



Overcoming the Barriers:

Crime Mapping in the 21st Century

Crossing the Borders of Crime: Factors Influencing the Utility and Practicality of Interjurisdictional Crime Mapping

By John E. Eck

ABSTRACT

Recent improvements in mapping software have made GIS applications to crime relatively inexpensive and effective. This has raised interest in mapping crime across borders and giving police managers the capability to see larger crime patterns. This capability suggests that Cross Boundary Crime Mapping Systems (CBCMS) have great utility. A CBCMS is a group of police agencies that share mappable data on a routine basis. This paper will discuss factors that influence the utility of creating a CBCMS, including the willingness to act on discovered patterns, the presence of shared crime patterns, data quality, administrative arrangements, and concerns about privacy and data sharing. Although technology has made cross-jurisdictional mapping possible, these issues are the most critical to success.

During the European Middle Ages, western mapmakers, who had forgotten the lessons of the Greek geographers, and not yet developed modern cartography, believed that unknown regions neighboring the small known world were inhabited with beasts we now know to be mythical. These creatures symbolized their fears of outlying perils that might threaten the known world. Fear of these creatures slowly receded as mapmakers learned more from explorers, sailors, and merchants (Wilford, 1982).

Today, as crime mappers use increasingly sophisticated software they are able to show crime patterns in ever greater detail. But, like the old mapmakers, they remain apprehensive about what lurks beyond our jurisdiction's borders. Do hidden forces across the line create crime on our side of the line? Are the citizens and police in the areas beyond our

Introduction

By David Weisburd,
Rachel Boba,
and Elizabeth Groff

Over the last decade, crime mapping has emerged as one of the most important and popular innovations in American policing (Weisburd and McEwen, 1998). Just a generation ago, few police agencies considered the geographic distribution of crime a central element of crime analysis and problem solving. The focus of crime prevention and control in police agencies was upon offenders and only rarely did crime places take central stage in the strategic approaches or plans of the police. When police departments did focus on the geographic distribution of crime, they were often forced to plow through poorly developed and organized data. Additionally, when they produced maps, if they wanted to identify discrete crime locations, they often had to do their work by hand.

(Continued on page 2)

John E. Eck is Associate Professor of Criminal Justice at the University of Cincinnati. He was formerly evaluation coordinator for the Washington/Baltimore High Intensity Drug Trafficking Area.

maps responsible for the crime patterns on our maps? Could mapping the crime in a neighboring, unknown land help us police our territory?

Fortunately, it takes less effort to view crime patterns on the other side of our borders than it took medieval mapmakers to chart the unknown beyond their maps. Further, crime mappers across the border may be asking the same questions about us. If they are, and if they too use computer mapping, then we might be able to develop a system that permits timely exchange of geographic crime information. Such a system could remove most of the mystery of cross border crime patterns and foster collaborative arrangements to address the causes of these patterns.

CROSS BOUNDARY CRIME MAPPING SYSTEMS

This paper describes the issues that police officials need to address in order to create useful Cross Boundary Crime Mapping Systems (CBCMS). A CBCMS is a relationship between two or more police jurisdictions (including sheriffs' departments, state police, and special district police agencies) that facilitates regular timely exchange of data describing crime or disorder events and their locations. Crime and disorder events are incidents such as robberies, burglaries, thefts, drug sales, noisy parties, traffic accidents, and other concerns that the public reports to the police. The police may record these incidents as offense, arrest, vehicle stop, and citizen call for service data. Incident data may also be recorded by agencies other than the police, such as prosecutors, courts, schools, public housing authorities, and parks departments. Private institutions such as security firms, shopping malls, and merchants may also record the data. These incidents form the bedrock data for crime mapping. Regardless of the source, the data must contain information describing specific locations, incident types, and dates of occurrence. Because police data is the most commonly used form of geographic crime event data, most of my remarks will refer to these forms of data. Nevertheless, most of my comments here about police data apply to data from other sources as well.

The definition of a CBCMS is broad and it allows for both very simple and very complex arrangements. If crime analysts from neighboring jurisdictions regularly meet for lunch and exchange crime data-packed zip disks so that they can detect crime patterns on both sides of the border, then their arrangement qualifies as a CBCMS. At the other extreme, a state police unit that routinely collates and maps crime data from small towns and counties throughout the state also qualifies as a CBCMS.

Not all data exchanges qualify as a CBCMS. Agencies that exchange maps, tables, and charts but do not exchange underlying data are not included in my definition. Also excluded here are singular episodes of collaboration—such as planning for a major sporting or political event—or data exchange as part of a single particularly serious and difficult criminal investigation. Regular crime data exchanges that do not involve

(Continued from page 1)

Today, computerized crime mapping has become a standard tool in American police agencies. Technological advances in crime analysis and crime mapping as well as the focus on analyzing data for more effective policing and crime prevention have brought crime mapping to the center of law enforcement practice and policy. Desktop computers now deliver the power of mainframe computers of the 1980s. Crime-analysis and crime-mapping software have become inexpensive and accessible to all types of police departments. Recent national surveys of police departments have found that between 58% and 86% use technology for crime mapping (Bureau of Justice Statistics, 1999; Mamalian and LaVigne, 1999; Weisburd, Greenspan, and Mastrofski, 1998), and the trend suggests that even more departments will begin to use technology for these purposes in the coming decade.

Despite this recent and widespread implementation of technology for crime analysis and crime mapping by police departments across the country, there is evidence that many police agencies face obstacles in using technology effectively (Crime Mapping Laboratory, Police Foundation, 2000; Mamalian and LaVigne, 1999; Rich, 1995). Most often the barriers faced have not centered around the availability of cutting edge technologies but rather are related to the integration of such technologies into the complex world of policing.

(Continued on page 3)

geographic information (for example, some intelligence systems) are excluded as well. So, to qualify as a CBCMS, the exchange must involve event-level data (rather than predigested summaries) on a recurring basis that includes information about where the events occurred.

