Advances in Policing—
New Technologies for
Crime Analysis

13
INTRODUCTION

The Stages of Technological Advancement in Policing
The First Stage (1881–1945)
The Second Stage (1946–1959)
The Third Stage (1960–1979)
The Fourth Stage (1980–present)

Crime Analysis
Strategic Crime Analysis
Tactical Crime Analysis

Geomapping Crime Patterns: Moving Beyond Push Pins

What Crime Maps Do: GIS as a Technical Aid to Problem-Oriented Policing

LINKAGES IN LAW ENFORCEMENT: GIS Applications to Sex Offender Management

Types of Data with Mapping Applications
Mapping and Accountability: GIS in Action
GIS and the Patrol Officer

LINKAGES IN LAW ENFORCEMENT: GIS Applications to Community Policing

Other Applications: Geographic Profiling

Twenty-First-Century Technologies in Policing

Closed-Circuit Television
Global Positioning Systems
Biometrics
   Facial Recognition Software
   Fingerprint Identification Systems

Interjurisdictional Communication Technologies
   Offender Databases
   Cross-Jurisdictional Radio Communications
   Electronic Warrant Processes
   Information Security Through Encryption

The World Wide Web and Community Policing

Improving Accountability—Mobile Communications with Patrol
   Mobile Digital Communications
   Automatic Vehicle Monitoring

Chapter Summary

LINKING THE DOTS
Throughout its history, the U.S. Border Patrol has faced the seemingly insurmountable task of detecting and apprehending the ever-present stream of drug traffickers and illegal immigrants. The 60-mile area around the U.S.–Mexico border in the San Diego area alone requires the management of more than 2,000 agents and 900 seismic sensors (DeAngelis 2000). To aid them in their efforts, the U.S. Border Patrol San Diego Sector has many high-tech tools at their fingertips, such as geographic information systems (GIS), seismic sensors (more than 900), and infrared night-vision equipment.

The agents use the GIS technology to map the locations of alien apprehensions as a means of determining why certain areas are higher in illegal migration and drug trafficking than others. Using real-time sensor feeds from the Intelligent Computer Aided Detection System (ICAD), agents monitor “hits” corresponding to potential illegal migrant entry into the country. After identifying a possible entry point, agents are able to map out the travel route that has the highest probability of leading to the apprehension of the illegal border crossers.

In addition to the tremendous challenges presented by the region’s mountainous terrain, illegal traffic has also found underground avenues of escaping detection. To combat this eventuality, the Border Patrol has used Global Positioning System (GPS) receivers and GIS to plot storm drain and sewer system routes that are facilitating traffic from Mexico into the United States.

The application of such technologies to the practice of law enforcement has revolutionized the capacity of police to both respond to crime that is taking place in real time and to proactively identify problems, analyze their causes, and develop strategic plans that truly enhance an agency’s crime prevention capabilities. For example, the U.S. Border Patrol also targets high-risk areas.
with warning signs in Spanish regarding the dangers of crossing the border illegally.

In this technological era, law enforcement has had to evolve to be better equipped to fulfill its mandate of contributing to public safety. Technology has proven invaluable in responding to the problem of linkage blindness across jurisdictions, as well as with other criminal justice agencies and sectors of the community. In an age faced with continuing threats of transnational crime and terrorism, the importance of continued technological advances cannot be overstated.

However, the increasing reliance on and availability of technology to law enforcement can be intimidating. This technology brings with it new legal challenges, particularly in relation to the balance between crime control and the private interests of citizens introduced in the beginning of this book. This chapter will begin with a brief overview of the development of technological advances to law enforcement, followed by a descriptive coverage of key technological applications in policing. Particular attention will be paid to the use of GIS in facilitating proactive police management in the twenty-first century.
Soulliere (1999) provides a useful conceptual framework for describing the advancement of technology in policing since its early professional origins. Although there is significant overlap with Kelling and Moore’s (1987) three eras of policing (see Chapter 2), she offers four useful stages to help conceptualize technological development in policing. Table 13.1 summarizes Soulliere’s stages of technological advancement.

### The First Stage (1881–1945)

As described in Chapter 3, much of policing’s initial technological advances can be attributed to the work of August Vollmer, who headed the early twentieth-century police department in Berkeley, California. Under his guidance, law enforcement increased its mobility through motor vehicle patrol and enhanced officer–precinct communications through telephone and radio. With his establishment of the first forensic laboratory, criminal investigators had access to an increasing array of technological expertise that would continue to increase exponentially throughout the development of law enforcement. For example, Vollmer’s crime laboratory pioneered the use of polygraph, as well as fingerprint and handwriting classification systems (Seaskate 1998).

Soulliere (1999) cites several ways in which these early technological advances impacted the police organization, including:

- The development of increasingly complex police organizations through the creation of specialized sections within large police organizations to handle the new technology, such as radio communications and forensic labs
- Increased mobility for patrol activities offered by the use of automobiles
- Increased officer safety made possible with enhanced communications and the use of automobiles

### Table 13.1

<table>
<thead>
<tr>
<th>Soulliere’s Stages of Technological Advancement in Policing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stage 1 (1881–1945)</strong></td>
</tr>
<tr>
<td>Mobile patrol</td>
</tr>
<tr>
<td>Radio communications</td>
</tr>
<tr>
<td>Telephone communications</td>
</tr>
<tr>
<td><strong>Stage 2 (1946–1959)</strong></td>
</tr>
<tr>
<td>Traffic-violation-detection instruments</td>
</tr>
<tr>
<td><strong>Stage 3 (1960–1979)</strong></td>
</tr>
<tr>
<td>911</td>
</tr>
<tr>
<td>Centralized dispatch</td>
</tr>
<tr>
<td>Civilian specialists</td>
</tr>
<tr>
<td>Research and development organizations</td>
</tr>
<tr>
<td><strong>Stage 4 (1980–present)</strong></td>
</tr>
<tr>
<td>Telecommunications advances</td>
</tr>
<tr>
<td>Mobile data communications</td>
</tr>
<tr>
<td>Expert systems</td>
</tr>
<tr>
<td>Imaging</td>
</tr>
<tr>
<td>Biometrics</td>
</tr>
<tr>
<td>GIS</td>
</tr>
</tbody>
</table>

The Stages of Technological Advancement in Policing

The Second Stage (1946–1959)

Roughly corresponding with the beginnings of Kelling and Moore’s Reform Era of policing, Soulliere (1999) claims that the second stage of technological advancement facilitated a major portion of the bureaucratization of policing organizations. During this stage, traffic police received a significant boost with the advent of the first instruments to measure both speeding violations and the condition of the driver. Although early instruments were rather crude indicators, they would grow over time to include the significant automobile surveillance mechanisms and blood-alcohol measures briefly discussed in Chapter 7.

