Roger Williams University

DOCS@RWU

2007

Police Information Systems

Sean P. Varano
Roger Williams University, svarano@rwu.edu

Jeffrey M. Cancino

James Glass

Roger Enriquez

Follow this and additional works at: https://docs.rwu.edu/sjs_fp

Part of the Criminology and Criminal Justice Commons, and the Legal Theory Commons

Recommended Citation

Chapter Nine

POLICE INFORMATION MANAGEMENT

Sean P. Varano, Jeffrey M. Cancino, James Glass, & Roger Enriquez

EXECUTIVE SUMMARY

Information has played a central role in modern police organizations since data

collection procedures were first instituted in the early 1930s. The amount and complexity

of information, along with the sophistication of analysis, has evolved substantially over a

short period. While the collection and analysis of information was intermittent in the

early 20th century, it has become routine for many police departments. For example,

a 2000 survey of law enforcement agencies found that 60 percent of all agencies use

computer-driven records management systems, 40 percent have automated personnel

records, 32 percent maintain computer generated dispatch data, and 30 percent perform

computer-driven crime analysis. Although such systems are more common among

larger agencies, a sizable percentage of smaller agencies also reported extensive use

of information systems. While 80 to 90 percent of law enforcement agencies serving

populations of 100,000 or more reported using computer-aided crime mapping, 30 to

50 percent of agencies serving populations between 25,000 and 100,000 also employed

some form of computer crime mapping (Hickman and Reaves 2003).

Crime analysis systems, one type of information management system used in

police organizations today, have been adopted with considerable fervor over the past

decade. Not only have law enforcement organizations adopted such technology, many

report that these systems are important to their organizational missions. Mamalian and

LaVigne (1999, 3) surveyed 2,004 police departments across the U.S. and showed that 85% of the respondents indicted that crime mapping was a valuable tool for their department. Recognizing the importance of information and technology, the federal government established the Crime Mapping Resource Center (now the Mapping & Analysis for Public Safety program) to educate and promote the successful management of information and technology in ways that have wide-range social, political, and economic implications for law enforcement and their constituents.

Computer-aided crime analysis is capable of revolutionizing policing by creating a framework for integrating information, technology, and police resources. Law enforcement organizations across the United States are using this approach to address a host of community problems. Research shows that police departments have linked information and technology to study violent, property and drug-related crimes (Groff and LaVigne 2001), hotspot identification and police workload need assessments (Rich 2001), and evaluate community policing initiatives (LaVigne and Wartell 1998).

While the term "information technology" covers a wide spectrum of topics, this chapter discusses the role of information and information systems in modern law enforcement agencies. We briefly discuss the evolution of information management from the pioneering Uniform Crime Report (UCR) to large scale federal funding that has pumped millions of dollars into local and state police organizations to enhance strategies for gathering and analyzing data. We also discuss the *role* that information plays in police organizations, followed by the symbolic nature of information. Here, information is characterized according to symbolic organizational accountability and prestige. The subsections that follow identify other sources of information, such as

Record Management Systems (RMS), dispatch systems, and intelligence systems (e.g., Field Interviews). The chapter concludes with illustrative (e.g., maps and figures) accounts of the San Antonio Police Department's (SAPD) strategies for using information to better inform patrol operations. Finally, we argue that the future of policing is most effective and efficient when information technology (i.e., its collection, process, and analysis) is less reactive, and is applied at the patrol level in more proactive ways. For example, the use of hand held wireless computers by officers is likely to be a common police practice for the purpose of retrieving information in a timely manner.

HISTORICAL PERSPECTIVE ON POLICE INFORMATION SYSTEMS

As American policing evolved from the political to the professional model, reformers recognized a need for: (1) the collection of information and (2) the use of technology (i.e., software) to analyze such information. Professional model reformers such as August Vollmer and O.W. Wilson endorsed a concept known as *knowledge based policing.* This concept emphasized administrative efficiency and organizational effectiveness via information and technology. Early technological advancements included the introduction of motorbikes, vehicles, and later, the use of forensic science to help solve crimes (Uchida 1993, 27). Advances were not limited to transportation, however. Indeed, one of the more salient contributions during the professional era was the use of mobile communication devices. For example, the introduction of motorized patrol corresponded with the need for officers to stay in communication with headquarters (i.e., dispatch). Police organizations accomplished this task by developing two-way communication devices, which in turn, allowed officers to stay in the field and respond to multiple calls for service.

While police reformers recognized that collection of information would be a slow and accumulative process, in 1930 it became a reality when the Federal Bureau of Investigation (FBI) established the Uniform Crime Report (UCR). The UCR was the first[1] systemic attempt to collect police data from jurisdictions across the United States. The UCR served as a model for other data systems in the criminal justice system. For example, in 1931 the Wickersham Commission praised the FBI and encouraged other criminal justice agencies to model databases after the UCR (Dunworth 2000). Arguably, the UCR can be viewed as a significant accomplishment in the criminal justice system. The commitment to collecting and "digesting" crime data was important in several respects. First, reformers were committed to efficient and effective policing and crime data would shed insight into their own departmental operations. Second, cross-jurisdictional data collection could reveal something about the relative "health" of communities.[2]

While imperfect, the UCR remained "the [n]ation's only barometer of crime levels" (Dunworth 2000, 375) for the next three decades. The President's Commission on Law Enforcement and Administration of Justice in 1965 identified several shortcomings regarding the quantity and quality of information collected within the framework of the criminal justice system. While the UCR was an important measure of crime trends, the Commission reported a gross underreporting of crime (i.e., dark figure of crime) that made assessment of crime trends difficult. For example,

---

[1] While the UCR was one of the first attempts to systematically collect crime data in the United States, Decker argues the attempts to quantify crime data dates back to the early 19th century and possibly earlier (as cited in Dunworth 2000, 374).

[2] Cross-jurisdictional comparisons of crime data are fraught with problems that could affect the picture of crime including different crime definitions and different data collection procedures. Although the FBI has warned against making cross-jurisdictional crime comparisons, it has been routinely conducted since the inception of the UCR.

victimization surveys revealed crime to be extensively *underreported*. The Commission

solidified the need for timely, accurate, and meaningful information. In addition, the

Commission identified the federal government as a key player in coordinating such

data collection strategies (Dunworth 2000, 376). The federal government would go

on to spend millions of dollars in grants to increase data collection procedures across

police departments.

THE ROLE OF INFORMATION IN POLICE ORGANIZATIONS

Before proceeding further, it is important to distinguish between three

concepts: (1) information, (2) information management, and (3) analysis. *Information*

refers to a broad range of data available to police executives, patrol officers, and

administrative staff, such as crime events, victim/offender characteristics, criminal

histories, dispatch records, and the like. Information is used to evaluate recent and

emerging trends, forecast future events, prepare and present reports, and inform local,

state, and federal agencies. Information, however, is not exclusive to crime. For

example, police departments collect non-crime related information regarding police

personnel, performance indicators, and other work-related information (e.g.,

citizen-police complaints).

A related concept, information management, relates not only to information

itself but how the information is further utilized within police organizations. Thus,

information management refers specifically to types of technology devised to collect,

analyze, and report information. For example, a police department often has one

system to manage criminal incident and arrest data, a separate system to manage

dispatch data, and a third system to manage administrative data. However, collection

of information does not necessarily ensure the capacity for the third concept: analysis.

From a practical perspective, police departments regularly characterize a*nalysis*

of information in terms of crime analysis. Crime analysis involves the collection and

processing of information for the purpose of problem solving and planning. Information

is analyzed in ways that represent spatial, temporal, and topological patterns of crime.

For purposes of this chapter, the terms *information, information management, and*

information technology are used interchangeably, and reflects the marrying of both

 information and technology that produce an analytical outcome that police can use in

their daily operations. In the next subsection, we consider the role that information

management plays in police organizations by addressing its symbolic characteristics,

followed by the strategic and tactical role of information management.

The Symbolic Role of Information

Manning (2001) argues that information and technology are an inherent part of

attempts to "rationalize" policing. In this respect, information-technology is viewed

not just as a discrete process with specific functionality, but part of a larger institutional

shift in policing. In general, the early 20th century involved a broader movement

toward organizational accountability and rationalization; and policing was a beneficiary

of this movement. For instance, collecting and analyzing information created a more

bureaucratic work environment for police (Gaines, Worrall, Southerland and Angell

2003). Information is crucial to the rationalization process of policing; it is central to

budgeting, management, personnel allocation, and career guidance. Moreover, it serves

"the public in an explicitly calculative fashion" (Manning 2001, 84).

Innovation in policing is driven by internal and external pressures to resemble rationalized bureaucracies. There are "market-driven demands" placed on police organizations to increase efficiency and effectiveness and information technology plays a part in this transformation (Manning 2001, 88). Information technology is characterized according to two distinct symbolic policing purposes: (1) formal authority and (2) organizational respect and prestige.

