameras (p. 3). Agencies were also asked to rate the importance of specific technology applications within each category. Specific applications that were rated most highly within the top five categories included the following (p. 7).[25]

- Communications: mobile and wireless personal computers, radios, bandwidth, and cell phones
- Patrol cars: mobile data terminals, lights, and sirens
- Management: records management systems, use of force, and computer aided dispatch
- Forensics: crime scene investigation and computers
- Video cameras: in-car and wireless cameras

Specific technology applications that ranked highly in other technology categories included fingerprints and digital imaging.

2.4.2. Other Sources of Information on Technology Needs in Law Enforcement

The National Institute of Justice (NIJ) has been an important sponsor of technology development and dissemination in law enforcement. NIJ solicitations typically reflect the input of practitioners and other experts and may thus serve as another barometer of priority technology needs in law enforcement. Recent NIJ solicitations have emphasized the development and refinement of sensors and surveillance equipment, communications technology, and body armor. NIJ has also sought to evaluate the impact of various technologies on policing.

In terms of sensors and surveillance, NIJ has emphasized the detection of concealed weapons, through-the-wall surveillance for locating or tracking people in buildings, and other applications like area surveillance and systems to enhance command and control. Priority issues for communications have included technology to detect, identify, and locate wireless communications; locator technologies for personnel and equipment; and airborne and satellite-based systems. To improve body armor for law enforcement, NIJ has supported the development of advanced ballistic-resistant materials, non-destructive inspection methods, equipment and protocols for testing, and advanced soft body armor designs.[26]

[25] The listed technologies received an average score of 3.5 or better on a five-point scale in which 5 denoted the highest priority.

[26] NIJ also sponsors the National Law Enforcement and Corrections Technology Centers (NLECTC) system, which consists of a number of regional centers and specialty offices that work with law enforcement and corrections

NIJ has also recognized the need for more evaluations of the benefits and limitations of technology in policing. Some of the technologies that NIJ has recently sought to evaluate include alcohol monitoring of offenders under supervision, offender tracking systems, DNA evidence, mobile identification biometric devices, GPS-based[27] automobile locator technology, automated license plate recognition, and trace detection technologies for narcotics, explosives, and other contraband.[28]

In addition to NIJ, the federal Department of Homeland Security (DHS) is likely to play an increasingly important role in the development of technology for policing. Although DHS focuses on the homeland security needs of federal law enforcement agencies, many technologies developed for this purpose also have applicability to the needs of state and local law enforcement with respect to counter-terrorism, emergency management, and everyday crime-fighting. DHS recently identified a number of priority areas (DHS, 2008):

- Border and maritime security, including inspection of hidden or closed compartments, improved personal protective equipment, non-lethal means of disabling vehicles and incapacitating subjects, and gunshot spotter technology
- Cargo security, including improved screening and examination for the detection and identification of contraband and NCB materials
- Chemical and biological defense, including handheld devices for biological and chemical detection and improved chemical-biological forensic analysis capability
- Cyber security
- Transportation security
- Incident management, including tools for managing incidents and monitoring both the location and physiological condition of personnel
- Information sharing
- Infrastructure protection
- Interoperability
- People screening, including mobile biometrics screening and behavioral sensors to detect deception or hostile intent

2.5. Conclusions

To summarize, various forms of technology are being adapted or developed for law enforcement purposes, and there are many specific technologies, both current and emerging, that can benefit law enforcement. In closing, we review a few broad points of emphasis from our overview of technology uses, impacts, and needs in law enforcement.

---

agencies to foster technological innovations (see http://www.justnet.org/Pages/home.aspx). NLECTC recently established special centers for communications, forensics, weapons and protective systems, and sensors, surveillance, and biometric technologies.

[27] Lockheed Martin was the Prime System Integrator for the U.S. Air Force in the initial development, design, build, launch and upgrades to the Global Positioning Satellite (GPS) system.

[28] PERF is currently working with the Mesa (AZ) Police Department on an NIJ-sponsored evaluation of automated license plate recognition technology. The aim of the study is to determine the extent to which this technology improves the recovery of stolen automobiles and the apprehension of auto thieves.

- Police agencies use IT extensively, but gaps remain in their IT capabilities. A high priority is the development and enhancement of integrated data systems, including systems and equipment that provide in-field access for officers. Better data systems and access would seem to hold much potential for increasing the effectiveness of police, particularly when coupled with crime analysis capabilities that can be used to improve strategy, resource allocation, and managerial control and accountability.

- Communications technology is a high priority for many agencies. Improving the inter-agency interoperability of communications is a particularly important concern. Other issues in communications include improving the ability of police to transmit and receive information from the public and the development/enhancement of locator technologies.

- Improving the ability of police to collect and process DNA evidence has great potential for improving criminal investigation, given both the strong experimental evidence for its effectiveness in clearing cases and the current backlogs that exist in DNA testing. Other technologies to improve suspect identification, including biometric technologies and mobile fingerprint readers, are also spreading in law enforcement and may improve operations.

- Police are increasingly using various forms of camera surveillance, ranging from individual cameras in patrol cars or on officers' uniforms to wireless networks of cameras providing live coverage of numerous areas simultaneously. Some evidence suggests that cameras are effective in reducing some forms of crime; they may become even more effective if coupled with emerging biometric technologies for subject identification. Police are also seeking technologically advanced surveillance equipment that has tactical uses, such as "see through the wall" devices for use in hostage situations.

- On a related note, the development of new sensors of various sorts is also highly relevant to law enforcement. Agencies are particularly concerned about acquiring better and, where possible, portable devices to detect contraband (e.g., drugs) and other dangerous objects and substances (e.g., concealed weapons and CBRNE substances).

- Many police agencies are highly interested in a wide range of equipment and gear to help them contend with explosives and CBRNE threats, a trend linked to contemporary concerns with terrorism and homeland security. Examples include robots for disarming explosive devices, protective gear against CBRNE threats, improved means of detecting CBRNE threats, and better tools to investigate and defend against cyber terrorism.

- The development of non-lethal weapons to control individuals and crowds is yet another priority issue for law enforcement technology. While the use of conducted energy devices and other non-lethal weapons (e.g., chemical sprays and soft projectiles) continues to spread, emerging technologies include various light and sound devices for handling crowds.

- Agencies have substantial needs for training in the use of various technologies and for technical advice on the acquisition of technology. This is especially the case for smaller police agencies.

- Finally, there is a need for more evaluation research to provide police with better evidence on which technologies are most valuable and cost effective for law enforcement uses. Such studies should seek to determine the types and uses of technology that are most effective and should delineate the implementation issues that impact the successful application of technology.

Chapter 3: The PERF Technology Needs Assessment Survey

3.1. Introduction

One of the primary components of the PERF-LM project on Future Law Enforcement Technology Needs was a survey conducted with a national sample of 216 state and local police agencies. The survey explored four primary issues: agencies' expectations about operational needs in the next three to five years; agencies' current uses and experiences with technology; new technologies that agencies believe would address their significant operational needs; and technology acquisitions the agencies expect to make in the next three to five years. This chapter discusses the methodology of that survey and highlights key findings.

3.2. Methods

3.2.1. Sample Selection

The PERF Technology Needs Assessment Survey was conducted with PERF-member police agencies. PERF is a national police membership organization, founded in 1976, that addresses issues pertinent to police in large city and county jurisdictions. PERF agencies are defined here as organizations led by persons with "general membership" in PERF. To be eligible for general membership in PERF, one must be the executive head of a state or local police agency that has 100 or more employees and/or serves a jurisdiction of at least 50,000 persons. Currently, there are 298 agencies in the United States that meet these criteria and that have a chief, sheriff, or commissioner who is a general member of PERF. This group served as the sampling frame for the technology survey.

It should be noted that PERF agencies do not constitute a scientifically selected, representative sample of all U.S. police agencies or any subset thereof (e.g., large agencies); hence, the findings discussed here may not be applicable to many other police agencies in the country. However, PERF agencies represent an important and influential group of the nation's largest police forces. PERF agencies are responsible for jurisdictions having more than half of the country's population and over 40% of its homicides. Further, studies have shown that PERF agencies are leaders with respect to innovations like community policing and the use of advanced information systems (Mastrofski et al., 2003; Skogan and Hartnett, 2006). For these reasons, PERF agencies may well be more advanced in the use of technology than are many non-PERF agencies, and they may also serve as a good bellwether of likely trends in police use of technology.

3.2.2. Response Rate and Characteristics of Responding Agencies

The technology survey was fielded from September through November of 2008.[29] The first survey wave was disseminated on September 17th. Two additional surveys waves followed

[29] The survey was developed by PERF staff. Comments on a draft version of the survey were provided by staff from Lockheed Martin and by a number of practitioners and researchers affiliated with the Society of Police Futurists

three (second survey wave) and five (third survey wave) weeks later; a reminder letter was sent out to non-responding agencies on November 3rd. During that period, 216 agencies responded to the survey, yielding a response rate of 72%. Each survey was completed by the agency's executive leader (the chief or sheriff) or by a representative designated by the executive. As surveys were received, they were reviewed for completeness and accuracy. Respondents were contacted about any survey items that were incomplete or possibly inaccurate. This was done to increase the accuracy of the data that were collected. **(**A copy of the full survey is provided in Appendix B.)

Characteristics of the responding agencies and their jurisdictions are presented in Table 3-1. (See Appendix D for a list of all responding agencies.) On average, the responding agencies had over 700 full-time sworn officers, nearly 1,000 full-time employees, and responsibility for a jurisdiction of nearly 639,000 people. Not surprisingly, the bulk of personnel in these agencies work in patrol, investigations, special units, or, in the case of Sheriffs' offices, detention. Crime analysis, planning and research, and information technology (IT)—functions to which technological innovation would seem very relevant—had relatively modest personnel allocations, averaging only 8 to 13 persons across the sample. Nevertheless, over half of the agencies (55%) indicated that they had a central office of some sort (e.g., a planning and research unit) that guides their technology acquisition decisions.

International. In addition, a draft version of the survey was pre-tested with six law enforcement agencies selected by project staff. (The authors bear all responsibility, however, for the final content of the survey.)

Table 3-1: Agency & Jurisdiction Characteristics

Agency Characteristics	Minimum	Maximum	Average
Full-time employees	19	27,298	993
Sworn officers	1	18,929	702
Patrol	0	7,981	369
Investigations	0	1,731	99
Crime Analysis	0	233	8
Training	0	316	16
Planning and research	0	69	3
Specialized units (e.g., SWAT)	0	1336	54
Information technology	0	369	13
Detention	0	16,431	117

	Minimum	Maximum	Yes (%)	No (%)
Office of technology acquisition	0	216	55.1	44.9
CALEA accredited	0	209	42.1	57.9

Jurisdiction Characteristics	Minimum	Maximum	Average
Residential population	5,000	37,771,431	638,826
Part I index crimes in 2007	42	220,798	12,397
Part I violent crimes in 2007	3	29,484	2,089
Dispatched calls for service	600	3,863,493	208,082
Jurisdiction size in square miles	1	155,959	2,077

3.3. Operational Needs of Law Enforcement

Prior to querying agencies about their experiences with and needs for technology, the survey first asked respondents about their anticipated needs for resources in 20 different operational areas over the next 3 to 5 years. Respondents were asked, on a 5-point scale, the extent to which they agreed or disagreed that their agency would have high priority needs for additional resources in each of the 20 operational areas. Response categories ranged from "strongly agree" to "strongly disagree." Note that the agencies were not asked to answer these questions with respect to their needs for technological resources in particular; rather, the intent was to identify key operational needs so that practitioners, researchers, and industry can consider if and how technology can be used to address these needs. (We say more about the latter issue in the next chapter.)

Table 3-2 ranks the operational needs based on the percentage of respondents that strongly agreed that these needs will require additional resources. (A more detailed listing of the results appears in Appendix E.[30]) In general, agencies gave greatest weight to a series of concerns reflecting better information and analysis, day-to-day operations, crime reduction, and staffing. Patrol officer response to calls for service ranked as the top operational need, with 74% of agencies strongly agreeing that this operational area will require additional resources in the next few years. Between two-thirds and three-fourths of respondents also strongly agreed that additional resources will be needed for information technology, crime analysis / information-led policing, proactive policing, and street crime. Other leading needs included dealing with electronic and cyber crime, training, hiring and retention, collection and processing of crime scene evidence, and coordination / interoperability with other first responders.

Table 3-2: Operational Needs Requiring More Resources in Next 3-5 Years

Rank	Operational Area	Percent that strongly agree
1	Patrol officer response to calls for service	73.6
2	Information technology (e.g., database integration and data sharing within in and across agencies	70.8
3	Crime analysis and information led policing	70.4
4	Freeing officer time for proactive strategies	69.9
5	Prevention and investigation of street crime	69
6	Prevention and investigation of electronic/cybercrime	55.6
7	Training	55.1
8	Hiring and retention	54.6
9	Collection and processing of crime scene evidence	47.2
10	Coordination and interoperability with other first responders	46.3
11	Officer oversight, supervision and accountability	45.6
12	Communications and dispatch	41.1
13	Security for police information systems	38.3
14	Weapons and equipment	30.2
15	Prevention and investigation of homeland security threats and terrorism	23.1
16	Pursuit management (e.g., foot and vehicle pursuits)	21.3
17	Prevention and investigation of organized crime	19.4
18	Tactical operations (e.g., hostage situations)	15.7
19	Handling explosives	9.7
20	Crowd and riot control	7.5

[30] Because the responses to this item were on a 5-point scale, we also calculated a numerical average for each item. These averages are shown in Table E-1 of Appendix E**.** The top ten needs based on these averages are very consistent with the top ten shown in Table 3-2.

As an added measure, agencies were also requested to select up to three operational needs from the list that would constitute their most important operational needs over the next three to five years. The most commonly selected needs are listed in Table 3-3. These six operational areas, which together accounted for two-thirds of all responses, are consistent with the top six needs listed in Table 3-2 (though rank ordering differs somewhat between the two lists).

Table 3-3: Most Important Operational Needs in Next 3-5 Years

Rank	Operational Need	Percent of votes
1	Information technology (database integration)	12.4
2	Crime analysis / information-led policing	11.6
3	Hiring and retention	11.1
4	Freeing officer time for proactive strategies	10.2
4	Patrol response to calls for service	10.2
5	Prevention and investigation of street crime	9.5

3.4. Technology Uses and Experiences

The survey then examined agencies' experiences and needs with respect to 52 specific types of technology used in law enforcement. These technologies, which are listed and defined in Appendix C**,** were grouped into the following general categories.

- Identification
- Sensors and surveillance
- Crime analysis / mapping
- Training
- Records management / data sharing
- Communications / dispatch / interoperability
- Weapons and equipment

The survey posed questions about the condition, effectiveness, and implementation of each listed technology currently used by the responding agencies. For each technology they did not use, agencies were asked: 1) whether the technology would help them address significant operational needs; and 2) how likely they are to acquire that technology in the next 3-5 years. In the next sections, we highlight technologies that ranked at the top on these various dimensions. More detailed breakdowns of all results are presented in Tables E-2 through E-6 of Appendix E.

3.4.1. Condition of Currently Used Technologies

Agencies were asked to characterize the condition of each listed technology they use as either "obsolete," "old but serviceable," or "up to date."[31] Table 3-4 ranks the technologies based on the percentage of users that characterized them as either obsolete or old but serviceable. Technologies at the top of this list include a mix of sensors and surveillance equipment, training equipment, and other equipment for personal or tactical uses. As shown in the first item in Table 3-4, portable devices for detecting concealed weapons were the form of technology users were most likely to deem as old or obsolete; 23% of agencies indicated that they use this form of technology, and 52% of those agencies indicated that their equipment was old or obsolete.

Table 3-4: Condition of Used Technologies

Rank	Type of Technology	Percentage using technology	Percentage old and obsolete
1	Portable devices for detecting concealed weapons	23.0	52.1
2	Pistol cam	3.3	50.0
3	Night vision devices	84.1	48.2
4	Night vision equipment	85.9	44.3
5	Long range broadcasting device	18.7	41.0
6	Use of force computer simulators	52.2	39.9
7	Video surveillance network	60.5	37.3
8	Electronic listening devices	48.1	37.0
9	Personal video/audio equipment (worn by officer	26.3	36.3
9	Special purpose vehicles (e.g., armored vehicles, ATVs)	70.0	36.3
10	Mobile command center	81.0	35.0
11	Aerial surveillance equipment	12.8	33.3
13	See through the wall technology (ultra wide band)	9.2	31.6
14	Patrol car cameras	64.4	31.0
14	Drug detection devices	20.6	31.0
15	Driving simulators	21.5	29.6
16	Gunshot detection devices	12.3	28.0
17	Inter-agency radios	79.4	27.7
18	700/800 MHz trunked communication system	72.8	26.7
19	Drug testing technology	49.3	26.2
20	Predictive modeling	31.3	25.7
21	Other biometric technology	10.9	25.0
22	Fully integrated vehicle system (voice activated)	6.2	25.0
23	Other computer-based training and simulators	22.4	24.5
24	Protective gear/clothing	79.4	22.9
25	GPS devices for tracking suspects	64.0	22.4
26	Language translators	39.6	21.7
27	Integrated databases (e.g., COPLINK®, regional data sharing, etc.)	61.1	21.3
28	Mobile laboratory	18.2	21.1
29	Investigative software (e.g., data mining software)	45.5	21.0

[31] We based these characterizations on those used by Schwabe et al. (2001) in a law enforcement technology survey conducted in 2000.

Table 3-4 (Continued):

Rank	Type of Technology	Percentage using technology	Percentage old and obsolete
30	Electronic interception	20.9	20.4
31	Ballistics imaging	25.6	20.0
31	Cyber forensics equipment	53.1	20.0
31	LED vision incapacitation device	5.7	20.0
	Computer-aided dispatch with GPS dispatching and tracking of patrol cars	55.2	19.8
32	Community notification via Internet, text messaging	65.2	19.4
33	Geographic Information Systems (GIS) software	84.7	19.3
34	Real-time crime monitoring center	19.5	19
35	Sensors for biological/chemical/nuclear materials	27.3	18.9
36	Digital forensic training	26.0	18.6
37	Robots for bomb disposal and tactical operations	41.6	17.2
38	DNA Testing Equipment	24.3	16.0
39	Fingerprint readers	57.6	15.7
40	Directed energy vehicle stopper	3.3	14.3
41	Software for risk factor analyses for victimization	13.7	13.8
42	Wireless access in patrol cars	84.2	13.7
43	Sound wave incapacitation weapon	3.3	12.5
44	Sensors for explosives	13.9	10.3
45	Next Generation 911 (text and voice messaging)	21.3	8.6
46	License plate readers	38.1	5.1

What is perhaps most notable in this list are those technologies that are both widely used and likely to be outdated. For example, night vision devices, use of force simulators, video surveillance networks, special purpose vehicles, and mobile command centers were used by 52% to 84% of the respondents. At the same time, roughly one-third to one-half of the agencies using these technologies rated them as old or obsolete. Hence, these technologies may require widespread replacement in coming years.