The Third Stage (1960–1979)

As society entered the computer age, Soulliere (1999) claims that police technology began to truly emerge. During this stage, call distribution centers, computerized databanks, and computer sections became commonplace in police agencies. Some of the significant technological advancements in this stage can be attributed to President Lyndon B. Johnson. In 1967, he created the President’s Commission on Law Enforcement and the Administration of Justice to analyze crime patterns in the country, as well as the resources available to combat them. The Commission’s report highlighted the slow infusion of technological advances into the criminal justice system, with particular attention paid to policing. To this end, the report stated (President’s Commission on Law Enforcement and the Administration of Justice 1967):

The police, with crime laboratories and radio networks, made early use of technology, but most police departments could have been equipped 30 or 40 years ago as well as they are today. . . . Of all criminal justice agencies, the police have had the closest ties to science and technology, but they have called on scientific resources primarily to help in the solution of specific serious crimes, rather than for assistance in solving general problems of policing. (p. 125)

A notable gap existed between the technologies that were currently available that had potential law enforcement applications and what police agencies were actually using. In response to this gap, the Johnson administration began “the flow, a trickle at first, of what eventually became billions of dollars in direct and indirect assistance to local and state law enforcement” (Seaskate 1998, p. 2).

The commission argued for the establishment of a single telephone number that citizens across the country could use to contact the police in the case of an emergency. In only a matter of years following AT&T’s announcement of the first 911 system in 1968, 911 became a driving force for police departments across the country (Seaskate 1998). As highlighted throughout earlier chapters, this increasing emphasis on calls-for-service would have both benefits (the seeming ease of access to the police in times of emergency) as well as detriments (this became the principal means of determining police resource deployment and performance evaluation). Skolnick and Bayley (1986) point out that patrol officers can become exhausted by rushing between calls for service, rather than taking the time needed to truly digest and understand the human situations in which they are regularly thrown.

During this third stage of development, large municipalities began the process of centralizing the dispatch of all fire, police, and medical services
(Seaskate 1998). The over-reliance of the average citizen on the use of 911, regardless of the nature or seriousness of the problem, has led to the establishment of 311 systems in many metropolitan areas to try and decrease the significant burden 911 has had on city emergency resources. The 311 system is available for all calls to police and fire personnel that are not emergencies. Other recent strategies for handling the call volume brought about by 911 include the differential response approaches described in Chapter 6.

Increased research on law enforcement applications and technological development was also a key characteristic of the third stage. The National Institute of Justice (NIJ) was created in 1968, and it continues to play a leading role in enhancing the field of law enforcement internationally (Soulliere 1999). An increasing reliance on civilian specialists within large police organizations also continued throughout this stage with developments in the areas of forensics and communications technologies.

### The Fourth Stage (1980–present)

Information access and use characterize Soulliere’s (1999) fourth stage of technological development. In addition to simply amassing a large volume of information—a task that law enforcement agencies have been successful at since their creation—technology now focuses on the speed and ease of information use. Moreover, technology developed throughout the fourth stage now provides law enforcement with access to data that would be unavailable to them without these tools. Collaboration in the research and development activities of traditional law enforcement and the military has resulted in many of the technologies introduced in this stage. Examples of such new tools include telecommunications, mobile data computers, expert systems, imaging, and biometric technologies (Soulliere 1999). Each of these areas will be described further throughout the chapter.

The importance of law enforcement access to such technological advancements is in many ways a balancing act between concerns for personal liberties and public security, as illustrated by Cowper (2003) (see Figure 13.1).

Kurzweil (2001) discusses the significant rate of technological development in modern society. He notes that although technology has always increased exponentially, earlier generations were at such an early stage of development that
the trends appear flat due to the low baseline. Kurzweil argues that although everyone in society generally expects technological progress to continue at the same pace, the rate of change is accelerating. Rather than just being increased incrementally every year, technological advancement is characterized by exponential growth, doubling every year. He organizes these observations into the **law of accelerating returns**:

- The enhanced methods resulting from one stage of progress are used to create the next stage.
- Consequently, the rate of progress of an evolutionary process increases exponentially over time.
- In addition, the speed and cost-effectiveness of a technological advancement will also increase exponentially over time.
- Finally, current methods of solving a problem in technology (such as shrinking transistors on an integrated circuit as an approach to making more powerful computers) will provide exponential growth until the method exhausts its potential. At that time, a fundamental change will result that will allow the exponential growth to continue.

Cowper (2003) summarizes the law of accelerating returns by stating that we will have 100 years of progress in the next 25 years and 20,000 years of progress in the next 100 years. Applications available to policing now or in the near future might have once seemed the work of science fiction rather than reality. Certainly the applications of technology to policing have greatly enhanced the ability of law enforcement organizations to meaningfully engage in the problem-solving process. Although many police departments continue to be behind the curve in terms of integrating new technologies into day-to-day operations, the success of many applications to sound policing will make ignoring progress increasingly difficult over time.

Crime Analysis

Integral to the process of problem solving discussed in the previous chapter is crime analysis. **Crime analysis** has been defined as involving “the collection and analysis of data pertaining to a criminal incident, offender, and target” (Canter 2000, p. 4). Ideally, crime analysis will guide police managers in making deployment and resource allocation decisions that are linked to a true understanding of the nature of the problem. The more important data bearing on all components of the crime triangle (see Chapter 12), the better equipped police organizations will be to develop innovative, “out of the box” solutions that include the full spectrum of suppression, intervention, and prevention options.

