Information Sharing: Exploring the Intersection of Policing with National and Military Intelligence

Gary Cordner and Kathryn Scarborough

This article explores the intersection of (1) policing and police intelligence with (2) national intelligence and military intelligence. The premise is that for more than 150 years, prior to the events of September 11, 2001, police intelligence had little connection to national or military intelligence. Basically, national intelligence focused on serious world-wide political and economic threats to the nation's well-being; military intelligence focused specifically on military threats to the national security; the police focused their intelligence work on criminals who posed threats to individuals and local communities. A fairly clear division of labor was in place, based largely on the type and scale of threats.

Since 9/11, however, it has become plausible that a small group of non-state actors, such as terrorists, could launch a serious attack against the nation using weapons of mass destruction, or even small arms, as in Mumbai. These individuals might live in a local U.S. community or halfway across the world, yet plan and execute a massive and violent attack against a local U.S. community. They might also commit ordinary crimes to help finance their larger intentions. In this new context of terrorism and asymmetric threats, a local police department might develop intelligence of significant interest to national and military intelligence, or vice versa.

Important historical, conceptual, and policy issues associated with the intersection of national, military, and police intelligence are discussed more fully elsewhere.[1] This article presents the results of a small-scale study in which subject matter experts were asked to respond to several scenarios related to intelligence and information sharing, asking both what *should* happen and what *would* actually happen.

U.S. POLICING

Policing in the United States is civilian (non-military), predominantly local (funded and directed by local governments), and extremely fragmented. It is not just that police are distributed all around the country[2] – they mostly answer to local elected officials. The U.S. has almost 18,000 separate law enforcement agencies, roughly 16,000 of which are local. Of the remaining 2,000 agencies, the vast majority represent special jurisdictions (university police, transit police, park police, etc.), followed by state agencies, and lastly by federal non-military agencies. Out of 837,000 full-time sworn police personnel (armed with arrest authority), 74 percent work for local agencies, 13 percent work for federal law enforcement, and 13 percent work for state or special jurisdiction law enforcement agencies.[3]

The two largest components of U.S. policing are both local: municipal police departments (cities, towns, townships, boroughs, villages) and county sheriff's offices.[4] Two characteristics of these types of law enforcement agencies are absolutely essential for understanding their capabilities and contexts: most are small (77 percent have fewer than twenty-five full-time sworn officers)[5] and they are all independent of each other.

There is no chain of command in the police industry – within individual agencies, yes, but among and between the 18,000 agencies, no.[6]

Along with industry structure, it is important to note a thing or two about police work and police culture. Particularly at the local and state levels, police officers in the field frequently act alone and without immediate supervision. Much of their work involves making "low visibility decisions" – especially when an officer's decision does not result in a report or an arrest (and most police actions and decisions do not), it is rarely subject to review. If an officer's decision does not result in a report or arrest, it probably will not produce any official information for later analysis. As Peter Manning notes, "information in police departments can best be characterized as systematically decentralized. Often, primary data known to one officer are not available to other officers" because they are stored in the officer's head or personal notes. Moreover, "all essential police knowledge is thought to be contextual, substantive, detailed, concrete, temporally bounded, and particularistic" while information in official reports and files is often viewed by officers and investigators as trivial, having been created and manipulated mainly for bureaucratic purposes.[7]

Additionally, police agencies and police culture tend to celebrate and reward good arrests. Information and intelligence, by themselves, are not traditional units of police work, they are not measured, and producing them is not rewarded. Also, information that is not directly connected to an incident, crime, or case does not have a natural home in the typical police records system – there is no file to put it in. Incidents, crimes, and cases are traditionally assigned to individual officers (or detectives) who are evaluated on how well they handle and dispose of these events. Consequently, the tendency is for officers and detectives to hold information closely in order to use it later to enhance their own productivity.