Symbolically, information technology represents the formal authority system of organizations (Manning 2003). Here, the quality or usefulness of information gathered is not necessarily important. Instead, information represents organizational-technocratic imperatives dictating that certain commands and processes are followed, regardless of their practical application. Stated differently, information technology is bureaucratic in nature and sets standards of accountability. Police case studies documenting the degree of information technology initiatives support the conclusion that technology is regularly underutilized (Skogan, Hartnett, DuBois, Bennis and Kim 2003). It is not uncommon to hear officers' frustrations about conducting field interviews (FI)[3] because such information is filed away and never analyzed. Officers are sometimes concerned that FI's serve a management versus crime fighting purpose.

Information technology also holds the symbolic potential for providing a degree of respect as it implies access to resources, commitment to innovation, organizational leadership, and a degree of sophistication among employees. A lack of information technology can also signify a "backward" agency unable or unwilling to keep up with

---

[3] A field interview or field interrogation (FI) is when an officer encounters an individual on the street that may or may not be involved in delinquent/criminal activity. A field interview can be a useful way of documenting where and when contact was made, but also document any other additional intelligence gleaned during the encounter. From an investigative standpoint, field interviews can be a way of documenting who frequents certain areas, associates of individuals in the case where more than one individual is interviewed, or personal identifiers such as vehicles, style of dress, tattoos, or other distinguishing marks.

technological changes. For example, in 1992 the Commonwealth of Massachusetts

merged the Metropolitan District Commission (MDC)[4] police force with the

Massachusetts State Police in an effort to better coordinate resources. The

Massachusetts State Police absorbed much of the MDC personnel into their operations.

Former MDC officers deeply resented the merger because they were reassigned from a

technologically advanced organization with mobile computers to a department that was

technologically antiquated. A former MDC officer reported that "a good number of

patrol cars *still* don't have mobile computers, nearly 15 years after the merger"

(O'Connell 2004). This attitude is reflective of the pride associated with being part

of "technologically advanced" organizations. Indeed, there is a history of assigning

accolades to public organizations based on their level of technology. New York Police

Department's Compstat program has received awards from Harvard University

and recognition from former Vice President Al Gore due to their commitment to

implementing information-driven crime reduction and management practices

(Weisburd, Mastrofski, Greenspan and Willis 2004).

The Strategic and Tactical Roles of Information Management

While information technology is symbolic in nature, value lies in its ability

to increase organizational effectiveness and efficiency. The rapid development

in information technology "has promised and sometimes delivered significant

improvements in information processing capabilities" (Dunworth 2000, 379).

There are three areas where information and information management (as defined

by the ability to record and analyze such data) capabilities have the greatest potential to

---

[4] The MDC performed, among other duties, primary patrol over urban roadways and most of the state owned public parks.

positively influence police organizations. Information management holds the potential to help: (1) better understand cross-sectional and longitudinal features of crime, (2) assist patrol through enhanced communication and remote connectivity, and (3) enhance personnel management (e.g., problem officer early warning systems). For the purpose of this chapter, we focus exclusively on crime analysis related data sources and analytical strategies.[5]

Sources and General Applications of Crime Data

As discussed earlier, police reformers developed the UCR as a way of providing a national crime measure. Recall that the UCR is limited because it only provides an aggregate picture of crime levels. More precisely, it represents only aggregated crime totals for predefined crime categories. For example, index crimes are considered the most serious and include murder and non-negligent manslaughter, forcible rape, robbery, aggravated assault, property crimes of burglary, larceny-theft, arson, and motor vehicle theft.[6] Yet there are limitations to UCR data that hamper its practical application in terms of tactical and strategic decision making (Maxfield 1999).

Police departments have more recently been developing record management systems that collect additional elements about crime events such as temporal characteristics, spatial locations, victim/offender characteristics, features of motivations, and weapon involvement, none of which are reported as part of the UCR. Crime information is often managed in Record Management Systems (RMS). Dunworth (2000,

---

[5] Walker, Alpert, and Kenney (2001) describe how police information can be used to predict problem behavior among police officers.

[6] Included among the non-index crimes are negligent manslaughter, nonaggravated assault, forgery and counterfeiting, fraud, embezzlement, stolen property, vandalism, prostitution, weapon offenses, sex offenses, drug laws, gambling, etc.

380) argues that a comprehensive and fully functioning RMS system "should include crime and arrest reports, personnel records, criminal [history] records, and crime analysis data." RMS systems can also store information that is important to officer safety, such as integrating weapon ownership information. In the case of domestic violence calls, such information would be useful in determining whether residents of the location legally own a firearm. A recently implemented RMS system in New Bedford, Massachusetts includes facial recognition software that can scan individual digital images and identify people who share common facial features but different names. These integrated systems present functionality that centralizes most crime-related information.

The generation of crime data (e.g., dispatch, criminal incident, arrest data, etc.) is usually initiated via citizen emergency calls for service to the police. In the case where a citizen discovers a crime, such as burglary, they are likely to call "911" and request that an officer respond to the scene.[7] The dispatch officer will determine the priority of the call based on the seriousness of the crime, as well as whether the incident is still in progress (a "hot call"). A police officer then responds to the crime, conducts a preliminary investigation to determine whether a crime has been committed, and "takes a report" if the decision is made that a crime has occurred. A police report typically contains basic information about the complainant or individual making the call, the location of the event, property damage information, victim information, and any known information about suspects. In most cases, the preliminary reports are handwritten on standard incident report forms at crime scenes.

The use of information systems for the purpose of recording crimes can vary

---

[7] This typical scenario differs by crime type. While citizens usually bring crimes to the attention of the police, other types of crime (e.g., truancy, curfew violations, drug sales/buys, prostitution, loitering, etc.) are more likely to be discovered through proactive police investigations.

across agencies. In some departments handwritten (or typed) reports are then sent to a team of data entry clerks for data processing. Officers in other departments are responsible for processing their own reports during their shift by returning to the station and recording the information in the departmental records management system. In more advanced departments officers have mobile data terminals or mobile computers in their patrol cars that allow officers to complete the electronic submission of the report while in the field.

Many larger departments, and some smaller agencies, have a specialized unit responsible for managing crime and other data sources (Hickman and Reaves 2003). These units are usually known by a name resembling "Management Information Systems (MIS)." MIS units are comprised of sworn personnel and non-sworn technical personnel who work in tandem to manage the large volume of information that comes into police departments. Data entry personnel are usually included in this unit. MIS units perform multiple functions that include maintenance of infrastructure (i.e., equipment, networks, software, and communication systems), data entry of police reports (if applicable), "cleaning data" by verifying the accuracy of the entry, and other tasks. Organizationally, MIS units are located within the administration (in contrast to enforcement) of police departments. The crime analysis unit in the Detroit Police Department, for example, is located within the Major Crimes Division while the Records Management Unit is located under the Administrative Assistant Chief.[8]

---

[8] See http://www.ci.detroit.mi.us/police/pdf/complete%20flowchart_www-4.pdf for Detroit Police Department's organizational chart.

Other Crime-Related Information: Dispatch Systems, Field Interviews, and Case Management Systems

Police organizations collect and use a variety of information. The following underscores three major information sources available to, and used by, police personnel. These include dispatch data, field interviews (i.e., intelligence), and case management systems. Police dispatch data are one of the most voluminous sources of information. Dispatch systems are commonly known as "E-911" or computer-aided dispatch (CAD) systems. These systems can be conceptualized as the link between citizens and government services. Early 911 systems can be traced to the 1950s but were not universally adopted until the 1990s where they are present in over 85% of all jurisdictions (Dunworth 2000, 385).

From an organizational perspective, dispatch data reflect citizen requests for service. Dispatch data *do not* necessarily provide an accurate picture of the total volume of crime in a location, but instead, reflects the level of citizen service needs. Police are often dispatched to a much larger volume of potential complaints than official crime statistics reveal (Maxfield, Lewis and Szoc 1980). On average, the City of San Antonio records approximately 85,000 official crime incidents per year, but over 850,000 calls for service. A substantial part of this discrepancy can be explained by police officers making the determination that a crime did not occur once they have responded to the location and conducted an investigation (Klinger 1997).

In many ways, dispatch operations serve to filter information between the police and public. Citizens requesting police services initiate such requests through centralized dispatch centers (e.g., E-911 systems). While the nature of dispatch varies

between agencies, dispatchers are responsible for directing non-emergency/emergency calls. For some minor non-emergency situations the dispatcher might instruct a caller to make a report at a local department substation or make a report via telephone or internet-based report system. Dispatchers also determine if a call is a high priority such as "man down" (presumably from a violent crime), "shots fired" or "crime in progress" and assign the necessary patrol resources to handle the situation in an expedited fashion. Dispatch data can be useful for determining police workload and response time.