An important caution must be stressed here. Crime analysis will only be as good as the data or information that is collected. Three **essential criteria for crime analysis** should be used by departments in designing data-collection processes and in interpreting the meaning of information resulting from crime analysis:

1. **Timeliness.** Does the pattern or trend presented reflect a current problem or issue or is it more representative of a previous situation? Deployment decisions with respect to both prevention and offender
apprehension efforts must be based on information that is as current as possible.

2. **Relevancy.** Do the measures used in the analysis accurately reflect what is intended? For example, whether a pattern is based on **calls-for-service data** or **incident data** can be a very important determination depending on what the police manager is trying to understand.

3. **Reliability.** Would the same data, interpreted by different people at different times, lead to the same conclusions?

Canter (2000) categorizes crime analysis into tactical and strategic functions.

### Strategic Crime Analysis

The collection and analysis of data spanning a long period of time is **strategic crime analysis**. It is said to be research focused as it includes the use of statistics to make conclusions (Canter 2000). This form of analysis can be useful to departments in terms of **crime-trend forecasting**, or using data to estimate future crime based on past trends (Canter 2000). With crime-trend forecasting, important decisions can be made with respect to the deployment of patrol allocation as a reflection of the changing volume of criminal activity.

Another important benefit of strategic crime analysis is the analysis of changing community dynamics and risk factors that might be contributing to the particular crime trends of a specific area (Canter 2000). Once again, this type of analysis over time can result in more informed decision making that is more likely to lead to police partnership with other city and community agencies that can help create more long-term, sustainable reductions in criminal activity.

### Tactical Crime Analysis

Whereas strategic crime analysis involves the review of data spanning generally a year or more, **tactical crime analysis** uses real-time data spanning several days. One of the principal uses of this type of analysis involves problem identification, or the **pattern detection** of multiple offenses over a short period of time that have common characteristics, such as type of crime, modus operandi, and type of weapon used (Canter 2000). One example of tactical crime analysis that will be discussed later in this chapter is geographic profiling, which can be used to suggest the likelihood of where an offender lives based on the pattern of where offenses occur. Tactical crime analysis can occur on as large an area as a department’s entire jurisdiction or as small as the few-block-radius of a hot spot.

**Linkage analysis** involves connecting a suspect to a series of incidents based on commonalities in modus operandi and suspect description, as well as known offenders who live close proximity to a given area (Canter 2000). Following a nationwide effort by state legislatures to implement sex offender registration laws (Terry and Furlong 2004), many police departments regularly search their databases of registered sex offenders when a known series of sexual offenses is identified.

Finally, **target profiling** involves the use of data to determine the potential risks certain areas may have for criminal victimization based on known offense
patterns in the area. Following the previous example, some departments have experimented with community risk profiles (i.e., day care centers, presence of parks, etc.) as a means of guiding the community notification process for the presence of registered sex offenders.

**Geomapping Crime Patterns: Moving Beyond Push Pins**

Based on the previous discussion of the applications of crime analysis to policing, the integral role that geographic information systems (GIS) play in the process is readily apparent. A GIS is an automated systems for the capture, storage, retrieval, analysis, and display of spatial data (Clarke 1990). Others have noted that “GIS technology is to geographical analysis what the microscope, the telescope, and computers have been to other sciences” (Cowen 2001, p. 3). By visually representing diverse data sources that can be geographically located, such as crime events, land usage, property values, racial ethnic composition, and so on, GIS enables planners to “manipulate and display geographical knowledge in new and exciting ways” (Cowen 2001, p. 3). Despite its diverse applications across various fields, the common focus of GIS is the enhancement of decision making.

In law enforcement, GIS has revolutionized the practice of electronic crime mapping, or visually displaying crime incidents on a mapped surface of a particular jurisdiction. However, the use of crime maps has a long history within policing. For example, the NYPD used pin maps to represent crime patterns at
Chapter 13: Advances in Policing—New Technologies for Crime Analysis

least as far back as 1900 (Harries 1999). Moreover, criminologists and sociologists have examined the spatial trends of crime and delinquency since as far back as mid-nineteenth century France’s Quetelet (Phillips 1972) and the Chicago school’s social ecology of crime efforts pioneered by Shaw and McKay (1942). The difference is, of course, that until the use of GIS became more commonplace in policing practice during the 1990s, crime patterns were literally represented by inserting push pins into the map of a jurisdiction that was usually mounted on the wall.

Although these early crime maps proved to be useful in visually showing where crimes occurred, patterns would be lost over time as more and more pins were added to the map. Additionally, these maps were very difficult to archive for later retrieval and analysis unless they were photographed (Shaw and McKay 1942).

What Crime Maps Do: GIS as a Technical Aid to Problem-Oriented Policing

GIS has revolutionized the way in which problem-oriented policing (POP) is conducted. This is largely due to law enforcement’s ability to overlay seemingly diverse types of data that all contribute a true understanding of a particular problem. For example, a series of burglaries taking place between the hours of 1:00 PM and 3:00 PM might be the first thing visually displayed on a crime map. This would correspond with the scanning or problem identification part of the problem-solving model detailed in Chapter 12. However, to get at the underlying causes of the burglary problem requires deeper probing and innovative thinking. In this case, the crime analyst might overlay the burglary incident data with available data about land usage in the area. The analyst might then learn that the burglaries are occurring within walking distance of an area high school.

Although this might seem to be an obvious linkage to many, individuals often overlook such connections. By visually displaying overlays of various potential data combinations, GIS can play a critical role in jump-starting the analysis process. With the current example, the police manager might begin to develop a series of hypotheses related to the fact that the burglaries might be caused by troublemaking youths playing hooky from their after-

One significant advantage of GIS is its capacity to combine many data sources to get a visual understanding of the nature of the problem.
GIS Applications to Sex Offender Management

GIS applications can also help to increase law enforcement’s capacity to engage in the collaborative problem solving with other criminal justice and community agencies. The visual representation of information can be a powerful tool in coming to a common understanding of the nature of problems even across planning groups with diverse perspectives.