Cross Boundary Crime Mapping Systems are feasible only with recent technological advances that have made crime mapping inexpensive, easy to use, and flexible. Advances in technology have made computer crime mapping available to virtually any police agency. In fact, the basic technology is within the means of many citizens' groups, businesses, and individual citizens. By technology, I am referring to computer hardware, networks, and data processing software, as well as the technical expertise of people who can set up and maintain such systems.

The minimum technological requirements for a CBCMS are that each participant agency be able to record and duplicate crime-event data in a format that can be read and correctly interpreted by the information systems of other members. That is, if jurisdiction A records that a burglary occurred at 6200 Rhymney Highway and this data is given to jurisdiction B, then jurisdiction B will be able to determine that the same event occurred at the same place. Or stated another way, crime maps produced by two or more jurisdictions using the same data will contain no substantive differences with regard to the locations of specific events and the depictions of crime patterns.

Clearly, the barriers to achieving this minimal level are not technological. Budgetary limitations, political support, organizational infrastructure, and other factors may put limits on the technology available to any particular group of agencies. But this is no different from any other police administrative matter, such as recruiting sufficient numbers of competent citizens to become police officers.

PLANNING A CBCMS

For a CBCMS to be effective, the five factors that need to be addressed are: action, patterns, data, administration, and access. They are listed in order of decreasing importance. That is, if questions regarding action cannot be resolved, there is little point in proceeding to questions regarding patterns. If patterns cannot be addressed, there is little value in exploring questions about data and other issues. There are two other factors that need to be mentioned briefly before we proceed. Technology, which has already been addressed, is not a potential barrier but an opportunity. What often appears to be a technological barrier is typically a political/budgetary barrier. If someone is willing to pay for the technology, then the technology is likely to be made available. But getting someone to pay for it often requires a political decision. Political and budgetary concerns vary so much among agencies that I will not talk much of politics. But why would someone want to pay for a CBCMS

(Continued from page 2)

This series, entitled "Overcoming the Barriers: Crime Mapping in the 21st Century," was developed jointly by the National Institute of Justice and its Crime Mapping Research Center, and the Police Foundation's Crime Mapping Laboratory to encourage debate regarding key issues in the implementation and integration of crime mapping into American police practice. The series, which is based on lectures presented at the Police Foundation, is concerned with the human as well as technological barriers that police agencies face. Importantly, we sought not just to define those barriers, but to provide ideas for overcoming them.

The first paper in this series, "Crossing the Borders of Crime: Factors Influencing the Utility and Practicality of Interjurisdictional Crime Mapping," is written by John Eck, Associate Professor of Criminal Justice at the University of Cincinnati. He is an internationally known expert in the prevention of crime at places, drug dealing and trafficking control, and police problem-solving strategies. Professor Eck addresses the issue of regional crime analysis mapping. Mapping across jurisdictions has emerged as a major problem in the integration of crime mapping into police problem solving. Crime problems often cross-jurisdictional boundaries. But crime analysis is often based within specific jurisdictions, and police agencies have found it difficult to move from the idea of cross jurisdictional crime mapping to actual imple-

(Continued on page 4)

and take on the administrative burden necessary to maintain it? Presumably because they expect it to facilitate effective action against crime or disorder patterns that cross two or more adjacent jurisdictions. As we shall see, all five factors—action, patterns, data, administration, and access—influence the political decisions needed to support a CBCMS.

ACTION

To what use will the information from the CBCMS be put? Will the members of a CBCMS take action to address the patterns they discover? These are the most important considerations in any decision to create a CBCMS. Simply knowing that a crime pattern extends into a neighbor's jurisdiction is interesting, but unless something is done with this knowledge it has no practical importance. Since border patterns are shared ones, the actions taken to address these patterns are likely to require coordinated efforts by two or more agencies. This raises the question of whether the participating agencies are willing and able to undertake coordinated efforts to address common crime and disorder problems. If the answer to this question is “no,” then developing a CBCMS may not be worth the trouble. Of course, it is possible to embarrass one's neighbor into action by revealing a pattern that is being addressed on only one side of the border. Such behavior, however, imperils future information exchange. For a CBCMS to be worthwhile, participating agencies need to develop basic procedures for addressing shared patterns and problems.

It might be tempting to follow the “build it and they will come” philosophy. Perhaps, once patterns are revealed, the members of a CBCMS will take up the challenge. One must be skeptical about the validity of this assumption. Most police agencies are already filled with data no one uses. Furthermore, it is not uncommon for a crime analysis unit's work to be ignored by operational personnel. So prudence dictates that the foundations for joint actions should be laid when the CBCMS is being planned, not after it has been created.

PATTERNS

Having decided to take action if interjurisdictional crime and disorder patterns are found, the next question is whether there are any such patterns. Clearly, there is little value in a CBCMS if member jurisdictions share no geographic crime and disorder problems. Since a CBCMS is an ongoing operation, requiring some level of effort to maintain over time, we are concerned with “typical” patterns for a region. A single instance of a shared crime pattern, when typically there are no shared patterns, is not an adequate rationale for a CBCMS. But how do we know that the single pattern we have experienced will never be repeated?

(Continued from page 3)

mentation of systems for examining crime across jurisdictional boundaries. In this, the police have faced not only technological, but also organizational, political, and social barriers. Indeed, as Professor Eck argues, the main impediments to the development of effective cross jurisdictional crime mapping systems lies not in the technologies available but in the organizational structures and patterns of police agencies.

David Weisburd is Senior Fellow, and formerly senior research scientist, at the Police Foundation. He is also a professor of criminology at the Hebrew University Law School in Jerusalem, and a Senior Research Fellow in the Department of Criminology and Criminal Justice at the University of Maryland, College Park.

Rachel Boba is Director of the Police Foundation's Crime Mapping Laboratory.

Elizabeth Groff is a former Social Science Analyst in the Crime Mapping Research Center.

Web Sites

Police Foundation

www.policefoundation.org

Crime Mapping Research Center

www.ojp.usdoj.gov/cmrc

One way of looking at this problem is to take a lesson from meteorology. In meteorology, storms are classified by their expected frequency. Thus, a 50-year storm is one that is likely to occur, on average, once every 50 years, and a 100-year storm occurs half as often. Since weak storms are more frequent than powerful storms, the more dangerous storms occur less frequently. Knowing this, planners and builders can make informed decisions as to what level of storm their works should withstand.