It is also important to recognize that U.S. police, not just the military and federal law enforcement agencies, engaged in intelligence-related abuses in the 1960s and 1970s.[8] Informants, undercover operations, and electronic surveillance were often used to gather information about civil rights and anti-war groups. Subsequent inquiries showed that many of the targets of these intelligence operations were not involved in any serious criminal behavior, but rather were engaged in political activities in opposition to prevailing government policies, such as the Vietnam War. Local police intelligence capabilities were significantly curtailed in the wake of exposes of these abuses, and in some jurisdictions have yet to recover.[9]

The point of these observations is that the structure of U.S. policing, the nature of police work, some historical stumbles, and common features of police culture all seem to conspire against an intelligence-led approach to policing and the free flow of information.[10] To this we can add the traditional tensions between levels of policing in our federal system. State and federal law enforcement are often represented or perceived as more important and more professional than local police – much to the resentment of local police. Local police sometimes also fear state and federal agencies, because those agencies have the authority to investigate public corruption and civil rights violations in local communities. Specifically on the issue of information sharing, a common complaint is that it is a one-way street – local police provide information to their state and federal "partners" but get little or nothing in return. The following

anecdote from one of the subject matter experts who participated in this project illustrates the common local police experience and perspective:

> Person is stopped off I-35 North of Georgetown, TX. Subject has possession of numerous photographs of large venue HVAC systems, such as stadia and arenas. Subject is a Middle Eastern engineering student. First photos are of subject inside Reunion Hotel in Dallas, obviously shot by someone else. Subject alone when stopped. Digital photographs copied by police. Local police notify Secret Service because of proximity to Western White House. Secret Service tails subject until they lose him. THEN they notify FBI, which enters information into Threat Matrix. Local police notified after subject left the country.

Frustration with federal-local information sharing has led the New York Police Department (NYPD) to station overseas personnel in eleven posts, including London, Paris, Abu Dhabi, and Amman.[11] Their post-9/11 reasoning is that (1) their city is a likely target of international terrorism, (2) they are not confident that the Federal Bureau of Investigation (FBI) or Central Intelligence Agency (CIA) or other federal agencies will share important information with them immediately, and therefore (3) they want their own people on the ground around the world in the places where key intelligence might be uncovered. They also argue that local police in Tel Aviv or Madrid are more likely to share information with U.S. local police than with U.S. federal officials.

In spite of all these longstanding and fundamental challenges, since 9/11 there is evidence of improved intelligence gathering and information sharing. Local police have been encouraged to collect and forward a new type of document, Suspicious Activity Reports (SAR).[12] State-level fusion centers have been created to serve as the link between local agencies and federal/national agencies and networks;[13] some of these have even been granted access to classified Department of Defense information systems.[14] Local and state agencies have reported increased contacts with the likes of the FBI, CIA, Centers for Disease Control (CDC), Federal Aviation Administration (FAA), and National Guard.[15] At the national level, reorganization of the intelligence community, increased emphasis on counter-terrorism in the FBI, creation of the National Counterterrorism Center, and establishment of an Information Sharing Environment all reflect serious attention toward intelligence and information sharing.[16] Numerous obstacles still exist,[17] but the consensus is that information sharing is improving.

THIS STUDY

This study examines how terrorism-related intelligence and information is shared between local police, on the one hand, and state police, federal law enforcement, intelligence agencies, and the military in the post-9/11 era. It was understood that federal laws, state laws, secrecy provisions, and security clearances all affect what can be shared in different situations.[18] Also, it was presumed that most local police had longstanding communication channels with state and federal law enforcement (whether effective or ineffective), but not with intelligence agencies or the military. Thus, if local police came into possession of information that might be of interest to a federal agency, intelligence agency, or the military, what would they do? Similarly, if the military or CIA

came upon some information in Central Asia with ramifications for a local community in Middle America, what would they do?

Methodology

Six short scenarios/vignettes were sent to a small non-random sample of subject matter experts in 2008. The scenarios were designed to represent a variety of realistic situations in which information sharing might be desirable and might or might not occur. The common ingredient in each scenario was a Kentucky connection, only because both authors taught at Eastern Kentucky University at the time. The main purpose was to ground the scenarios in a typical and realistic setting, without introducing the complexity that might ensue if the location was New York, Los Angeles, or Washington, DC.

Responses to the scenarios were obtained from fourteen experts. Of these, ten were police executives (identified hereafter as PE) or police intelligence (PI) practitioners, two were associated with military intelligence (MI), one was associated with federal law enforcement (FE), and one was an academic expert (AE). The police respondents represented six different states while the other respondents were also distributed around the country.