The authors of this text participated on a citywide task force in New York City composed of representatives from law enforcement, probation and parole, family and criminal courts, mental health, treatment providers, and victim advocates to examine the issue of sex offender management in the community (Grant and Terry 2000). Although New York City had a large registered sex offender population at the time (over 3,000 offenders), there was as yet no comprehensive plan for the management of these offenders in the community involving collaboration between each of the key stakeholders. Building on the recognition across team members of the clear need for such a collaborative approach to sex offender management, as well as a need to better understand the dynamics of the problem through data collection, the New York City Sex Offender Management Team had tremendous momentum from the start, with agencies opening their doors to facilitate the data collection process.

Beginning at the first team meeting, the partners sought to identify a mechanism for gaining a complete understanding of the sex offender population currently residing in the community. Although it was initially suggested that each of the five district attorneys represented conduct searches on sex offenders within their own databases to form an initial population for study, it became immediately apparent that the most

Hot spots can be made readily apparent through the use of GIS density-mapping tools.

(continues)
noon classes. In addition to providing a large pool of individuals from which investigators might seek to learn information about the incidents, police planners may also begin to collaborate with the school to develop responses that increase truancy enforcement in area schools.

Types of Data with Mapping Applications

The data that can be used for mapping purposes are many, limited only by the creativity of the planning body. Any data that can be geocoded, or for which there is geographic reference information, can be used for GIS analysis (Harries 1999). Although early forms of geocoding only permitted street addresses as the geographic unit upon which to map data, now blocks and census tracts can also be used. Crime incidents are readily applicable for geocoding purposes given that they are almost always available as street addresses or otherwise location based (Harries 1999). Crime-mapping applications of GIS include

- mapping incident types and modus operandi, and
- mapping attributes of victims and suspects (Harries 1999)

Based on an initial pattern analysis, overlays with other forms of data can help to develop a broader understanding of a particular problem. For example, pattern analysis might indicate a problem of disorderly conduct and assaults in
an area. An overlay with available liquor stores and bars in the area may present the planner with a series of hypotheses as to what factors might be driving the problem. An additional benefit of GIS analyses is that they are directly compatible with statistical analyses to further refine causal projections. Thus, a city planner might be able to statistically link the rate of disorderly conduct and assaults in city jurisdictions with the overall density of alcohol availability or other possibilities. Although such analyses can only show planners the possible relationship between two variables, or correlations, rather than saying conclusively that X causes Y (causation), there can be no doubt that such findings greatly enhance the level of informed decision making of law enforcement or other key stakeholders in a city.

**Mapping and Accountability: GIS in Action**

Crime mapping can increase the accountability of a department by visually demonstrating incident patterns for which departmental administrators can hold commanding officers accountable over time. A proactive police manager should use GIS and other problem-solving tools to create sound strategic and tactical decisions for officer deployment, for resource deployment, and for partnering with other agencies to facilitate sustained crime reductions. The CompStat model of the New York City Police Department institutionalized the use of GIS for departmental planning purposes with such apparent success that similar versions of CompStat have been implemented in departments across the country.

The NYPD Crime Control Model, or CompStat, cannot be oversimplified to refer simply to quality-of-life policing, aggressive policing, or even simply data-driven policing, as is commonly found in the literature about the model. Rather, as police scholar Phyllis McDonald (2002) emphatically states, “this proliferation of singularly focused descriptors does a disservice to the management principles of CompStat and its potential for use in other jurisdictions. CompStat (the abbreviation for “computer-driven crime statistics”) is a comprehensive, continuous analysis of results for improvement and achievement of prescribed outcomes” (p. 7). In other words, CompStat involves managing police operations by institutionalizing accountability and analysis processes that are the embodiment of the problem-oriented policing model.

McDonald (2002) offers a concise overview of the key elements of the CompStat model and issues involved in its replication in other departments. To summarize, these elements include:

- Specific objectives
- Accurate and timely intelligence
- Effective tactics
- Rapid deployment of personnel and resources
- Relentless follow-up and assessment

As we have seen in earlier chapters, police organizations, like any other form of bureaucracy, are often extremely difficult to change. How then did such a seemingly proactive, forward-looking model become implemented in the country’s largest police department? In his prior position as head of the New York City Transit Police in the early 1990s, former police commissioner William Bratton had seen tremendous successes in focusing departmental operations on specific measurable objectives and an ongoing review of outcome achievement.
Following a series of complementary strategies in then notoriously dangerous New York City subways, such as increased undercover and uniformed police presence and the removal of graffiti and other signs of disorder, dramatic declines in robberies, fare evasion, and general disorder resulted. New Yorkers once again began to feel safe about riding the subways.

When Bratton came to the helm of the NYPD in 1994, he began a dramatic reengineering effort that included interviews and focus groups involving representatives of every rank and bureau in order to assess the state of command in the department (Silverman 1999). Seven specific objectives were created to guide the future direction of the NYPD (McDonald 2002):

- Get guns off the street.
- Curb youth violence in the schools and on the streets.
- Drive drug dealers out of the city.
- Break the cycle of domestic violence.
- Reclaim the city’s public spaces.
- Reduce auto-related crime.
- Root out corruption and build organizational integrity in the NYPD.

To achieve these outcomes, as well as to measure departmental progress toward them, ready access to timely data was essential. However, a significant problem became immediately apparent: The NYPD was not equipped to provide up-to-date crime reports. In fact, there was generally a reporting lag of three to six months for crime statistics, and even then any meaningful analysis on the incident-based level was near impossible (Silverman 1996). Headquarters was not systematically tracking crime activity in the precincts, let alone using such information to evaluate the performance of its commanding officers (Silverman 1999). As a result, precinct commanders did not view crime reduction as a paramount job responsibility. Common to departments across the country, efficiency concerns in responding to crime were seen as being more important. Detective bureaus and other specialized functions thus only rarely collaborated with patrol, and often directly clashed over territorial and other concerns.