We can think of crime patterns in the same way. Minor problems are far more frequent than serious problems (most police agencies receive far more complaints about noise than robberies, for example, and individual homicides are far more common than serial killings). A CBCMS should be able to address those patterns that occur on a regular basis (say, patterns that show up on average about once or more a month). The rarer the pattern, the more difficult it will be to create a CBCMS to handle it and this will make the CBCMS more expensive. For example, in a particular region a serial murder spree is likely to show up once a decade, on average, but patterns of drug-related shootings occur on average five times a year. Designing the CBCMS to address the drug-shooting patterns makes a great deal of sense, but should the system also be designed to address serial murders? Like storms, the rare patterns we care most about, and worry about being unprepared for, are those with the most serious consequences. So there is a trade-off between frequency and seriousness. It might be possible to create a two-tiered system. For everyday use—the once-a-month or once-a-year patterns—we create a full-blown CBCMS. Then, for less frequent patterns—those that occur once a decade—members of the CBCMS create emergency plans that allow rapid integration of data that is not normally used.

I will focus on the common crime patterns and will also assume that our data is exceptionally error free. Data errors make all analysis more difficult and the results less useful. In reality, the patterns that show up on maps will result from a combination of real underlying patterns and errors. Separating reality from data errors will never be fully successful. For this reason, data errors are addressed in the following section, but for the time being let's ignore this serious problem.

There are eight basic types of patterns that concern us, the first of which is an absence of patterns. A brief description of each follows, as well as maps of three hypothetical jurisdictions.

Pattern Zero: No Pattern

In this circumstance, crime and disorder events are spread in a seemingly random fashion. Therefore, knowledge about the location of one or more events tells the analyst nothing important about the location of the next event—it could happen anywhere. If this lack of pattern is typical, there is no compelling reason for agencies to develop a CBCMS. This suggests a troublesome paradox. To determine that one needs a CBCMS, does one have to create a CBCMS? The answer is no, since there are ways around such a perverse state of affairs. During the initial planning stages for a CBCMS, potential members can bring test maps of their border areas for comparison. By discovering a persistent absence of patterns, they may save a great deal of time.

Pattern One: No Shared Pattern

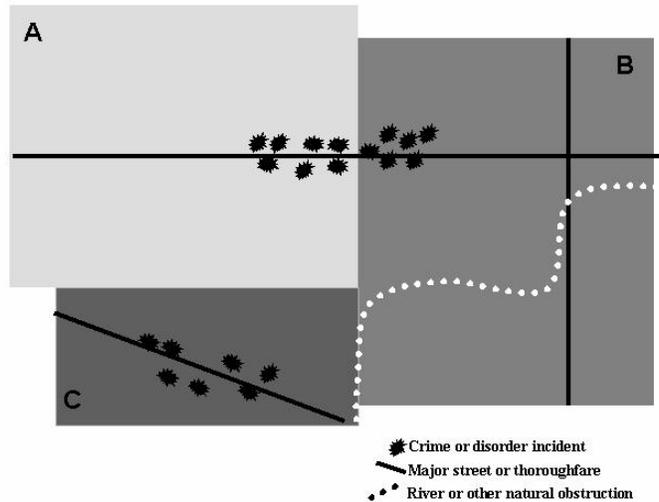
Crime or disorder events may have patterns, but they may not be shared across the jurisdictions in question. In Figure 1 (see next page), jurisdictions B and C do not share crime patterns. Neither do jurisdictions A and C. This may occur when a natural boundary, such as a river, inhibits the movement of people. Or it may occur because the road network and land-use patterns that influence crime do not intersect the boundaries. If this pattern is normal, a CBCMS is not very useful. Again, comparing crime maps early in the planning

process should alert CBCMS planners to this possibility. In a circumstance such as the one shown in Figure 1, it does not make much sense for jurisdiction C to participate in a CBCMS with the other two jurisdictions.

Pattern Two: Shared Patterns

Street networks frequently puncture borders, particularly in urban and suburban areas. Major streets form the backbone of many crime and disorder patterns (Brantingham, 1993) and when they cross boundaries, two or more jurisdictions will often share the crime patterns. Jurisdictions A and B in Figure 1 share such a crime pattern and might benefit from a CBCMS.

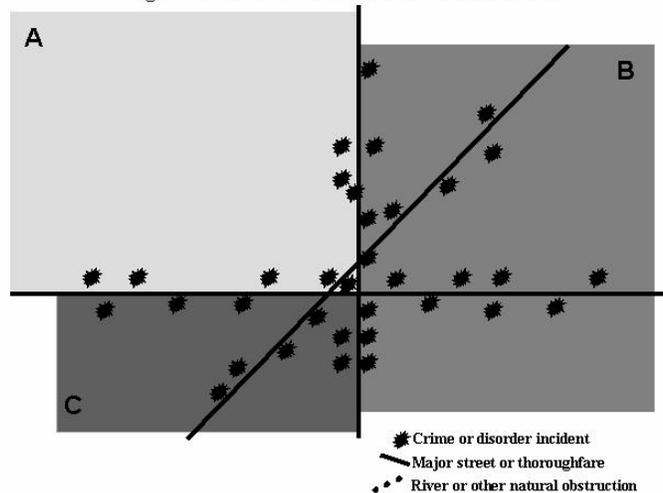
Figure 1: UNSHARED AND SHARED PATTERNS



Pattern Three: Shared Boundary Problems

Arterial routes often form boundaries between two jurisdictions, particularly in dense urban areas. In these circumstances, shared patterns may form along the boundary (Figure 2). Shared boundary problems involve the movement of offenders across and along, whereas Pattern Two problems involve movement only along a street. It may require greater cooperation to successfully solve shared boundary problems than to address Pattern Two problems because a longer border is involved. Clearly, a CBCMS is useful for these Pattern Three problems.