Field interviews (FI) are a source of information derived from police-citizen contacts. As previously mentioned, police-citizen FI contacts serve as an intelligence-gathering tool. Information is recorded on FI cards (actual card or other form) that contain personal information of those contacted including name, date of birth, residence, and other distinguishing features including style of dress and tattoos. FIs can be useful for documenting individuals who, for example, "hang out" in high crime neighborhoods or crime prone locations such as city parks or shopping malls. Field interview forms also capture information on vehicles (e.g., make, model, year, and vehicle identification number) associated with the encounter. Interviews are proactive in nature and may prove useful in the future. More advanced RMS systems will include a FI component that has the capability to query individuals and vehicles against other data systems.

In terms of case management systems, police regularly collect and/or access information that is managed by external third parties. Automated fingerprint systems, national and state criminal history data, and firearm identification systems

are regularly used by police organizations. Automated Fingerprint Identification Systems (AFIS) collect and store images of fingerprints. AFIS systems are coordinated at the state and national level. The Integrated Automated Fingerprint Identification System (IAFIS) is a national database that stores ten-print fingerprint images and integrates this information with criminal history information. Fingerprints are collected for criminal (e.g., pursuant to an arrest) and non-criminal (e.g., when individuals apply for employment requiring criminal history checks) purposes. Prior to implementation of the IAFIS system in 1999, manual fingerprint searches took approximately three months. Requests are now submitted electronically and take approximately 2 hours, thereby increasing public safety.

The National Crime Information Center 2000 (NCIC 2000), a revised version of the NCIC system, is maintained by the United States Department of Justice's Criminal Justice Information Center and provides a variety of information to law enforcement agencies. Among these law enforcement services are criminal history, fingerprint searches that query "wanted persons" files, and probation and parole information. The enhanced NCIC 2000 system also supports graphical files such as mug shot photos, images of signatures, and images of personal possessions (e.g., automobiles). In general, the availability of digital images and other data elements can increase officer safety. For example, the NCIC 2000 system includes interoperability features that directly interface with mobile computer systems in patrol cars. Overall, NCIC 2000 represents an assortment of sources for investigators and patrol officers. The efficacy of the NCIC 2000 system is highly contingent on the quality of initial data entry.

Using Information in Police Organizations

The capacity of police organizations to collect information has evolved considerably since the UCR. Government units have invested billions of dollars over the past few decades to build the information-technology infrastructure for law enforcement. The Office of Community Oriented Policing Services (COPS), one of the United States Department of Justice's major grant funding agencies, reports that it has committed over $1 billion in technology grants since 1995 (Office of Community Oriented Policing Services 2002). The COPS office allocated nearly $400 million to crime fighting technologies in 2003 (United States Department of Justice 2005). Information technology now represents a key area of police expenditures.

Information is the lifeblood of the modern police agency. In essence, the collection and management of information plays a critical role in many police organizations. Current technological infrastructures permit organizations to collect and record a plethora of data. Such information has the potential to "revolutionize" policing in ways not fully realized (Dunworth 2000, 379). The challenge presented to executives and analysts is what to do with this information and, furthermore, how can this data assist an organization in achieving multiple organizational goals. Related to this challenge is analyzing data in ways that are useful for patrol officers.

Crime analysis offers significant ways to improve the daily operations of law enforcement agencies. It provides the capacity for "systematic analysis of data drawn from a series of criminal incidents rather than focusing upon a single incident" (Dunworth 2000, 390). Reuland (1997) identified four functions of crime analysis: administrative support, investigation, clearing, and prevention.

Administratively, information can be used to create patrol officer deployment strategies. Deployment strategies are commensurate with the size of the jurisdiction, nature of the crime problem, and complexity of the organizational structure. In smaller jurisdictions, for example, deployment strategies are relatively one-dimensional (e.g., patrol officer). Large cities, in contrast, have to coordinate coverage of multiple precincts and a variety of specialized units including traffic, investigations, and administrative support.

Crime analysis is also useful from the perspective of crime prevention and intervention. Police departments have invested heavily toward increasing their capacity to successfully reduce levels of crime. Depending on the problem, an analysis plan might involve dispatch data, incident/arrest data, information on probationers/parolees, criminal history systems, and field interviews or other intelligence files. Information is limited only by the data available to crime analysts and their creativity in understanding how it can be applied.

In contemporary police organizations, specialized crime analysts may be sworn police personnel or non-sworn civilians. It has evolved into a largely specialized function that requires analysts who possess sufficient skills, analytical competencies, and an understanding of police-related business (Hickman and Reaves 2003). In smaller-to-midsize agencies, sworn officers who have demonstrated these competencies are responsible for crime analysis. In contrast, in large departments, civilians assume analyst roles. The following subsection describes ways that information and technology are used within the San Antonio Police Department (SAPD) to help understand crime patterns and trends.

Crime Analysis in Action: San Antonio Police Department

"Knowledge" represents the "linchpin of effective crime control and prevention" strategies (Glensor, Correia and Peak 2000, 123). Organizations can be differentiated based on their ability to collect, analyze, and disseminate information. The challenge faced by police departments is bridging the analysis of information with individual officer decision-making in an intentional way (Greene 2000). Greene (2000) articulates a model of moving the consumption of information beyond management, and down to line-level officers providing policing services. Based on SAPD's various kinds of data collection, quality of Research and Planning Unit analysts, and overall use of technology, we argue that such developments have the potential to influence data-driven patrol operations.

The SAPD employs over 2,000 sworn personnel; approximately 1,000 are assigned to patrol. Geographically, the city is divided into six service areas and 113 patrol districts (see Figure 1). These patrol districts vary in size from .3 to 26.3 square miles with populations ranging from less than 1,000 to over 22,000. Each of the 113 patrol districts is manned by at least one officer per eight-hour shift throughout the year. The geographic dimensions of patrol districts are drawn in such a way as to normalize the anticipated workload. As Figure 1 shows, Loop 410 creates a beltway around the City of San Antonio. This roadway represents the major route connecting all of San Antonio.

Figure 1. Service Area (n=6) and Patrol Districts (n=113) Maps of San Antonio, TX.
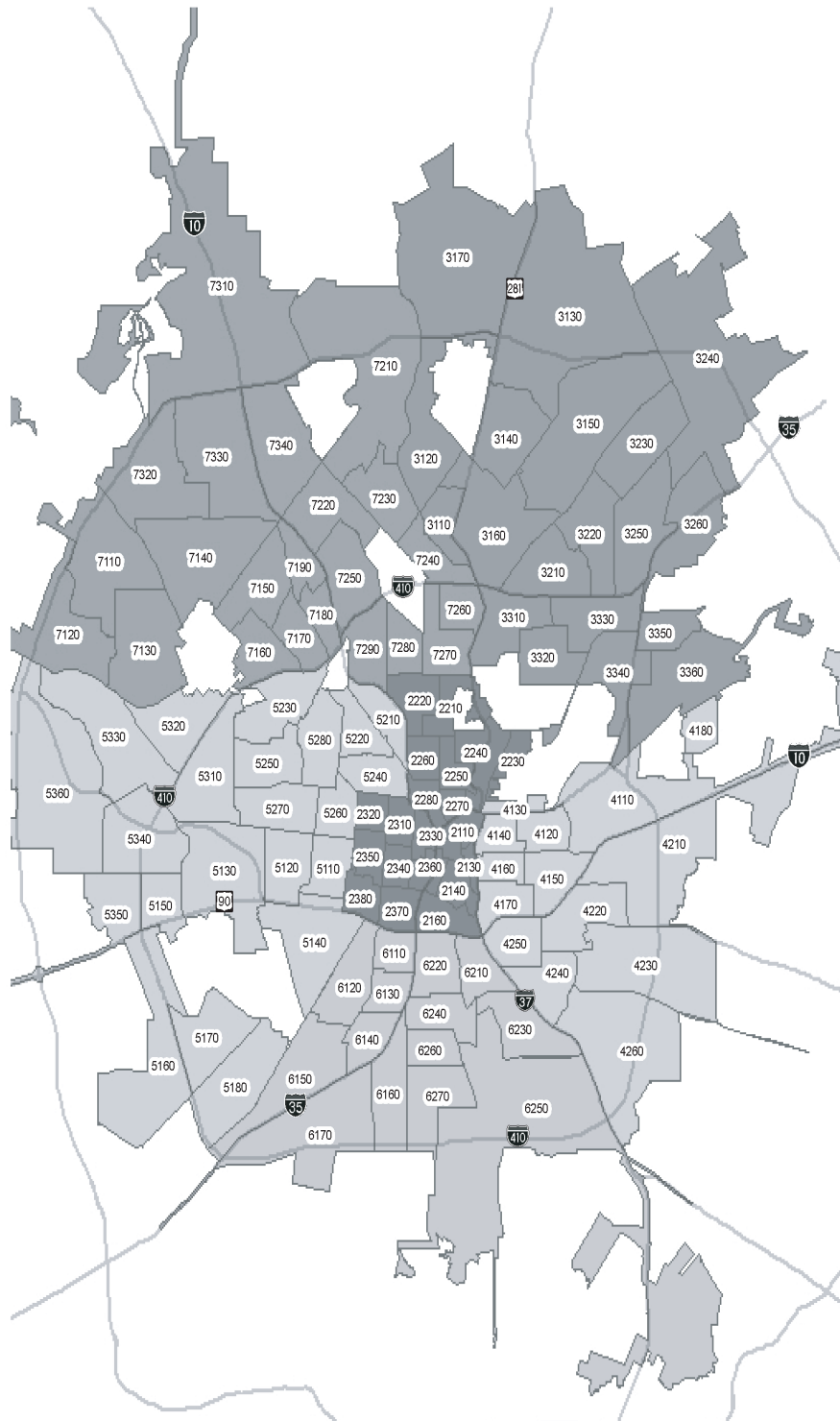
To truly "revolutionize" policing as suggested by Dunworth (2000), information technology must have the capacity to create data-driven patrol approaches. By data-driven patrol, we are referring specifically to patrol and investigative strategies that are grounded in temporal and spatial characteristics of crime. Crime analysis units and/or personnel represent basic commitments to implementing data-driven patrol.