Note, however, that in most cases agencies rated their equipment as old but serviceable rather than obsolete. Rarely did more than 10% of users rate any form of technology as obsolete, particularly for the more commonly used technologies (see Table E-2 of Appendix E).

3.4.2. Effectiveness of Currently Used Technologies

Agencies were next asked to rate the effectiveness of each technology as "not effective," "moderately effective," or "very effective." In Table 3-5, the technologies are ranked based on the percentage of users that characterized them as very effective. At the top of the list are conducted energy devices (a form of non-lethal weapon), used by 82% of the responding agencies, and body armor, used by 98%. Nine out of 10 user agencies felt that these technologies were very effective. Many of the most effective technologies were widespread among the agencies. However, a few, including DNA testing equipment, robots for tactical operations, and drug testing technology, were possessed by no more than half of the agencies.

These latter technologies may thus represent potential growth areas for law enforcement technology.[32]

Table 3-5: Effectiveness of Currently Used Technologies

Rank	Technology	Percent that have it	Percent of agencies that have the technology who find it very effective
1	Conducted Energy Devices (e.g., Taser® or Stinger®)	82.4	92.6
2	Body armor	97.7	89.4
3	Fingerprint readers	57.6	77.5
4	Robots for bomb disposal and tactical operations	41.6	74.7
5	Wireless access in patrol cars	84.2	73.3
6	700/800 MHz trunked communication system	72.8	72.8
7	GPS devices for tracking suspects	64	69.6
8	DNA Testing Equipment	24.3	68.6
8	Drug testing technology	49.3	68.6
9	Special purpose vehicles (e.g., armored vehicles, ATVs)	70	64.6
10	Mobile command center	81	63.5
11	Geographic Information Systems (GIS) software	84.7	63.3
12	Mobile laboratory	18.2	63.2
13	License plate readers	38.1	62.5
14	Digital forensic training	26	62.3
15	Ballistics imaging	25.6	61.8
16	Protective gear/clothing	79.4	61.4
17	Patrol car cameras	64.4	60.2
18	Inter-agency radios	79.4	59.9
20	Real-time crime monitoring center	19.5	59.5
21	Cyber forensics equipment	53.1	58.7
21	Use of force computer simulators	52.2	58.7
22	Electronic interception	20.9	58.1
23	Personal video/audio equipment (worn by officer)	26.3	57.4
24	Computer-aided dispatch with GPS dispatching and tracking of patrol cars	55.2	55.6
25	Integrated databases (e.g., COPLINK®, regional data sharing, etc.)	61.1	55.1
26	Community notification via Internet, text messaging	65.2	54.1
27	Aerial surveillance equipment	12.8	53.8
28	Sensors for explosives	13.9	53.6
29	Next Generation 911 (text and voice messaging)	21.3	51.1

[32] A caveat is that we could not explore the full meaning of the effectiveness ratings in this survey format. Saying that a technology is effective, for instance, could signify that it works as intended, that it significantly enhances operations, or some combination thereof.

Table 3-5 (Continued):

Rank	Technology	Percent that have it	Percent of agencies that have the technology who find it very effective
30	Investigative software (e.g., data mining software)	45.5	50.5
31	Electronic listening devices	48.1	49.5
32	Language translators	39.6	48.8
33	Sensors for biological/chemical/nuclear materials	27.3	47.4
34	Driving simulators	21.5	46.7
34	Other computer-based training and simulators	22.4	46.7
35	Other biometric technology	10.9	45.8
36	Night vision devices	84.1	45.1
37	Portable devices for detecting concealed weapons	23	40.4
38	LED vision incapacitation device	5.7	40
39	Long range broadcasting device	18.7	39.5
40	Video surveillance network	60.5	38.9
41	Drug detection devices	20.6	33.3
42	Predictive modeling	31.3	30.3
43	Software for risk factor analyses for victimization	13.7	28.6
43	Sound wave incapacitation weapon	3.3	28.6
44	Fully integrated vehicle system (voice activated)	6.2	27.3
45	Directed energy vehicle stopper	3.3	20
46	Gunshot detection devices	12.3	19.2
47	See through the wall technology (ultra wide band)	9.2	11.1

3.4.3. Challenges of Implementing Currently Used Technologies

Finally, the survey explored implementation challenges associated with each technology that agencies reported using. More specifically, agencies were asked whether any or all of the following had posed challenges to implementing each technology: the technology not working as expected; difficulty in using the technology; training needs associated with using the technology; and economic or political challenges (e.g., acquisition costs, lawsuits, or political resistance). Respondents were also given the option of indicating "no challenges." A detailed breakdown showing the commonality of each type of implementation challenge for each type of technology appears in Table E-4 of Appendix E. Here, we focus on some of the broader patterns.

Table 3-6 shows the prevalence of each type of implementation challenge averaged across all types of technology. We note first that many agencies did not report any major challenges in implementing the listed technologies. For the average technology, 49% of users indicated no implementation challenges. Implementation challenges that did occur were most likely to involve economic or political liabilities. Across all types of technologies, such problems were encountered on average by one-quarter of users. As discussed below, additional data from the survey suggests that these problems were generally linked to financial issues. Turning to other implementation challenges, about 8% of users typically reported the technology not working as expected, and 16% reported that training needs posed a challenge to the use of these technologies.

Table 3-6: Implementation Challenges Associated with Technology

Type of Challenge	Percent of Agencies Reporting Challenge (averaged across technologies)
Economic and political liabilities	25.5
Need for training	15.8
Difficulty in using technology	5.4
Technology not working as expected	7.8
No challenges	49.3

Many of the technologies that were most likely to have implementation problems were technologies that are not yet very common in policing. Examples include fully integrated, voice-activated vehicle systems (used by 6% of agencies), sound wave incapacitation weapons (used by 3% of agencies), aerial surveillance equipment (used by 13% of agencies), and directed energy vehicle stoppers (used by 3% of agencies). Roughly 71% to 85% of the agencies using these technologies appear to have had implementation challenges of some sort, though these challenges may have differed from those highlighted in the survey (see Table E-4, Appendix E).[33]

3.5. Technologies Not Used That Would Address Significant Operational Needs

When an agency did not use a technology on the list, the agency was asked the extent to which that technology, if acquired, would address significant operational needs of the agency. Response categories included "fully", "moderately", "slightly", or "not at all."

Table 3-7 ranks the technologies based on the percentage of non-users stating that the technology would fully address significant operational needs. For each technology, Table 3-7 shows the percentage of agencies that did not use the technology and the percentage of those agencies stating that the technology would fully address operational needs. A number of IT and communications-related technologies top this list, including wireless access in patrol cars, inter-agency radios, computer-aided dispatch with GPS tracking, "trunked" communications systems, and integrated databases. Fifty to sixty-one percent of non-users indicated that these technologies would fully address important needs.

[33] To illustrate, 15% of the agencies using fully integrated vehicle systems indicated no implementation challenges. Conversely, this indicates that 85% did experience implementation problems. However, the percentages of users indicating that they experienced the specific challenges listed in the survey sum to only 46% (assuming that no agency experienced more than one problem). It seems, therefore, that that these agencies experienced implementation problems other than those listed in the survey.

Table 3-7: Extent to Which Technologies Would Address Operational Needs for Non-users

Rank	Type of Technology	Percent that don't use technology	Percent saying technology would fully address operational needs
1	Wireless access in patrol cars:	15.8	60.6
2	Inter-agency radios	20.6	55.8
3	Computer-aided dispatch with GPS dispatching and tracking of patrol cars	44.8	54.8
4	700/800 MHz trunked communication system	27.2	51.8
5	Integrated databases (e.g., COPLINK®, regional data sharing, etc.)	38.9	50
6	Body armor	2.3	40
7	Fingerprint readers	42.4	37.9
8	GPS devices for tracking suspects	36	35.1
9	Video surveillance network	39.5	34.9
10	Investigative software (e.g., data mining software)	54.5	34.5
10	Special purpose vehicles (e.g., armored vehicles, ATVs)	14.1	34.5
11	Next Generation 911 (text and voice messaging)	78.7	32.1
12	Use of force computer simulators	47.8	32
13	Community notification via Internet, text messaging	34.8	31.9
14	Cyber forensics equipment	46.9	31.3
14	Geographic Information Systems (GIS) software	15.3	31.3
15	Real-time crime monitoring center	80.5	30.5
16	Mobile command center	19	30
17	DNA Testing Equipment	75.7	28.7
17	License plate readers	61.9	28.7
18	Night vision devices	15.9	27.3
19	Predictive modeling	68.8	27
20	Digital forensic training	74	26.3
21	Language translators	60.4	25.5
22	Patrol car cameras	35.6	24.3
23	Driving simulators	78.5	23.3
24	Conducted Energy Devices (e.g., Taser® or Stinger®)	17.6	22.2
25	Drug testing technology	50.7	22.1

Table 3-7 (Continued):

Rank	Type of Technology	Percent that don't use technology	Percent saying technology would fully address operation needs
26	Protective gear/clothing	20.6	22
27	Drug detection devices	79.4	21.8
28	Other computer-based training and simulators	77.6	21.5
29	Directed energy vehicle stopper	96.7	20.7
30	Portable devices for detecting concealed weapons	77	20.1
31	See through the wall technology (ultra wide band)	90.8	19.9
32	Personal video/audio equipment (worn by officer)	73.7	18.6
33	Software for risk factor analyses for victimization	86.3	17.3
34	Ballistics imaging	74.4	16.1
35	Mobile laboratory	81.8	15.4
36	Fully integrated vehicle system (voice activated)	93.8	15.3
37	Other biometric technology	89.1	14.1
38	Robots for bomb disposal and tactical operations	58.4	14
39	Aerial surveillance equipment	87.2	13.3
40	Gunshot detection devices	87.7	12.1
41	Sensors for explosives	86.1	10.7
42	LED vision incapacitation device	94.3	10.6
43	Pistol cam	96.7	10.4
44	Electronic interception	79.1	10.3
45	Long range broadcasting device	81.3	10.1
46	Sensors for biological/chemical/nuclear materials	72.7	9.3
47	Sound wave incapacitation weapon	96.7	8.4
48	Electronic listening devices	51.9	8.3

Technologies that are highly valued but relatively less common may represent potential growth areas in law enforcement technology. These include computer-aided dispatch with GPS, integrated databases, fingerprint readers, investigative software, and Next Generation 9-1-1, all of which were unavailable to 39% to 79% of agencies.

3.6. Likely Technology Acquisitions

Finally, using a scale of "very likely," "somewhat likely," or "not likely," we asked agencies how likely it is that they will acquire each technology (that they are not currently using) during the next three to five years. In Table 3-8, the technologies are ranked based on the percentage of non-users indicating they are very likely to acquire them.

As in Table 3-7, a number of technologies related to IT and communications ranked highly on this list; examples include wireless access in patrol cars, integrated databases, inter-agency radios, and GIS software. In addition, technologies designed to reduce or minimize harm from police use of force also ranked highly. Indeed, computer simulators for use-of-force training ranked as the technology most likely to be purchased by non-users in the near future. Nearly half of the agencies did not possess such equipment, but almost two-thirds of those agencies expected to obtain it soon. Conducted energy devices also ranked in the top ten, though a substantial majority of agencies already possess such devices.

Table 3-8: Likelihood of Technology Acquisitions

Rank	Technology	Percent that don't have it	Percent very likely to acquire it
1	Use of force computer simulators	47.8	61
2	Wireless access in patrol cars	15.8	56.3
3	Integrated databases (e.g., COPLINK®, regional data sharing, etc.)	38.9	42.5
4	Body armor	2.3	40
5	Geographic Information Systems (GIS) software	15.3	34.4
6	Inter-agency radios	20.6	32.6
7	Computer-aided dispatch with GPS dispatching and tracking of patrol cars	44.8	30.9
8	Conducted Energy Devices (e.g., Taser® or Stinger®)	17.6	29.7
9	700/800 MHz trunked communication system	27.2	28.6
10	Community notification via Internet, text messaging	34.8	26.8
11	Video surveillance network	39.5	24.1
12	Next Generation 911 (text and voice messaging)	78.7	23.9
13	License plate readers	61.9	22.5
14	Patrol car cameras	35.6	20.3
15	Fingerprint readers	42.4	20.2
16	Investigative software (e.g., data mining software)	54.5	15.8
17	Real-time crime monitoring center	80.5	11.8
18	Cyber forensics equipment	46.9	10.3
19	Mobile command center	19	10
20	Predictive modeling	68.8	9.9
21	Night vision devices	15.9	9.1
22	Software for risk factor analyses for victimization	86.3	7.2
23	GPS devices for tracking suspects	36	6.6
24	Special purpose vehicles (e.g., armored vehicles, ATVs)	30	6.3
25	Gunshot detection devices	87.7	5.9
25	Digital forensic training	74	5.9
26	Drug testing technology	50.7	5.7
27	Language translators	60.4	4.8
28	Personal video/audio equipment (worn by officer)	73.7	4.5
29	Driving simulators	78.5	4.3

Table 3-8 (Continued):

Rank	Technology	Percent that don't have it	Percent very likely to acquire it
30	DNA Testing Equipment	75.7	3.8
31	Other biometric technology	89.1	3.7
31	Portable devices for detecting concealed weapons	77	3.7
32	Sensors for explosives	86.1	3.4
33	Fully integrated vehicle system (voice activated)	93.8	3.1
34	Electronic interception	79.1	3
34	Long range broadcasting device	81.3	3
35	Sensors for biological/chemical/nuclear materials	72.7	2.6
36	Other computer-based training and simulators	77.6	2.5
36	Sound wave incapacitation weapon	96.7	2.5
36	Robots for bomb disposal and tactical operations	58.4	2.5
37	Directed energy vehicle stopper	96.7	2.4
38	Mobile laboratory	81.8	1.8
39	See through the wall technology (ultra wide band)	90.8	1.6
40	Pistol cam	96.7	1.5
41	LED vision incapacitation device	94.3	1.5
42	Drug detection devices	79.4	1.2
43	Aerial surveillance equipment	87.2	1.1
44	Electronic listening devices	51.9	0.9
45	Ballistics imaging	74.4	0.6

On a related note, the survey also asked agencies to describe any plans they had for acquiring new technologies or updating existing ones. Coding of these responses (which were open-ended) revealed that commonly mentioned plans for acquiring or updating technology involved records management systems, computer-aided dispatch, communications, mobile field devices and capabilities, video devices, crime analysis, and information sharing technology. In addition, several agencies mentioned plans for finding various forms of assistance for acquiring technology, including grants, third-party solutions, partnering, and networking.

3.7. Future Technology Development and Barriers to Technology Acquisition

Two of the concluding items on the survey asked agencies to describe technologies they would most like to see developed for law enforcement as well as barriers they might face over the next 3-5 years in acquiring technology. Both items were open-ended, and respondents were free to choose from the prior lists of technologies and implementation problems or to cite other technologies and issues.

Consistent with findings described above, coding of responses to the technology development item suggests that agencies place their greatest emphasis on technologies linked to interagency information sharing, less-lethal weapons and related devices (notably, vehicle stopping technology), portable field devices and capabilities, video and other forms of surveillance, crime analysis, records management, and computer-aided dispatch.

With respect to barriers to technology acquisition, agencies overwhelmingly cited costs and monetary constraints. Indeed, roughly 8 of every 10 responses dealt with financial constraints, lack of funding, or ancillary costs of technology (e.g., costs associated with training and maintenance).

Chapter 4: The PERF-Lockheed Martin Law Enforcement Future Technologies Workshop

4.1. Introduction

The second component of the Law Enforcement Future Technologies Project consisted of a two-day workshop held in November 2008 at Lockheed Martin's Center for Innovation, an advanced technology R&D facility (http://www.lockheedmartin.com/innovation) in Suffolk, Virginia. This event brought together a select group of law enforcement practitioners from around the country to discuss technology uses and needs in a forum that allowed for deeper exploration of these issues than was possible in the national survey. It also provided an opportunity to contrast the national survey results with the views of a more select group of experts on law enforcement technology. The sections below discuss the methods and findings of the workshop.

4.2. Selection of Participants

Fifty-five practitioners from twenty-nine police agencies throughout the country participated in the workshop. The agencies and participants were chosen primarily by PERF staff. PERF sent invitations to 51 agencies that were selected based on a combination of factors: 1) quick response to the national technology survey; 2) agency reputation for technological advancement and innovation; and 3) geographical location. With respect to the latter consideration, we included agencies representing several different regions throughout the country. However, agency selection was more heavily weighted towards nearby agencies that had lower travel costs (i.e., agencies from Virginia, Maryland, Washington, D.C., and North Carolina). In addition to the state and local agency participants, representatives from several federal agencies attended the workshop as observers.[34]

In addition to inviting a variety of agencies, we sought to invite a diverse group of individuals that could speak to the technological needs of different functional areas in law enforcement (e.g., patrol, investigations, crime analysis). The workshop invitation letter therefore asked each agency to, if interested, nominate up to one participant from each of five functional groups: 1) command staff; 2) patrol; 3) investigations; 4) crime analysis (or related functions like research and planning); and 5) communications and dispatch.

Nominations were received from 29 agencies and 1 to 5 representatives were selected from each (due to cost considerations, not all nominees could be invited). Selections were made so as to maintain as much balance as possible among the five functional groups. In total, 55 participants were selected. The breakdown of participants by functional area was as follows:

- 10 Command staff
- 12 Patrol personnel

[34] The workshop included federal representatives from the Office of Community Oriented Policing Services, the Bureau of Justice Statistics, the Federal Bureau of Investigation, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives.

- 9 Investigative personnel
- 17 Crime analysis / planning and research
- 7 Communications and dispatch

A listing of all participants and their agencies is provided in Appendix F.[35]

4.3. Workshop Methodology and Content

Day one of the workshop, a half-day, featured introductory presentations on the goals and objectives of the workshop and on preliminary results of the national survey discussed previously. Participants also viewed technology demonstrations and exhibits arranged by Lockheed Martin.

Day two of the workshop involved a number of thematic sessions. Some sessions involved discussions among the full group of attendees. In other sessions, participants were divided into functional area subgroups. The sessions were organized in the following manner.

- Session 1: Operational needs in law enforcement (full group discussion)
- Session 2: Operational needs and key technologies for functional areas (subgroup discussions)
- Session 3: Technology priorities for functional areas (subgroup discussions)
- Session 4: Reports on functional subgroup discussions (full group discussion)
- Session 5: Barriers to technology development and acquisition (full group discussion)

During the full group sessions, participants completed online polls (described below) and took part in moderated discussions. Each attendee had access to a computer and could make comments electronically as well as verbally. Electronic comments were observable in real-time to all participants (including the session moderator), thus facilitating simultaneous electronic and verbal discussions. This method yielded a wealth of commentary from a wide range of participants, a point to which we return.