Figure 2: SHARED BOUNDARY PROBLEMS



Pattern Four: Barrier Borders

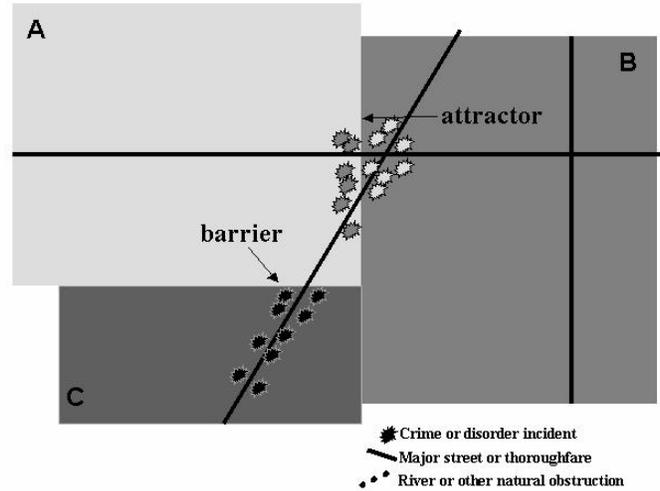
In the previous patterns, crime clustered along borders because of street layouts. If the arterial streets did not cross or form borders, then crime patterns would not be on borders.

In Patterns Four and Five, the border (rather than the street) is a cause of the crime pattern because offenders take borders into account when deciding where to commit offenses. When borders form a barrier, offending patterns stop at the border. In Figure 3 (see next page), offenders committing crimes along the arterial route in jurisdiction C do not continue committing crimes along the arterial route once it crosses into jurisdiction A. This might be because of different police practices across the border. If this is a typical pattern, then the utility of a CBCMS is ambiguous. Neither jurisdiction may feel that cooperation with the other is necessary to address the problem. In Figure 3, agency C might view the problem as its individual concern and agency B might agree. Nevertheless, information exchange may prove fruitful if agency C can learn why the crime does not spill over the border. Agency A also might find collaboration beneficial to assure that spillover does not occur in the future.

Pattern Five: Attracting Borders

Pattern Five is the opposite of Pattern Four. Borders attract crime or disorder if offenders find that the boundary provides protection. An offender might be able to elude the police by crossing into the neighboring jurisdiction and then quickly returning to his home jurisdiction. In Figure 3, offenders from A go to B to commit crimes, and vice versa. Although this example shows a symmetrical relationship, this may not always be the case—one jurisdiction can be a net crime exporter and the other a net crime importer. When borders attract offenders, crime targets nearest the border will be at higher risk than targets further away. This is because an offender needs to escape back over the border as quickly as possible, and the further he penetrates into the neighboring jurisdiction the longer it will take him to get back to safety.

Figure 3: BORDERS AS BARRIERS AND ATTRACTORS

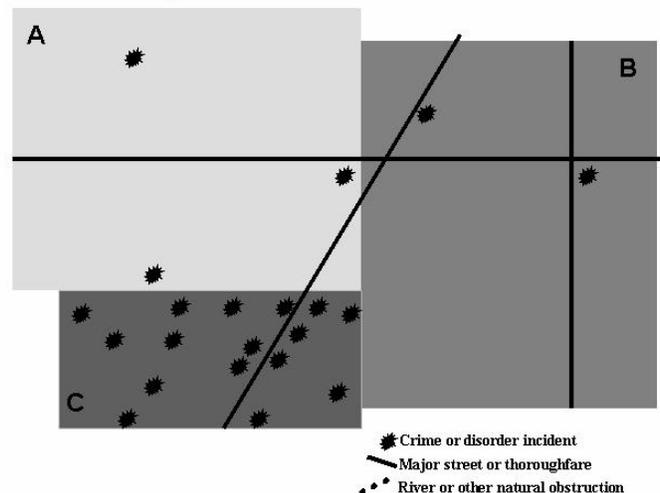


Borders that attract crime are probably more common in situations where cooperation between jurisdictions is minimal and interjurisdictional rivalries are high. The literature on this issue is sparse and anecdotal. Fraser (1971) describes border-related cattle rustling along the fifteenth-century, Anglo-Scots border that was eliminated only after the two countries merged and law enforcement was unified. Wambaugh’s (1984) description of violence along the U.S.-Mexican border is closer to our time period. And Kotlowitz (1998) describes the difficulties of crime and policing in two Michigan cities separated by race and a narrow river. A CBCMS would be quite useful in these circumstances, but may be difficult to create if rivalries and distrust are long standing and well entrenched.

Pattern Six: Pseudo Barriers

It may be difficult to discern the effect that a border has on crime patterns. A variety of factors—land use, housing stock, race, income, topography, and other things—may concentrate crime or disorder on one side of a border. Such concentrations occur within jurisdictions so it is not surprising to find them between jurisdictions. I call these pseudo-barrier effects because it appears that the border acts as a barrier when it is really something else that is causing the crime pattern (i.e., the pattern would exist even if the border were removed). In Figure 4, jurisdiction C has a great deal of crime, but it does not spill over into the adjacent

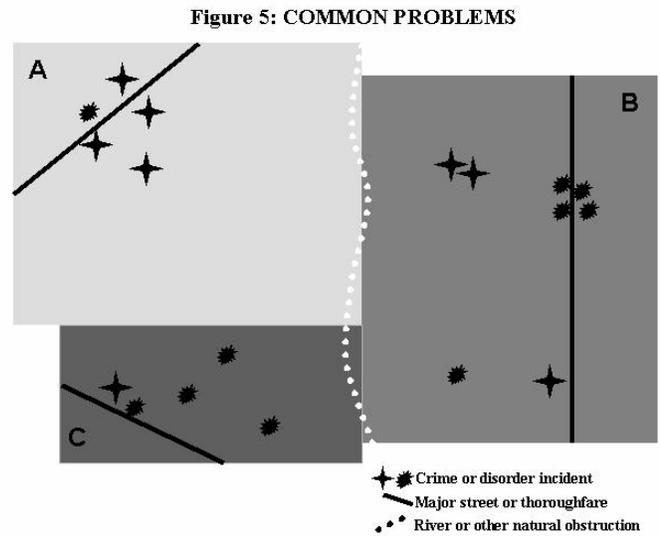
Figure 4: PSEUDO BORDER EFFECTS



jurisdictions. Agencies A and B might think that they receive some spillover from C and may be willing to develop a CBCMS, but it is not clear that agency C would see much benefit from participating.