The small size of the sample significantly limits any claims of statistical validity, as does the weighting of the sample toward police respondents. It is best to think of this study as an initial exploration of information sharing among police, intelligence agencies, and the military without any pretense that it accomplished a scientific measurement of the phenomenon.

Scenarios

We asked the subject matter experts to respond to several hypothetical scenarios that combined crime, terrorism, and information sharing issues. Six scenarios were presented following some general instructions:

> Listed below are several hypothetical scenarios that might involve information sharing among local, state, and federal law enforcement, intelligence agencies, and military agencies. Each scenario has a Kentucky connection, but you may feel free to apply it to your own local jurisdiction. We would appreciate any insight you could provide regarding two things in each scenario:
>
> - What *would* probably happen today in regard to information sharing?
> - What *should* happen, in your opinion?
>
> **Scenario A**: U.S. Army forces in Afghanistan find a computer in a terrorist camp that contains images of a chemical plant in Ashland, KY.
>
> **Scenario B**: A CIA agent in Africa observes a U.S. citizen meeting with elements of Al Qaeda. It is determined that the U.S. citizen lives in Elizabethtown, KY, which is near Fort Knox.
>
> **Scenario C**: A police officer in Hopkinsville, KY, near Fort Campbell, is told by a citizen that she (the citizen) knows an active duty soldier who has

rocket-propelled grenades (RPG) in his garage. She says that he (the soldier) often talks about how easy it would be to shoot down a passenger airplane near the Nashville airport.

Scenario D: A police officer in Lexington, KY, while handling a domestic dispute call at a residence in the city, sees quite a few interesting pieces of art. Casual inquiry reveals that the husband in the house is an Army reserve doctor recently returned from a tour of duty in Iraq. The officer wonders whether the pieces of art might be stolen antiquities.

Scenario E: A police officer in Louisville, KY responds to a call at a private residence. The parents of a 15-year-old boy show the officer the boy's computer, on which they found an elaborate plan to assemble a fertilizer truck bomb and explode it outside an Army recruiting station in Cincinnati, OH.

Scenario F: An FBI analyst develops an intelligence report that indicates that organized groups are smuggling significant quantities of cigarettes out of Kentucky for resale in northern states where taxes are higher, and then sending the profits overseas to groups that are affiliated with Hezbollah.

SHARING BY AND WITH LOCAL POLICE

The post-9/11 focus on local police has mainly been on their role as "eyes and ears" in local communities throughout the nation. In this respect they are seen as very important collectors of information, of raw data that can be fed into the intelligence process in order to help analysts and others "connect the dots." Community policing is seen by some as an ideal local police strategy because it helps officers get to know their communities and builds trust, making it more likely that residents will share important information with the police.[19] It has become common to refer to local police as "first preventers" who are most likely to be in a position to prevent a terrorist act, both by gathering information and by taking action, when appropriate. This first preventer role is paired with the more familiar "first responder" role to make a logical and meaningful package that (1) demonstrates the synergy between effective crime reduction tactics and counterterrorism and (2) encourages local police to take their counterterrorism role more seriously.[20]

The *National Strategy for Information Sharing* reiterated this expanded role for local police and provided a few specific examples:

> These partners are now a critical component of our Nation's security capability as both "first preventers" and "first responders," and their efforts have achieved concrete results within their communities, as the following examples illustrate:
>
> - A narcotics investigation – conducted by Federal, State, and local law enforcement officials and resulting in multiple arrests – revealed that a Canadian-based organization supplying precursor chemicals to Mexican methamphetamine producers was in fact a Hezbollah support cell.
> - A local police detective investigating a gas station robbery uncovered a homegrown jihadist cell planning a series of attacks.

- An investigation into cigarette smuggling initiated by a county sheriff's department uncovered a Hezbollah support cell operating in several States.[21]

Scenarios C, D, and E all focused on suspicious activity discovered by local police. None apparently involved international terrorism, but one or two might involve domestic terrorism, one might involve transnational crime, and all three involved the military in some way.