For the subgroup sessions, attendees were divided into groups based on their functional area of expertise.[36] These groups took part in structured discussions, moderated by one staff member from PERF and one from Lockheed, in which they were tasked with identifying key operational needs and technologies for their functional area.[37]

4.4. Key Operational Needs and Technologies by Functional Area: Reports of the Functional Breakout Groups

The workshop employed two primary approaches to identifying top operational needs and technologies in policing: a poll of all workshop participants and functional group breakout

[35] Of the agencies represented in attendance, 20 also completed the national survey.
[36] In a few cases, participants were re-assigned to different functional groups in order to achieve more balance in the group sizes.
[37] The workshop content and format were developed jointly by staff from PERF and Lockheed Martin.

discussions. In this section, we present results from the discussions held in the functional group breakout sessions. Section 4.5 provides further detail about the poll results and combines the findings of both methods to identify the highest priority needs and technologies.

In the functional group breakout sessions, each group addressed a number of standardized questions regarding operational needs and important technologies for the group's functional area. Key issues highlighted here for each functional group include:

- The top three operational needs and the role of technology in addressing those needs
- The top three technologies for addressing each of those needs
- Three to five priority technologies for the next three to five years
- Three to five priority technologies for beyond the next five years.

The list of operational needs and technologies developed for the national survey provided a guide for these discussions, but participants were free to choose other needs and technologies.

Table 4-1 summarizes the key operational needs identified by each functional group and the technologies they felt were most important to addressing those needs. Table 4-2 presents the future technology priorities identified by each group for the next 5 years and beyond. We caution the reader that these results are based on discussions involving small groups of participants who may not be representative of law enforcement practitioners more broadly. Nevertheless, the results provide some sense of both the overlapping and unique needs of personnel in different functional areas of law enforcement, and they are based on the judgments of a well-informed and diverse group of practitioners. Our focus, moreover, was on searching for commonalities in the workshop findings that, combined with the results from the national survey (see Chapter 3), may illuminate priority technologies for law enforcement. We discuss that process further in the next section.

Table 4-1: Top Operational Needs and Top Technologies for Addressing Those Needs by Functional Area

Group	Top Operational Needs	Most Relevant Technologies
Command	Information management systems	1) Records management systems 2) Database access and integration technology
	Surveillance technologies	1) Video technologies 2) Biometrics sensors 3) Chemical, biological, radiological/nuclear, and explosive detectors
	Training	1) Simulator training systems 2) Virtual training 3) E-training
Patrol	Patrol response to calls for service	1) Wireless access in patrol cars 2) Computer-aided dispatch with GPS 3) Interagency radios
	Information technology (database integration / data sharing)	1) Wireless access in patrol cars 2) Integrated databases 3) Real-time crime monitoring
	Weapons and equipment	1) Simulator training systems 2) Directed energy vehicle stoppers 3) Conducted energy devices (i.e., Taser®s)

Table 4-1 (Continued):

Group	Top Operational Needs	Most Relevant Technologies
Investigations	Database integration / data sharing	1) Secure networks 2) Investigative software (e.g., data mining) 3) Wireless access
	Crime analysis / information-led policing	1) Investigative software (e.g., data mining) 2) Training software 3) GIS software
	Prevention and investigation of street crime	1) Case management software 2) Surveillance technology 3) Technology for collecting and processing evidence
Crime Analysis	Information management and reporting	1) Automated and electronic field reporting 2) Pre-processing and standardization of data 3) GIS software (analytic tools)
	Promising practices for organizing crime analysis functions	Not applicable
	Training, hiring, and retention	1) Online training for analysts 2) Standardized certification 3) Training in advanced analytics
Communications and Dispatch	Dispatch management of officers	1) Computer-aided dispatch systems 2) Standardization in dispatching
	Intelligent computer-aided dispatch systems	1) Smart trend analysis 2) Smart integration 3) External data feeds
	Interoperability	1) Power frequency and spectrum 2) GPS

Table 4-2: Future Technology Priorities by Functional Area

Group	Priority Technologies for the Next 3-5 Years	Priority Technologies for Beyond the Next 5 Years
Command	Real-time GPS tracking for offenders	Less than lethal systems
	Measured police intervention technologies	Risk management tools
	Live field scanners for identification (e.g., fingerprints)	Affordable broad area surveillance systems
Patrol	Directed energy vehicle stopper	In-car video
	Personal video / audio equipment	Video surveillance network
	Body armor	Robots and unmanned aerial vehicles
Investigations	Integrated databases and reporting software	Portable lie detectors
	Rapid DNA crime scene testing	Unmanned systems (e.g., unmanned ground and aerial vehicles)
	Surveillance advancements	Biometrics advancements
Crime Analysis	NIEMS standards	Non-terrestrial data links
	Off-the-shelf analytic products	Personal, mobile, networked information sharing devices
	Artificial intelligence and data mining	Security identity management
	Mobile communications networks and data sharing	Real-time, virtual, regional data fusion
Communications and Dispatch	Interoperability	National / global power and frequency spectrum adaptability
	Smart integration	Inexpensive encryption
	GPS	Multimedia integration (computer-aided dispatch and closed-circuit television)

4.5. Assessing the Top Operational Needs and Technologies for Law Enforcement: A Synthesis of the Workshop Survey and Breakout Group Results

The results of the last section illustrated a wide range of needs and technologies that are valued in law enforcement. In this section, we provide a summary assessment of top needs and technologies based on the findings presented above and the results of a poll conducted with the workshop participants. Drawing upon both sets of results, PERF and Lockheed staff distilled a series of "short lists" of the top operational needs and technologies for law enforcement.

4.5.1. Workshop Poll Methodology

Before presenting the leading operational needs and technologies, we first provide an overview of the workshop poll and the methods used to analyze the poll results. In subsequent sections, we highlight key results of the poll.

The poll was conducted at the end of the first session on operational needs, just prior to the breakout group discussions. First, each participant was presented with the list of 20 operational needs developed for the national survey (see Chapter 3) and asked to select the three most important needs that his/her agency will face in the next three to five years. They were then asked to repeat the exercise, focusing on the top operational needs for their specific functional area (e.g., patrol, investigations, etc.). (Note that both methods yielded the same top ten operational needs, which are discussed in the next section.)

Lockheed staff developed a ranking for each set of responses using TOPSIS (Technique for Order Preference by Similarity to Ideal Solution), a methodology for ranking alternatives based on multiple decision criteria (Hwang and Yoon, 1981). As decision criteria, each need selected by a respondent was weighted according to whether it was chosen as the first, second, or third most important need.[38]

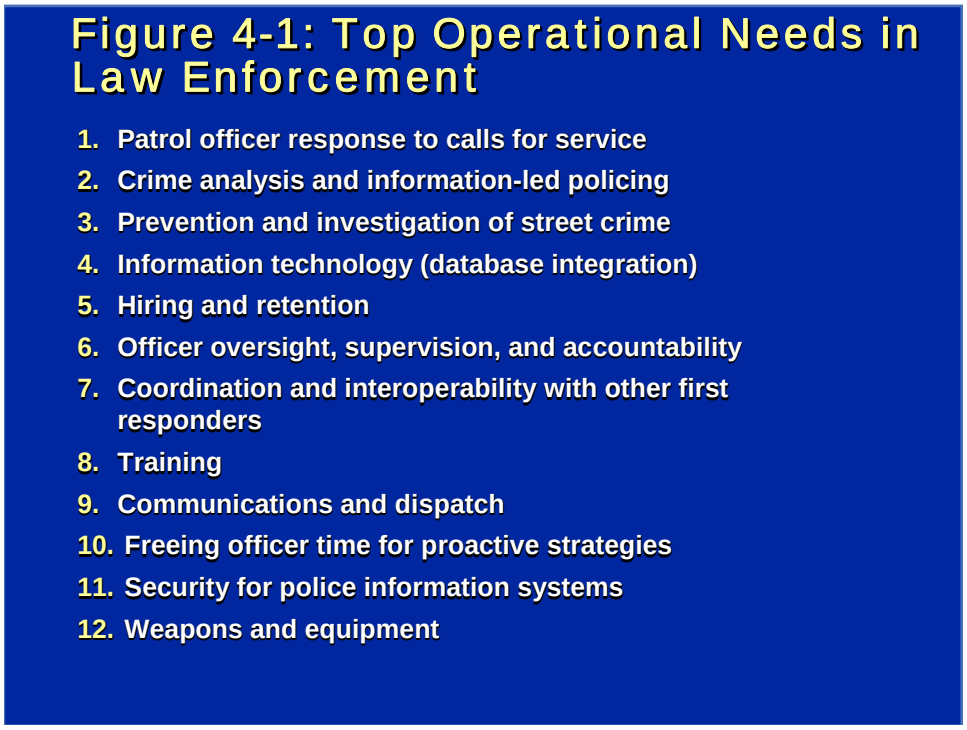
This exercise was then repeated with the workshop survey results disaggregated by functional group. That is, a separate TOPSIS ranking was calculated for individuals belonging to the patrol group, individuals belonging to the investigations group, and so on. In each case, the rankings were based on how the respondents rated the importance of the operational needs to their functional area. The final selection of the top operational needs, discussed below, was based on the TOPSIS rankings (both the combined and disaggregated rankings) as well as the top needs identified in the functional group breakout sessions.

A similar process was utilized to identify top technologies. In the workshop poll, participants were asked to identify up to four top technologies in each of three categories: 1) current technologies for addressing priority operational needs; 2) promising near-term (i.e., 3 to 5 year) technologies for addressing priority operational needs; and 3) promising long-term (i.e., beyond 5 years) technologies for addressing priority needs. (Participants were asked to choose the technologies from the list that was developed for the national survey [see Chapter 3] and to answer the questions in reference to their own functional area.) Lockheed analysts then used the TOPSIS methodology to develop overall and disaggregated rankings for each technology question.[39] Top technologies are identified below based on the various TOPSIS rankings and the top technologies identified in the breakout sessions.[40]

[38] A weight of 1.0 was given to each respondent's first choice, a weight of 0.67 was given to each respondent's second choice, and a weight of 0.5 was given to each respondent's third choice.
[39] For each question, the respondent's choices were weighted as follows: 1.0 for the first choice, 0.9 for the second choice, 0.8 for the third choice, and 0.7 for the fourth choice.
[40] A more detailed discussion of the TOPSIS analysis and results is available from Lockheed staff.

4.5.2. Top Operational Needs

The top operational needs as identified by PERF and Lockheed staff are shown in Figure 4-1. The list includes any operational need that ranked among the top 10 in the overall survey of workshop participants.[41] (Each of those ranking in the overall top 10 also ranked in the top 10 for at least two, and usually three or more, of the disaggregated group rankings.) In addition, the list includes any leading operational need identified by one or more of the functional breakout groups.[42,43] Due to the subjective nature of the final selection method and the relatively small size of the workshop survey sample, we emphasize this group of needs overall and do not emphasize rankings within the group.



Note also that this list is largely consistent with the top needs identified earlier from the national PERF survey (see Chapter 3). All of the needs presented in Figure 4-1 appeared among the top 13 operational needs requiring additional resources in the national survey (see Table 3-2). Figure 4-1 also includes all of the top 5 most important operational needs identified in the national survey (see Table 3-3). In contrast, needs that ranked highly in the national survey but

[41] The same technologies appeared in the top 10 irrespective of whether the respondents were judging the importance of the needs for law enforcement in general or for their functional area in particular.

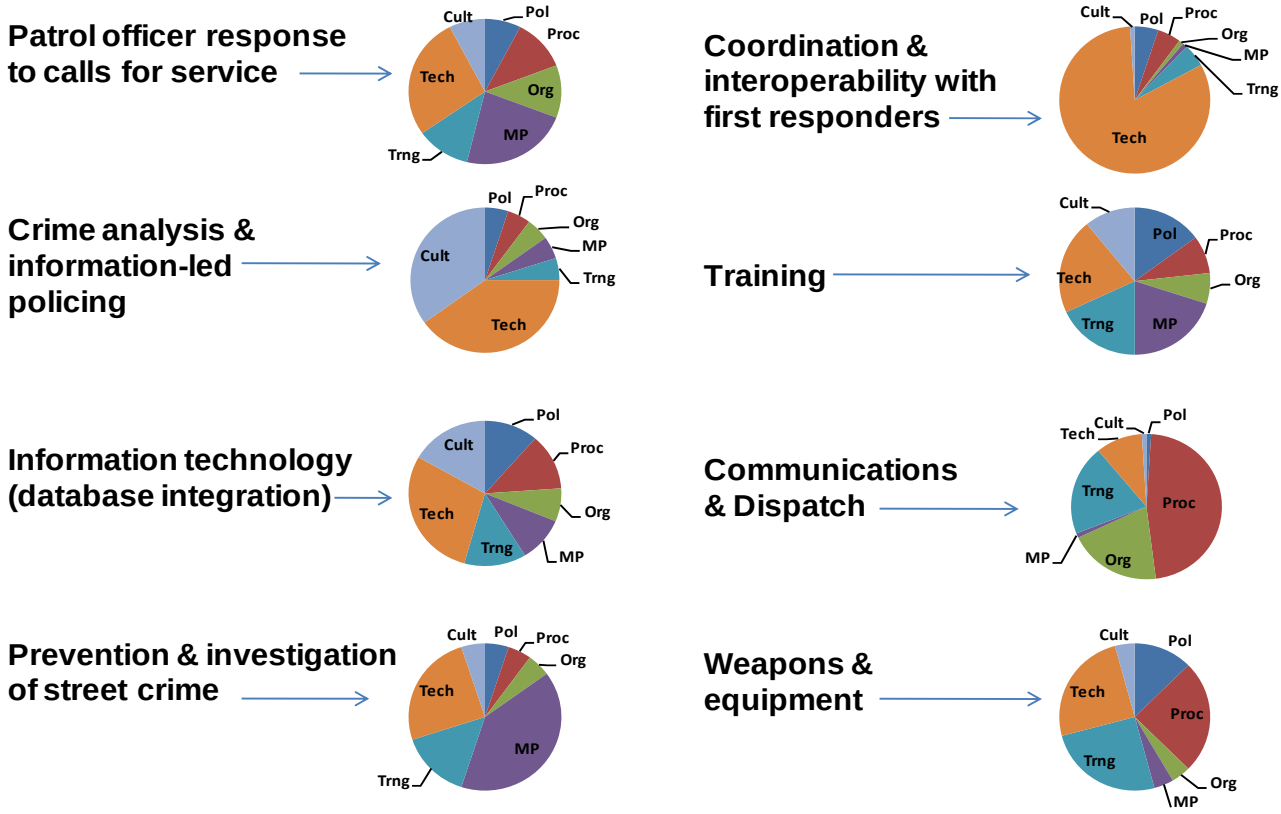
[42] Security for police information systems and weapons and equipment did not appear in the workshop survey top 10 but were included because they were cited as leading operational needs by the command and patrol breakout groups, respectively.

[43] Note that our lists of top operational needs and technologies are based on the lists of needs and technologies that were developed for the national and workshop surveys. Other needs and technologies identified by the breakout groups (see Tables 4-1 and 4-2) were not included in our summary assessments (nor were they recoded to fit into our listed categories).

less so in the workshop included prevention and investigation of electronic/cyber-crime and collection and processing of crime scene evidence.[44]

Another issue addressed in the workshop was technology's role in meeting operational needs relative to those of other factors, including policy, procedures, culture, organizational structure, manpower, and training. This issue is highlighted in Figure 4-2, which presents a series of pie charts that represent the relative roles of technology and other factors in addressing several of the top operational needs identified above. These charts are based on the work of the breakout groups, who were asked to estimate the relative importance of technology and the other factors to each of their key operational needs. In cases where multiple breakout groups identified the same key need, the pie chart for that need reflects an average of the groups' estimates. Top operational needs that do not appear in Figure 4-2 did not appear among the top three needs in any of the breakout group reports; consequently, there are no estimates of technology's role in dealing with them. (They ranked highly overall, nonetheless, in the workshop poll results.)

Figure 4-2: Technology's Role in Addressing Operational Needs



Tech = Technology, Pol = Policy, Proc = Procedures, Org = Org Structure, MP = Manpower, Trng = Training, Cult = Culture

[44] The identification of top operational needs from the national survey was based on the number of votes each need received rather than on a TOPSIS analysis. Accordingly, the lists of top needs from the workshop and national survey are not entirely compatible. As noted, nonetheless, they are largely consistent.

In most cases, workshop participants estimated that technology could address roughly 25% to 40% of law enforcement's top operational needs. Estimates ranged from a low of 10% for communications and dispatch management, which the communications group felt is heavily influenced by procedures and organizational structure, to a high of 82% for coordination and interoperability with other first responders.

4.5.2. Top Technologies

Top technologies identified from the workshop poll and breakout group discussions appear in Figures 4-3, 4-4, and 4-5. Figure 4-3 presents technologies that currently have high impact in meeting operational needs, and figures 4-4 and 4-5 list promising technologies for, respectively, the next three to five years and beyond. The technologies are not listed in any particular order; as before, we emphasize the overall lists rather than rankings within the lists. With very few exceptions, the highlighted technologies met at least one of three criteria: 1) they ranked in the top 10 in the overall TOPSIS analysis of the workshop poll results; 2) they ranked in the top 10 for 3 or more functional groups in the TOPSIS analysis of the disaggregated workshop poll results; or 3) they were one of the top technologies identified by at least two of the breakout groups. Hence, our emphasis is on identifying technologies that are perceived to be (or to potentially be) highly effective and that have broader applicability across functional areas in law enforcement.