Pattern Seven: Common Problems

Some shared problems may be hidden from view, even with a fully functioning CBCMS. The crime and disorder problems faced by the neighboring jurisdictions may not be visible as geographic clusters and they may not occur along or near borders. Two different crimes are shown in Figure 5, but they are spread out away from borders. Consequently, agencies A, B, and C may see little value in exchanging information, though they are part of a larger pattern. Car theft from automobile dealerships, for example, may be endemic throughout a region. The same offenders may be involved, or different offenders may use the same methods to steal the cars. A regional approach may help curb the problem, but may be difficult without some regional crime analysis. Because a CBCMS can facilitate the sharing of a variety of data (see the following discussion of descriptive information), it may be useful even if the geography of crime does not present a compelling reason to create one.



To summarize our discussion of crime patterns and highlight the implications, we discussed two important points: (1) the frequency of crime patterns, and (2) what they look like. The implications for practice are straightforward. Prior to establishing a CBCMS, the agencies involved should use their existing data analysis systems to determine what types of crime and disorder problems are frequent and which are rare. The CBCMS should be able to address the frequently occurring problems, but plans should be established for addressing the rare, serious problems should these problems become apparent. In addition, planners need to identify the typical forms taken by common problems. We have discussed seven generic patterns. Some of these provide compelling justification for the creation of a CBCMS, while other patterns are less supportive.

DATA

Having established that there are common crime and disorder patterns that touch neighboring jurisdictions, we need to turn to the question of data quality. Ideally, we would have a full record of every crime and disorder event that has occurred. We would know what type of event it was, when it occurred, and where it occurred. We could then accurately describe crime patterns. Unfortunately, this is not the case. Crime and disorder data contain many errors. Much crime is not reported, so the biggest data error is not having known about events that occurred. Other events are not accurately described. One might not know about important characteristics of the event—what it is, when it occurred, or where it happened. These errors can confound analysis and preclude effective action. And the confusion arising from errors in crime and disorder data becomes compounded when we compare across jurisdictional borders. As important as data quality is for normal crime analysis work, it is even more critical when examining data from different

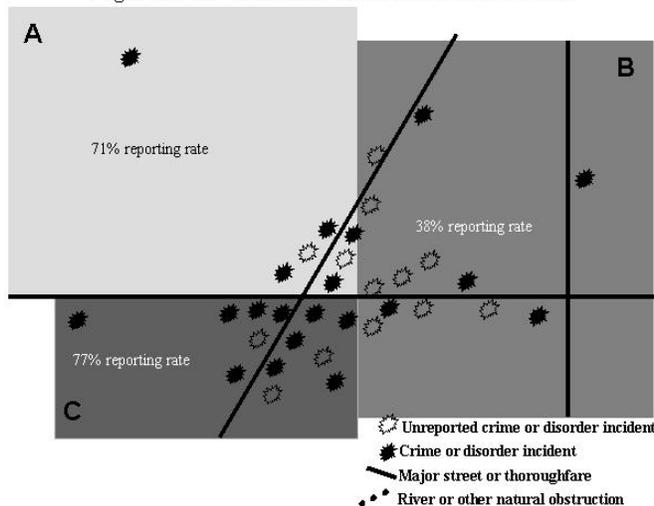
jurisdictions that may suffer from different rates of error. Consequently, they require serious attention. We will examine five sources of errors in crime and disorder data.

Citizen Reporting Differences

One thing that we can be certain of is that much crime and disorder is not reported to the police (and even fewer crime and disorder events result in arrests, prosecutions, and convictions). This has major consequences for detecting crime patterns as a simple example illustrates. Suppose that in a four-square-block neighborhood there have been fifteen break-ins to homes over the last month, whereas normally in this and adjacent neighborhoods five break-ins per month is typical. If all fifteen break-ins are reported, this surge in crime should become evident even before the fifteenth break-in and the area at greatest risk will quickly become apparent. Suppose that the reporting rate for break-ins in this neighborhood is 67 percent. It will take longer to detect the pattern and fix its geographic location. If the reporting rate is 33 percent, then the break-in pattern may not be detected because the frequency of occurrence is so low. Even if it is detected, it will take longer and the exact location of the pattern will be harder to discern. This is the basic problem with reported events and mapping. Let us now see how this influences detecting patterns that cross borders.

Imagine two adjacent agencies exchanging data on sexual assaults. Citizens in jurisdiction A report 65 percent of the sexual assaults to their police, but citizens in jurisdiction B report 30 percent of their sexual assaults to their police. Thus, the crime pattern on the A side of the border will be more complete than the crime pattern on the B side. Reporting rate differences can hide crime patterns on the side of the border with the lowest reporting rate. It is important to remember, however, that the reporting rate that matters is the rate in the area of the crime pattern, not the agency-wide average. If women report 43 percent of the sexual assaults in the immediate area on both sides of the border where the sexual assaults are occurring, then the gaps in the data will be the same on both sides. This suggests that it is important to know where and why reporting rates differ. Differences caused by the police, or perceptions of the police, could result in widely misleading maps of border crime problems. It may appear that the pattern is restricted to one side of the border when it is actually greater on the side where there is no evident pattern.

Figure 6: REPORTING RATES AND PATTERNS



The problem of differential event-reporting rates is illustrated in Figure 6. Two jurisdictions (A and C) have similar reporting rates, but the third (B) has a dramatically lower reporting rate. Since the crime maps would show only the solid event icons, an analyst might assume that jurisdiction B did not share the same crime pattern as the other two jurisdictions. In fact, we can see that the overall pattern reaches into jurisdiction B along two separate arterial routes.