Most project interviewees agreed that the local police department in Scenario C should, and would, forward its information about the soldier with the RPG to federal and/or military authorities. There was some disagreement over details, such as whether the investigation should be handled by the appropriate Joint Terrorism Task Force (JTTF) or the military. Some variation in responses might have resulted because the scenario did not clearly specify whether the soldier's garage was on or off the military base. One respondent indicated that the proper response *should* involve both information sharing and collaboration:

> The local police should investigate the soldier with members of the FBI and the military in a joint investigation since both criminal and possible terrorism activity may be involved. If follow up is warranted with the TSA and the Nashville airport, it should be the responsibility of the FBI. But in this case both criminal and national security intelligence may be obtained and can be disseminated to sworn law enforcement in the Nashville Airport area if a reasonable suspicion of an attack on a plane is detected. If the reason for wanting to shoot the plane is one of terror as opposed to some personal animosity, then the subject should also be entered into VGTOF (the Violent Gang and Terrorist Organization File in NCIC). (PI)

This same respondent, though, indicated that what *would* happen might be less collaborative – the local police would conduct an investigation and they might contact the Transportation Security Administration (TSA) or the Nashville airport. From an information-sharing and intelligence standpoint, the possibility of the local police department conducting its own investigation without informing any other authorities would be the least desirable response, but also problematic could be joint investigations if they were initiated outside post-9/11 information-sharing procedures. For example, if the police and the Fort Campbell MPs conducted an investigation, or if the police and the local FBI office conducted an investigation, the raw information might never make it to the local agency's intelligence unit, the state fusion center, the applicable JTTF, or the National Counterterrorism Center (NCTC). One respondent noted:

> Sharing of information with the military is always a problem. There are also problems associated with local information that is sent to the FBI first instead of traveling through normal local reporting structures first. If suspect information goes directly to the FBI, or other federal entity, the information is not generally disseminated down to the local level in a timely manner. Unfortunately, when this occurs, local intelligence information is often lost. Additionally, vulnerability assessments could be updated and local law enforcement resources could be allocated towards prevention efforts when local intelligence is received in a timely manner. (PI)

Scenario D was at most criminal in nature (possible possession of stolen art from Iraq) but involved a military service member. Respondents seemed to be split about evenly on whether the matter would be handled strictly by the local police or referred to either military or federal law enforcement. Since the evidence that a crime had occurred was limited, some thought the likelihood of any action was minimal. Most seemed to agree, though, that the proper action would be to share the information with the military. For example:

> Contact with military investigators should be made by the local agency sharing what the officer observed. Military should investigate and provide a follow up call back to the initiating agency as to whether or not the art is possibly stolen. In this case, if the military determines that there is reasonable suspicion that the paintings are stolen, possession of those paintings is then a crime and intelligence reports on the subject can be shared between the military police and the initiating agency. (PI)

Scenario E involved a possible threat to a military recruiting station. Because it involved the threat of explosives, it elicited a familiar difference of opinion about whether the proper federal agency to contact should be the FBI or the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). These two agencies have feuded for years over the lead federal role in explosives investigation, resulting in conflict between the agencies, competition over specific cases, and mixed signals sent to state and local law enforcement. A 2009 U.S. Department of Justice Inspector General's report indicates that this situation still persists.[22]

There was also a split of opinions on whether the local police would conduct their own investigation, whether they would hand it off to the FBI, whether the military would be notified in a timely manner, and whether a joint investigation would ensue. Two examples:

> My guess is this would be handled completely by local authorities. It appears to be only peripherally related to the military. Ideally, the recruiting commander would be contacted, which would probably result in contact from Army CID. The information should be shared here, but it may never get out of CID. (MI)

> The local agency would share the information with the FBI and in turn the FBI would most likely investigate the boy directly prior to contacting the military. If the FBI determines that the subject is indeed a possible threat, he would be entered into VGTOF. (PI)

There was more agreement about what *should* happen in this scenario – information should be shared and a joint investigation should be conducted. Responses varied on whether the conduit for information sharing should be a regional or state fusion center or some other network such as the Terrorism Early Warning Groups (TEWG) that have been set up in some areas of the country. Since the scenario involved two local police departments in different states, as well as the military connection, established channels would seem to be important in making sure that information and intelligence sharing crossed state borders as well as agency boundaries.