"Crime analysis" refers loosely to the analysis of crime patterns. There is no commonly agreed upon crime analysis "template" or standardized analytical strategy to address crime problems. Common strategies for presenting police information are through summary statistics that document citywide crime frequencies. Table 1 shows the total number of serious personal and property crimes that occurred in San Antonio between 2002-2004. These crime codes do not represent an exhaustive list of all crimes that occurred during the specified period; instead, they reflect serious crime categories that drive community and law enforcement concerns. Considering the frequency of different types of crimes, the data indicate that burglary is the most reported, followed by auto theft, aggravated assault, and robbery.

Table 1. Yearly Crime Trends in San Antonio, TX.

Crime Type	2002	2003	2004	% Change (2002-2004)
Murder	100	85	95	-5%
Aggravated Assault	7194	4570	4948	-31%
Rape	464	537	677	46%
Robbery	2114	2071	2132	1%
Arson	582	550	538	-8%
Auto Theft	5743	6202	5667	-1%
Burglary	13368	14619	14720	10%

Another concern is crime *trends*. Trends represent an evolving change in crime patterns. Table 1 presents the change in crime between 2002-2004. Interestingly, trends were not consistent across crime types. For example between 2002-2004, San Antonio experienced a 5 percent decrease in homicide and a 31 percent decrease in aggravated assault, but witnessed a 46 percent increase in rape. For property crimes, there was a 10 percent increase in burglary, but an 8 percent decrease in arson and 1 percent decrease in auto theft.

The information presented in Table 1 lacks tactical significance. This information gives command staff or patrol officers no ability to understand changing crime patterns faced in the past, thereby limiting any ability to make changes in patrol strategy to address emerging crime patterns. Figure 2 presents a snapshot of 30-, 60-, and 90-day crime trends based on the analysis date of January 11, 2005. The table disaggregates many of the crime categories from Table 1 into more distinct groupings. Murder, for example, is disaggregated into capital murder, murder, and manslaughter. Robbery is similarly disaggregated into aggravated robbery and robbery of businesses and individuals. The "aggravated" designation refers to the use of a weapon during commission of the crime. Disaggregating tactical crime trends gives additional insight into emerging crime problems.

Figure 2. Tactical Analysis of Recent Crime Trends in San Antonio, TX.

CITYWIDE

CRIMES AGAINST PERSONS

CRIME TYPE	LAST 30 DAYS	LAST 60 DAYS	LAST 90 DAYS	2003 YTD	2004 YTD	% Change
Capital Murder		1	3	28	17	-39%
Murder	3	7	15	66	71	8%
Manslaughter		1	4	16	13	-19%
Agg Sexual Assault	20	62	99	774	793	2%
Sexual Assault	21	59	121	815	784	-4%
Agg Robbery Individual	80	167	251	818	989	21%
Agg Robbery Business	36	81	126	578	476	-18%
Robbery Individual	50	108	166	784	790	1%
Robbery Business	5	19	34	155	144	-7%
Agg Assault	36	102	187	1,021	938	-8%
Assault	428	1,057	1,878	10,176	9,495	-7%
Agg Family Assault	6	35	59	336	282	-16%
Family Violence	620	1,476	2,426	10,715	11,358	6%
Deadly Conduct	45	101	166	820	855	4%

PROPERTY CRIMES

	LAST 30 DAYS	LAST 60 DAYS	LAST 90 DAYS	2003 YTD	2004 YTD	% Change
Burg Habitation	492	1,301	2,209	10,361	10,134	-2%
Burg Building	201	742	1,119	5,073	4,993	-2%
Burg Vehicle	1,134	3,267	5,507	23,837	25,469	7%
Theft Vehicle	259	745	1,287	6,655	6,219	-7%
Arson	26	57	94	563	466	-17%

OTHER CRIMES

	LAST 30 DAYS	LAST 60 DAYS	LAST 90 DAYS	2003 YTD	2004 YTD	% Change
Drug Arrest	448	935	1,421	6,045	6,327	5%

Analyses of crime data focus on questions of when (temporally) and where (spatially) crime occurs. Crime is not a social phenomenon that occurs at random. Crime follows certain temporal patterns by time of day, day of week, and season. Traffic problems, for example, may be more prevalent during early morning or late afternoon when people are commuting to/from work. Citizen complaints for disorderly youth might be greatest after school dismisses. In fact, research suggests that temporal patterns to juvenile crime corresponds closely with school dismissal hours (Snyder and Sickmund 1999).

The chart presented in Figure 3 represents temporal characteristics of 2004 armed and unarmed robberies that occurred in San Antonio. The chart reveals the relationship between weekday and time of day the robberies occurred. The three time categories reflect periods between 8am-3pm, 4pm-11pm, and midnight to 7am.[9] Visual inspection of the chart indicates an interesting data pattern. Late night robberies (those occurring between midnight and 7am) occur on weekend nights and least frequently during weekday nights. Robberies that occur on weekdays occur earlier than those that occur on weekends. The smallest percentage of robberies occurred during day light hours regardless of weekday. There was, however, a notable peak in robberies that occurred during the workday on Mondays.

---

[9] Each category goes through the end of a particular hour. For example, the first category covers the period between 8am and 3:59 pm. The three groups are exhaustive and mutually exclusive of one another.

It is possible that such temporal patterns are influenced by land use. Robinson's (2004) notion of "spatial interplay" suggests that geographical concentration of crime is associated with land use (e.g., commercial versus residential). Socialization patterns may vary based on day of week, which increases chances of victimization. Further inquiry into this situation could possibly reveal victims of weekday robberies that occur between 4pm and 11pm are employees of local companies socializing with colleagues who become unwitting victims. Similarly, robberies that occur on weekend nights might be reflective of cultural norms that delay socialization patterns to later on weekends. Nevertheless, understanding such temporal patterns provides insight into how patrol resources should be deployed and how prevention efforts might be implemented.