Figure 4-3: Current High-Impact Technologies

1. DNA testing equipment
2. Integrated databases
3. Geographic information systems (GIS) software
4. Computer-aided dispatch with GPS tracking of patrol cars
5. Video surveillance networks
6. Wireless access in patrol cars
7. Inter-agency radios
8. Use of force computer simulators
9. Other computer-based training and simulators
10. Fingerprint readers
11. Conducted energy devices (e.g., Tasers) / non-lethal weapons
12. Investigative software (e.g., data mining software)
13. Body armor

Figure 4-4: Promising Technologies (3-5 Years)

1 DNA testing equipment
2 Integrated data bases
3 Computer-aided dispatch with GPS tracking of patrol cars
4 Predictive modeling
5 Real time crime monitoring center
6 Inter-agency radios
7 Video surveillance networks
8 Geographic information systems (GIS) software
9 Investigative software (e.g., data mining software)
10 Patrol car cameras
11 Aerial surveillance equipment (e.g., drones)
12 Computer-based training and simulators

Figure 4-5: Promising Technologies (Beyond 5 Years)

1 DNA testing equipment
2 Integrated data bases
3 Personal video/audio equipment (worn by officers)
4 Predictive modeling
5 Investigative software (e.g., data mining software)
6 Aerial surveillance equipment (e.g., drones)
7 Real-time crime monitoring center
8 Inter-agency radios
9 Video surveillance networks
10 Software for risk factor analysis
11 Geographic information systems (GIS) software
12 Computer-aided dispatch with GPS tracking of patrol cars
13 Next generation 9-1-1 (text and voice messaging)

Several technologies—DNA testing equipment, integrated databases, GIS software, computer-aided dispatch with GPS, video surveillance networks, inter-agency radios, investigative software, and computer-based simulation and training—appear in both the current high impact and promising future technology lists. Further these technologies generally ranked highly on the national survey, based on the percentage of users that judged them to be very

effective and/or the percentage of non-users that felt they would fully address important needs (see Chapter 3). Accordingly, these would appear to be high impact technologies with much potential for future expansion and refinement. Other promising technologies appearing in figures 4-4 and 4-5 include predictive modeling (a variant of crime analysis and GIS), real-time monitoring (a variant of video surveillance networks and integrated databases), aerial surveillance drones, audio/video equipment worn by officers, patrol car cameras (presumably more advanced than those in common use today), and more advanced (i.e., Next Generation) 9-1-1 systems.

Overall, the high impact and promising technologies in figures 4-3 through 4-5 also ranked relatively high on the national survey. Most ranked in the top 10 or the top half of the national survey rankings for effectiveness and/or the potential to address operational needs (see Chapter 3).

4.6. Challenges to Technology Implementation and Other Discussion Points

As described earlier, workshop participants were able to provide both verbal and written commentary during the full group sessions. This section highlights several themes that emerged from the sessions. Often, these issues were raised in multiple sessions. Many of the comments address complications associated with technology acquisition and implementation, which was the theme of the workshop's final session. With each theme, we present a few illustrative quotes from participants.

- **Training, Skills, and Project Management**

Many attendees emphasized the importance of training to ensure that end users can utilize technology. In addition to having technical skills, police agencies also need staff with the skills to acquire and implement technology. Adopting or upgrading technology raises a number of issues regarding planning, personnel, and funding. One key issue is finding personnel that can bridge the gap between technical issues and policing needs. It is important to have good project management and people with the right skills to function as project managers. Sworn personnel often do not have much expertise in technology or project management. Civilian technical experts, on the other hand, often do not clearly understand policing functions and needs. Personnel rotation can aggravate these problems. A mix of personnel with different skills and perspectives should be involved in planning and implementing technology projects. Many participants noted that they need people that can work with vendors and industry to ensure timely implementation occurs. Participants discussed planning issues, with specific reference to the skills, time, and support needed for technology projects. Many suggested it is good to have projects underway and to wait for the optimal time to roll out them out.

"Technology is only as good as the end user. Training is always an issue. Showing all of the capabilities of the technology, and actually using it, is difficult."

"Agree… if training is not provided for technology it becomes useless, but follow up training for technology not used often is also a must"

"When a bad system (or good system made bad through lack of training or support) is made to be used by field personnel it makes it more difficult for future projects to get funding or support from the field personnel"

"I would like to see best practices on e-training for law enforcement. With budgets dwindling, it is common sense to see that e-training is the future. If YouTube and Myspace can be so compelling, [then] templates to promulgate mission, lessons learned, etc can be effectively applied via electronic mediums."

"There should be a planned effort and check off within the jurisdiction to ensure there is not duplicated effort or [that] solutions [are not] already in place before a project proceeds to the point of purchase."

- **Partnership**

Partnership between agencies and IT personnel or vendors was raised as an operational need. To have a productive partnership, there must be accountability during the whole process of purchase, implementation, and, if required, upgrades. Police agencies must also find ways to make technology vendors more attentive to the unique needs and requirements of police agencies. Participants felt that having partnerships with good relationships and communication is vital for the acquisition process.

"Not only holding the LE or IT personnel accountable, but also the vendor accountable as to what the product was supposed to do, keeping it up to date, and supporting the product properly for a reasonable period"

"Many technology vendors do not target the end user, but the person who controls the budget. If there is a disconnect between these parts of your organization, your risk goes way up in buying the wrong stuff."

- **Leadership / Mission / Culture**

The importance of having leaders who understand the importance of technology was a theme participants discussed. How the technology links with the agency's overarching strategic goals is vital to the success of the technology and implementation projects. The culture of the agency was also linked to these discussions; if an agency's culture is supportive of new technology, they often have IT governance structures, training, and implementation plans.

"It is important that members of the Command Staffs stay familiar or at least aware of what the available technologies are so they can effectively prioritize the needs of the department(s). This is just as important as the officer on the street being trained to utilize the technology. "

"Agree 100%...technology is a means to achieve the strategic goals of the organization."

"Good commanders recognize the need to share the responsibility of technological expertise."

On a related note, there were a number of comments about Compstat that seemed to affirm the need for better and more timely data but that also serve as caveats about the limits of some technology-driven innovations. Some participants felt that Compstat focuses too much attention on "old" data (rather than real-time patterns), and that too much time and effort is focused on preparing for Compstat meetings rather than on solving problems and developing long-term strategies. The comments suggested that there is a need to use data and Compstat in better ways for long-term purposes.

- **Information Sharing (Internal and External)**

Data sharing—both within an agency and across agencies—is an important issue. Finding ways to disseminate information more quickly and provide easier access to a variety of personnel are both desired. However, data integration and sharing raise a number of technical issues like integration of hardware and software and compatibility and standardization of systems across and within agencies.

Having the ability to sharing information with partners, other agencies, and the community was raised, as were concerns about security, legal issues, and policies. The importance of having this capability was rated very high, with many participants suggesting that technology can help but that the main issue is policy and standards that have to be updated and changed; often, this is too difficult.

Many participants discussed the requirements for timely, up to date, and accurate information sharing capabilities. Participants agreed on the importance of having the ability to get information to and from different work groups and of ensuring that end users have access. Having the ability to link information sources such as spreadsheets and databases was raised as an important issue that technology can help fix.

"Criminals have tons of advantages: They don't have to worry about non-disclosure agreements, MOUs, Intergovernmental agreements, certifications, security standards, budgets, politics, etc... they can be much more nimble than we are-- and many criminal enterprises use the web and other technology very effectively and quickly"

"Not sharing between jurisdictions hurts LE and hinders solving real crime problems"

"We have several different stand alone spreadsheets and databases and the integral warehouse idea is crucial."

"*Information sharing has more to do with agency policy than technology. Everybody has something of value, but they don't necessarily share."*

"In law enforcement we are good at establishing databases. This group is on target regarding the discussion of data integration. The massive amounts of data that we create are often difficult to merge within our own agencies. When the shared integration (agency to agency) occurs, the process becomes more complex. The establishment of a common platform is key. "

"Without online reporting how can one be aware of what is going on? For those agencies that do not have online reporting, like our dept, the info is not available in our RMS until weeks after the fact. We are reactive at best with old data."

"There would be no limit to the applications... video, mapping, incident reporting, crime analysis, photos, ticket-writing..."

- **The Role of Crime Analysis**

Participants discussed the importance of crime analysis and its place within the agencies. The role of crime analysis and how crime analysts are organized (centralized or decentralized) was debated between participants with a variety of views. The discussion also covered technology requirements for crime analysis.

"If the analysis and data are only looked at to prepare for the [Compstat] "meeting", then the process is a failure. The analysis should be shared and discussed daily. We currently struggle over the weekends because the analysts don't work weekends."

"I would argue that ALL officers are crime analysts... "

"Sorry, can't agree on this (unless I completely re-define analysis as meaning basic abilities requiring programmers to create simple push button tools based on what I think I need). If you go back to a more realistic definition, you see that officers as analysts has been a failure in this country overall (exceptions granted) for many reasons."

"I think centralized (but mobile capability and freedom to go do what they need to do) has been winning the day on this debate overall for a while now. A lot [is] out there on this issue and the pros/cons of each [centralized/decentralized]. But the big issues are [that] non-centralized [analysts] aren't protected, don't keep up with technology, end up as administrative assistants, and, in the long run, just don't add the kind of value the centralized [analysts] do ([i.e.,] more tech savvy, more up-to-date, learning from peers, but still tied to needs when done right). "

"All encompassing databases with an analysis tool to data mine them. For example, suppose we had a database that housed all police data and merged it with all manners of public information that could be gleaned from the web and other places. Let's say there was a series of crimes that would appear to be unrelated when viewed by the data available to the police. However, when referenced with public data, it shows a pattern that these crimes occur when a particular movie showing as local theaters lets out."

- **Best Practices and Research**

Participants discussed the importance of knowing what worked and what was useful in different situations, as well as sharing specific examples of best practices from their agencies. Having a forum such as this to share best practice examples was mentioned as being very beneficial.

Research was a key theme participants discussed at times. It was highlighted that many would like to know more about what is out there, how it helps and hear from other agencies that have addressed similar issues using specific technology.

Some participants felt that national organizations (like DOJ, PERF, or IACP) should facilitate / sponsor forums for: information exchange about products and best practices; dissemination of technology standards and open source technologies; technology testing; and funding support. This would help agencies find solutions to common problems.

"We should evaluate lessons learned from our European brothers and sisters. Camera technology does not reduce crime but assists in the documentation of it. Further developing technology is analytical study of the camera systems. When a mesh network captures events, the info can be great to determine what is useful and what is not."

"*Profession-level guidance may mitigate the information challenge inherent in police officers (chiefs) having to evaluate technologies beyond their competence."*

"What about a "lessons learned" report in which an organization evaluated or collected information on various technologies so agencies know the relative worth of various products? There could be a section on CADs, C/A tools, weapons, etc."

- **Funding**

Funding was a major topic of discussion in the barriers session. Obtaining longer term grants and consideration of implementation and ongoing costs were topics of concern to participants. A few participants felt it would be useful for some cost benefit analysis to determine savings and value. (Recall that economic and funding considerations were the major barrier to technology implementation in the national survey.)

"One barrier to consider is that technologies may be obtained through various grants as a funding source. However if the deployment of those technologies is not planned out properly, it is easy to overlook the on-going costs that departments will bear, and ultimately the technologies become outdated or not useful for the purpose [for which] they were intended."

"Because of the amount if time it takes to get purchases approved when spending public money, sometimes technology purchases are outdated by the time they are implemented"

"Answering cost savings questions associated with the acquisition of a piece of technology is futile; technology is there to help us do our jobs better, not to replace us"

"I have found leasing so far impossible because of restrictions of my Municipal Purchasing Ordinances"

"Some options for us: We can't use any bond-funded initiative for leasing because the bond has to be secured by a hard asset that's owned. We can't generally get budget approval because we're on a one-year budget cycle and leasing would require us to commit to payments over a multiple-year period, which we can't guarantee. Some grants specifically prohibit this. This is

what I learned over a very painful process of meetings with multiple units of municipal government in an effort to get this done."

- **Standards / Policy / Legal / Civil Rights**

Participants raised issues of civil rights, legal issues, standards, and differing policies as barriers to acquiring and utilizing technology. Many agencies highlighted concerns over interpretations of legislation that have hindered some technological tools in helping to reduce crime.

"Political liabilities will include the current and future US Supreme Court appointments, with [the] potential of LE efforts being deemed as a threat to personal privacy, "right-to-know", or [as a] perceived violation of an individual's civil rights. LE has a much tougher time than [the] military in being able to employ certain types of technology. "

"The idea, or various people's interpretation, of what a right to privacy is definitely comes into play as a barrier. Such as those who seem to feel that Red Light Camera systems that document violators on public roadways is a violation of their right to privacy. The courts or legal system need to really consider what the intent of some of these laws or rights are."

Chapter 5: Conclusions and Next Steps

The PERF-Lockheed Martin project on Future Law Enforcement Technology Needs entailed a partnership between researchers, practitioners, and industry to identify key technology needs in law enforcement and to identify, evaluate, and prioritize cutting-edge, relevant technologies that hold the greatest priority for policing. Although various forms of new technology hold promise for enhancing the operation of the nation's approximately 18,000 law enforcement agencies, there is little to guide these agencies in selecting, procuring, and implementing technology. Further, there is little in the way of systematic and timely research on technology needs and impacts in law enforcement. Recent work that has been done in this area has also tended to focus on technologies related to homeland security concerns. Our project instead looks more broadly at technology applications in everyday police work. This partnership between PERF and Lockheed Martin, which brought together a leading association of innovative police practitioners and an industry leader in the development of technology with military and policing applications, is one of the first of its kind. Given the complexity of integrating technology into the operations of a law enforcement agency, we believe that partnerships such as this one are critical to advancing technology applications in policing.

As noted at the beginning of the report, the project objectives were to explore and document:

- The operational needs of law enforcement agencies
- The law enforcement perspective on technology—including beliefs about its effectiveness
- A prioritized list of technologies to develop for law enforcement
- Barriers to the acquisition and use of technology in law enforcement

We investigated these issues in three ways:

- An extensive review of the prior literature on law enforcement technology
- A national survey of 216 police agencies affiliated with PERF (a national association of police executives from many of the nation's largest police agencies)
- A workshop / focus group event involving dozens of well-informed law enforcement practitioners from around the country

Below, we summarize key conclusions from the project, focusing primarily on the results of the survey and workshop. (In order to keep this section concise, we focus on the top needs and technologies that emerged from the workshop and survey results. However, it is important to note that there are many other important needs and technologies reviewed in the main body of the report.)

5.1. Operational Needs in Law Enforcement

Through both the national survey of PERF agencies and the technology workshop, we sought to identify key operational needs that law enforcement agencies will face in the near future. Our intent was to identify these needs so that police practitioners, researchers, and industry can consider if and how technology can be used to address these needs.

The following five operational areas, which emerged as very high priorities in both the survey and workshop, appear to represent the most pressing needs in law enforcement. (They are listed in no particular order.)

- Managing calls for police service
- Crime analysis and information-led policing
- Information technology and database integration
- Prevention and investigation of street crime
- Hiring and retention of police officers

Other operational needs that stood out in the results of the survey and/or the workshop included:

- Freeing officer time for proactive, crime prevention strategies
- Coordination and interoperability with first responders
- Training for police personnel
- Communications and dispatch
- Officer oversight, supervision, and accountability
- Weapons and equipment
- Security for police information systems
- Prevention and investigation of electronic and cyber-crime

Although technology cannot be the sole solution to these needs (other critical factors, for example, include organizational policies, procedures, structures, manpower, training, and culture), it can play an important role. Here are just a few of the ways that technology is relevant to important operational needs in law enforcement:

- Police increasingly recognize that their deployment and strategies should be guided by information and analysis that helps them focus on the places, persons, times, problems, and situations that contribute most to crime. IT can facilitate this orientation by improving the integration, analysis, and dissemination of information both within and across agencies. IT can also increase the efficiency of police in ways that ultimately improve their service and performance.

- Responding to calls for service is a central everyday task in policing. Moreover, it is a very resource-intensive task that can greatly limit the ability of agencies to devote resources to crime prevention strategies. Long delays in response can also adversely affect citizen satisfaction with police. Technologies that help agencies better manage calls for service and deploy their resources in more effective ways (e.g., computer-aided dispatching with GPS and automated offense reporting) thus have the potential to both improve citizen satisfaction and facilitate crime prevention.

- The ability to communicate and coordinate actions with other first responders (i.e., fire and rescue and emergency medical personnel) is a need that has received heightened emphasis in recent years due to concerns about responses to potential terrorist attacks and disasters. Communications technology is central to this need.

- Technology has the potential to enhance and economize various forms of police training, such as simulation training in the use of force. At the same time, agencies must ensure that personnel are properly trained in the use of technology.

- Hiring and retention of officers has been a major concern for policing agencies during the last few decades. Technology can be used to market law enforcement (sleek websites provide one example) but also can serve as a magnet for younger recruits interested in working with the latest technology. Agencies must attract and retain personnel with skills in the selection, implementation, and use of technology.

- Better technologies for collecting and processing criminal evidence can enhance case clearance rates and potentially reduce crime rates.

- Having the means to control individuals and groups with less lethal weapons can reduce injuries and deaths to civilians and officers while also minimizing legal and political liabilities for police.

5.2. The Law Enforcement Perspective on Technology Effectiveness

Although many forms of technology have the potential to improve police efficiency and effectiveness, the impact of any particular technology on police effectiveness may be limited by several factors, including: technical (i.e., engineering) problems; difficulty in using the technology; ancillary costs associated with using the technology (e.g., costs associated with training, technical assistance, and maintenance); the availability of other complementary technologies within an agency; the availability of qualified people to select, implement, and use technology; unanticipated effects on organizations, officers, or citizens; the prevalence of the problem(s) the technology is intended to address; or a misunderstanding of the problem(s) the technology is intended to address. For any of these reasons, some technologies will perform better than others, and some may not perform as intended at all. Some technologies may also create economic and political liabilities for police. Understanding which technologies are most useful to police and why has obvious value to agencies allocating scarce resources.

Although evaluation research on technology and policing has been quite limited, there is evidence from such studies that police work has been enhanced by technologies like IT, DNA testing technology, non-lethal weapons (i.e., Tasers®), and closed circuit television (CCTV). Further, law enforcement practitioners generally believe that technology enhances their work. Our survey of PERF agencies examined agencies' perspectives about the effectiveness of 52 types of technology. Agencies generally rated these technologies as moderately or very effective; rarely did more than a small share rate a technology as ineffective. Participants in the PERF-Lockheed workshop also believed that technology could play a substantial role in addressing the operational needs highlighted above. Below, we discuss technologies that the study participants felt are particularly effective.

5.3. Priority Technologies for Law Enforcement

Participants in the PERF-Lockheed workshop identified several technologies that are particularly critical to addressing high priority needs in law enforcement. These are listed in Table 5-1. Workshop participants also identified technologies that, in their view, have high potential for improving policing during the next 3 to 5 years and beyond. These technologies are listed in Table 5-2. Using results from the PERF survey, tables 5-1 and 5-2 also show: 1) how commonly PERF agencies use each technology; 2) how current users rate the effectiveness of each technology; and 3) the extent to which current non-users think each technology would address the needs of their agency.

As these lists show, workshop participants placed much emphasis on technologies related to IT, crime analysis, and communications. Other priority technologies include non-lethal weapons and equipment for training, surveillance, and the collection and processing of evidence. Overall, most of the high impact and promising technologies in tables 5-1 and 5-2 rated highly on the PERF survey—higher percentages of users judged them to be very effective and higher percentages of non-users felt they would fully address important operational needs. Although many of these technologies are fairly common in policing, there is substantial room for expanding their use. This is particularly true for some of the less commonly used technologies like DNA testing equipment and personal audio/video devices.