One respondent provided detailed information on additional steps that would be taken in his jurisdiction. This response strayed from the basic questions about information and intelligence sharing, but is worth reviewing because it illustrates the

kinds of concerns that local agencies have beyond just investigating a possible crime; they also tend to worry about others who might be involved, others who might have similar ideas, copycats, as well as fallout in the local community.

> The local police agency School Resource Officer (SRO) would be briefed and analysis would be conducted as to evidence of theft or purchase of various items needed to carry out any attack. Local police would also update local military recruiting stations and look for pre-incident indicators. A coordinated follow up with the military would be conducted.
>
> Since this type of information involves the internet and therefore could permeate our schools, our computer crimes unit would be used to monitor this type of activity as it relates to this suspect. Chances are if one student has this type of information, there are many more out there that may also be involved in criminal activity and not discovered by parents, schools, or others. The local police agency would not be satisfied with catching one student, but rather they would embark on an effort to educate parents and schools on how to be more vigilant at detecting these types of crimes. Specific computer and internet investigations into this activity may be warranted. (PI)

STATE POLICE

The post-9/11 environment has had potentially significant consequences for state police agencies.[23] Each state has set up some type of homeland security apparatus to advise the governor and the legislature, oversee statewide threat assessment and infrastructure protection, receive and distribute DHS funds, provide training and assistance to local jurisdictions, etc. In many if not most states, the state police have naturally assumed a large role in these activities, since they are usually the largest state public safety agency (other than corrections, which has limited expertise on the counterterrorism issue and little responsibility for terrorism prevention, response, or investigation). The development of state fusion centers has also typically been with substantial state police involvement – the state police usually had a pre-existing intelligence unit,[24] and they were often already serving as a principal point of contact for federal law enforcement and national intelligence agencies.

Interestingly, though, none of the scenarios used in this project elicited many responses that involved state police *per se*. One or two responses included the state police among the range of agencies that should be notified about some information or threat revealed in the scenario. One respondent referred several times to the fact that the state police in his state dominate the new fusion center but that information sharing is no better than in the past.

> Our state police Intelligence Branch has been a failure for decades for agencies other than themselves. Even past state police intel commanders will admit that, because of the very nature of the state police to horde information and not share it with others. I have witnessed local intelligence meetings where the state police and at times the FBI have attended and the meeting starts with asking them what they have brought to share. After hearing each of them (mostly state police) say they have nothing to report the group goes around the room and everyone says the same thing. A few words are given of thanks and the meeting has adjourned only to reconvene after the state police have left the building. Then the real

> information is shared among the locals with a vow of not giving anything to the state police.
>
> We have many statutes that require us to report to the state police but none to require them to share information back to anyone. To state the problem simply: the state police have an inherent distrust for local LE and all local LE does is mirror that distrust right back at them. (PE)

Several factors may account for the apparent low level of state police involvement in the new information sharing environment. One possibility is that the scenarios simply did not incorporate elements that would have made state police participation more relevant. A second is that state police are a relatively small slice of the law enforcement pie. Also, state fusion centers may have superseded state police agencies as the principal state-level cogs in the system – if so, this probably just reflects how the new system is supposed to operate. Additionally, though, it is probably the case that many local agencies have their own direct connections to the JTTF, FBI, or other federal agencies, so that no state-level involvement is initiated in many situations. From an efficiency standpoint this may seem desirable; however, it might limit information sharing and intelligence development if pertinent information does not also find its way to broader networks such as the state fusion centers or the NCTC.

FEDERAL LAW ENFORCEMENT

Scenario F used for this project specifically involved intelligence developed by an FBI analyst relating cigarette smuggling and an international terrorist group. The general consensus of respondents was that the FBI would either keep the intelligence to itself and conduct an investigation, or they would collaborate with other federal/national/military agencies for additional information gathering and investigation. Two interviewees thought that the FBI would work with the ATF due to the cigarette (tobacco) angle. Three mentioned that the FBI would involve the appropriate JTTF, which might be a means of limited information sharing with local police, although the intelligence would probably be classified and therefore not widely shared. Also, one respondent indicated that the frequency of JTTF meetings might not be sufficient to count on them for timely information sharing.