Figure 3. Temporal Characteristics of 2004 Armed Robberies in San Antonio, TX.
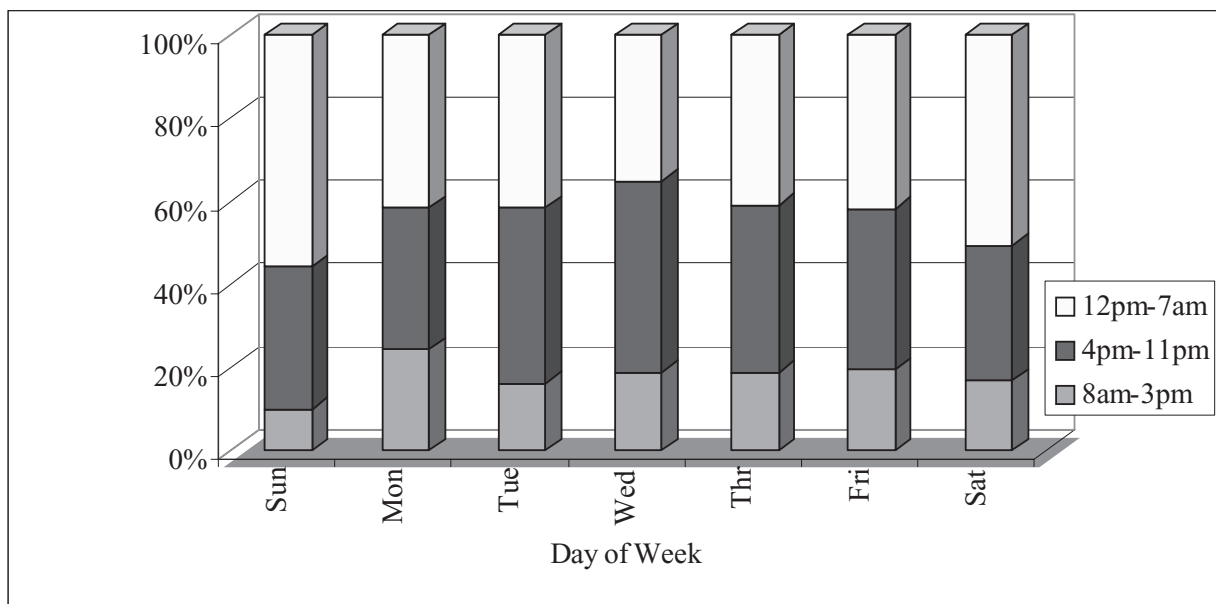
Crime also follows certain spatial patterns. The idea of crime "hot spots" for example denotes that crime is not randomly assigned but instead is disproportionately concentrated in certain locations. Most police departments divide their jurisdiction into smaller geographical units known as "zones," "precincts," "sectors," or " districts," and assign officers to such geographical locations across shifts. The SAPD divides the city into 6 service areas and 113 patrol districts (see Figure 1). Some agencies use geographical units based on Census Bureau "tracts" or "block groups." Geographical assignments ensure that resources are not heavily committed to certain areas, while ignoring others.

Figure 4 depicts the locations of all 2004 robberies that occurred in San Antonio. Each dot represents one robbery event that was recorded by SAPD. This style of computer map is sometimes referred to as a "pin map." When computers were not available, departments placed pins on large city maps that were mounted on walls. Each pin represented a crime event and police personnel used such maps as a way to track crimes geographically (Mamalian and LaVinge 1999). Several important features should be readily apparent. First, there were no reported robberies in a large part of San Antonio during 2004. Similarly, robberies were highly concentrated in the central part of the city. The graphic suggests that robberies tend to cluster in groupings. Although Figure 4 provides some inferences where robberies are disproportionately concentrated, it is difficult to make absolute conclusions regarding density.

Figure 4. Spatial Distributions of 2004 Robberies in San Antonio, TX.
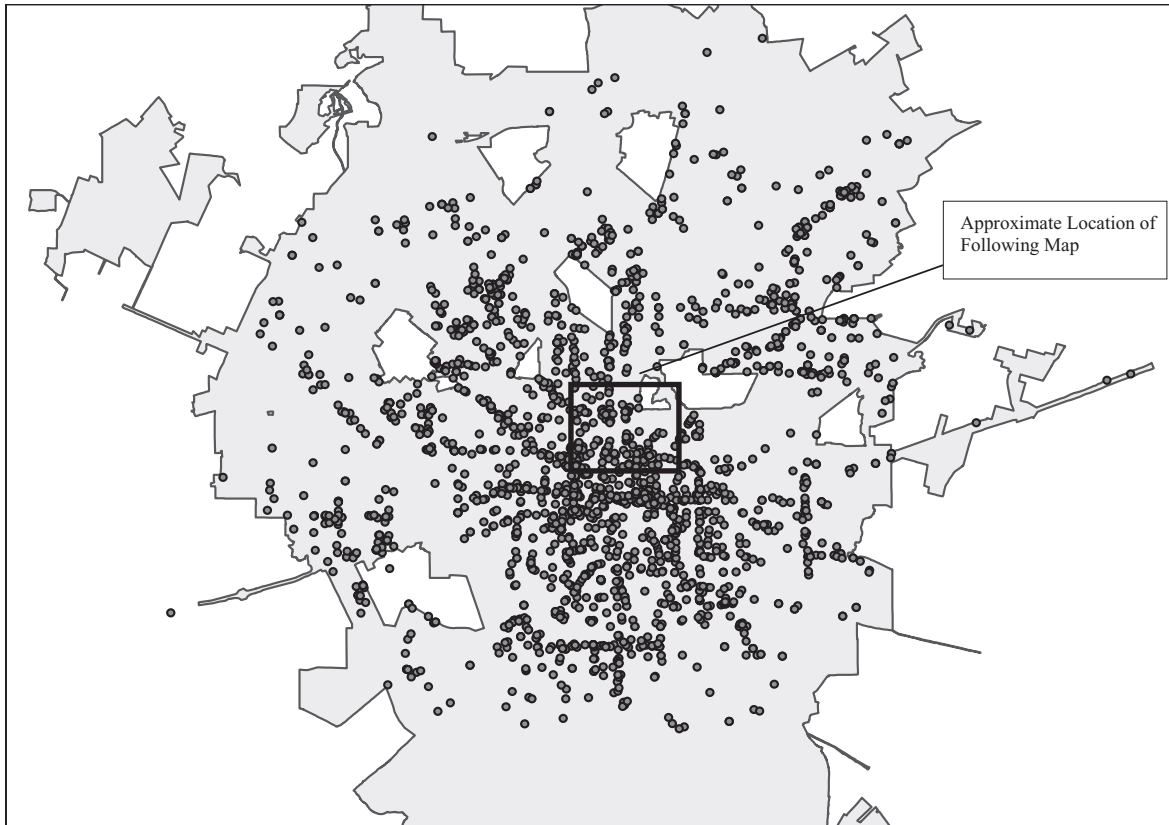
While citywide pin maps depicting the locations of crime events are interesting, their limitations are notable. They are of little value if one is attempting to utilize such information to direct crime reduction patrol strategies. To account for this problem, hot spot analysis has been developed as a way of determining specific locations where crime is disproportionately concentrated. Hot spot analysis amounts to a statistical evaluation that evaluates the clustering of events. Hot spot analysis can be conducted using a host of analytical tools, yet one of the most common is a free software program developed on behalf of the National Institute of Justice known as *CrimeStat*.

Figure 5 presents a hot spot analysis of San Antonio's 2004 robbery incidents. The map includes crime incident location but also shows an overlay of nine specific robbery hotspots computed with *CrimeStat*. The computation was based on statistically significant clustering of 20 or more robbery events. The advantage is that it specifies possible geographical points where robberies concentrate. Such analysis would then prompt additional analysis with the intent of identifying what may be responsible for these events. It could be that features of land use explain high concentrations of robbery.

Figure 5. Hot Spot Analysis of 2004 Robberies in San Antonio, TX.
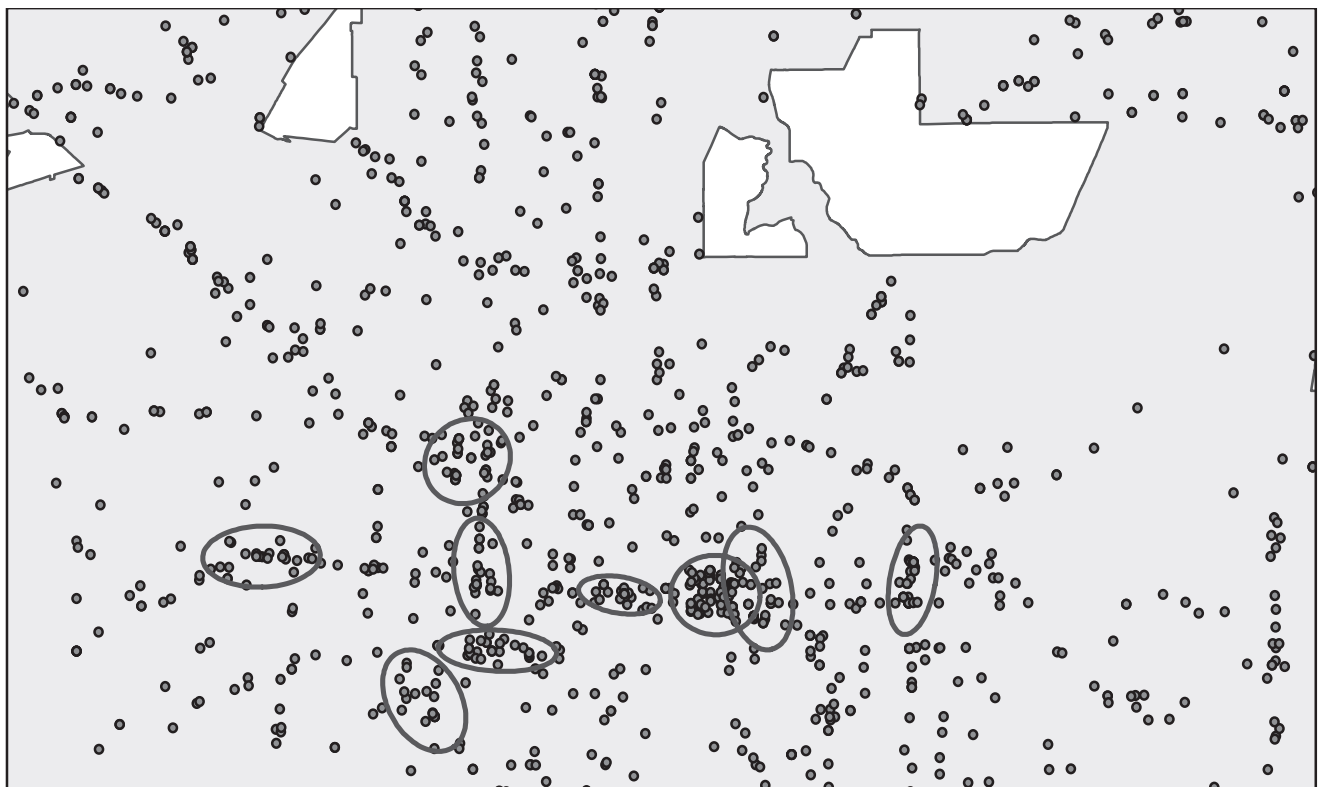
Another strategy for understanding the dynamics of crime hotspots is to map such events with residential locations of known perpetrators. Figure 6 depicts the same nine