Table 5-1: High Impact Technologies

High Impact Technologies (Workshop)	% of Agencies Using the Technologies (PERF Survey)	% of Users Rating the Technologies as Very Effective (PERF Survey)	% of Non-Users Stating the Technologies Would Fully Address Needs (PERF Survey)
DNA testing equipment	24%	69%	29%
Integrated databases	61%	55%	50%
Geographic information system (GIS) software	85%	63%	31%
Computer-aided dispatch with GPS tracking of patrol cars	55%	56%	55%
Video surveillance networks	61%	39%	35%
Wireless access in patrol cars	84%	73%	61%
Inter-agency radios	79%	60%	56%
Use of force computer simulators	52%	59%	32%
Other computer-based training and simulators (not for use of force or driving)	22%	47%	22%
Fingerprint readers	58%	78%	38%
Conducted energy devices (i.e., Tasers®)	82%	93%	22%
Body armor	98%	89%	40%
Investigative software	46%	51%	35%

Table 5-2: Promising Technologies for the Next 3-5 Years and Beyond

Promising Technologies (Workshop)	% of Agencies Using the Technologies (PERF Survey)	% of Users Rating the Technologies as Very Effective (PERF Survey)	% of Non-Users Stating the Technologies Would Fully Address Needs (PERF Survey)
DNA testing equipment	24%	69%	29%
Integrated databases	61%	55%	50%
Geographic information system (GIS) software	85%	63%	31%
Computer-aided dispatch with GPS tracking of patrol cars	55%	56%	55%
Predictive modeling	31%	30%	27%
Real-time crime monitoring center	20%	60%	31%
Inter-agency radios	79%	60%	56%
Video surveillance network	61%	39%	35%
Investigative software	46%	51%	35%
Patrol car cameras *	64%	60%	24%
Audio/video equipment (worn by officer) **	26%	57%	19%
Aerial surveillance equipment	13%	54%	13%
Software for risk factor analysis for victimization**	14%	29%	17%
Computer-based training and simulators (other than for use of force or driving)*	22%	47%	22%
Next generation 9-1-1 (text and voice messaging)**	21%	51%	32%

* Technology rated as promising for the next 3-5 years only.
** Technology rated as promising for beyond the next 5 years only.

Several technologies—DNA testing equipment, integrated databases, GIS software, computer-aided dispatch with GPS (geographical positioning systems), video surveillance networks, inter-agency radios, investigative software, and computer-based training equipment—appear in both lists. These technologies thus appear to be high impact technologies with particularly high potential for future expansion and refinement. Indeed, according to the PERF survey, roughly a quarter or more of agencies without the following technologies are very likely to acquire them in the next few years: use of force computer simulators, wireless access in patrol cars, integrated databases, GIS software, inter-agency radios, computer-aided dispatch with GPS,

conducted energy devices, and video surveillance networks. Other promising technologies for the future include predictive modeling (a variant of crime analysis and GIS), real-time crime monitoring systems (which may combine integrated databases, crime analysis, GIS, and video surveillance networks) aerial surveillance drones, audio/video equipment for officers in the field, and enhanced 9-1-1 systems with advanced text and voice messaging capabilities.

We should also note that there are a number of widely used technologies that may need replacement in coming years. Examples include night vision devices, use of force simulators, video surveillance networks, special purpose vehicles, and mobile command centers. High percentages of agencies use these technologies according to the PERF survey, yet many reported that their equipment is old or outdated. Although these are not all high impact technologies, updating them may be an important issue for many agencies.

5.4 Barriers to Technology Acquisition and Use in Law Enforcement

Factors that impede or facilitate the application of technology in law enforcement were explored in both the PERF survey and the PERF-Lockheed workshop. Key issues that emerged are highlighted below.

- Financial Constraints

In the PERF survey, agencies overwhelmingly cited costs and monetary constraints as a barrier to technology acquisition. Financial constraints may impede the ability of agencies to acquire technology and handle its ancillary costs (costs associated with training and maintenance). Likewise, obtaining long-term grants for technology and dealing with implementation and ongoing ancillary costs were topics of concern to participants in the workshop.

- Training, Skills, and Project Management

End users must have the proper training to use technology. In addition, police agencies need staff with the skills to acquire and implement technology. Key issues include having personnel that can bridge the gap between technical problems and policing needs and having personnel with good project management skills.

- Partnership

Partnership between agencies and technology providers was raised as an important issue. This requires accountability throughout the process of purchasing, implementing, and, if required, upgrading technology. Police must also find ways to make technology vendors more attentive to the unique needs and requirements of police agencies. Partnering among law enforcement agencies, industry and academia will be key in rapidly leveraging all but the most inexpensive technical solutions. Future alliances must be developed to focus on how to best leverage partnerships and redesign the operational model of law enforcement. The new model would heavily leverage service industries for IT, surveillance, data repositories, etc., that have moderate/high costs and high refresh rates. This new model must also leverage regional

repositories of special use equipment/hardware so that no agency bears the cost burden of individual pieces of equipment that might only be used randomly throughout the year.

- Leadership, Mission, and Culture

Technological progress is facilitated when agency leaders understand the importance of technology and can link technology to the agency's overarching strategic goals. IT governance structures, training, and implementation plans facilitate technological progress.

- Impediments to Information Sharing

Data integration and sharing—both within and across agencies—raises a number of technical issues like integration of hardware and software and compatibility / standardization of systems. Other potential obstacles include security concerns, legal issues, and policies that restrict data sharing.

- Understanding Best Practices

Participants in the workshop indicated a strong desire to learn more about the experiences of other agencies in implementing technology. Attendees felt that the PERF-Lockheed workshop was very useful and that national organizations (like the U.S. Department of Justice, PERF, and the International Association of Chiefs of Police) should facilitate or sponsor similar forums for: information exchange about products and best practices; dissemination of technology standards and open source technologies; technology testing; and funding support. This would help agencies find solutions to common problems.

- Other Political, Economic, and Legal Issues

In the PERF survey, economic and political liabilities constituted the leading challenge to implementing various forms of technology. Although these problems were often linked to the financial issues discussed above, they may also include problems like lawsuits and political resistance to the use of particular technologies. Workshop participants also cited civil rights, legal issues, and differing agency policies as barriers to utilizing some technologies.

5.5. Future Steps

As noted above, participants in the PERF-Lockheed workshop felt that the workshop was very valuable and that having more such forums would benefit the policing profession in ways such as: (1) identifying future partnership opportunities to advance capabilities for law enforcement; (2) recognizing that solutions exist in nontraditional venues; (3) developing standards for police technology; (4) disseminating best practices in technology implementation and use; and (5) helping agencies find funding and assistance for technology acquisition. PERF, Lockheed Martin, and others should build on this experience by sponsoring future workshops and conferences on law enforcement technology and by facilitating networking among technology specialists in policing.

Having identified broad technology categories for law enforcement, there is now a need to better understand which specific devices will best meet these technology needs. Further, we must identify best practices for the implementation and use of these technologies. We therefore recommend case studies to examine the implementation and use of these key technologies in agencies that have applied them successfully. Such studies should examine technical and organizational issues involved in planning and implementing these technologies, everyday uses of the technologies, and measurable outcomes associated with the uses of the technologies.

Similarly, there is a need for more evaluation research to provide police with better evidence on which technologies are most valuable and cost effective for law enforcement uses. Researchers, practitioners, and technology developers should collaborate in such work to identify the types and uses of technology that are most efficacious for policing and to delineate the implementation issues that impact the successful application of technology.

Appendix A

References

Allen, G. (2008, March 12). *Law enforcement could have new LED light weapon* [Television broadcast]. New York: CBS Broadcasting (accessed at cbs11tv.com).

Braga, A.A. (2007). *Effects of hot spots policing on crime*. A Campbell Collaboration systematic review available at http://www.aic.gov.au/campbellcj/reviews/titles.html.

Bratton, W. (1998). *Turnaround: How America's top cop reversed the crime epidemic*. New York: Random House.

Colvin, C. (2001). *Evaluation of innovative technology: Implications for the community policing roles of law enforcement officers.* San Francisco: Psychology Department, San Francisco State University.

Daneman, M. (2008). Five cities test high-tech 9-1-1 system. *USA Today*. Retrieved July 8, 2008 from www.usatoday.com.

Danziger, J. N. & Kraemer, K. L. (1985). Computerized data-based systems and productivity among professional workers: The case of detectives. *Public Administration Review, January/February*, 196-209.

Falcon, W. (2005). Special technologies for law enforcement and corrections. *National Institute of Justice Journal 252*, 21-27.

Frank, J., Brandl, S.G., & Watkins, R.C. (1997). The content of community policing: A comparison of the daily activities of community and "beat" officers. *Policing: An International Journal of Police Strategy and Management*, 20, 716-728.

Fridell, L.A. & Pate, A.M. (2001). The other side of force: Felonious killings of law enforcement officers. In Dunham, R.G. & Alpert, G.P. (eds.), *Critical Issues in Policing: Contemporary Readings* (4th ed.), 636-663. Prospect Heights, IL: Waveland Press.

Hwang, C.L. & Yoon, K. (1981). *Multiple attribute decision making: Methods and applications, a state of the art survey*. Berlin: Springer-Verlag.

Hickman, M.J. & Reaves, B.A. (2006a). *Local police departments,* Washington, D.C.: Bureau of Justice Statistics, U.S. Department of Justice.

Hickman, M.J. & Reaves, B.A. (2006b). *Sheriffs' Offices, 2003* Washington, D.C.: Bureau of Justice Statistics, U.S. Department of Justice.

Hohmann, J. (2008). Washington, D.C. puts itself under surveillance. *Los Angeles Times.* Retrieved June 17, 2008 from www.laTimes.com.

Home Office. (2005). *DNA Expansion Programme 2000-2005: Reporting Achievement*. London: Home Secretary of the United Kingdom. Retrieved from: http://www.homeoffice.gov.uk/documents/DNAExpansion.pdf

International Association of Chiefs of Police. (2005). *Law enforcement priorities for public safety: Identifying critical technology needs.* Alexandria, VA: Author.

Johnson, K. (2008). States expand sampling of DNA. *USA Today*. Retrieved April 14, 2008 from www.usatoday.com.

Jenkinson, E., Neeson, C., & Bleetman, A. (2006). The relative risk of police use-of-force options: evaluating the potential for deployment of electronic weaponry. *Journal of Clinical Forensic Medicine*, 13, 229-241.

Justice and Safety Center. (2002). *National assessment of technology and training for small and rural law enforcement agencies (NATTS): A descriptive analysis.* Richmond, KY: Eastern Kentucky University.

Koper, C. S. & Roth, J.A. (2000). Putting 100,000 Officers on the Street: Progress as of 1998 and Preliminary Projections Through 2003. Pp. 149-178 in Roth, Jeffrey A., Joseph F. Ryan, and others. *National Evaluation of the COPS Program -- Title I of the 1994 Crime Act.* Washington, D.C.: U.S. Department of Justice.

Koper, C. S., Moore, G. E. & Roth, J.A. (2002). *Putting 100,000 Officers on the Street: A Survey-Based Assessment of the Federal COPS Program.* Washington, D.C.: The Urban Institute.

Lipscomb, D. C. (2008). Video cameras proposed on guns for D.C. police. *The Washington Times*. Retrieved May 14, 2008 from www.washingtontimes.com.

Lovrich, N.P., Gaffney, M.J., Pratt, T.C., Johnson, C.L., Asplen, C.H., Hurst, L.H., & Schellberg. (2003). *National forensic DNA study report: Final report.* Pulman, WA: Division of Governmental Studies and Services, Washington State University and Smith Ailing Lane, P.S.

Mastrofski, S.D., Parks, R.B., & Wilson, D.B. (2003). *Influences on the Adoption of Community Policing in the United States: Final Report to the National Institute of Justice*. George Mason University: Center for Justice Leadership and Management.

Mazerolle, L. G., Watkins, C., Rogan, D. & Frank, J. (1999). *Random gunfire problems and gunshot detection systems*. Research-in-Brief. Washington, D.C.: National Institute of Justice, U.S. Department of Justice.

Mazerolle, L., Hurley, D., & Chamlin, M. (2002b). Social behavior in public space: An analysis of behavioral adaptations to CCTV. *Security Journal*, 15, 59-75.

Mazerolle, L., Rogan, D., Frank, J., Famega, C. & Eck, J. E. (2002a). Managing citizen calls to the police: The impact of Baltimore's 3-1-1 call system. *Criminology & Public Policy, 2*, 97-124.

McCarron, H. (2008). Foxborough police put firearms training simulator to work. *Wicked Local.* Retrieved April 3, 2008 from www.wickedlocal.com/foxborough/news.

Musheno, M. C., Levine, J. P. & Palumbo, D. J. (1978). Television surveillance and crime prevention: Evaluating an attempt to create defensible space in public housing. *Social Science Quarterly, 58*(4), 647-656.

National Law Enforcement and Corrections Technology Center. (Fall 2006). 30 years, 3,000 saves. *Techbeat*. Rockville, MD: Author

National Research Council. (2004). *Fairness and effectiveness in policing: The evidence*. Skogan, W. & Frydl, K. (eds.). Washington, D.C.: The National Academies Press.

Nunn, S. (1994). How capital technologies affect municipal service outcomes: The case of police mobile digital terminals and stolen vehicle recoveries. *Journal of Policy Analysis and Management, 13*(3), 539-559.

Nunn, S. (2001). Cities, space, and the new world of urban law enforcement technologies. *Journal of Urban Affairs, 23*, 259-278.

Nunn, S. (2001). Police information technology: Assessing the effects of computerization on urban police functions. *Public Administration Review, 61*, 221-234.

Nunn, S. & Quinet, K. (2002). Evaluating the effects of information technology on problem-oriented-policing: If it doesn't fit, must we quit? *Evaluation Review, 26*, 81-108.

Office of Community Oriented Policing Services. (2008). *Building a 311 system: A case study of the city of Minneapolis*. Washington, D.C.: U.S. Department of Justice.

Police Executive Research Forum. (2007). *Violent crime in America: "A tale of two cities."* Washington, D.C.: Author.

Police Executive Research Forum. (2008). Violent crime in America: What we know about hot spots enforcement. Washington, D.C.: Author.

Reed Jr., B. (May 2008). Future technology in law enforcement. *FBI Law Enforcement Bulletin.*

Roman, J.K., Reid, S., Reid, J., Chalfin, A., Adams, W., & Knight, C. (2008). *The DNA field experiment: Cost-Effectiveness analysis of the use of DNA in the investigation of high-volume crimes.* Washington, D.C.: The Urban Institute.

Roth, J. A., Koper, C.S., White, R. & Langston, E.A. (2000). Using COPS Resources. Pp. 101-148 in Roth, Jeffrey A., Joseph F. Ryan, and others. *National Evaluation of the COPS Program -- Title I of the 1994 Crime Act.* Washington, D.C.: U.S. Department of Justice.

Schultz, P. D. (June 2008). The future is here: Technology in police departments. *Police Chief Magazine, 75*.

Schwabe, W. (1999). *Needs and prospects for crime-fighting technology: The federal role in assisting state and local law enforcement.* Santa Monica: RAND Corporation.

Schwabe, W., Davis, L.M., & Jackson, B.A. (2001). *Challenges and choices for crime-fighting technology: Federal support of state and local law enforcement.* Santa Monica: RAND Corporation.

Sherman, L.W. & Eck, J.E. (2002). Policing for crime prevention. In Sherman, LW., Farrington, D.P., Welsh, B.C., & MacKenzie, D.L., *Evidence-based crime prevention*, 295-329. New York: Routledge.

Skogan, W.G., & Hartnett, S.M. (2005). The diffusion of information technology in policing. *Police Practice and Research: An International Journal*, 6, 401-417.

Smith, M.R., Kaminski, R.J., Rojek, J., Alpert, G.P., & Mathis, J. (2007). The impact of conducted energy devices and other types of force and resistance on officer and suspect injuries. *Policing: An International Journal of Police Strategies & Management*, 30, 423-446.

Sparrow, M.K., Moore, M., & Kennedy, D.M. (1990). *Beyond 9-1-1: A new era for policing*. New York: Basic Books.

TriData Corporation. (1998). *Inventory of state and local law enforcement technology needs to combat terrorism.* Arlington, VA: Author.

U. S. Department of Homeland Security. (2008). *High-priority technology needs* (2nd ed.) (DHS Science and Technology Directorate Publication). Washington, D.C.: Author.

U. S. Department of Justice. (1999). *National evaluation of state and local law enforcement technology needs to combat terrorism.* Research-in-Brief. Washington, D.C.: Author.

U.S. Government Accountability Office. (2005). *Community policing grants: COPS grants were a modest contributor to declines in crime in the 1990s*. Washington, D.C.: Author.

Washington Times. (2008). Video cameras proposed on guns for D.C. police. *The Washington Times*. Retrieved May 14 from www.washingtontimes.com.

Webby, S. (2008). New tool for police is a blast of sound. *The Mercury News* Retrieved February 25, 2008 from www.mercurynews.com.

Weisburd, D., McNally, A.M., Mastrofski, S.D., Greenspan, R., & Willis, J.J. (2003). Reforming to preserve: Compstat and strategic problem solving in American policing. *Criminology and Public Policy*, 2, 421-455.

Welsh, B. C. & Farrington, D.P. (2004). Surveillance for crime prevention in public space: Results and policy choices in Britain and America. *Criminology & Public Policy, 3*, 497-526.

Willis, J. J., Mastrofski, S. D., Weisburd, D. & Greenspan, R. (2004). *Compstat and organizational change in the Lowell Police Department: Challenges and opportunities.* Washington, D.C.: Police Foundation.

Zaworski, M. J. (2004). *Assessing an automated, information sharing technology in the post "9-11" era – Do local law enforcement officers think it meets their needs?* (Doctoral Dissertation). Miami: Florida International University.

Appendix B

POLICE EXECUTIVE RESEARCH FORUM

Technology Needs Assessment

ID NUMBER

In an effort to help shape the future direction of technologies developed by industry for law enforcement agencies, the Police Executive Research Forum (PERF), with support from the Lockheed Martin Corporation, is assessing the technology needs of law enforcement agencies. In order to learn more about law enforcement agencies' experiences with technology and their future technological needs, we would like to ask for your cooperation in completing the following survey. The survey is divided into three main sections: (1) background questions about your agency and jurisdiction; (2) questions about your agency's operational needs in the next three to five years; and (3) questions about the technology your agency currently uses or might consider using.

As a reminder, all agency responses will be kept confidential.

We appreciate your contribution to this very important project.

INSTRUCTIONS:

- There are three ways to respond to this survey. If at all possible, we prefer that you use the Internet method as it reduces our data entry time and promotes accuracy. If completing the survey online, please make sure to enter your ID NUMBER, which is located at the top right of this page. Without the ID NUMBER, USER NAME and PASSWORD, you will not be able to complete the survey online.