> It is likely this will be a strictly FBI operation. Although it would be good for local authorities to know about the investigation, I don't see it as necessary. It should be something that gets briefed in the next JTTF meeting. The difference in *probably* and *should* here is the frequency of the JTTF meetings. They should be no longer than quarterly (monthly is better) but I have heard that some JTTFs are meeting only rarely now. (MI)

This scenario raises a typical "need to know" vs. "need to share" issue. The new information-sharing environment is supposed to put greater emphasis on need to share.[25] One method for doing that, in this scenario, would be for the FBI to forward the intelligence report to the NCTC, which would presumably share it with other agencies as deemed appropriate. Another avenue would be to enter pertinent information in the NCIC VGOTF file. The former method would theoretically be more proactive, since it might result in intelligence about cigarette smuggling being widely shared with agencies

that could then use it in a variety of ways. The latter method would be more reactive – if an officer stopped a vehicle or person somewhere and made a NCIC query, they could be notified of the possible terrorism connection.

One respondent pointed out the importance of collaboration with local police in a situation of this type: "the local agency should be involved to assist with intelligence information they may have on the location, undercover vehicle stops, etc." (PI). Another potential value of following the "need to share" philosophy in this scenario was outlined by a different respondent.

> This type of generic information has been widely circulated for some time now; however, instead of working closely with local law enforcement agencies, this type of crime is typically worked solely by the FBI/JTTF for follow up.
>
> Since these types of crimes are not worked by local law enforcement officers, they lack the knowledge needed to effectively investigate crimes of this nature. It would be beneficial if more training was provided to local law enforcement in this area. Local law enforcement needs to recognize when this type of information should be forwarded to the appropriate intelligence agencies. More importantly, critical information on these types of crimes comes not only through reports or information analysis, but also through human sources. Human source development training should be enhanced to help local police officers develop homeland security sources at the local level. The private sector should also be better trained and utilized for recognition and timely reporting of suspicious criminal activity related to our homeland security. (PI)

Information sharing by and with federal law enforcement agencies was potentially involved in all the other scenarios used in this project. As previously noted, one concern is that information shared directly by a local police agency with the FBI, while appropriate for handling a particular investigation, may not get the wider dissemination or availability it deserves unless it is also sent to the local agency's intelligence unit, a fusion center, the NCTC, and/or the VGOTF. Also, cases involving explosives or cigarette smuggling should probably trigger collaboration between the FBI and ATF, but this may not always occur.

Scenario A involved military discovery of information in Central Asia with a possible terrorism link back to the U.S. (images of a chemical plant). Several respondents indicated that this information would probably be transmitted to the FBI, but whether it would then be shared with local or state police in the threatened jurisdiction might be problematic. Among the responses were these:

> May make the FBI Threat Matrix, but will not be released to local law enforcement unless authorized at the "Secret" level. I do not expect that local law enforcement would be notified, albeit they should. (PE)
>
> The State Fusion Center will receive the information – if it is not classified as "Top Secret;" and if they do they will most likely only share with their state police. At this point in time, the likelihood of the local police department or county sheriff being notified is slim to none. (PE)
>
> The information *would* flow from military channels to the FBI. The information would be classified and passed through to the local JTTFs. The information would stay at that level with no notification of the local agency … the [local]

> agency *should* be contacted and the substance of the information *should* be passed on. The source information does not need to be included. (PI)
>
> If the military chose to share this information, they would be forced to share it at the federal level which usually means the FBI. The FBI would assume responsibility for follow up and investigation. Local police agencies would have to rely on the release of information from a local FBI/JTTF office in order for the local police to be involved. Many local police departments do not have direct contact with FBI/JTTF offices. (PI)

As responses to these scenarios illustrate, there remains a good bit of skepticism about the free flow of information from federal law enforcement agencies. Improved systems for information sharing have been established but they are not always used. The 2007 *National Strategy for Information Sharing* and 2008 *Information Sharing Environment* provide additional enhancements that should continue the improvements already made. Traditional obstacles and barriers certainly remain even though progress has been made.