robbery hotspots with an overlay of residential locations of individuals on probation for

robbery. One of the crime truisms is that offenders commit crimes in close proximity to

where they live. Thus, a police crime reduction effort could possibly begin with identifying

individuals with known histories, and who reside near these locations.[10] The figure

indicates that some hotspots encompass the residence of one or more known robbers while

several do not. If this information was being used for investigative purposes, detectives

could link characteristics of the events reported by victims to help solve the crime.

Figure 6. 2004 Robbery Hotspots & Home Address of Robbery Parolees in San Antonio, TX.

---
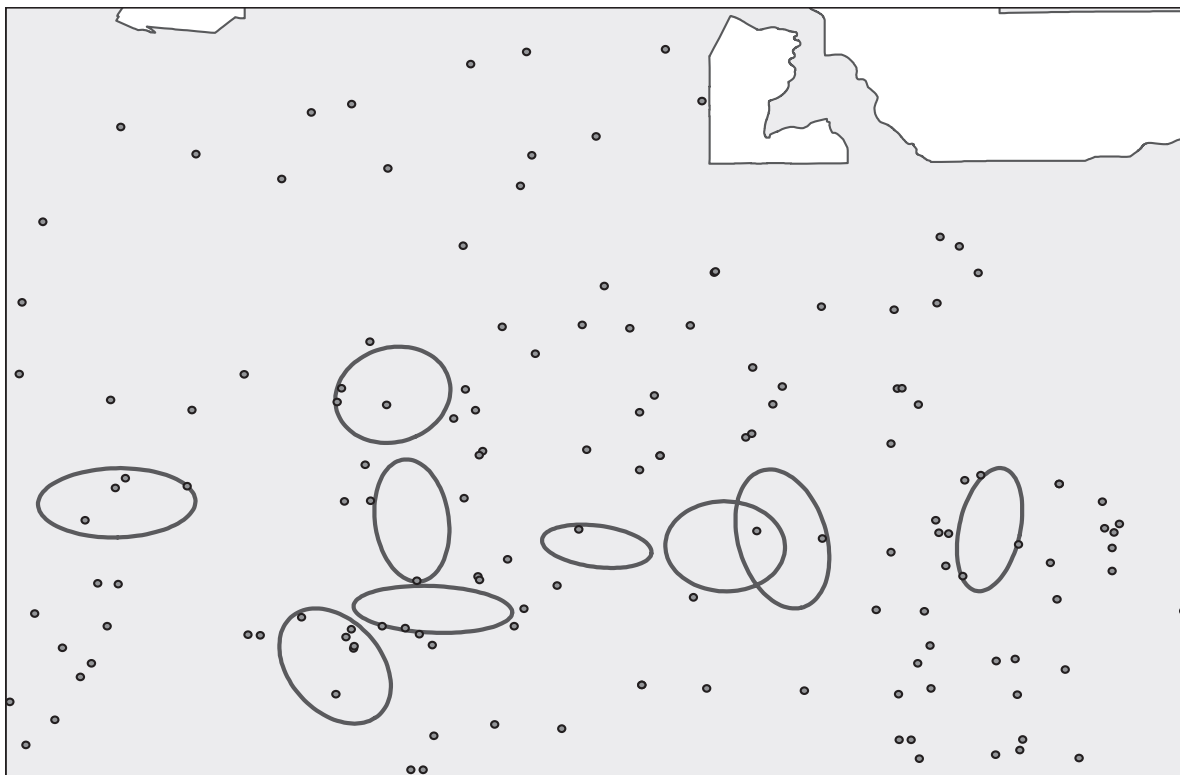
[10] This discussion is much more complex than suggested here. Rengert (2004) argues the distance that offenders travel to commit their crimes is closely connected to the type of crime. Individuals are likely to travel further distances for confrontational crimes to avoid being recognized. However, knowing where offenders live provides a meaningful point of analysis for any problem-solving effort.

Finally, we use a slightly different hot spot analysis technique to demonstrate the relationship between "time" of data and concentrations of motor vehicle theft. The hot spot analysis technique is a spatial tool provided by a leading spatial software program. As shown in Figure 7, the light gray areas are locations with low concentrations of auto theft while the dark gray, white, and black areas are the highest. One advantage of this strategy is that it presents a more complete picture of all crime events. Combining this information with a time of day analysis could possibly reveal points of police intervention.

Figure 7. Temporal and Spatial Distributions for 2004 Burglaries of Vehicles in San Antonio, TX.

A Shift Hotspots (6am-2pm)

B Shift Hotspots (2pm-10pm)

C Shift Hotspots (10pm-6am)

The most interesting finding is that there appears to be a strong spatial quality to auto thefts in San Antonio. Auto thefts that occur during A and B shifts were highly concentrated along Loop 410. Loop 410 connects most areas of San Antonio with an interstate and parallel service roads that run along the main thoroughfare. The service road creates an easy exchange of traffic between the major roadway and surface roads that result in a complex but reasonably efficient traffic network. Numerous commercial establishments are located on the 410 service road throughout San Antonio. Thus, the high concentration of auto thefts along Loop 410 is likely related to the high concentration of commercial retail establishments. There is also a high concentration of auto thefts in the center city during A shift (6am to 2 pm). Features of land use and routine activities of residents and tourists should also be considered when examining the A and B shift crime patterns. Large numbers of shoppers frequent the commercial establishments during the day and evening hours creating sufficient opportunities for criminals to strike.

The figure for shift C (10 pm to 6 am) shows remarkably different patterns when compared to A and B shifts. The Loop 410 patterns observed during the A and B shifts largely disappear. While there appears to be higher concentrations of auto thefts in North San Antonio during C shift, nighttime auto thefts follow greater levels of geographical dispersion. One might argue that thefts are more likely due to the cover of darkness.

Overall, the data presented above is not an exhaustive crime analysis strategy. Instead, it represents one approach to integrating a variety of analytical techniques when processing information. Note that the evidence presented moved from a discussion on broad crime trends to a more narrow focus on type of crime, time of crime, crime location, and offenders.

MOVING BEYOND THE SYMBOLISM OF INFORMATION: THE FUTURE OF INFORMATION MANAGEMENT IN POLICE ORGANIZATIONS

At the dawn of the 21st century, police organizations are under pressure to institutionalize information technology. On one hand, internal pressures result from new management models that place greater demands on efficiency and accountability. On the other hand, external pressures are characterized by the publics' demand for law enforcement organizations to resemble more professional bureaucracies. Recent attention to terrorism and national security has also placed pressure on police departments to collect, analyze, disseminate, and act upon terrorism-related intelligence. The fact remains that police departments are ill-prepared in responding to terrorism. While the federal government often assumes the role in collecting and disseminating terrorism-related information, local law enforcement is the first-line of defense. Consequently, local and state agencies need the appropriate infrastructure to collect and share data in a timely manner.

As the law enforcement community looks toward the year 2020, a series of recommendations are intended to increase the use of information technology. We recommend that attention focus on three core areas. Police organizations must: (1) continue to expand the technological infrastructure, (2) expand technical and analytical capacities, and (3) become information-driven aimed at proactive police strategies.

