When a crime has been committed and police have responded to the scene, law enforcement activity transitions in focus from situation management toward the goal of successfully identifying individual perpetrators and bringing them to justice. In this process of evidence collection and suspect identification, technology has many roles to play in broadening the capability and increasing the effectiveness of investigators.

Major findings from the chapter include:

- Most local police departments (90 percent) reported that they lacked technology to detect or analyze cyberattacks. Even for departments in large urban areas (more than 225,000 population), three quarters of departments reported that they lacked these capabilities. Among state police organizations, two-thirds do not currently use or have access to these technologies.

- The tasks associated with police interaction with the court system apparently represent an important opportunity to integrate technology into law enforcement. Only 5–15 percent of local departments and 10–25 percent of state police indicated that they link or share computerized files of summonses or warrants with other agencies. Furthermore, only 5 percent of local police reported having a video or other systems that allowed them to file cases with prosecutors remotely.
CRIMINAL INVESTIGATION

Digital Crime Scene Photography

The technique of photography has been important to law enforce-
ment since soon after its invention and commercialization. The abil-
ity to capture accurate photographic evidence at a crime scene serves
purposes from advancing an ongoing investigation to presenting a
completed case in a court of law. Recent advances in digital
photography, by increasing the speed of the technique, decreasing
the individual cost of photos, and making the photographic output
readily sharable over electronic networks, has the potential to be
even more useful to law enforcement. As a result, it is of interest how
many departments have access to the technique. The RAND Law
Enforcement Survey found 31 percent of local police departments
have digital crime scene photographic systems, while 13 percent of
state police report using them (LETS, 16b).1

Fingerprint Identification

The FBI's Automated Fingerprint Identification System (AFIS) allows
police to rapidly check fingerprints against those in a national
database to identify known criminals or a suspect whose prints are in
the system. AFIS is one component of the Integrated Automated
Fingerprint Identification System (IAFIS), which is described in the
accompanying text box.

Sixty-two percent of respondents to the RAND Forensics Survey have
exclusive use of an AFIS terminal and another 28 percent have shared
access to the system. Most state police have either exclusive owner-
ship of an AFIS system, shared ownership of one, or have an AFIS
terminal with access to a remote AFIS site. Fewer local police have
AFIS access. Among local police, a far higher percentage of larger de-
partments than smaller ones have access to AFIS.

1For the LETS survey to local police, percentages have been statistically adjusted to
represent the entire population. See Appendix A for a description of the adjustment
methodology. For the LETS survey to state police and the FTS survey to crime labs,
results are reported as unadjusted percentages.
In order to interface with automated fingerprint matching systems, fingerprints can be captured digitally or can be collected in the “traditional” ink-on-paper method and scanned into a computer. Because of the increase in speed and efficiency of digital capture, this method represents an improvement over traditional methods. The RAND Law Enforcement Survey found that 21 percent of local departments make widespread use of digital imaging for fingerprints, 9 percent make limited use of such technology, and 70 percent do not use it. The percentage of departments making widespread use of this technology increases with size of population served. One-third of state police reported widespread use of digitized fingerprints.

Among local departments, 2 percent expressed no need for future acquisition or use of digitized fingerprints. Sixty-five percent saw cost as a factor inhibiting acquisition of this technology emphasizing the barrier to replacing the current traditional methods—given the relative cost differentials—with a new technology. Thirteen percent saw training as a limiting factor. Training was even more of a factor for state police with 20 percent highlighting it as a potential barrier to acquisition. This suggests that there are potential technology adoption issues associated with this technology in addition to how its cost compares to current methods.

Although many parts of a police department may be involved in fingerprinting and print collection, crime labs perform much of the analysis of the evidence. The RAND Forensic Survey found that requests for latent print processing accounted for about 16 percent of all requests to crime labs. On average, labs reported processing 90 percent of requests received (FTS, 22).

Crime labs experiencing problems in obtaining latent print analysis in sufficient time to meet legal or other timeframe requirements were asked to indicate whether this was due to backlogs, lack of technology or equipment, prohibitive costs, and/or lack of trained personnel. Nearly all respondents said that backlogs were a reason for the problems. More than half cited lack of trained personnel, while 12 percent cited lack of technology or equipment. None of the respondents saw prohibitive cost as a reason for their problems with latent prints (FTS, 28a). This suggests that, for crime labs, the human factors (in this case lack of personnel in addition to their training) asso-
Challenges and Choices for Crime-Fighting Technology

Associated with the technology are by far the dominant influence on effective deployment of the techniques.

Suspect Composites

Just as is the case for photography, digital technology has the potential to improve the way law enforcement agencies generate and use composite sketches of crime suspects. The RAND survey found that 14 percent of local police departments make widespread use of digital imagery for suspect composites, 31 percent make limited use of it, and 55 percent do not use it. The percentage of departments making widespread use of this technology increases with size of population served. Two-thirds of state police reported limited use of suspect composites (LETS, 36g).