CompStat was devised as a means of reforming the NYPD by pushing all precincts to generate weekly crime activity reports so that they could be held accountable for the achievement of the seven specific objectives outlined in the reengineering process (McDonald 2002). In the beginning, Patrol Bureau staff computerized the data and compiled it into the “CompStat Book,” which featured year-to-date crime complaints and arrests for every major felony category, in addition to gun arrests (Silverman 1999). This data would then be compared on citywide, patrol borough, and precinct levels. In addition, precinct commanders quickly became accountable not only for the crime activity, but also for any inaccuracies in the data itself. Over time, data became even more readily available by being downloadable directly from the department’s On-Line Booking Service (OLBS). Headquarters eventually came to rank order precincts in terms of overall crime changes within their jurisdiction.

By requiring timely and accurate data, it quickly became clear to precinct commanders that their role had changed; they were now being held accountable for the crime under their charges. As such, they began to realize that they had to stop simply responding to crime and had to begin to proactively...
think about ways to deal with it from all angles: suppression, intervention, and prevention.

To solidify this message, the department began to hold regularly scheduled CompStat meetings in which precinct commanders and their staff met directly with top departmental brass to discuss crime trends and issues in their precincts. In a very intimidating environment, precinct commanders must stand before a lectern in front of three large video screens that flash GIS-generated maps of recent crime patterns (Figure 13.2). Commanders are then asked about what tactics they have tried to address the patterns, what resources they have tried or needed, and with whom they have collaborated. The session thus becomes a brainstorming problem-solving session about how better to proactively respond to crime. Suggestions for strategy directives are made and are relentlessly followed up upon at subsequent meetings by top brass to further ensure accountability. Having the top brass available as part of this process ensures that departmental resources will be directed to precinct needs, even across precinct and unit lines. Thus, in addition to implementing accountable problem solving, CompStat seeks to reduce the problems of linkage blindness.

**FIGURE 13.2**

Layout of the CompStat Room

Source: Reprinted with permission of Launcelott Smith.
In order to be better prepared for the CompStat meetings, each borough implemented **Pattern Identification Modules (PIMs)** composed of housing, transit, patrol, detective, organized crime, and robbery squads to review daily index crime reports and thus identify crime clusters or patterns that need to be addressed. Figure 13.3 provides a conceptual framework of this planning process.

Over time, the CompStat process has evolved to include other data for analysis, including census data, arrest and summons activity, available resources, average response time, domestic violence incidents, unfounded radio runs, and personnel absences (Silverman 1999). Former Commissioner Howard Safir also added citizen complaints and charges of officer misconduct to the process. Time-of-day photos might also be presented in CompStat meetings to monitor changes in precinct dynamics by shift period.

Many scholars and practitioners have argued that CompStat has played a critical role in the significant crime reductions witnessed by New York City following its implementation (Silverman 1999). Others are more skeptical of these claims, arguing that the crime reduction in New York City can be attributed to larger patterns in society (Karmen 1996). The answer is likely somewhere in the middle; however, the tremendous impact CompStat has had on police management practices internationally cannot be denied. Although some reports have pointed to the demoralizing effects of the process on precinct commanders and officers who feel a pressure to produce numbers, many others cite the significant increases in job satisfaction found by those who feel empowered by the problem-solving aspects brought to the job.

An important concern has been whether the pressure to keep crime statistics low has led to a zero-tolerance policing style that loses sight of community concerns, further inhibiting police–community relations. The answer to this issue is unclear, and it is probably too soon to come to any concrete conclusions.

---

**FIGURE 13.3**

*Conceptual Framework of the CompStat Planning Process*

- Precinct crime data
- Arrest profiles
- Compstat Meetings
  - Top brass
  - Precinct commanders and staff
- Citizen complaints and charges of brutality
- PIMS
- STRATEGY DIRECTIVES
These questions will have to be tracked by practitioners and academicians alike as the model is implemented across diverse contextual conditions within the United States and abroad.

**GIS and the Patrol Officer**

As GIS crime mapping became recognized as an important tool in both tracking and responding to crime on a neighborhood level, departments across the country sought to expand its use beyond administrative planning to reach the patrol officers and community residents. For example, the Camden New Jersey Police Department began providing officers with access to crime-mapping information on desktop computers and even wireless laptops in patrol cars (American City and Country 2002). The department enabled officers to access crime locations, crime types, and times throughout the city in order to focus patrol efforts. The

**GIS Applications to Community Policing**

Beginning in 1995, the Chicago Police Department (CPD) implemented one of the most easy-to-use and accessible GIS systems in the country as a complement to its department-wide Chicago Alternative Policing Strategy (CAPS) community-policing approach. Called Information Collection for Automated Mapping (ICAM), the program enables departmental personnel to generate maps of reported offenses by type, including charts of the ten most frequently reported offenses, through a series of easy mouse clicks (Rich 1996).

CAPS was implemented in 1993 in pilot districts and has since been expanded to all twenty-five of the city’s policing districts. CAPS emphasizes officer problem solving by assigning officers to their beats for at least a year, altering dispatch schedules so that the time spent responding to crime outside of their beats is limited, and requiring officer attendance at community meetings (Rich 1996). Early evaluations of CAPS effectiveness showed significant declines in reported crime, victimization, and fear of crime (Skogan 1996).

ICAM is viewed as a complement to CAPS. CAPS enables officers to better understand the problems in their assigned areas and thus be better facilitators of collaborative problem-solving efforts with community residents (Rich 1996). As part of the ICAM development process, focus groups were held with officers and detectives to seek their understanding and cooperation and ensure that the completed program suited their information needs. Once the department got the officers’ buy-in, maps were regularly shared at beat meetings. Because of the success of the ICAM, a Citizen ICAM program has been developed. With Citizen ICAM, citizens can generate much of the same information (without specific identifiers) that an officer can, thereby facilitating joint police–community planning efforts. Initially, confidentiality issues slowed citizen access to ICAM due to the specific details of street locations. However, it is now running for anyone to see at http://citizenicam.chicagopolice.org/ctznicam/ctznicam.asp.