Differing policing practices can create major differences in crime-event patterns. An agency with a drug-dealing hotline is likely to encourage the reporting of drug dealing that will go unreported in the neighboring jurisdiction without this facility. Shoplifting

reports from merchants may be influenced by county district attorneys' willingness to prosecute. So a map of shoplifting across county borders may show a slackening of these crimes in the county with low prosecution rates. Research has consistently shown that less serious crimes are reported less frequently than more serious crimes (Gove, Hughes, and Geerken, 1985; Schneider and Weisma, 1990). Consequently, calls-for-service data used to examine disorder and incivilities may be more sensitive to differences in police practices than serious crime.

Agency Recording

Even after a citizen has notified the police of a possible crime or disorder event, the police must record that event before data describing its location can be made available. Federal and state crime-recording standards may reduce the differences in crime-recording practices, although differences cannot be eliminated completely. More serious than crime-recording differences may be the differences in agency recording of disorder events and citizen calls for police service. There are far fewer standards for these types of events. Two adjacent agencies may have very different rates for recording noise complaints, for example. So even if crime-recording practices differ little among adjacent police agencies, they may differ considerably in their recording of noise complaints, prostitution calls, drug sales, disorderly conduct calls, and other incivilities.

Arrest data is particularly susceptible to police practice. In fact, it is probably a better indicator of the locations of police enforcement efforts than the nature of crime or disorder. Consequently, a pattern of arrests on one side of the border that does not continue on the other side may indicate only that one agency is focusing its attention on the border, while the other agency has its attention focused elsewhere.

Event Classification

Agency procedures for labeling crime and disorder events are related to recording practices. For broad crime categories, such as index crimes, this may not pose much of a problem, particularly if the member agencies are within the same state and share the same legal codes. Consider, however, two agencies separated by a state border. In one state, vehicle break-ins are classified as a type of burglary, while in the other state they are classified as a theft (if something is taken) or criminal damage (if nothing is taken). Clearly, these classification differences need to be taken into account if these two agencies are to create an effective CBCMS.

If one is interested in minor infractions or citizen call types, then the labels may not correspond, even when the agencies are within the same county. Members of a CBCMS will need to develop translation methods that allow correct interpretation of each other's data, or they will have to establish a common classification system.

Descriptive Information

In addition to the category of the event, crime analysts would like to have data describing the circumstances of the incident. Date, time, and place information may pose few problems, but other data might be more problematic. For example, one agency may record whether an assault or homicide was gang related, and another may not. Or both may record this information, but use different criteria for making this determination. Mapping gang violence across these two jurisdictions would be highly problematic in these circumstances. Like classification definitions, members in a CBCMS may find it advantageous to come to some agreement over basic data, particularly for regularly occurring shared problems.

Geocoding

Geocoding is a process to ensure that each crime or disorder event can be located on the digitized maps contained within mapping programs. These “base maps” tell the computer mapping program which addresses are valid. The program cannot locate addresses that it does not recognize, so analysts geocode data by matching the addresses recorded in reports with the addresses in the computer file. Some addresses do not match any valid street or number for various reasons. Police officers often misspell street names, give intersections as addresses, record a “street” as an “avenue” or a “road,” or do any number of things to addresses that causes the mapping software either to place the event at the wrong location or to reject the address as “not valid.” Correcting these errors is a major part of geocoding. Seldom can all events be correctly geocoded. Therefore, crime mappers often refer to their geocoding rate—the proportion of events assigned a valid address. Adjacent agencies with very different geocoding rates may find that border patterns are misleading. Like citizen reporting, what may matter most is not the agency average over all crimes, but the geocoding rate for the events that occur near the border.

Because computer-based crime mapping is relatively new to policing, little is known about the effects of varying geocoding rates. Nevertheless, one thing is clear. Like an unreported crime, an event that cannot be geocoded will not appear on a map. So the consequences of differential geocoding rates on either side of a border will be similar to differential citizen reporting rates. Even less is known about the effects of different geocoding procedures. All geocoding procedures will result in some event remaining ungeocoded. Could different procedures result in different events being left ungeocoded? Could this also distort border crime patterns? Although this is possible, we know little about it. Agencies participating in a CBCMS may want to conduct tests to determine if this is a problem.

We have examined five types of data errors that can influence the effectiveness of a CBCMS. Four of these are under the direct control of participating agencies—agency recording, classification, additional information, and geocoding. However, the police do not have strong direct control over the first, and possibly the most important, source of error—reporting.

ADMINISTRATION

As we saw when we looked at errors in crime and disorder data, police agency practices may have to be altered so that border patterns can be easily detected. Also, participants in a CBCMS must have a working agreement as to the actions they will take if they find shared patterns. In addition to agreements about joint action and data quality, there are at least three other agreements that participating agencies must address before a CBCMS can become operational. These are timeliness, data transfer, and governance, all of which affect the costs of the system and may have serious implications for the political support of a CBCMS.

Timeliness of Data Availability

What is the schedule of data availability in adjacent police agencies? In agency A, crime-event data is available for analysis within forty-eight hours of the event. In agency B, the same types of data become available within fifteen working days. And in agency C, data does not become available for analysis for thirty days. It is clear that if these three agencies are to create a CBCMS, the timeliness of the data will be dictated by the slowest of the three, agency C. Only after the thirtieth day will a complete picture of the geography of the crime appear, but this picture is already thirty days out of date. If one of these agencies misses its schedule (say a shortage of data-entry personnel forces agency B to have lags in data availability of up to forty days), then the timeliness of the CBCMS data will be affected. Why is this important?

If the agencies were planning to use their CBCMS for tactical operations, then this could become a major problem. And the faster that members of the CBCMS want to move from detection to action, the more critical timeliness becomes. To solve this problem, all agencies would at least have to upgrade their data processing to the timeliness of the timeliest. This will require changes in work schedules, staffing, and budgets, all of which may be far more difficult than installing the technology for exchanging data. Because these changes can have direct impact on the internal workings of participating agencies, the cost of creating a CBCMS cannot be measured by the costs of equipment and personnel needed to establish and maintain it. The costs also include infrastructure changes within each participating agency.