Among local departments, only 5 percent saw no need for future acquisition or use of digitized composite sketches. Forty-eight percent saw cost as a factor limiting acquisition or use of this technology. Twenty-one percent saw training and 11 percent effectiveness or reliability as limiting factors (LETS, 36g). This suggests that agencies have some concerns about how digital composites will be effectively integrated into their current operations.

Cybercrime

With the advent of the Internet, the connection of more and more computers to the common network, and the growth of e-commerce, cybercrime has become an increasing challenge for both the country as a whole and the law enforcement community. An ABC Television News report of February 28, 1998, estimated that U.S. corporations sustain damages in excess of $10 billion annually from cyberattacks (Sandia National Laboratories, 1998, p. 32). Thirty percent of respondents to a recent survey from both private and public sectors reported having been subjected to cyberattacks (Computer Security Institute, 1999). The Presidential Commission on Critical Infrastructure Protection concluded, “Federal R&D efforts are inadequate for the size of the R&D challenge presented by emerging cyber threats” and expressed their belief that “real-time detection, identification, and response tools are urgently needed” (President’s Commission, 1997, p. 89).
Victims of cybercrime are often more concerned with repairing the damage and limiting further damage than in reporting it as a crime, and rely much less on law enforcement for assistance. The differences in how private entities respond to these crimes, in addition to the broad variety of cybercrimes that can be perpetrated, are increasingly problematic for law enforcement. The need to attract human resources with the needed knowledge to respond to these crimes, coupled with the cost of the necessary computer technology, make it even more difficult and straining to already burdened organizations (Joint Report, 2000).

The LECTAC Law Enforcement Operations Subcommittee has identified cybercrime as a high priority concern (LECTAC, 2000, p. 39). The LECTAC Forensic and Investigative Sciences Subcommittee has called for a higher emphasis on methods and best practices for electronic evidence and electronic crime-monitoring in general (LECTAC, 2000, p. 37). Looking into the future, a British panel forecasting toward 2010 anticipates increasing difficulty for law enforcement from information and communications technology (ICT)-linked crime.

The domination of, and changes brought about by, these technologies will have a profound effect upon crime. In particular the potential for its increased speed and scale. Crimes such as electronic theft and fraud will occur more quickly, reducing the likelihood of being caught in the act. Information about how to compromise a system will be available more quickly and to more people. As the lingua franca of the internet, sites or communication in English may disproportionately be targets for crime and disruption.

As well as its speed and scale, ICTs offer greater complexity. This will be significant in terms of setting standards; international crime;

---

2A recent New Jersey study (Joint Report, 2000) addressed the following types of computer crime:

- Crimes against children,
- Bias and hate crimes,
- Hacking,
- Internet fraud,
- Identity theft,
- Internet gambling, and
- E-commerce in alcoholic beverages and tobacco.
police jurisdictions; judicial systems; and legislation. The accept-
ability of digital evidence in court—and the ability for it to be
understood—are issues to consider. Potential solutions to crime
need to be understood by those using them—complex or lengthy
security procedures will most likely be ignored. ICTs will also allow
the increasingly sophisticated use of cryptography and steganogra-
phy to conceal illegal transactions (Crime Prevention Panel, 2000,
p. 4).

E-mail and the Internet promote asynchronous, global, collaborative
communication, which tends to flatten hierarchy and break down
walls between organizations. This will create both new challenges
and opportunities.

To cope with info-crimes, the police and other authorities will need
to adapt their techniques to the characteristics and tricks of the
Information Marketplace, as they have begun to do. But the broad
framework in which they perform these jobs can remain the same.

In order for law enforcement to adapt to these changes, changes are
required far above the local level: Increased coordination of laws
among different states and different nations will be critical for the
simple reason that cyberspace does not recognize [state or] national
boundaries (Dertouzos, 1997, p. 289). Currently, law enforcement at
the state and local level is not prepared for these types of challenges,
even without their international complications.

The RAND Law Enforcement Survey asked respondents to rate the
quality or adequacy of technologies currently owned or available to
their agency to detect and analyze cyberattacks. Ninety percent of lo-
cal police departments indicated such technology was not currently
in use or available to their agency; although a quarter of departments
serving urban populations of more than 225,000 did indicate access
to or usage of these technologies. Of these departments, 15 percent
rated the technologies available to their agency as being modern/

---

3Material derived from a computer, electronic system, or presented in an electronic
form.
4Steganography, the means by which images are hidden within others, can be used to
send seemingly innocent images that contain illegal images or information.
5See Barksdale, p. 95 in Hesselbein et al. (1998).
state of the art (LETS, 28h). Among state police, two-thirds did not
currently use or have available to their department technologies to
detect and analyze cyberattacks. Of those that did, only two depart-
ments rated the technology as being modern/state of the art (LETS,
28h).