Other departments across the country have produced their own mapping programs, including Web-based citizen crime reports, as will be discussed later.

**QUESTIONS**

1. Does your local police department have a website? How does it compare to ICAM?
2. Which GIS elements would you include on a department website?
3. What applications of available GIS crime data are there in your community?
maps also enable officers to pinpoint business-contact information when an alarm is sounded, rather than having to call a dispatcher for the information (American City and Country 2002).

In 1998, the NIJ awarded the leading GIS software provider, Environmental Systems Research Institute, Inc. (ESRI), a $500,000 grant to work with local law enforcement agencies and universities to effectively utilize GIS as a crime-fighting tool (Carney 1998). Collaborating with several local law enforcement agencies, ESRI developed an accessible GIS interface for large-scale departmental needs.

**Other Applications: Geographic Profiling**

Geographic profiling, the combined use of geography, psychology, and mathematics to identify the location of an offender, is most commonly associated with tracking down serial killers, rapists, and arsonists. However, it is actually useful as an investigative tool in any case in which an individual offender has committed criminal activity across a series of locations (including crimes as diverse as robbery, burglary, theft, and fraud). Building from the significant empirical efforts of Brantingham and Brantingham (1981), geographic profiling suggests investigative alternatives based on the “hunting behavior” of the offender.

Leading geographic profiler Kim Rossmo argues that criminals are no different in offending as ordinary citizens are in going about their day-to-day activities (Onion 2002).

Following this logic, geographic profiling uses the nearness principle, which means that offenders will remain within a limited range that is comfortable to them when committing their offenses (Rossmo 1998), just as animals will tend to forage within a limited range from their base (Onion 2002). Geographic profiling incorporates all possible methods of transportation available to an offender in providing a calculation of the area in which the offender is most likely to reside.

This research has led to the creation of a computerized geographic-profiling workstation called Rigel. Rigel incorporates statistical analyses, GIS, and database management functions to generate investigative suggestions. Crime scenes are broken down into type (i.e., primary and secondary, see Chapter 8), and then entered by location. Based on the theoretical principles of geographic profiling, addresses of suspects can be evaluated by their probability of being the actual offender (Harries 1999). This can help investigators to sort through their existing databases, such as those of registered sex offenders, and other investigative information. When there is not a specific suspect pool, geographic profiling can help to pinpoint the highest probability areas to focus the search. As with the offender-profiling process discussed in Chapter 8, geographic profiling should only be considered an additional tool for investigators; solving the offense will require a sound investigative strategy.

**Twenty-First-Century Technologies in Policing**

In addition to GIS, over the past decade numerous other technologies have become available to law enforcement, from record management systems (RMS) that help departments store and retrieve the immense amount of data they re-
ceive on a day-to-day basis all the way to sophisticated weaponry and intelligence technologies that have reached law enforcement by way of the military. Covering all of these advances in significant detail is beyond the scope of this text; however, the remainder of this chapter will provide an overview of some significant technological developments that are becoming part of everyday law enforcement activities.

Closed-Circuit Television

The use of closed-circuit television (CCTV) and other forms of public surveillance technology in the United States have witnessed significant growth in recent years as not only police departments, but also airport security and other public entities, have increasingly turned to video surveillance in their efforts to reduce crime and increase public safety. The use of this technology in the United States may not be nearly as prevalent as it is in countries such as England, where there is a camera on nearly every street corner and in every public building; however, it is becoming increasingly popular, particularly following the events of September 11. Law enforcement is now readily turning to surveillance systems such as CCTV as a means of trying to sort through the tremendous traffic at our borders, airports, and dense city streets.

After spending almost two years in CCTV control rooms across England, Goold (2004) concluded that in many cases actual surveillance outcomes have less to do with technological factors than they do with working cultures and new technology research seeks to merge facial recognition software with CCTV surveillance cameras.
the attitudes of individual camera operators. In particular, Goold found that once established, many surveillance systems in public areas quickly become prone to institutional inertia, with both camera operators and scheme managers being either unwilling or unable to update their systems or change their working practices in response to technological advances. Technology does not exist in a vacuum; it is shaped by social factors and by the attitudes and practices of those who use it (Bijkker et al. 1987). In addition, technical workers, such as CCTV operators, often shape the implementation of new technology by fitting it into their existing routines. Technological change may as often be subsumed into existing organizational structures as it effects organizational change (Barley 1986).

No one can erase the images caught on airport CCTV cameras of the September 11 hijackers boarding their plane in Boston. Certainly such retrospective images can be used as evidence of what transpired in a given incident, but law enforcement has become increasingly more interested in finding better ways to harness CCTV technology to identify known offenders passing through a checkpoint, such as a wanted felon or individual on a terrorist watch list. As such, new advances have sought to merge CCTV systems with promising approaches in the field of biometrics, as will be discussed below.

Some agencies have developed innovative ways of overcoming the limitations of private security systems, which in many cases are useful only for recording crimes in progress rather than providing aid to responding units at the scene. For example, the Seal Beach Police Department installed a network that transmits the output of bank security cameras directly to dispatch and to responding units in real time in a high-robbery-incident suburb of Los Angeles (Garcia 2001). The network transmits video over the air through encrypted wireless communication paths in the same manner that images are sent over the Internet.

Global Positioning Systems

Tracking offenders or patrol officer deployments have also been enhanced by the use of Global Positioning Systems. **Global positioning systems (GPS)** use satellite-based technologies for the purpose of tracking the movement of patrol cars or specially equipped stolen vehicles. In some cases, officers can be equipped with GPS-enabled cellular phones, providing an important alternative to conventional address matching for an officer responding to a call. GPS technology has also significantly enhanced aerial photography of crime-incident locations, allowing for greater visualization of the complete context of a situation (Harries 2001). The State of Iowa has capitalized on the surveillance capacity of GPS to monitor the real-time location of high-risk offenders released from prison. With the use of an offender-monitoring system, law enforcement and correctional agencies can keep offenders away from areas where children are likely to congregate (e.g., schools and daycare centers) (Greene 2003).