Effectiveness may not equate with speed, however. Although tactical patrol operations are designed to be quick for serious long-term problems, they are unlikely to result in long-term solutions. Instead, a problem-solving effort is required and problem solving for these sorts of problems typically unfolds over a longer period of time. If the officers examining a prostitution problem are looking at long-term trends in prostitution activity—maybe going back several years—it may not be all that important whether or not the data is current to within 24 hours, a week, or even the last month. So it is quite possible that a CBCMS has far more applicability for agencies that are routinely involved in looking for long-term prevention of problems than for those who are looking for a method of jumping on short-term crime spurts as quickly as possible.

Data Transfer

How will data be transferred among member agencies? Will portable mass storage media (like zip drive cartridges) be hand delivered or mailed on a regular schedule? Or will a secure network be used to transfer files?

If the members of the CBCMS are using different types of software, how will translation among formats be achieved? Will this be left to the recipient of the data? Or will the sender translate? Will this translation be into a common format that everyone uses or into all of the different formats being used by members?

Who is responsible for geocoding? Do the source members geocode or should the recipients do this? As we have seen, there are some potentially serious consequences from using data from another agency with different geocoding procedures. Perhaps a common standard for geocoding needs to be established or perhaps the data should be exchanged prior to geocoding and have the users geocode the imported data in the same way they geocode their own data.

Governance

Is anyone in charge of the operations of the CBCMS, and, if so, who? Governance questions can be answered in a number of ways. One alternative is to have no one in charge. Crime analysts from adjacent jurisdictions might create an informal alliance and regularly exchange data. If agency B is concerned about burglary patterns, a B analyst might call his counterparts in A, C, and D to have them download their burglary data. Meanwhile, the analyst from C might request information on drug arrests. This is a highly personal style and it has its strengths and weaknesses. This approach cuts through a great deal of red tape and can often get things done faster and cheaper. However, it may take some time for a new analyst to develop a relationship with neighboring analysts. An analyst who is not held in high esteem by his or her colleagues may get slower responses to his or her requests. Furthermore, addressing many of the concerns raised earlier requires a tighter form of coordination and planning.

Instead of a personalized relationship, a form of distributed authority might be established. Member agencies may develop and sign a Memorandum of Understanding (MOU) that lays out expectations and basic procedures. Based on the MOU, everyone is in charge of assuring compliance. This removes some of the difficulties of the personal style of governance, while preserving the flexibility of the system. The downside of distributed authority is that large-scale and expensive improvements are difficult to accomplish because there is no spokesperson or ultimate authority.

Creating a single administrator for the CBCMS helps address this concern. The single administrator could be the biggest, or the most technologically advanced, or the most politically powerful agency of the group. In a county with many small agencies, the sheriff's office might serve such a role, for example. Or the leader could be a small technologically sophisticated and well-funded agency within a region of larger agencies with tighter budgetary constraints and less technology.

Another approach to establishing a single administrator is to use an independent agency. In the Washington, D.C.-Baltimore region, the Washington/Baltimore High Intensity Drug Trafficking Area (W/B HIDTA), a regional drug enforcement project funded by the Office of National Drug Control Policy, partially fulfills this function. The W/B HIDTA has a working relationship with all of the major agencies in the region, and it has the flexibility to provide the hardware and software support. While the W/B HIDTA provides technological and administrative support, a separate board made up of member agencies sets policies for this CBCMS. Regional planning agencies or universities could also serve in such a role.

Finally, it is possible for the members to pool their resources and hire a private contractor to operate their CBCMS. Doing so would require police agency members to develop some sort of board to oversee the contract, and one of the members would have to serve as fiduciary for the arrangement. The added expense might be worthwhile if the reliability of the system and the technical support were significantly greater than alternative approaches.

In summary, operating a CBCMS involves a series of complex decisions as to how rapidly data will become available, how it will be transferred, and the form of the administrative apparatus. These decisions can have major impacts on the internal workings of the participating agencies and, in some cases, may reduce their autonomy.

DATA DISSEMINATION AND PRIVACY

Data dissemination policies create special problems. Federal, state, and local laws can restrict the dissemination of data in order to preserve citizen confidentiality and privacy, to prevent untimely disclosure of police operations, and to protect the safety of officers. The CBCMS member agency operating under the most restrictive data dissemination rules can set the ceiling on the data that can be disseminated among all members. If all participating agencies work under the same set of rules, this may not be a problem. But consider the problems that arise when a large city, with stringent privacy ordinances and operational procedures, works with smaller neighboring cities with fewer restrictions. In this case, the data that the large city cannot pass on will have a major influence on the entire CBCMS. The difficulties posed by privacy and security requirements depend on a number of factors. Are all the agencies in the CBCMS under the same restrictions? In a federalist system, the source of the privacy requirements may come from a variety of levels—local, state, and federal. If the CBCMS members are within the same governmental unit (e.g., within the same state), there may be fewer conflicts because they operate according to the same

set of rules (although there is no guarantee of this, as the previous example suggests). But if the sources of dissemination restrictions vary for the members—as may occur when a CBCMS crosses state lines—one can expect potential problems.

To what uses do the member agencies intend to put the data? Often there may be exceptions for exchanging data among police agencies and the restrictions apply only to divulging data to organizations or individuals outside of law enforcement. Although this may reduce some of the problems, it will create difficulties if members want to use the information to inform the public, develop community partnerships, or engage in multi-agency problem-solving efforts. To make full use of this data, agencies in a CBCMS will have to modify their policies for releasing data, and these decisions can involve political institutions outside of police agencies. These problems are not insurmountable, but the financial costs of keeping such information exchanges within the rules may be significant. If rule changes cannot be made, it may still be possible to create maps that preserve the required level of ambiguity for use by non-police organizations .