Given the apparent lack of availability of cybercrime resources in lo-
cal departments, it was of interest whether these organizations were
seeking assistance (and from where they were seeking it) to deal with
this threat. When asked to identify where they had sought assistance,
a full 73 percent of the police departments did not list any sources of
help. Of those indicating that their department had sought assis-
tance, the advice was overwhelmingly sought from in-house sources
(Table 11). In addition it is noteworthy that such a small fraction of
local departments have sought help in this area from any source.
Although the implications of this result are somewhat ambiguous—
since they could mean either that cybercrime is not occurring within
the jurisdictions of most local departments or simply that the de-
partments are not being called on to respond to it—it might imply
that these departments should be better informed of the resources
which are available to assist them in this area. These data are dis-
cussed in more detail in later chapters on federal support of state and
local police organizations.

Table 11

<table>
<thead>
<tr>
<th></th>
<th>In-House</th>
<th>Local Agency</th>
<th>State Agency</th>
<th>Manufacturer</th>
<th>NLECTC</th>
<th>FBI</th>
<th>ATF</th>
<th>Nat’l Labs</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local police</td>
<td>24%</td>
<td>14%</td>
<td>14%</td>
<td>2%</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>State police</td>
<td>53%</td>
<td>7%</td>
<td>20%</td>
<td>7%</td>
<td>0%</td>
<td>20%</td>
<td>0%</td>
<td>0%</td>
<td>7%</td>
</tr>
</tbody>
</table>

SOURCE: LETS, 32a. Numbers are percent of departments reporting they received
technology-related support from indicated sources in the past year. Local depart-
ments are statistically adjusted percentages based on sample weighting.
SUSPECT APPREHENSION

Summons and Warrants

Court-related functions—which include executing arrest warrants, providing court security, serving civil processes, and serving as witnesses—are all labor intensive. Because of their duties and responsibilities at the local level, most law enforcement organizations are involved in a number of court-related functions. Most local police execute arrest warrants. Additionally, nearly all sheriffs’ departments provide court security and serve civil processes (Table 12).

Because of the labor-intensive nature of these processes, technology has a significant opportunity to positively affect their execution. Technology can increase the efficiency of court-related functions if files, such as those containing information on summonses and warrants, can be shared with other agencies. From the RAND survey results, it is clear that little has been done to integrate technology into the court process at the local level, regardless of size of department. Only 5–15 percent of local police actually share or link computerized files of summonses and warrants with other agencies. Those state police (about 10–25 percent) that do link with or share such files do so with either other state agencies or other agencies. Very few of these departments link or share files with nearby cities or with county agencies (LETS, 23i,m).

Table 12

Percent of Agencies with Primary Responsibility for Court-Related Functions, 1997

<table>
<thead>
<tr>
<th></th>
<th>County Police</th>
<th>Municipal Police</th>
<th>Sheriff</th>
<th>State Police</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute arrest warrants</td>
<td>87%</td>
<td>93%</td>
<td>98%</td>
<td>55%</td>
</tr>
<tr>
<td>Provide court security</td>
<td>10%</td>
<td>22%</td>
<td>93%</td>
<td>8%</td>
</tr>
<tr>
<td>Serve civil process</td>
<td>17%</td>
<td>5%</td>
<td>93%</td>
<td>6%</td>
</tr>
</tbody>
</table>

SOURCE: Reaves and Goldberg, 1999, p. xvi. Data are for agencies with 100 or more officers. “State Police” are primary state police.
Mug Shots

Beyond the advantages of digital photography at crime scenes that were discussed above, this technology can also improve the efficiency of the mug shots taken when individuals are brought into custody. It appears that this digital technology is somewhat more widespread than that used in crime scene photography. The RAND survey found that 43 percent of local police departments make widespread use of digital imaging for mug shots, 19 percent make limited use of this technology, and 38 percent do not use it. The percentage of departments making widespread use of this technology also increases with size of population served.

In contrast to its adoption at the local level, only 13 percent of state police reported widespread use of digitized mug shots.

Among local departments, 6 percent expressed no need for future acquisition or use of digital mug shots. Forty-seven percent saw cost as a factor acquisition or use of this technology (LETS, 36f). Like the digital fingerprint case discussed above, this cost concern could represent as much satisfaction with currently used “lower tech” methods (which reduce the perceived benefit of changing) as the absolute costs of the systems themselves. This could be particularly important for departments that do not have to process a large volume of individuals taken into custody.

Remote Case Filing

Because of the travel and time that can be involved, the process of filing cases with prosecutors represents another key area in which technology could have a significant effect on law enforcement productivity and effectiveness. Information and communications technologies, in particular by allowing remote filing of cases, could potentially reduce workload and free up officers for other activities. From the results of the RAND Law Enforcement Technology Survey, it is clear that this particular technological capability is almost entirely absent from U.S. police forces. Only 5 percent of local police surveyed by RAND reported having a video or other system for remote case filing with prosecutors. None of the state police respondents reported having a remote case filing system (LETS, 16h).