The Escambia County Sheriff’s Department’s SWAT team used a broadband-via-satellite system when responding to an emergency call involving a shooting victim and a barricaded suspect. Through communication with the Mobile Command Center’s satellite system, SWAT officers were able to determine that the suspect had fled the scene and that the victim was likely dead (Hughes Network Systems 2002). Pictures of the suspect were immediately obtained via satellite and distributed to patrol, a process that used to take hours or days.
Biometrics

Biometrics involves the automatic, real-time identification of individuals based on their physiology or behavior (Cowper 2003). Biometrics thus encompasses a diversity of technologies, including voice recognition, fingerprint identification, lip movement, retinal scanning, facial recognition software, DNA profiling, thermal imagery, and iris/retinal scanning, to name just a few.

Facial Recognition Software The field of biometrics, particularly facial recognition software, might overcome the limitations of CCTV systems, both by reducing the need for expensive human operators and by making the suspect-identification process faster and more reliable. Several promising studies support the potential applications of facial recognition software; however, little is known about how such systems will function in real-life situations (Norris and Armstrong 1999).

Like any technology, the potential impact of facial recognition technology—from preventing crime to infringing civil liberties—depends on the quality of the
database from which possible “hits” are derived. For example, an under-inclusive database might exclude potential terrorists but “catch” a child-support violator; whereas a mistargeted database may send out too large a net that might unnecessarily infringe on people’s civil liberties and reduce the effective application of the technology. Cole’s (2001) groundbreaking analysis of the history of identification technologies highlights the need for further study of the information elements that comprise biometric databases.

Fingerprint Identification Systems Automated Fingerprint Identification Systems (AFISs) were introduced in Chapter 8. An advanced system to aid in the processing, storage, and matching of fingerprints has been introduced by the FBI. Called the Integrated Automated Fingerprint Identification System (IAFIS), this enhanced technology offers a two-hour turnaround on electronically submitted criminal print searches from federal, state, and local law enforcement agencies (Smith 1998).

Interjurisdictional Communication Technologies

At the core of linkage blindness is minimal amount of critical communication that occurs among different law enforcement jurisdictions as well as other sectors of the criminal justice system and community at large. Given the diversity of criminal justice core functions, the gathering and sharing of criminal justice information is particularly complex (Tomek 2001). The need to build information-sharing capacities, both technological and organizational, is evidenced by the NIJ’s decision to make information sharing the number one priority for information technology solutions among state and local agencies, as well as internationally (Tomek 2001).

The need for information continuity and access is key for informed decision making by all criminal justice stakeholders. One of the biggest challenges to larger information-sharing collaborations is the large differences across agencies in terms of agency protocols, standards, and even measures for the collection and utilization of data (Tomek 2001). The Department of Homeland Security is working to reduce this difficulty. In law enforcement’s effort to prevent terrorism, the DHS has initiated the Homeland Security Information Network (HSIN). HSIN enables state and urban law enforcement agencies to collect and disseminate information among federal, state, and local agencies in order to prevent terrorist activity. This computer-based communications system was developed by state and local authorities in order to connect all fifty states, Washington, D.C., and major metropolitan areas (DHS 2007).

Offender Databases Efforts have been made in recent years to develop sufficient technologies capable of overcoming many of the barriers involved in cross- and interjurisdictional information sharing. The San Diego County Automated Regional Justice Information System (ARJIS) system warrants further description as to the possibilities in interjurisdictional information sharing. ARJIS combines information from thirty-eight state, local, and federal law enforcement agencies into one website that can be accessed by registered police, court, and correctional officials (Walsh 2003). ARJIS includes crime-incident databases that are updated every 24 hours, most-wanted lists, and interactive maps. Simi-
larly, the Pennsylvania Integrated Justice Network (JNET) connects all of its criminal justice agencies together for the sharing of critical information, including offender photos and images of distinguishing marks. In one case, an offender was apprehended based on the victim being able to describe the perpetrator’s tattoo to the police (Walsh 2003).

Cross-Jurisdictional Radio Communications Federal efforts at improving cross-jurisdictional radio communications include the NIJ’s **Advanced Generation of Interoperability for Law Enforcement (AGILE)**. AGILE provides direct connections between the radio systems of law enforcement agencies with overlapping or adjacent jurisdictions (Kaluta 2001). The possibilities of such technologies for enhancing national security needs has been demonstrated by early successes of the system as an enhancement to San Diego County’s ARJIS (Scanlon 2000). AGILE has also been used to establish an emergency-only radio channel for presidential inaugurations, linking the Secret Service, the FBI, the U.S. Capitol Police, the U.S. Park Police, and the Metropolitan Police Department (Kaluta 2001).

Electronic Warrant Processes Some jurisdictions have developed solutions to the numerous problems involved in the arrest-warrant process. With the traditional process, courts issue paper warrants that are subsequently used by law enforcement agencies to create a wanted person record in their own systems, which can then be checked by law enforcement officials throughout the country through the use of the FBI’s National Crime Information Center (see Chapter 8). One of the problems with this process is the delay between when the court issues or cancels a warrant, creating serious officer safety concerns (Perbix 2001). Additional concerns arise from the lack of synchronization across the systems, in which warrants entered into one system are not entered into another (adding to the linkage blindness problem).

**Electronic warrant systems**, such as the Colorado Integrated Criminal Justice Information System (CICJIS), link the state’s main criminal justice systems (including law enforcement, prosecutors, courts, adult and juvenile corrections) so that data entered by one agency’s system is automatically transferred and loaded into another agency’s system, thereby reducing linkage blindness and reducing the amount of inconsistent data (Perbix 2001).