  Option 1 - An electronic version of this questionnaire is located on the Internet at:
  http://survey.policeforum.org/technologyneeds.pdf

  If you choose to complete the survey via the Internet, you will be prompted to enter the following information:

  USER NAME: TECH
  PASSWORD: NEEDS533

  Option 2 - Fax the completed survey to the Police Executive Research Forum at (202) 466-7826.

  Option 3 - Mail the completed survey to:

  Bruce Kubu - Technology Needs Assessment
  Police Executive Research Forum
  1120 Connecticut Ave.
  Suite 930, NW
  Washington, DC 20036

- If you choose to either mail or fax this survey, please use either blue or black ink and print as neatly as possible using only CAPITAL letters.
- Please respond to questions as they pertain to your entire agency.
- Do not leave any items blank.
- Please retain a copy of the completed survey for your records as project staff may call to clarify responses.
- If you have any questions regarding the survey, please contact Bruce Kubu (202-454-8308 or bkubu@policeforum.org).

POLICE EXECUTIVE RESEARCH FORUM

Technology Needs Assessment

ID NUMBER

I. Background Characteristics of Your Agency and Jurisdiction

Agency Characteristics

1. **How many total full-time employees does your agency have?** ☐☐☐☐☐ Employees

   1a. **How many are sworn officers?** ☐☐☐☐☐ Sworn officers

2. **How many full-time employees does your agency have in each of the following areas?**

Patrol	☐☐☐☐☐	**Planning and research**	☐☐☐☐☐
Investigations	☐☐☐☐☐	**Specialized units (e.g., SWAT)**	☐☐☐☐☐
Crime analysis	☐☐☐☐☐	**Information technology**	☐☐☐☐☐
Training	☐☐☐☐☐	**Detention**	☐☐☐☐☐

3. **Does your agency have a planning and research unit or other central office that guides decisions about technology acquisition?**
   - ○ **Yes**
   - ○ **No** ⇨ **If NO, how does your agency research and determine its technological needs and procurements?**

     ☐

4. **Is your agency currently accredited by the Commission on Accreditation for Law Enforcement Agencies (CALEA)?**
   - ○ **Yes**
   - ○ **No**

Jurisdiction Characteristics

5. **What is the size of the residential population that your agency serves?** ☐☐☐☐☐☐☐☐
6. **How many Part I index crimes occurred in your jurisdiction in 2007?** ☐☐☐☐☐☐
7. **How many Part I violent crimes occurred in your jurisdiction in 2007?** ☐☐☐☐☐☐
8. **What was the total number of dispatched calls for service (including both citizen and officer generated calls for service) in 2007?** ☐☐☐☐☐☐
9. **What is the size of your jurisdiction in square miles?** ☐☐☐☐☐☐☐☐

POLICE EXECUTIVE RESEARCH FORUM

Technology Needs Assessment

ID NUMBER

II. Operational Needs in the Next 3-5 Years

10. How strongly do you agree or disagree that your agency will have high-priority needs for additional resources in the following operational areas during the next 3-5 years? Consider all resource needs such as personnel, technology, equipment, etc. Please use the following scale: (1) strongly agree, (2) somewhat agree, (3) neither agree nor disagree, (4) somewhat disagree, and (5) strongly disagree.

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Patrol officer response to calls for service	○ 1	○ 2	○ 3	○ 4	○ 5
Freeing officer time for proactive strategies	○ 1	○ 2	○ 3	○ 4	○ 5
Prevention and investigation of street crime	○ 1	○ 2	○ 3	○ 4	○ 5
Prevention and investigation of organized crime	○ 1	○ 2	○ 3	○ 4	○ 5
Prevention and investigation of homeland security threats and terrorism	○ 1	○ 2	○ 3	○ 4	○ 5
Prevention and investigation of electronic/cybercrime	○ 1	○ 2	○ 3	○ 4	○ 5
Crime analysis and information-led policing	○ 1	○ 2	○ 3	○ 4	○ 5
Training	○ 1	○ 2	○ 3	○ 4	○ 5
Hiring and retention	○ 1	○ 2	○ 3	○ 4	○ 5
Officer oversight, supervision and accountability	○ 1	○ 2	○ 3	○ 4	○ 5
Information technology (e.g., database integration and data sharing within and across agencies)	○ 1	○ 2	○ 3	○ 4	○ 5
Communications and dispatch	○ 1	○ 2	○ 3	○ 4	○ 5
Coordination and interoperability with other first responders	○ 1	○ 2	○ 3	○ 4	○ 5
Weapons and equipment	○ 1	○ 2	○ 3	○ 4	○ 5
Security for police information systems	○ 1	○ 2	○ 3	○ 4	○ 5
Crowd and riot control	○ 1	○ 2	○ 3	○ 4	○ 5
Tactical operations (e.g., hostage situations)	○ 1	○ 2	○ 3	○ 4	○ 5
Handling explosives	○ 1	○ 2	○ 3	○ 4	○ 5

↳ **Question 10 CONTINUED on top of next page...**

↳ **Question 10 CONTINUED from previous page...**

10. How strongly do you agree or disagree that your agency will have high-priority needs for additional resources in the following operational areas during the next 3-5 years? Consider all resource needs such as personnel, technology, equipment, etc.

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Collection and processing of crime scene evidence	○ 1	○ 2	○ 3	○ 4	○ 5
Pursuit management (e.g., foot and vehicle pursuits)	○ 1	○ 2	○ 3	○ 4	○ 5
Other (please specify):	○ 1	○ 2	○ 3	○ 4	○ 5
↳					
Other (please specify):	○ 1	○ 2	○ 3	○ 4	○ 5
↳					
Other (please specify):	○ 1	○ 2	○ 3	○ 4	○ 5
↳					

11. Please indicate which of the operational needs listed in Question 10 will be of the MOST importance to your agency in the next 3-5 years. Please list up to three areas.

1)

2)

3)

POLICE EXECUTIVE RESEARCH FORUM

Technology Needs Assessment

ID NUMBER

III. Technology Currently in Use and Experiences with Technology

12. For each type of technology listed below that your agency has used, please answer questions (a) through (c). Please answer questions (d) and (e) for those technologies your agency has not used. Please note that you will either be filling out columns A through C OR D through E for each type of technology.

	Technology your agency currently has:			Technology your agency has not used:	
	(a) Condition of most of your technology?[1] 1=obsolete 2=old, but serviceable 3=up to date 9=don't know	(b) Effectiveness of most of your technology?[2] 1=not effective 2=moderately effective 3=very effective 9=don't know	(c) Implementation challenges (mark all that apply)?[3] 1=doesn't work as expected 2=difficult to use 3=need training 4=economic or political liabilities 5=no challenges	(d) Would it address significant operational needs?[4] 1=fully 2=moderately 3=slightly 4=not at all	(e) Likely to acquire this technology in the next 3-5 years?[5] 1=very likely 2=somewhat likely 3=not likely
Identification					
DNA testing equipment	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Ballistics imaging	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Fingerprint readers	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Other biometric technology (e.g., facial, iris, or voice recognition technology)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Drug testing technology	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Cyber forensics equipment	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Mobile laboratory	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐

↳ **Question 12 CONTINUED on top of next page...**

[1] How would you characterize the condition of most of your agency's technology?

[2] How effective is most of your technology in achieving the purposes for which it was acquired?

[3] What have been the key challenges to implementing the technology in your agency?

[4] To what extent would this technology address a significant operational need(s) of your agency?

[5] If not prohibitively expensive, how likely would your agency be to acquire this technology?

POLICE EXECUTIVE RESEARCH FORUM

Technology Needs Assessment

ID NUMBER

↳ Question 12 CONTINUED from previous page...

	Technology your agency currently has:			Technology your agency has not used:	
	(a) Condition of most of your technology? 1=obsolete 2=old, but serviceable 3=up to date 9=don't know	(b) Effectiveness of most of your technology? 1=not effective 2=moderately effective 3=very effective 9=don't know	(c) Implementation challenges (mark all that apply)? 1=doesn't work as expected 2=difficult to use 3=need more training 4=economic or political liabilities 5=no challenges	(d) Would it address significant operational needs? 1=fully 2=moderately 3=slightly 4=not at all	(e) Likely to acquire this technology in the next 3-5 years? 1=very likely 2=somewhat likely 3=not likely
Sensors and Surveillance					
Video surveillance network	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
License plate readers	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Patrol car cameras	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Gunshot detection devices (e.g., ShotSpotter)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Electronic listening devices	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Electronic interception	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Portable devices for detecting concealed weapons	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Drug detection devices	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
"See through the wall" technology (ultra wide band)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Night vision devices	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Aerial surveillance equipment (e.g., drones)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
GPS devices for tracking suspects	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐

↳ Question 12 CONTINUED on top of next page...

POLICE EXECUTIVE RESEARCH FORUM

Technology Needs Assessment

ID NUMBER

↳ Question 12 CONTINUED from previous page...

	Technology your agency currently has:			Technology your agency has not used:	
	(a) Condition of most of your technology? 1=obsolete 2=old, but serviceable 3=up to date 9=don't know	(b) Effectiveness of most of you technology? 1=not effective 2=moderately effective 3=very effective 9=don't know	(c) Implementation challenges (mark all that apply)? 1=doesn't work as expected 2=difficult to use 3=need more training 4=economic or political liabilities 5=no challenges	(d) Would it address significant operational needs? 1=fully 2=moderately 3=slightly 4=not at all	(e) Likely to acquire this technology in the next 3-5 years? 1=very likely 2=somewhat likely 3=not likely
Crime Analysis/Mapping					
Geographic Information Systems (GIS) software	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Real-time crime monitoring center	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Predictive modeling	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Investigative software (e.g., data mining software)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Software for risk factor analyses for victimization	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Training					
Use of force computer simulators	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Driving simulators	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Other computer-based training and simulators	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Digital forensic training	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Records Management/Data Sharing					
Integrated databases (e.g., COPLINK, regional data sharing, etc.)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Wireless access in patrol cars	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Community notification via Internet, text messaging	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐

↳ Question 12 CONTINUED on top of next page...

POLICE EXECUTIVE RESEARCH FORUM

Technology Needs Assessment

ID NUMBER

↳ Question 12 CONTINUED from previous page...

	Technology your agency currently has:			Technology your agency has not used:	
	(a) Condition of most of your technology? 1=obsolete 2=old, but serviceable 3=up to date 9=don't know	(b) Effectiveness of most of your technology? 1=not effective 2=moderately effective 3=very effective 9=don't know	(c) Implementation challenges (mark all that apply)? 1=doesn't work as expected 2=difficult to use 3=need more training 4=economic or political liabilities 5=no challenges	(d) Would it address significant operational needs? 1=fully 2=moderately 3=slightly 4=not at all	(e) Likely to acquire this technology in the next 3-5 years? 1=very likely 2=somewhat likely 3=not likely
Communications/Dispatch/ Interoperability					
Computer-aided dispatch with GPS dispatching and tracking of patrol cars	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
700/800 MHz trunked communications system	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Inter-agency radios	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Language translators	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Next generation 911 (text and voice messaging)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Weapons and Equipment/Robotics/ Tactical					
Fully integrated vehicle system (voice activated)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Personal video/audio equipment (worn by officer)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Body armor	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Pistol cam	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
LED vision incapacitation device	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Directed energy vehicle stopper	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐

↳ Question 12 CONTINUED on top of next page...

POLICE EXECUTIVE RESEARCH FORUM

Technology Needs Assessment

ID NUMBER

↳ **Question 12 CONTINUED from previous page...**

	Technology your agency currently has:			Technology your agency has not used:	
	(a) Condition of most of your technology? 1=obsolete 2=old, but serviceable 3=up to date 9=don't know	(b) Effectiveness of most of your technology? 1=not effective 2=moderately effective 3=very effective 9=don't know	(c) Implementation challenges (mark all that apply)? 1=doesn't work as expected 2=difficult to use 3=need more training 4=economic or political liabilities 5=no challenges	(d) Would it address significant operational needs? 1=fully 2=moderately 3=slightly 4=not at all	(e) Likely to acquire this technology in the next 3-5 years? 1=very likely 2=somewhat likely 3=not likely
Weapons and Equipment/Robotics/ Tactical (cont'd.)					
Sound wave incapacitation weapon	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Conducted Energy Devices (e.g., Taser or Stinger) and other non-lethal weapons	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Long range broadcasting device	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Sensors for explosives	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Sensors for biological/ chemical/nuclear materials	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Protective clothing/gear	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Robots for bomb disposal and tactical operations	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Mobile command center	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Special purpose vehicles (e.g., armored vehicles, ATVs)	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Night vision equipment	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Other technologies					
Other (please specify):	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐
Other (please specify):	☐	☐	○ ○ ○ ○ ○ 1 2 3 4 5	☐	☐

13. **Describe in general terms the technologies, either mentioned previously or not, that your agency would like to see developed for law enforcement applications.**

14. **Describe any plans your agency has for acquiring new or emerging technology or updating existing technology.**

15. **Describe any significant barriers that your agency may face over the next 3 to 5 years in acquiring technology.**

POLICE EXECUTIVE RESEARCH FORUM

Technology Needs Assessment

ID NUMBER

Thank you for taking the time to participate in this survey!

Please direct any questions or comments to Bruce Kubu (bkubu@policeforum.org or 202-454-8308).

Please provide the information requested below. We will use this information only for purposes of calling to clarify information.

TITLE

LAST NAME

FIRST NAME

AGENCY

UNIT

EMAIL ADDRESS

TELEPHONE ( ) - EXT.

Appendix C

Survey Technology Term Definitions – Survey Item 12[45]

Identification

1. DNA testing equipment: Any piece of equipment that tests for the presence of DNA and also equipment that specifically identifies a person's DNA. This can include presumptive testing at a crime scene or technology used in a lab to further refine the owner of specific DNA found at a crime scene.

2. Ballistics imaging: This equipment allows investigators to capture a digital image of the markings made by a firearm on bullets and cartridge casings. These images can then be entered into a database for side-by-side comparisons which are then examined more closely by a human ballistics expert.

3. Fingerprint readers: Electronic scanners used to digitally read the fingerprints of an individual. The latest technology comes in handheld devices for use by officers on the street without having to get to a lab or a police station.

4. Other biometric technology (e.g., facial, iris or voice recognition technology): Scanners and devices that can recognize individuals by anatomical, biological or behavioral characteristics.

5. Drug testing technology: Devices used to test for the presence of drugs in suspects.

6. Cyber forensics equipment: Devices that allow law enforcement officers to analyze hard drives, cell phones, digital cameras and other electronics in order to sometimes determine the location of a subject or whether or not a crime using the equipment had been committed.

7. Mobile laboratory: A mobile laboratory that allows officers to conduct various tests on scene. Some common tests would include fingerprint scanning, presumptive DNA tests and tests for the presence of drugs.

Sensors and Surveillance

8. Video surveillance network: An integrated system of surveillance cameras placed at strategic locations in order to capture suspects and crimes. This technology can also be used in court as evidence.

[45] The authors thank Tara Black for research assistance in compiling these definitions.

9. License plate readers: An infrared camera attached to the top of police cars. The cameras scan and read the license plates of nearby cars and then run them through a statewide database to determine if the car has been reported.

10. Patrol car cameras: Cameras attached to a patrol car that captures officer and subject interactions. These cameras are most utilized during traffic stops.

11. Gunshot detection devices (e.g., ShotSpotter®): A system that can triangulate the position of gunfire, map it and relay the information to police dispatchers.

12. Electronic listening devices: A wireless device that can listen, record and store voices used in aiding officers to determine perpetrators of a crime. These devices can be used in public as well as private places provided the right steps have been taken to get permission for their use.

13. Electronic interception: Devices or equipment for interception of electronic communications, including phone and email communications.

14. Portable devices for detecting concealed weapons: Handheld devices used to detect the presence of a weapon on a person. Some technology uses radar in its detection while other technology uses the ultrasound in its detection of concealed weapons.

15. Drug detection devices: Devices used to test for the presence of drugs on suspects or in suspect's property. This technology can be used to test a substance to verify it as an illegal substance.

16. "See through the wall" technology (ultra wide band): A UWB is a signal sent by a stationary sensor through walls that allows officers to see into a building or barricaded area in order to determine the best method of entry into a hostage or barricaded situation. This technology can also be used to determine if a building is occupied.

17. Night vision devices: Portable devices (generally goggles) that allow officers to see at night as if it were daytime.

18. Aerial surveillance equipment (e.g., Unmanned Aerial Vehicle/Unmanned Aircraft System): An unmanned, remote-controlled surveillance aircraft. The UAS could be used to give officers a birds-eye view of a dangerous situation (barricaded suspect) or to cover a large area in a short amount of time in search of individuals.

19. GPS devices for tracking suspects: Officers may use the GPS systems already in place in cell phones to track suspects. Some police departments use GPS chips to track known offenders and use that information to correlate their whereabouts to known acts of crime.

Crime Analysis/Mapping

20. Geographic Information Systems (GIS) software: A computerized crime mapping software that collects and analyzes crime data. This analysis allows officers to focus in on particularly high crime areas and seek out possible preventative measures.

21. Real-time crime monitoring center: A technology center housing various databases of information (e.g., a catalogue of perpetrator tattoos and their meanings) available to officers in real-time. These centers also use satellite imaging and computerized mapping systems to identify geographic patterns of crimes.

22. Predictive modeling: A system that analyzes available crime data and then predicts where future crimes may occur enabling officers to focus on higher crime areas.

23. Investigative software (e.g., data mining software): A system that sifts through several pieces of data and recognizes patterns. Police use it to predict the outcomes and occurrences of future crimes.

24. Software for risk factor analyses for victimization: Intelligent software for identifying people and businesses at risk for victimization based on previous victimization and other risk factors.

Training

25. Use of force computer simulators: Devices intended to simulate encounters with citizens during which use of force is required in order to give the officers experience with such citizen encounters.

26. Driving simulators: Devices intended to simulate driving in a police vehicle during a routine shift. Simulators are intended to acquaint the officer with possible situations he or she may encounter while in their cruiser.

27. Other computer-based training and simulators: These could include simulators for activities other than use of force or driving (for example, personal interaction) and other forms of training (like instructional materials and tests) that are delivered by computer.

28. Digital forensic training: Training provided to officers in order to help them recognize, investigate and document crimes committed using electronic or digital devices and to collect evidence from computers and other digital devices.

Records Management/Data Sharing

29. Integrated databases (e.g., COPLINK®, regional data sharing, etc.): Software that allows police to search for large amounts of crime data in both their records and those of other law enforcement agencies.

30. Wireless access in patrol cars: Allows officers to access various databases and surveillance cameras while on patrol in their vehicles. Allows for real-time surveillance of possible criminal activity.

31. Community notification via Internet, text messaging: A system that allows officers to communicate with a large number of community members via the internet and text messaging. Officers can use this technology to alert citizens to possible suspects on the loose or to make general announcements concerning public safety.