Recommendation One: Expand Information Infrastructure

The most important concern is for police organizations to build the capacity to collect and analyze information. An adequate collection process rests on the quality of the physical infrastructure, adequacy of software, and degree to which the equipment and

286

software "fit" the business model. The Department of Justice's Office of Community Oriented Policing Services (COPS) has developed an excellent guide to assist law enforcement agencies that are in the process of planning or implementing such initiatives (see Harris and Romesburg 2002).

Infrastructure

Computer technology accelerates at such a quick pace that it is difficult to stay ahead of the curve. The sophistication of software applications and demand to expand the breadth of data collection requires that systems be developed to handle not just current technical needs, but anticipated future needs. It is vital that planning stages be coordinated by an individual (or individuals) who understands information technology and data collection (e.g., how cases are processed, how information is shared throughout an organization, etc.). Currently, there is an assortment of crime mapping software applications available. Some proprietary record management systems include crime analysis modules that provide a seamless integration of data collection and analysis functions. It is important that crime analysis software applications, systems both integrated with RMS systems or those that function independently, have the capacity to create customized reports. This capacity provides managers and analysts with the ability to create reports to fit local needs.

Newer RMS systems do not include adequate analysis functions. For example, the NIBRS-compliant RMS system in Massachusetts provides little-to-no ability to create customized crime analysis reports. In addition, the standardized off-the-shelf reports are inadequate for any analysis beyond basic summary statistics. To further complicate matters, there is a limited capacity to extract and upload data into standard database

287

systems, thereby limiting the ability to perform rudimentary crime analysis. Hence, RMS systems amount to expensive file cabinets that function merely to store information. Infrastructure planning should also consider the different kinds of analysis tools. Common off-the-shelf crime mapping and spatial analysis tools provide the ability to import, spatially analyze, and present crime data. These programs are quickly becoming standard crime analysis tools.

Other types of software infrastructure that directly impact police performance are data mining sources, such as Arizona's Coplink and Chicago's Citizen Law Enforcement Analysis and Reporting (CLEAR) system. Coplink is a web-based software that permits police personnel to consolidate, share, warehouse, and identify relationships within other sources of criminal information. CLEAR is a comprehensive database that contains millions of incident reports and other information dating several years that can be linked with a single query. More importantly, such queries can be performed from any of the 2,000 wireless, touch screen notebooks in Chicago Police Department vehicles.

Another way to utilize technology in the interest of public safety is for all states to employ Victim Information and Notification Everyday (VINE) systems by the year 2020. In 1997, Arkansas was the first state to implement VINE. In general, VINE system consists of a network of computers placed in county jails, prosecuting attorney's offices, the Department of Correction, the Attorney General's Office, and the Department of Community Correction, and local courts. Information is shared among these agencies in order to input and disseminate information on an offender's custody status. Using a touch-tone telephone, victims may register with the VINE system. After registration is completed, a victim will be notified of custody and/or

court status changes of an offender. Victims may also inquire about the status of an offender 24 hours a day, 7 days a week.

In terms of expanding the technological hardware used in the field, federal grants from the U.S. Department of Justice have allowed police officers to take a variety of information to the streets. Using handheld computers officers are better equipped to process information. For example, the Wayne County Sheriff's Office in Michigan has successfully used these hand-size computers when serving warrants and identifying suspects via mug shots and criminal histories. It is highly possible that by the year 2020, these hand held computers will be equipped with in the field finger printing functions, as well as detection of bio-hazardous materials and gases for first responders.

Data Quality

Data quality is a critical, yet overlooked, aspect of information management. The saying "garbage in, garbage out" is more important than it might first appear. There is an alarming lack of oversight of data collection/data entry processes in many organizations. Responsibility for the supervision of data entry varies between agencies. Below are some common practices:

Generates Data	Quality Control Responsibility	Recording Mechanism
Patrol Officer	Patrol Shift Supervisor	Data Entry Personnel
Patrol Officer	Data Entry Staff Supervisor	Data Entry Personnel
Patrol Officer	None	Data Entry Personnel
Patrol Officer	None	Directly Into RMS System by Officer
Patrol Officer	Computer System Validation Rules	Directly Into RMS System by Officers

The five models indicate both different levels and types of supervision. Data quality control functions relate most specifically to ensuring reports are complete and accurate.

Common mistakes include missing data, miscoding crime types (e.g., simple assault versus aggravated assault), or miscoding of weapons. For example, a distinguishing characteristic between simple and aggravated assault is the presence and/or use of a weapon. Moreover, assault and battery are differentiated from other forms of assault in that the victim must be harmed through physical contact. Issues of quality control would ensure that weapon codes are properly recorded when weapons are used or that the nature of "harm" is recorded in situations of assault and battery. There is no "best" model for quality management, yet the chosen model should be able to measure data quality levels. The bottom line is that subsequent analysis depends on the initial quality of data entry.

Recommendation 2: Enhance Analytical Capacity

Community and problem-oriented policing advocates have long supported the adoption of problem-analysis strategies that move beyond reactive policing. Therefore, we propose a model where police personnel are trained and encouraged to consider proactive strategies aimed toward reducing the *causes of crime*. The "crime triangle" concept suggests that a motivated offender and vulnerable victim must come together in time and space for a crime to occur. Thus, proactive policing strategies should consider features of offenders, victims, and locations that are conducive to crime.

The analytical capacities of organizations are also contingent on their ability to use data sources to *answer* questions. Personnel should be trained in the practical application of crime analysis and crime forecasting techniques. Crime analysis capabilities often develop in ad hoc ways. In departments where crime analysts are sworn officers, it is not uncommon to find that such officers do not have specialized crime analysis training. Instead, such personnel are selected (sometimes against their will) because

they are known to have a "knack" for computers. Thus, the actual use and application of information is limited by technical abilities.

Another way police departments can develop their analytical capacity is to civilianize their research and planning units. There are two major benefits of hiring civilians for the purpose of managing data. First, by hiring civilians, departments avoid significant sworn officer turnover within these specialized units. When sworn officers are re-assigned, promoted, or retire, units are compromised with high attrition rates and burdened with re-training duties. The second benefit is that civilians are more likely to hold an area of expertise and have some aspect of formal training, such as a degree in geography or information technology. Numerous universities across the country offer degrees that take advantage of cutting-edge software. Currently, San Antonio, Dallas, and Boston Police Departments' research and planning units are civilianized. However, these units still report to sworn police management that resides under the Office of the Chief.

Recommendation 3: Creating Information Driven Organizations

There are two crucial components for transforming police departments into information-driven organizations. First, we recommend institutionalizing procedures for moving information (e.g., crime analysis) out of the conference room and into the hands of patrol and investigative personnel. Second, police must make the organizational changes necessary for utilization of information management resources. Such strategies relate to resource allocation (e.g., deployment) and changes to reward systems.

Moving Information Out of the Conference Room

Earlier in this chapter we identified the adoption of technology throughout the field of law enforcement, yet the practical significance of such change remains unclear. One

291

reason is that police managers have not been successful in demonstrating the tactical or strategic significance of analysis strategies. Just a short time ago "crime reports" were limited to "green bar" paper reports that were generated on mainframe style computer systems. These reports were not useful due to their size and complexity. While mangers might have considered these reports useful for documenting crime trends or basic features of crime events, they were limited for patrol officers and detectives. Thus, crime analysis was largely a management function and had little practical appeal for patrol.

The development and integration of personal computers and software that allows users to easily manipulate data presents opportunities to share information. Analysts have the technical capacity to manipulate data into charts, tables, graphs, or maps. Despite such capabilities, the average patrol officer does not take advantage of this information. Hence, it is the police managers' duty to figure out *how* information should be institutionalized tactically. Crime analysis reports should be made regularly available to those closest to the crime problem – patrol officers and detectives.

Changing Reward Systems

Police managers may experience resistance when trying to convince line-level personnel to *use* information technology because there is a lack of incentives built into the current reward system. Employees are likely to operate in a way consistent with reward systems. Departments that prize traffic tickets and base annual reviews on such criteria should not be surprised to find that most officers devote a substantial amount of time to traffic enforcement. Compstat and similar initiatives are based on the idea of delegating responsibility for reducing levels of crime. The command staff is expected to be aware of current crime trends and initiate directives at reducing local problems. They are rewarded

when crime is down and held accountable when crime is up. This type of a strategy codifies the role of timely and accurate information by linking it directly to performance measures. This provides incentives that encourage information driven crime reduction strategies.

CONCLUSION

The access to, and analysis of, information has transformed policing in many ways. The role of information has evolved since the pioneering Uniform Crime Report. The collection, analysis, and sharing of information is the future of law enforcement. It can alter how police managers *and* line-level officers fundamentally approach their jobs in the fight against traditional street crime. Information sharing also appears to lie at the heart of emerging law enforcement issues such as local, regional, and national efforts to combat terrorism (Carter, 2004).