Information Security Through Encryption Given the confidential information being shared by criminal justice agencies through these enhanced technologies, serious privacy concerns inevitably arise. Secure law enforcement communication over the Internet or intranets can be achieved with **virtual private networking (VPN)**. VPN uses encryption software to scramble the contents of communications so that even if the system becomes available to hackers, they are unable to read the information (Taylor 2000). In addition to an advanced encryption algorithm that is virtually impossible to break, VPNs pass encrypted communications through a “tunnel” between communicating agencies, ensuring that users meet a high level of identification to be able to access the information (Taylor 2000). With the establishment of proper identification and access protocols, VPNs offer law enforcement agencies the ability to exchange and track important information, such as gang memberships, enhancing contact between the communicating agencies.
The World Wide Web and Community Policing

With its focus on collaborative problem solving and communication with the public, community policing is even more information intensive than traditional policing methods (Monahan 1998). New communication technologies such as the Internet have proven instrumental in furthering departmental community-policing objectives. Important features that are used by many departmental websites in reaching their constituent audiences include (Hart 1996):

- Officer photo galleries, including photos and biographical sketches
- Libraries devoted to crime prevention
- Safety tips, including information about known scam cases operating within the jurisdiction
- Virtual tours of the department
- Recruitment tool with links to personnel information about the hiring process
- Citywide and neighborhood crime statistics, including crime-mapping capabilities on more advanced sites, such as the Chicago Police Department’s Citizen ICAM
- Departmental wanted lists and upcoming court cases
- Capacity for anonymous and/or confidential reporting of crime information or complaints about officer conduct

Department websites move beyond the realm of being public relations tools toward true support for community policing activities to the extent that the department shares important details about activities and arrests rather than the filtered information generally provided to citizens by the media (Price 2001). Departmental posting of such information, however, should be balanced against the privacy needs of victims and nonconvicted offenders.

Improving Accountability—Mobile Communications with Patrol

Radio communications with patrol cars revolutionized the ability of departments to monitor the activities of line officers. Although such technology did not take away the high level of discretion available to officers as part of the nature of the job, enhancements to dispatch communications capabilities had a profound effect on the nature of the job. More recently, cellular phone technology has provided an alternate communication forum for some jurisdictions.

Mobile Digital Communications Mobile digital communications (MDC) offer nonverbal means of communicating information between communication centers and patrol (Thibault et al. 2001). Such communication is achieved through the use of a mobile digital terminal within the patrol car. In some jurisdictions, MDC options allow for electronic submission of reports, thereby reducing the volume of paperwork. More recently, some departments have installed new laptop computers into patrol cars, offering officers instant access to information, such as notes from the communications officer, and even the Internet. Soon officers will not have to leave their cars to write even more detailed reports (Johnson 2003). The Internet also facilitates interjurisdictional
information-exchange opportunities immediately available to officers, again providing an important tool in the reduction of linkage blindness.

**Automatic Vehicle Monitoring.** Through the use of automatic vehicle monitoring (AVM) technologies, departments are able to know the location and status of patrol vehicles, including whether the door of the vehicle has been left open and so on (Thibault et al. 2001). AVM systems are thus vitally important in aiding officers in high-speed pursuit situations and in determining whether the officer is in need of backup.

---

**Chapter Summary**

- Technology has advanced significantly in the past twenty years, and the application of this technology has benefited law enforcement officers in both proactive and reactive methods of policing.
- The most important factors in crime analysis are timeliness, relevancy, and reliability, all of which are necessary to examine data effectively.
- With GIS crime mapping, a map is created that police officers can use to analyze where and when crime occurs. It has many benefits, particularly with regard to proactive policing. It can help the police develop strategies to combat crime, particularly in crime hot spots.
- Advanced technology allows for the collection of more timely and accurate data, helping patrol officers respond more quickly and effectively to crime.
- One of the leading technologies of the twenty-first century is CompStat, which envelopes the problem-oriented policing model and assists in more effective management of areas where crime occurs.
- Surveillance technology such as CCTV is extremely beneficial in tracking all types of criminals, from shoplifters to terrorists. Through the taped monitoring of movements, combined with emerging biometrics of face recognition technology, there are many potential applications of CCTV.
- GPS is important in facilitating law enforcement operation in both investigatory and deployment capacities.
- Interjurisdictional communication technologies useful to law enforcement include offender databases and electronic warrants systems.

---

**Linking the Dots**

1. What have been some of the most significant technological advancements in policing since 1980? Explain their significance.
2. What are some of the dangers associated with the advancement in police technology? How are these dangers balanced with the benefits of such technology?
3. Do you think CompStat is partially responsible for the significant drop in crime in New York City over the past decade?
4. How does law enforcement’s use of technology benefit the community?
5. How can technology be used to help combat terrorism?
Chapter 13: Advances in Policing—New Technologies for Crime Analysis

**KEY TERMS**

311 system 324  
911 system 323  
Advanced Generation of Interoperability for Law Enforcement (AGILE) 341  
Automated Regional Justice Information System (ARJIS) 340  
Automatic vehicle monitoring (AVM) 343  
Biometrics 339  
Buffer zones 330  
Calls-for-service data 326  
Causation 331  
Chicago Alternative Policing Strategy (CAPS) 335  
Closed-circuit television (CCTV) 337  
CompStat 331  
Correlations 331  
Crime analysis 325  
Crime mapping 327  
Crime-trend forecasting 326  
Electronic warrant system 341  
Environmental Systems Research Institute, Inc. (ESRI) 336  
Essential criteria for crime analysis 325  
Facial recognition software 339  
Geocoded 330  
Geographic information systems (GIS) 327  
Geographic profiling 336  
Global positioning systems (GPS) 338  
Homeland Security Information Network (HSIN) 340  
Incident data 326  
Information Collection for Automated Mapping (ICAM) 335  
Integrated Automated Fingerprint Identification System (IAFIS) 340  
Law of accelerating returns 325  
Linkage analysis 326  
Mobile digital communications (MDC) 342  
Nearness principle 326  
Pattern detection 326  
Pattern Identification Modules (PIMs) 334  
Record management systems (RMS) 336  
Relevancy 326  
Reliability 326  
Rigel 336  
Social ecology of crime 328  
Soulliere’s stages of technological advancement 322  
Strategic crime analysis 326  
Tactical crime analysis 326  
Tactics 333  
Target profiling 327  
Timeliness 325  
Virtual private network (VPN) 341

**REFERENCES**


References