Communications/Dispatch/Interoperability

32. Computer-aided dispatch with GPS dispatching and tracking of patrol cars: A dispatch system that allows dispatchers to view an officer's location or progress to the scene on a map of the area due to GPS systems in patrol cars.

33. 700/800 MHz trunked communication system: An integrated system that allows expanded coverage and a common infrastructure on which public safety agencies can communicate.

34. Inter-agency radios: Communication devices that allow agencies to talk with one another and share information regarding suspects, crimes and trends.

35. Language translators: Handheld devices that allow officers on patrol to speak with subjects whose first language is not English.

36. Next Generation 911 (text and voice messaging): National 911 system whose goals include being able to take 911 calls via text message, compatibility with Voice over Internet Protocol services, being able to receive data from OnStar® systems.

Weapons and Equipment/Robotics/Tactical

37. Fully integrated vehicle system (voice activated): A fully integrated system in a patrol vehicle that works with manufacturers' equipment and can be activated by voice commands, touch screen, keyboard, etc., enabling the officer to not to have to manually turn electronics on/off.

38. Personal video/audio equipment (worn by officer): Device that is clipped to the officer's shoulder that can record audio and video and take still photographs.

39. Body armor: Vests and other protective clothing worn by officers to prevent or lessen injuries relating to gunshots.

40. Pistol cam: A 1.5 ounce camera placed below the barrel of a police officer's firearm. This camera begins recording both video and audio once the officer has drawn his or her gun.

41. LED vision incapacitation device: A device that flashes LED lights at multiple frequencies. These frequencies cause 'flash blindness' and disorients a suspect.

42. Directed energy vehicle stopper: A device that emits microwaves or electromagnetic pulses resulting in the disruption of a vehicles electronic components thereby stopping the intended vehicle.

43. Sound wave incapacitation weapon: A non-lethal weapon that uses microwaves or sonic waves in order to cause pain or minor discomfort in order to regain control of a large crowd or subject.

44. Conducted Energy Devices (e.g., Taser® or Stinger®) and other non-lethal weapons: Portable, hand-held devices used to stun or temporarily paralyze a subject in order for the officer to gain control over a non-compliant individual. These devices are generally non-lethal.

45. Long range broadcasting device: A device that can be used to amplify an officer's orders over a greater distance or force someone who has barricaded themselves in a location to come out.

46. Sensors for explosives: Devices used to detect the presence of elements found or used in the creation of explosive devices.

47. Sensors for biological/chemical/nuclear materials: A device that can be mounted on police vehicles or bicycles that can alert officers to the presence of a 'dirty bomb'.

48. Protective gear/clothing: Apparel designed specifically for police officers in order to protect them from shrapnel, bullets or any other dangerous projectile or weapon.

49. Robots for bomb disposal and tactical operations: Unmanned robots controlled from a distance by bomb specialists in order to safely dismantle a bomb.

50. Mobile command center: A vehicle equipped with items required to respond to an emergency situation. These vehicles generally have a communications component that allows the agency to communicate with other agencies.

51. Special purpose vehicles (e.g., armored vehicles, ATVs): Vehicles with designed for a specific task in mind. These vehicles are outfitted with the latest appropriate technology required for the job.

52. Night vision equipment: Portable devices (generally goggles) that allow officers to see at night as if it were daytime.

Appendix D

Responding agencies (PERF Survey)

Fort Smith (AR) Police Department
North Little Rock Police Department
Douglas Police Department
Gilbert Police Department
Glendale Police Department
Mesa Police Department
Oro Valley Police Department
Peoria (Arizona) Police Department
Alameda County Sheriff's Office
Bakersfield Police Department
California Highway Patrol
Chula Vista Police Department
Escondido Police Department
Fremont Police Department
Garden Grove Police Department
Huntington Beach Police Dept.
Indio Police Department
Inglewood Police Department
Irvine Police Department
Long Beach Police Department
Los Angeles Co Sheriff's Dept.
Los Angeles Police Department
Modesto Police Department
Mountain View Police Department
National City Police Department
Novato Police Department
Oakland Police Department
Palm Springs Police Department
Palo Alto Police Department
Pasadena Police Department
Pleasanton Police Department
Pomona Police Department
Redlands Police Department
Redwood City Police Department
Richmond Police Department
Rio Vista Police Department
Riverside Police Department
Sacramento Police Department
San Diego Police Department
San Francisco Police Department
San Jose Police Department
San Mateo Police Department
Tracy Police Department
University of CA-San Francisco Police Dept.
Ventura Police Department
West Covina Police Department
Arvada Police Department
Aurora (CO) Police Department
Boulder Police Department
Colorado Springs Police Department
Denver Police Department
Fort Collins Police Department
Danbury Police Department
Glastonbury Police Department
Manchester Police Department
Milford Police Department
New Haven Police Department
Stamford Police Department
Yale University Police Department
New Castle Co Government
Boca Raton Police Department
Cape Coral Police Department
Citrus County Sheriff's Office
Clearwater Police Department
Coral Springs Police Department
Daytona Beach Police Department
Delray Beach Police Department
FL Department of Corrections
Ft. Pierce Police Department
Gainesville Police Department
Hallandale Police Department
Jupiter Police Department
Lakeland Police Department
Lauderhill Police Department
Martin Co Sheriff's Department
Miami Police Department
North Miami Beach Police Dept.
North Port Police Department
Orange County Sheriff's Office
Palm Bay Police Department
Palm Beach Police Department
Pinellas County Sheriff's Dept.
Polk County Sheriff's Office
Sarasota Police Department
St. Johns County Sheriff's Office
Titus Police Department
Alpharetta Police Department
Athens-Clarke County Police Department

Atlanta Police Department
Dalton Police Department
Savannah Police Department
Honolulu Police Department
Davenport Police Department
West Des Moines Police Department
Addison Police Department
Arlington Heights Police Dept.
Elgin Police Department
Evanston School District Dept of Public Safety
Glenview Police Department
Illinois State Police
Naperville Police Department
Oak Park Police Department
Schaumburg Police Department
University of Illinois at Chicago
Waukegan Police Department
Fort Wayne Police Department
Indianapolis Police Department
Lenexa Police Department
Topeka Police Department
Wichita Police Department
Louisville Metro Police Department
Brookline Police Department
Cambridge (MA) Police Department
Fitchburg Police Department
Framingham Police Department
Haverhill Police Department
Lawrence (MA) Police Department
Lowell Police Department
Lynn Police Department
MIT Police Department
New Bedford Police Department
Peabody Police Department
Worcester Police Department
Baltimore County Police Department
Baltimore County Sheriff's Office
Frederick Police Department
Gaithersburg Police Department
Howard County Department of Police
Montgomery County Police Department
Takoma Park Police Department
Grand Rapids Police Department
Kalamazoo Public Safety
Lansing Police Department
Michigan State University Police
Oakland Co Sheriff's Department
Wyoming Police Department
Brooklyn Center Police Department
Duluth Police Department
Hennepin Co Sheriff's Office
Minneapolis Police Department
Minnetonka Police Department
Jefferson City Police Department
Kansas City Police Department
Lee's Summit (MO) Police Department
Springfield Police Department
St. Louis Co Police Department
St. Louis Metropolitan Police Department
Durham Police Department
Fayetteville Police Department
Greenville Police Department
Jacksonville (NC) Police Department
New Bern Police Department
Wilmington Police Department
Winston-Salem Police Department
Fargo Police Department
Grand Forks Police Department
Lincoln Police Department
Essex County Sheriff's Department
New Jersey State Police
Newark Police Department
Trenton Police Department
West Orange Police Department
Albuquerque Police Department
Las Vegas Metropolitan Police Department
Reno Police Department
University of Nevada - Las Vegas
Cheektowaga Police Department
Nassau County Police Department
New Rochelle Police Department
Rochester Police Department
Suffolk County Police Department
White Plains Police Department
Yonkers Police Department
Hamilton Police Department
Kettering Police Department
Springboro Police Department
Tulsa Police Department
Eugene Police Department
Portland Police Bureau
Lancaster Bureau of Police
Philadelphia Police Department
York City Police Department
Charleston County Sheriff's Office
Greenville City Police Department
North Charleston Police Department
Franklin Police Department
Nashville Metro Police Dept.
Arlington Police Department

Austin Police Department
Bryan Police Department
Dallas Police Department
Farmers Branch Police Dept
Garland Police Department
North Richland Hills Police Dept.
San Antonio Police Department
San Marcos Police Department
Sugar Land Police Department
Albemarle County Police Dept.
Arlington County Police Department
Fairfax County Police Department
Henrico Co Division of Police
Newport News Police Department
Norfolk Police Department
Prince William Co Police Dept.
Virginia Beach Police Department
Pierce County Sheriff's Department
Seattle Police Department
Vancouver Police
Washington State Patrol
Appleton Police Department
Green Bay Police Department
La Crosse Police Department
Port Washington Police Department
University of WI-Madison Police Department
Waukesha Police Department
Waco Police Department

Appendix E

Table E - 1

Operational areas that will have high priority needs for additional resources in the next 3-5 years (%)

Operational Area	Strongly agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Strongly disagree	Average (1-5)
Patrol officer response to calls for service	73.6	20.4	5.1	0.5	0.5	1.34
Freeing officer time for proactive strategies	69.9	27.3	1.9	0.9	0	1.34
Prevention and investigation of street crime	69	26.9	2.8	1.4	0	1.37
Prevention and investigation of organized crime	19.4	42.1	26.4	8.3	3.7	2.35
Prevention and investigation of homeland security threats and terrorism	23.1	40.7	22.7	11.1	2.3	2.29
Prevention and investigation of electronic/cybercrime	55.6	35.2	6.9	1.9	0.5	1.56
Crime analysis and information led policing	70.4	23.1	6	0.5	0	1.37
Training	55.1	38.4	6	0.5	0	1.52
Hiring and retention	54.6	35.6	8.8	0.5	0.5	1.56
Officer oversight, supervision and accountability	45.6	44.7	9.3	0.5	0	1.65
Information technology (e.g., database integration and data sharing within and across agencies)	70.8	25.9	3.2	0	0	1.32
Communications and dispatch	41.1	40.2	16.4	1.4	0.9	1.81
Coordination and interoperability with other first responders	46.3	40.7	10.6	2.3	0	1.69
Weapons and equipment	30.2	46	20.9	2.3	0.5	1.97
Security for police information systems	38.3	40.7	18.2	2.8	0	1.86
Crowd and riot control	7.5	42.5	35.5	10.3	4.2	2.61
Tactical operations (e.g., hostage situations)	15.7	48.1	29.6	6	0.5	2.27
Handling explosives	9.7	35.6	33.3	14.8	6.5	2.73
Collection and processing of crime scene evidence	47.2	42.6	9.3	0.9	0	1.64
Pursuit management (e.g., foot and vehicle pursuits)	21.3	41.2	28.7	8.3	0.5	2.25

Table E - 2

Condition of Current Technology

Type of Technology	Percentage using technology	For Users, what is the condition of the technology (%) Obsolete	Old, but serviceable	Up to date	Don't know
Identification					
DNA Testing Equipment	24.3	2	14	68	16
Ballistics imaging	25.6	7.3	12.7	67.3	12.7
Fingerprint readers	57.6	2.5	13.2	80.2	4.1
Other biometric technology	10.9	8.3	16.7	50	25
Drug testing technology	49.3	1	25.2	67	6.8
Cyber forensics equipment	53.1	3.6	16.4	74.5	5.5
Mobile laboratory	18.2	7.9	13.2	65.8	13.2
Sensors and Surveillance					
Video surveillance network	60.5	7.9	29.4	61.1	1.6
License plate readers	38.1	1.3	3.8	93.7	1.3
Patrol car cameras	64.4	6.8	24.2	67.4	1.5
Gunshot detection devices	12.3	12	16	56	16
Electronic listening devices	48.1	2	35	57	6
Electronic interception	20.9	4.5	15.9	56.8	22.7
Portable devices for detecting concealed weapons	23	2.1	50	41.7	6.3
Drug detection devices	20.6	0	31	47.6	21.4
See through the wall technology (ultra wide band)	9.2	0	31.6	31.6	36.8
Night vision devices	84.1	5.7	42.5	48.9	2.9
Aerial surveillance equipment	12.8	3.7	29.6	48.1	18.5
GPS devices for tracking suspects	64	1.5	20.9	75.4	2.2

Type of Technology	Percentage using technology	For Users, what is the condition of the technology (%) Obsolete	Old, but serviceable	Up to date	Don't know
Crime Analysis/Mapping					
Geographic Information Systems (GIS) software	84.7	4	15.3	79.5	1.1
Real-time crime monitoring center	19.5	7.1	11.9	69	11.9
Predictive modeling	31.3	4.5	21.2	62.1	12.1
Investigative software (e.g., data mining software	45.5	4.2	16.8	77.9	1.1
Software for risk factor analyses for victimization	13.7	0	13.8	51.7	34.5
Training					
Use of force computer simulators	52.2	9.3	30.6	57.4	2.8
Driving simulators	21.5	11.4	18.2	56.8	13.6
Other computer-based training and simulators	22.4	6.7	17.8	60	15.6
Digital forensic training	26	1.9	16.7	66.7	14.8
Records Management/Data Sharing					
Integrated databases (e.g., COPLINK®, regional data sharing, etc.)	61.1	2.4	18.9	76.4	2.4
Wireless access in patrol cars:	84.2	1.1	12.6	86.3	0
Community notification via Internet, text messaging	65.2	0.7	18.7	78.4	2.2
Communications/Dis-patch/Interoperability					
Computer-aided dispatch with GPS dispatching and tracking of patrol cars	55.2	2.6	17.2	78.4	1.7
700/800 MHz trunked communication system:	72.8	2.7	24	70.7	2.7
Inter-agency radios	79.4	3	24.7	69.3	3
Language translators	39.6	1.2	20.5	61.4	16.9
Next Generation 911 (text a0 voice messaging	21.3	4.3	4.3	59.6	31.9

Type of Technology	Percentage using technology	For Users, what is the condition of the technology (%) Obsolete	Old, but serviceable	Up to date	Don't know
Weapons and Equipment/Robotics/Tactical					
Fully integrated vehicle system (voice activated)	6.2	25	0	41.7	33.3
Personal video/audio equipment (worn by officer)	26.3	3.6	32.7	58.2	5.5
Body armor	97.7	0	4.3	94.7	1
Pistol cam	3.3	50	0	0	50
LED vision incapacitation device	5.7	10	10	50	30
Directed energy vehicle stopper	3.3	14.3	0	28.6	57.1
Sound wave incapacitation weapon	3.3	12.5	0	37.5	50
Co0ucted Energy Devices (e.g., Taser® or Stinger®)	82.4	0	4	95.4	0.6
Long range broadcasting device	18.7	5.1	35.9	48.7	10.3
Sensors for explosives	13.9	3.4	6.9	65.5	24.1
Sensors for biological/chemical/nuclear materials	27.3	1.7	17.2	70.7	10.3
Protective gear/clothing	79.4	0.6	22.3	75.3	1.8
Robots for bomb disposal and tactical operations	41.6	5.7	11.5	78.2	4.6
Mobile command center	81	10.1	24.9	64.5	0.6
Special purpose vehicles (e.g., armored vehicles, ATVs)	70	6.8	29.5	63	0.7

Table E - 3

Effectiveness of Current Technology Used

Type of Technology	Percentage using technology	For users, what is the effectiveness of the technology (%) Not effective	Moderately Effective	Very effective	Don't know
Identification					
DNA Testing Equipment	24.3	2	19.6	68.6	9.8
Ballistics imaging	25.6	7.3	20	61.8	10.9
Fingerprint readers	57.6	3.3	15	77.5	4.2
Other biometric technology	10.9	16.7	20.8	45.8	16.7
Drug testing technology	49.3	1	24.5	68.6	5.9
Cyber forensics equipment	53.1	1.8	36.7	58.7	2.8
Mobile laboratory	18.2	5.3	21.1	63.2	10.5
Sensors and Surveillance					
Video surveillance network	60.5	7.1	47.6	38.9	6.3
License plate readers	38.1	3.8	28.8	62.5	5
Patrol car cameras	64.4	6.8	30.1	60.2	3
Gunshot detection devices	12.3	19.2	38.5	19.2	23.1
Electronic listening devices	48.1	2	42.6	49.5	5.9
Electronic interception	20.9	2.3	20.9	58.1	18.6
Portable devices for detecting concealed weapons	23	4.3	48.9	40.4	6.4
Drug detection devices	20.6	0	42.9	33.3	23.8
See through the wall technology (ultra wide band)	9.2	5.6	50	11.1	33.3
Night vision devices	84.1	5.2	45.7	45.1	4
Aerial surveillance equipment	12.8	3.8	26.9	53.8	15.4
GPS devices for tracking suspects	64	1.5	26.7	69.6	2.2
Crime Analysis/Mapping					
Geographic Information Systems (GIS) software	84.7	4	31.6	63.3	1.1
Real-time crime monitoring center	19.5	7.1	21.4	59.5	11.9
Predictive modeling	31.3	7.6	48.5	30.3	13.6
Investigative software (e.g., data mining software)	45.5	7.4	37.9	50.5	4.2
Software for risk factor analyses for victimization	13.7	3.6	35.7	28.6	32.1

Type of Technology	Percentage using technology	For Users, what is the effectiveness of the technology (%) Not effective	Moderately Effective	Very effective	Don't know
Training					
Use of force computer simulators	52.2	4.6	31.2	58.7	5.5
Driving simulators	21.5	6.7	31.1	46.7	15.6
Other computer-based training and simulators	22.4	4.4	35.6	46.7	13.3
Digital forensic training	26	1.9	20.8	62.3	15.1
Records Management/Data Sharing					
Integrated databases (e.g., COPLINK®, regional data sharing, etc.)	61.1	2.4	39.4	55.1	3.1
Wireless access in patrol cars:	84.2	2.3	24.4	73.3	0
Community notification via Internet, text messaging	65.2	2.2	37.8	54.1	5.9
Communications/Dispatch/Interoperability					
Computer-aided dispatch with GPS dispatching and tracking of patrol cars	55.2	5.1	32.5	55.6	6.8
700/800 MHz trunked communication system	72.8	0	24.5	72.8	2.6
Inter-agency radios	79.4	3	34.1	59.9	3
Language translators	39.6	3.7	30.5	48.8	17.1
Next Generation 911 (text and voice messaging)	21.3	4.3	14.9	51.1	29.8
Weapons and Equipment/Robotics/Tactical					
Fully integrated vehicle system (voice activated)	6.2	27.3	27.3	27.3	18.2
Personal video/audio equipment (worn by officer)	26.3	1.9	38.9	57.4	1.9
Body armor	97.7	0	6.3	89.4	4.3
Pistol cam	3.3	40	20	0	40
LED vision incapacitation device	5.7	0	20	40	40
Directed energy vehicle stopper	3.3	20	0	20	60
Sound wave incapacitation weapon	3.3	14.3	14.3	28.6	42.9