I have considered data dissemination and privacy last because the other concerns need to be confronted first, but this does not mean that data dissemination and privacy are minor concerns. As public and private organizations collect more and more information on people, places, and events, and as they exchange more and more of this data, there is increasing concern over their impact on personal liberties and civil institutions. For example, suppose we had a CBCMS made up of three adjacent police agencies, each of which had installed closed circuit television (CCTV) along high-crime and disorder streets. Furthermore, some of these streets are on the borders of these jurisdictions and others cross from one to another. The CCTV images can be archived and retrieved. They can also be exchanged, and, even more important, they can be exchanged in real time. In fact, it may not be difficult to imagine a mapping capability that would allow real-time tracking of citizens using public streets as they move from jurisdiction to jurisdiction. One could also envision the value of this for investigative purposes, gang-intelligence gathering, and many other normal police functions. Citizens of each of these jurisdictions might approve of their police monitoring their street activity, but would they approve of other police having access to this information or tracking them throughout a metropolitan area?

CONCLUSIONS

In this paper I have explored five issues that should influence decisions to establish a Cross Border Crime Mapping System. I have explained why the value of a CBCMS is greatest when the jurisdictions involved share crime patterns around common borders and are willing to act together to address these patterns once they are discovered. I have also shown why the costs of establishing a CBCMS cannot be measured by the costs of the equipment, software, and technical personnel. Significant changes in organizational procedures and policies may be required to exchange quality data on a timely basis. Although technology enables police to share information useful for mapping, the most important considerations are the nature of crime patterns and the willingness of police agencies to make the necessary internal changes. For these reasons, careful planning should precede the establishment of a CBCMS.

The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

REFERENCES

- Bureau of Justice Statistics. 1999. *Law Enforcement Management and Administrative Statistics, 1997*. Washington DC: Bureau of Justice Statistics.
- Brantingham, P. and Brantingham, P. 1993. "Environment, Routine, and Situation: Toward a Pattern Theory of Crime." In Ronald V. Clarke and Marcus Felson, eds. *Routine Activity and Rational Choice*. Advances in Criminological Theory, volume 5. New Brunswick: Transaction Publishers.
- Crime Mapping Laboratory, Police Foundation. 2000. *Integrating Community Policing and Computer Mapping: Assessing Issues and Needs Among COPS Office Grantees*. Washington DC: US Department of Justice, Office of Community Oriented Policing Services.
- Fraser, G. 1971. *The Steel Bonnets: The Story of the Anglo-Scottish Border Reivers*. London: Pan Books.
- Gove, W., Hughes, M. and Geerken, M.. 1985. "Are Uniform Crime Reports a Valid Indicator of the Index Crimes? An Affirmative Answer with Minor Qualifications." *Criminology*. 23:451-501.
- Kotlowitz, A. 1998. *The Other Side of the River: A Story of Two Towns, a Death and America's Dilemma*. New York: Doubleday.
- Mamalian, C., and LaVigne, N. 1999. *Research Preview: The Use of Computerized Crime Mapping by Law Enforcement: Survey Results*. Washington DC: US Department of Justice, Office of Justice Programs.
- Rich, T. 1995. *The Use of Computerized Mapping in Crime Control and Prevention Programs*. Washington DC: US Department of Justice, Office of Justice Programs.
- Schneider, V. and Weisma, B. 1990. "Limits and Use of the Uniform Crime Reports." In D. MacKenzie, P. Baunach, and R. Roberg, eds. *Measuring Crime: Large Scale, Long Term Efforts*. Albany, NY: SUNY Press.
- Wambaugh, J. 1984. *Lines and Shadows*. New York: Bantam Press.
- Weisburd, D., Greenspan, R., and Mastrofski, S. 2001. *Compstat and Organizational Change: Findings from a National Survey*, Report to the National Institute of Justice (NIJ Grant # 98-IJ-CX-0070). Washington, DC: Police Foundation.
- Weisburd, D. and McEwen, T. (Eds.) 1998. *Crime Mapping and Crime Prevention*. Criminal Justice Press: Monsey, NY.
- Wilford, J. 1982. *The Mapmakers: The Story of the Great Pioneers in Cartography from Antiquity to the Space Age*. New York: Vintage Books.

Acknowledgements

Thanks to David Weisburd and the Police Foundation for inviting me to Washington, D.C. to talk about these issues, and to Nancy LaVigne and Eric Jefferis of the National Institute of Justice for their comments and suggestions. They all provided me with excellent suggestions for improving this paper. I would be remiss if I did not also thank Tom Carr, Jeffrey Gersh, and others at the Washington/Baltimore High Incident Drug Trafficking Area who introduced me to this topic (although none of us knew it at the time). Of course, I, alone, am responsible for all errors in this paper, real or imagined.

ABOUT THE POLICE FOUNDATION

The Police Foundation is a private, independent, not-for-profit organization dedicated to supporting innovation and improvement in policing through its research, technical assistance, and communications programs. Established in 1970, the foundation has conducted seminal research in police behavior, policy, and procedure, and works to transfer to local agencies the best new information about practices for dealing effectively with a range of important police operational and administrative concerns. Motivating all of the foundation's efforts is the goal of efficient, humane policing that operates within the framework of democratic principles and the highest ideals of the nation.

OFFICE OF RESEARCH

D. Kim Rossmo, PhD
Director of Research

Rachel Boba, PhD
Director, Crime Mapping Laboratory

Justin Ready, MA
Senior Research Associate

David Weisburd, PhD
Senior Fellow

Edwin E. Hamilton, MA
Senior Research Analyst

Erin A. Lane, MPM
Research Associate

Mary Velasco, BS
Research Associate

Tamara Sorenson, MA
Research Assistant

Jim Griffin, MA
Graduate Research Intern

Linda Yoskowitz, BA
Senior Administrative Assistant

BOARD OF DIRECTORS

Chairman
William G. Milliken

President
Hubert Williams

David Cole

Wade Henderson

William H. Hudnut III

W. Walter Menninger

Laurie O. Robinson

Henry Ruth

Stanley K. Sheinbaum

Maria Vizcarrondo-DeSoto

Alfred A. Slocum

Kathryn J. Whitmire



1201 Connecticut Avenue, NW, Washington, DC 20036-2636
(202) 833-1460 ♦ Fax (202) 659-9149 ♦ e-mail: pinfo@policefoundation.org
www.policefoundation.org