> Since 9/11, information sharing between the federal government and state and locals has improved. Most of the improvement has come through the FBI's Joint Terrorism Task Force (JTTF), which has tripled in number from 34 before September 11 to 100 today. In Los Angeles and other large departments across the country, there are active levels of communication and cooperation with the Department of Homeland Security and the FBI.
>
> Despite this progress, the level of cooperation seems to vary greatly, depending on the personalities of individual bureau and police chiefs. Too often, the FBI cuts itself off from local police manpower, expertise, and intelligence. More than 6,000 state and local police now have federal security clearances, but the historical lack of trust is still an issue. For example, many police chiefs complain of calls they get from their JTTF alerting them to a potential threat, but when they ask for the detailed information needed to launch an investigation, they are told by the bureau: "We can't tell you" or "You don't need to know." [26]

NATIONAL INTELLIGENCE AGENCIES AND THE MILITARY

This project's Scenario B posed the situation of a CIA agent in Africa observing a U.S. citizen meeting with elements of Al Qaeda. This is a situation involving international terrorism, a covert observation made overseas, and information collected by a national intelligence agency. The respondents were mixed on whether the information would be kept by the CIA, shared with the military, or shared with the FBI. Most were fairly certain that local and state police in the citizen's hometown and state would probably not be informed.

> Unless the CIA agent has a friend in the FBI in Kentucky, it is likely this information will not go beyond the CIA. What *should* happen is that both the KY FBI and Army Intelligence should be notified of the person and a joint investigation conducted to determine if there is any link to activities occurring in Kentucky. The FBI would likely run the investigation, but Fort Knox security should be notified and kept up on any potential links/threats to the base. (MI)

> A peripheral check into the subject's background *would* be performed by the CIA and without further results would cause the subject to be entered into a database accessed only by the CIA or Military. This information might be shared with Fort Knox but not with local agencies surrounding the base … The subject *should* be thoroughly investigated by the FBI including contacting local agencies to see if the subject might be wanted on criminal charges unrelated to terrorism. Often an arrest and follow up interview can provide an opportunity to obtain further information regarding the terrorism angle. The subject should also be entered into VGTOF through NCIC to alert local police once they have contacted the subject that he may be involved in terrorism activities. (PI)

> Currently, the information would not necessarily be disseminated to local law enforcement agencies in a timely manner. Information sharing on U.S. Citizens abroad is usually limited to local law enforcement sending local information up the intelligence chain about subject activities while they were in the U.S. Local police would not receive information directly from the CIA, but would rely on information passed from the CIA to the FBI and then hopefully to the local police. Information collected abroad would need to be sanitized to enable timely dissemination to local law enforcement. (PI)

A consequence in this scenario of restricted information sharing *up* from the local police level was also anticipated by one police executive.

> The information will stay with the CIA and maybe will be shared with the FBI. I do not believe the information will be pushed down to any lower levels at this time. However, due to the nature of information not going up from the local level to the Fusion Center, there may be valuable information about this citizen in local police data bases and because of the lack of trust, lack of cooperation and lack of quality information sharing back and forth between local LE and state police, the information will therefore never be shared with the CIA. (PE)

Scenario A is the only one that began with the military, in this case soldiers discovering a computer in a cave in Central Asia containing images of a U.S. chemical plant. Several respondents suspected that the information would be retained by the military, while others believed it would be shared with the FBI.

> The information *should* be forwarded by the DOD intelligence component through the National Counterterrorism Center (NCTC), which would forward it to the KY fusion center who then share it with all appropriate LE agencies in KY … [but] there is a good chance the NCTC would not receive the information. (AE)

> Given there is no information in the scenario about pending attack (only images), it is likely nothing would be done and no information shared until after [final analysis of the computer]. Usually, the Army/DOD is pretty good about getting information like this to the FBI. It would likely flow to the SAC with responsibility for Ashland. From there, it all depends on the relationship between the Kentucky FBI and local entities. (MI)

> This would be classified by the military at the Secret, most likely Top Secret level, and sent to analysis by Central Command. I do not expect to hear anything further on this in time to be actionable. May make the FBI Threat Matrix, but will not be released to local law enforcement unless authorized at the Secret level. I do not expect that local law enforcement would be notified, albeit they should. (PE)

None of the project interviewees expected any prompt information sharing with the local police in the chemical plant's jurisdiction. Notification to the chemical plant's corporate security seemed about as likely as to local police. One specific problem interfering with sharing of the information was its likely classification as secret or top secret.