Type of Technology	Percentage using technology	For Users, what is the effectiveness of the technology (%) Not effective	Moderately Effective	Very effective	Don't know
Weapons and Equipment/Robotics/Tactical (Continued)					
Conducted Energy Devices (e.g., Taser® or Stinger®)	82.4	0	5.8	92.5	1.7
Long range broadcasting device	18.7	0	52.6	39.5	7.9
Sensors for explosives	13.9	7.1	17.9	53.6	21.4
Sensors for biological/chemical/nuclear materials	27.3	7	22.8	47.4	22.8
Protective gear/clothing	79.4	1.2	26.5	61.4	10.8
Robots for bomb disposal and tactical operations	41.6	3.4	17.2	74.7	4.6
Mobile command center	81	5.9	30.6	63.5	0
Special purpose vehicles (e.g., armored vehicles, ATVs)	70	6.8	27.9	64.6	.7

Table E - 4

Implementation of Technology

Type of Technology	Percentage using technology	For Users, what are the implementation challenges of the technology (%) Doesn't work as expected	Difficult to use	Need training	Economic or political challenges	No challenges
Identification						
DNA Testing Equipment	24.3	0	3.8	5.8	34.6	48.1
Ballistics imaging	25.6	3.6	5.5	10.9	23.6	45.5
Fingerprint readers	57.6	3.3	4.1	14.9	15.7	60.3
Other biometric technology	10.9	4.2	16.7	20.8	16.7	45.8
Drug testing technology	49.3	0	2.9	5.8	18.4	68
Cyber forensics equipment	53.1	0	2.7	30	21.8	41.8
Mobile laboratory	18.2	0	2.6	5.3	21.1	63.2
Sensors and Surveillance						
Video surveillance network	60.5	7.9	12.6	9.4	37.8	37.8
License plate readers	38.1	11.3	5	15	18.8	57.5
Patrol car cameras	64.4	11.2	9.7	11.2	24.6	45.2
Gunshot detection devices	12.3	15.4	0	0	34.6	42.3
Electronic listening devices	48.1	7.9	8.9	6.9	26.7	46.5
Electronic interception	20.9	2.3	6.8	11.4	20.5	36.4
Portable devices for detecting concealed weapons	23	60	33.3	66.7	80	93.8
Drug detection devices	20.6	8.9	2.2	17.8	8.9	45.7
See through the wall technology (ultra wide band)	9.2	15	5	5	15	30
Night vision devices	84.1	7.4	8	9.7	16	55.1
Aerial surveillance equipment	12.8	0	7.4	11.1	44.4	25.9
GPS devices for tracking suspects	64	4.4	5.2	10.4	17	57
Crime Analysis/Mapping						
Geographic Information Systems (GIS) software	84.7	4	11.3	26.6	14.7	46.3
Real-time crime monitoring center	19.5	7.1	4.8	21.4	25.6	42.9
Predictive modeling	31.3	7.6	13.6	23.9	10.6	42.4
Investigative software (e.g., data mining software)	45.5	80	94.4	95	94.1	97.3
Software for risk factor analyses for victimization	13.7	0	3.4	20.7	17.2	41.4

Type of Technology	Percentage using technology	For Users, what are the implementation challenges of the technology (%) Doesn't work as expected	Difficult to use	Need training	Economic or political challenges	No challenges
Training						
Use of force computer simulators	52.2	3.7	6.4	14.7	22	53.2
Driving simulators	21.5	0	6.7	11.1	28.9	44.4
Other computer-based training and simulators	22.4	2.2	2.2	8.7	21.7	47.8
Digital forensic training	26	33.3	60	87.5	88.9	90
Records Management/Data Sharing						
Integrated databases (e.g., COPLINK®, regional data sharing, etc.)	61.1	7.9	9.4	22	32.3	44.1
Wireless access in patrol cars:	84.2	9.1	5.1	10.8	27.3	55.1
Community notification via Internet, text messaging	65.2	1.5	3.7	11.1	20	60.7
Communications/Dispatch/Interoperability						
Computer-aided dispatch with GPS dispatching and tracking of patrol cars	55.2	8.5	8.5	17.1	22.2	49.6
700/800 MHz trunked communication system:	72.8	6	0.7	4.6	26.3	57.6
Inter-agency radios	79.4	5.4	4.8	12.6	30.5	43.1
Language translators	39.6	3.6	13.3	16.9	9.6	43.4
Next Generation 911 (text and voice messaging)	21.3	2.1	2.1	10.4	16.7	41.7
Weapons and Equipment/Robotics/Tactical						
Fully integrated vehicle system (voice activated)	6.2	23.1	0	7.7	15.4	15.4
Personal video/audio equipment (worn by officer)	26.3	3.6	5.4	7.1	23.2	48.2
Body armor	97.7	0.5	1.4	1	10.1	78.4
Pistol cam	3.3	14.3	0	0	14.3	0
LED vision incapacitation device	5.7	0	0	8.3	16.7	33.3
Directed energy vehicle stopper	3.3	0	0	0	28.6	28.6
Sound wave incapacitation weapon	3.3	0	0	12.5	25	25
Conducted Energy Devices (e.g., Taser® or Stinger®)	82.4	0.6	1.2	9.2	27.7	57.8

		For Users, what are the implementation challenges of the technology (%)				
Type of Technology	Percentage using technology	Doesn't work as expected	Difficult to use	Need training	Economic or political challenges	No challenges
Long range broadcasting device	18.7	2.6	10.3	5.1	12.8	59
Sensors for explosives	13.9	6.9	0	13.8	10.3	48.3
Sensors for biological/chemical/nuclear materials	27.3	3.4	5.2	19	17.2	44.8
Protective gear/clothing	79.4	0	7.8	14.5	23.5	53.3
Robots for bomb disposal and tactical operations	41.6	4.6	2.3	10.3	18.4	60.9
Mobile command center	81	3.5	2.9	8.2	25.3	57.6
Special purpose vehicles (e.g., armored vehicles, ATVs)	70	1.4	2.7	6.8	29.3	55.1

Table E - 5

Technology Addressing Operational Needs

A. Type of Technology	Percent that don't use technology	For agencies not using technology, would it address significant operational needs (%) Fully	Moderately	Slightly	Not at all
Identification					
DNA Testing Equipment	75.7	28.7	24.2	19.1	28
Ballistics imaging	74.4	16.1	20.6	32.3	31
Fingerprint readers	42.4	37.9	31	9.2	21.8
Other biometric technology	89.1	14.1	29.2	27	29.7
Drug testing technology	50.7	22.1	32.7	17.3	27.9
Cyber forensics equipment	46.9	31.3	34.4	11.5	22.9
Mobile laboratory	81.8	15.4	26.6	24.3	33.7
Sensors and Surveillance					
Video surveillance network	39.5	34.9	37.3	13.3	14.5
License plate readers	61.9	28.7	41.9	17.8	11.6
Patrol car cameras	35.6	24.3	45.9	21.6	8.1
Gunshot detection devices	87.7	12.1	24.2	34.6	29.1
Electronic listening devices	51.9	8.3	26.9	37	27.8
Electronic interception	79.1	10.3	29.7	34.5	25.5
Portable devices for detecting concealed weapons	77	20.1	37.1	23.9	18.9
Drug detection devices	79.4	21.8	38.2	27.3	12.7
See through the wall technology (ultra wide band)	90.8	19.9	30.6	29.6	19.9
Night vision devices	15.9	27.3	54.5	12.1	6.1
Aerial surveillance equipment	87.2	13.3	28.2	28.7	29.8
GPS devices for tracking suspects	36	35.1	33.8	20.3	10.8
Crime Analysis/Mapping					
Geographic Information Systems (GIS) software	15.3	31.3	34.4	15.6	18.8
Real-time crime monitoring center	80.5	30.5	37.1	18	13.8
Predictive modeling	68.8	27	41.8	19.1	11.3
Investigative software (e.g., data mining software)	54.5	34.5	43.4	17.7	4.4
Software for risk factor analyses for victimization	86.3	17.3	34.6	35.2	12.8
Training					
Use of force computer simulators	47.8	32	41	16	11
Driving simulators	78.5	23.3	44.8	17.2	14.7

A. Type of Technology	Percent that don't use technology	For agencies not using technology, would it address significant operational needs (%) Fully	Moderately	Slightly	Not at all
Other computer-based training and simulators	77.6	21.5	46.2	19	13.3
Digital forensic training	74	26.3	42.1	14.5	17.1
Records Management/Data Sharing					
Integrated databases (e.g., COPLINK®, regional data sharing, etc.)	38.9	50	32.5	5	12.5
Wireless access in patrol cars:	15.8	60.6	18.2	0	21.2
Community notification via Internet, text messaging	34.8	31.9	41.7	13.9	12.5
Communications/Dispatch/Interoperability					
Computer-aided dispatch with GPS dispatching and tracking of patrol cars	44.8	54.8	32.3	6.5	5.4
700/800 MHz trunked communication system:	27.2	51.8	14.3	12.5	19.6
Inter-agency radios	20.6	55.8	30.2	9.3	2.3
Language translators	60.4	25.5	41.5	22	10.6
Next Generation 911 (text and voice messaging)	78.7	32.1	46.9	11.7	6.8
Weapons and Equipment/Robotics/Tactical					
Fully integrated vehicle system (voice activated)	93.8	15.3	35.2	28.6	20.9
Personal video/audio equipment (worn by officer)	73.7	18.6	42.3	26.3	12.8
Body armor	2.3	40	40	0	20
Pistol cam	96.7	10.4	23.8	40.1	25.7
LED vision incapacitation device	94.3	10.6	32.2	33.7	23.6
Directed energy vehicle stopper	96.7	20.7	32	29.6	17.7
Sound wave incapacitation weapon	96.7	8.4	30.2	35.6	25.7
Conducted Energy Devices (e.g., Taser® or Stinger®)	17.6	22.2	47.2	16.7	13.9
Long range broadcasting device	81.3	10.1	22.6	36.3	31
Sensors for explosives	86.1	10.7	30.5	38.4	20.3
Sensors for biological/chemical/nuclear materials	72.7	9.3	34.7	32	23.3
Protective gear/clothing	20.6	22	41.5	26.8	9.8
Robots for bomb disposal and tactical operations	58.4	14	14.9	29.8	41.3
Mobile command center	19	30	45	2.5	22.5
Special purpose vehicles (e.g., armored vehicles, ATVs)	30	19.4	29	25.8	25.8

Table E - 6

Technology Acquisition

Type of Technology	Percent that don't use technology	For agencies not using technology, likelihood of acquiring this technology in the next 3-5 years (%)		
		Very likely	Somewhat	Not likely
Identification				
DNA Testing Equipment	75.7	3.8	8.8	87.4
Ballistics imaging	74.4	0.6	11.5	87.9
Fingerprint readers	42.4	20.2	29.2	50.6
Other biometric technology	89.1	3.7	20.7	75.5
Drug testing technology	50.7	5.7	23.8	70.5
Cyber forensics equipment	46.9	10.3	29.9	59.8
Mobile laboratory	81.8	1.8	11.8	86.4
Sensors and Surveillance				
Video surveillance network	39.5	24.1	30.1	45.8
License plate readers	61.9	22.5	32.6	45
Patrol car cameras	35.6	20.3	25.7	54.1
Gunshot detection devices	87.7	5.9	11.9	82.2
Electronic listening devices	51.9	0.9	18.3	80.7
Electronic interception	79.1	3	13.3	83.7
Portable devices for detecting concealed weapons	77	3.7	23	73.3
Drug detection devices	79.4	1.2	27.1	71.7
See through the wall technology (ultra wide band)	90.8	1.6	14.4	84
Night vision devices	15.9	9.1	51.5	39.4
Aerial surveillance equipment	87.2	1.1	7.1	91.8
GPS devices for tracking suspects	36	6.6	44.7	48.7
Crime Analysis/Mapping				
Geographic Information Systems (GIS) software	15.3	34.4	28.1	37.5
Real-time crime monitoring center	80.5	11.8	25.4	62.1
Predictive modeling	68.8	9.9	33.1	56.3
Investigative software (e.g., data mining software	54.5	15.8	41.2	43
Software for risk factor analyses for victimization	86.3	7.2	24.3	68.5

Type of Technology	Percent that don't use technology	For agencies not using technology, likelihood of acquiring this technology in the next 3-5 years (%)		
		Very likely	Somewhat	Not likely
Training				
Use of force computer simulators	47.8	61	19.2	74.7
Driving simulators	78.5	4.3	13.5	82.2
Other computer-based training and simulators	77.6	2.5	27.7	69.8
Digital forensic training	74	5.9	28.8	65.4
Records Management/Data Sharing				
Integrated databases (e.g., COPLINK®, regional data sharing, etc.)	38.9	42.5	32.5	25
Wireless access in patrol cars:	15.8	56.3	15.6	28.1
Community notification via Internet, text messaging	34.8	26.8	31	42.3
Communications/Dispatch/Interoperability				
Computer-aided dispatch with GPS dispatching and tracking of patrol cars	44.8	30.9	35.1	33
700/800 MHz trunked communication system:	27.2	28.6	14.3	55.4
Inter-agency radios	20.6	32.6	27.9	37.2
Language translators	60.4	4.8	29.6	64.8
Next Generation 911 (text and voice messaging	78.7	23.9	39.3	34.4
Weapons and Equipment/Robotics/Tactical				
Fully integrated vehicle system (voice activated)	93.8	3.1	14.9	82.1
Personal video/audio equipment (worn by officer)	73.7	4.5	29.5	66
Body armor	2.3	40	40	20
Pistol cam	96.7	1.5	7.9	90.6
LED vision incapacitation device	94.3	1.5	11.5	87
Directed energy vehicle stopper	96.7	2.4	12.7	84.9
Sound wave incapacitation weapon	96.7	2.5	4.9	92.6
Conducted Energy Devices (e.g., Taser® or Stinger®)	17.6	29.7	21.6	48.6

Type of Technology	Percent that don't use technology	For agencies not using technology, likelihood of acquiring this technology in the next 3-5 years (%)		
		Very likely	Somewhat	Not likely
Long range broadcasting device	81.3	3	10.1	87
Sensors for explosives	86.1	3.4	16.3	80.3
Sensors for biological/chemical/nuclear materials	72.7	2.6	16.6	80.1
Protective gear/clothing	20.6	0	37.2	62.8
Robots for bomb disposal and tactical operations	58.4	2.5	7.4	90.1
Mobile command center	19	10	32.5	57.5
Special purpose vehicles (e.g., armored vehicles, ATVs)	30	6.3	27	66.7

Appendix F

List of Workshop Attendees

Name	Title	Department
Mario Lattanzio	Commander	Mesa Police Department
Mark Weldon	Lieutenant	Los Angeles County Sheriff's Department
Darryl Hoover	Sergeant	San Diego Police Department
Dave Knopf	Lieutenant	San Jose Police Department
Sandi Lehan	Ms.	SPAWAR SYS PAC, San Diego, CA
Jim Beuthel	Sergeant	Aurora Police Department
Molly Miles	Ms.	Colorado Springs, CO
Michael Scott	Special Agent	Bureau of Alcohol, Tobacco, Firearms and Explosives
Brian Reeves	Dr.	Bureau of Justice Statistics
Carl Peed	Director	COPS Office
Daniel Hickson	Director	Metropolitan Police Department, DC
Lynn Burns	Crime Analyst	Metropolitan Police Department, DC
Yinka Alao	Mr.	Metropolitan Police Department, DC
Sarah Hoyos	Senior LE Analyst	Metropolitan Police Department, DC, Research & Analysis
Bill Tegeler	Deputy Director of Management Services	Police Executive Research Forum
Bruce Kubu	Senior Research Associate	Police Executive Research Forum
Bruce Taylor	Director of Research	Police Executive Research Forum
Christopher Koper	Deputy Director of Research	Police Executive Research Forum
Chuck Wexler	Executive Director	Police Executive Research Forum
Craig Fraser	Director of Management Services	Police Executive Research Forum
Rachael Bambery	PERF Senior Research Fellow	Police Executive Research Forum
Matt White	Manager	Jacksonville Sheriff's Office
Orestes Chavez	Lieutenant	Miami Police Department
Tony Utset	Senior Executive Assistant	Miami Police Department
Frederica Burden	Officer	Miami Police Department
John Bolduc	Lieutenant	Port St. Lucie Police Department
Wade Willnow	Detective	Port St. Lucie Police Departmetn
Martin Ryczek	Captain	Chicago Police Department
Mia Ogliore	Commanding Officer Sergeant	Chicago Police Department - Detective Division Administration
Jonathan Lewin	Commander	Chicago Police Department – information Services Division
Bryan Roach	Deputy Chief	Indianapolis Police Department
David Linn	Directory of Technology	Montgomery County Police, MD
Hank Stawinski	Major	Prince George's County Police Department
Paul Przybilla	Information Technology Division Manager	Hennepin County Sheriffs Office
Jefrey Egge	Sergeant	Minneapolis Police Department
John Rowan	Lieutenant	Suffolk County (NY) Police Department
John Sumwalt	Sergeant	Suffolk County (NY) Police Department
Will Dalsing	Corporal	Tulsa Police Department

Nola Joyce	Ms.	Philadelphia Police Department
Peter Scheets	Deputy Chief	Bryan Police Department
John A. Jackson	Sergeant	Houston Police Department
Bianca Conn	Crime Analyst	Chesapeake Police Department
M. Marie Kane	Lieutenant	Chesapeake Police Department – Criminal Investigations Section
Greg Staylor	Police Lieutenant/ 9-1-1 Coordinator	Chesapeake, Virginia Police Department
Tony Castillo	Deputy Director Emergency Communications	Emergency Preparedness and Response
Elizabeth R. Rios	Special Agent	FBI – Norfolk
James Fox	Chief	Newport News Police Department
John J. Butch	MPO	Newport News Police Department
Mark Wagner	Detective	Newport News Police Department
Jeffery Balen	Sergeant	Norfolk Police Department
Mike Loftin	Investigator	Norfolk Police Department
Wallace R. Driskell	Captain	Norfolk Police Department
Luis Ortiz	NPD Crime Analysis	Norfolk Police Department – Crime Analysis
Jeff Locke	Patrol Officer	Portsmouth Police Department
Garrett Shelton	Assistant Chief of Police	Portsmouth Police Department
Tom Pulaski	Mr.	Prince William County Police Department, VA
Bob Christman	Sergeant	Virginia Beach Police Department
John Borman	Detective	Virginia Beach Police Department
Tom Mitchell	Support Division Manager	Virginia Beach Police Department
Daniel Plott	Captain	Virginia State Police
Jim Reynolds	Trooper	Virginia State Police
Gunnar Kohlbeck	Lead Management Specialist	Virginia State Police – Planning and Research Unit
William R. Maki	Deputy Chief	Waynesboro, VA Police Department