The salience of information management has captured the attention of the law enforcement industry. Today, many police agencies report the use of computer-related information management systems. Recent statistics indicate that nearly two-thirds of all police departments use records management computer systems, forty percent report computerized personnel records, thirty percent computer-driven crime analysis, and almost twenty percent automated booking systems. Most dramatically, almost 60 percent of all police departments serving populations greater than 250,000 report using computerized information systems when determining how to allocate resources (Hickman and Reaves 2003). It is expected that these numbers will continue to rise.

Compstat has played a critical role toward advancing information-driven decision-making in contemporary police organizations. Compstat was implemented in

the mid-1990s as a mechanism for bringing crime reduction strategies to the forefront of law enforcement in New York City (see Bratton 1998 for a more complete discussion). Like other police departments, the New York City Police Department lost focus on the importance of its crime control mission as command staff and line officers were victim to low expectations and little accountability for crime rates (Weisburd et al. 2004). Weisburd et al. (2004) argued that part of the reason behind the lack of accountability was that NYPD was "flying blind." "It lacked timely, accurate information about crime and public safety problems as they were emerging; had little capacity to identify crime patterns; and had difficulty tracking how its own resources were being used" (2). Compstat represented a critical organizational shift focused on infrastructure, disseminating information about crime patterns, and crime reduction strategies.

Surveys of police organizations reveal Compstat or similar models have been adopted at increasing rates over the past 25 five years. A sample of over 500 of the nations largest law enforcement agencies indicated a rapid diffusion of Compstat starting around 1998 (Weisburd et al. 2004). Approximately 20 percent of the sample reported implementation of a Compstat-like management model by 1999; a high rate considering the national attention to NYPD's success commenced just 3-4 years prior. Respondents indicated Compstat had the greatest potential to reduce serious crime, but also other residual benefits such as increasing policing skills. The authors extrapolated the 1974-1999 trend through 2029 and predicted that technology will reach a saturation point of 90 percent by the year 2007. If this is accurate, Compstat will represent one of the most quickly adopted forms of innovation (Weisburd et al., 2004).

While information management certainly has the potential for "revolutionizing" policing, it is important to consider *how* information is used for it to truly impact the law enforcement community. Manning (2003) and others (e.g., Dunworth 2000) effectively argue that information technology has largely failed to achieve its potential to change policing. Compstat and similar models have been institutionalized but with the rare exception such initiatives continue to play a largely symbolic role. One of the most pressing issues the law enforcement community will face over the coming decades is how to better utilize information in ways that change how policing is fundamentally performed.

Information and information management will likely have their most dramatic impacts on policing when they move out of the conference room and into the hands of line-level patrol officers. Crime analysis still remains primarily a management function even in some of the most progressive police departments. New technology has provided the ability to detail more crime specifics, depict more dynamic visual presentations of crime, and even forecast crime trends. However, information technology will continue to be symbolic until it moves beyond a glossy report and changes line-level crime reduction strategies.

As police organizations develop their capacity for analyzing crime, they fall short in devising strategies for actually using information technology in a meaningful way. Little consideration has been given to how data driven decision-making can benefit the patrol officer. The success of Compstat and similar information management models lie in their ability to directly impact patrol functions. If information management is to revolutionize policing by the year 2020, then collection and analysis of information must become integrated into patrol operations by using the latest hardware and software in the field.

REFERENCES

Bratton, Willaim J. 1998. *Turnaround: How America's Top Cop Reversed The Crime Epidemic*. New York: Random House.

Carter, David L. 2004. *Law Enforcement Intelligence: A Guide For State, Local, And Tribal Law Enforcement Agencies*. Washington, DC: Office of Community Oriented Policing Services.

Dunworth, Terrance. 2000. Criminal justice and the IT revolution. In *Criminal Justice 2000: Volume 3, Policies, Processes, And Decisions Of The Criminal Justice System.* Edited by Julie Horney. Washington, DC: Office of Justice Programs.

Gaines, Larry K., John L. Worrall, Mittie D. Southerland and John E. Angell. 2003. *Police Administration, 2nd Ed.* Boston: McGraw Hill.

Glensor, Ronald. W., Mark E. Correia and Kenneth J. Peak, eds. 2000. *Policing Communities: Understanding Crime and Solving Problems*. Los Angeles: Roxbury.

Greene, Jack R. 2000. "Community policing in America." *Criminal Justice 2000: Volume 3, Policies, Processes, And Decisions Of The Criminal Justice System.* Edited by Julie Horney. Washington, DC: Office of Justice Programs.

Groff, Elizabeth R. and Nancy G. LaVigne. 2001. "Mapping an Opportunity Surface of Residential Burglary." *Journal of Research in Crime and Delinquency 38:* 257-278.

Harris, Kelly J. and William H. Romesburg. 2002. *Law Enforcement Tech Guide: How to Plan, Purchase and Manage Technology (Successfully!): A Guide For Executives, Managers, and Technologists*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Hickman, Matthew J. and Brian A. Reaves. 2003. *Local Police Departments 2000*. Washington, DC: United States Department of Justice, Bureau of Justice Statistics.

Klinger, David A. 1997. "Negotiating Order in Patrol Work: An Ecological Theory of Police Response to Deviance." *Criminology 35:* 277-306.

LaVigne, Nancy G. and Julie Wartell. 1998. *Crime Mapping Case Studies: Success in the Field*. Wasington, DC: Police Executive Research Forum.

Mamalian, Cynthia A. and Nancy G. LaVinge. 1999. *The Use of Computerized Crime Mapping By Law Enforcement: Survey Results*. Washington, DC: United States Department of Justice, National Institute of Justice.

Manning, Peter K. 2001. "Technology's Ways: Information Technology, Crime Analysis and the Rationalizing Of Policing." *Criminal Justice: The International Journal of Policy and Practice 1:* 83-103.

Manning, Peter K. 2003. *Policing Contingencies*. Chicago: University of Chicago Press.

Maxfield, Michael G. 1999. "The National Incident-Based Reporting System: Research and Policy Applications." *Journal of Quantitative Criminology 15:* 119-149.

Maxfield, Michael G., Dan A. Lewis and Ron Szoc. 1980. "Producing Official Crimes: Verified Crime Reports as Measures of Police Output." *Social Science Quarterly 61:* 221-236.

O'Connell, R. B. 2004. Personal interview. Boston, MA.

Office of Community Oriented Policing Services. 2002. *COPS Fact Sheet: Making Officer Redeployment Effective (MORE)*. Washington, DC: United States Department of Justice, Office of Community Oriented Policing Services.

Rengert, George F. 2004. "Journey to Crime." In *Punishment, Places and Perpetrators: Developments in Criminology and Criminal Justice Research*. Edited by Gerben Bruinsma, Jan De Keijser, Henk Elffers and Jan William De Keijser. Portland, OR: Willam Publishing.

Reuland, Melissa. 1997. *Information Management and Crime Analysis: Practioners' Recipes for Success*. Washington, DC: Police Executive Research Forum,.

Rich, Thomas. 2001. *Research in Brief: Crime Mapping and Analysis by Community Organizations In Hartford, Connecticut*. Washington, DC: United States Department of Justice, National Institute of Justice.

Robinson, Jennifer. 2004. *Spatial Interplay: Measuring the Effects of Conjoined Cues in Environmental Criminology*. Unpublished manuscript, Boston, MA.

Skogan, Wesley G., Susan M. Hartnett, Jill DuBois, Jason Bennis and So Y. Kim. 2003. *Policing Smarter Through IT: Learning From Chicago's Citizen and Law Enforcement Analysis and Reporting (CLEAR) System*. Washington, DC: Office of Community Oriented Policing Services.

Snyder, Howard and Melissa N. Sickmund. 1999. *Juvenile Offenders and Victims: 1999 National Report*. Washington, DC: Office of Juvenile Justice and Delinquency Prevention.

Uchida, Craig D. 1993. "The Development of the American Police: An Historical Overview." In *Critical Issues in Policing.* Edited by Roger G. Dunham and Geoffrey P. Alpert. Prospect Heights: IL: Waveland.

United States Department of Justice. 2005. *FY2004 Budget Summary*. Washington, DC: United States Department of Justice,.

Walker, Sam, Geoffrey P. Alpert and Dennis J. Kenney. 2001. *Early Warning Systems: Responding To the Problem Police Officer*. Washington, DC: United States Department of Justice, National Institute of Justice.

Weisburd, David, Stephen D. Mastrofski, Rosann Greenspan and James J. Willis. 2004. *The Growth of Compstat in American Policing*. Washington, DC: The Police Foundation.