> The issues are two-fold: first, although necessary for national security, the laws pertaining to sharing intelligence information between law enforcement and the military (*posse comitatus*) have not been updated and do not adequately address the loss of information in the critical need to exchange information. Secondly, instead of sanitizing information so it can be easily disseminated to law enforcement officers, similar information would usually be over-classified and therefore would never be disseminated to those who need the information the most. (PI)

Despite the fact that this information would most likely be held closely and not promptly shared with local authorities (if shared at all), several respondents felt wider sharing would be beneficial.

> The differences between what is likely and what should be are these: (1) the information about the images should be initially released as soon as they are discovered (initial analysis). Doesn't have to be extensive, but the authorities in Ashland should know about it early; (2) there should be some formal information sharing arrangements between DOD and FBI about cases like this (if they don't already exist); (3) there should be an investigation opened by the FBI and locals to determine if there is something that should be investigated further indicating a potential attack and why the images were gathered. (MI)

> This information should be shared with the FBI to evaluate as national security intelligence. Follow up should be completed by the FBI with any law enforcement agencies which may respond to a call for service in the event something happens to the plant. Since the information does not center around a person (yet), the right to privacy is not an issue and the intelligence generated from it may be shared. (PI)

> This type of information should be shared and analyzed at a variety of levels in order to obtain a better view of its relevance to local criminal activities. The information should be shared through timely channels and analyzed not only by the military, but at the national, state, regional, county, tribal and local levels. By viewing the information from a variety of perspectives, there would be a greater chance of filling the intelligence gap and turning information into actionable intelligence. Sharing information would also foster greater cooperation between agencies rather than local law enforcement learning about local threats through the National media. Timely sharing of information would also allow local law enforcement officers to implement a more effective collection plan of new information, which may generate more pieces of intelligence related to local threats. (PI)

DISCUSSION

It seems apparent that procedures and protocols for counterterrorism information sharing have not achieved full implementation. Subject matter experts responding to six scenarios often differed in what they thought *should* happen, and often judged that what *would* happen would be less than full-scale information sharing. Most expected that investigations would be narrower and less collaborative than desirable. In many cases the experts thought information sharing would not be as systematic as it should, between and among intelligence agencies and especially with local police. Some opportunities to engage local police in intelligence gathering were not expected to be utilized because doing so might require intelligence agencies to take police into their confidence. Over-classification of intelligence was expected to interfere with information sharing. Often, the likelihood of information sharing was seen as dependent on the existence of personal contacts and relationships.

Part of the explanation for differences in what *should* happen follows from the complexity of the inter-organizational environment surrounding counter-terrorism. The police system has 18,000 separate agencies, including 18,000 CEOs and, potentially, 18,000 terrorism liaison officers. The number of national intelligence and military intelligence agencies is much smaller but each of these agencies is large and complex in its own right. This extremely large inter-organizational set exists within a maze of federal and state law, bureaucratic rules, traditions, customs, and politics.

Another part of the explanation is that the situation is new and evolving. Local police have little experience at counterterrorism or domestic/homeland security intelligence. Before 9/11 they had little reason to interact with national intelligence or military intelligence agencies. The notion of transnational crime was exotic enough for most police agencies – international terrorism seemed even less likely to affect Main Street, city hall, or hometown security. Now, suddenly, there are state fusion centers and a complicated information sharing environment of new alphabet-soup federal agencies including the Office of the Director of National Intelligence (ODNI), NCTC, and the Interagency Threat Assessment and Coordination Group (ITACG).

Besides complexity and newness, though, there seems to be a great deal of residual resentment and tension clogging counterterrorism information-sharing channels, affecting what *would* happen in various scenarios. The "need to know" mentality still seems to outweigh the "need to share" mentality. Petty inter-agency jealousies seem to remain, as evidenced most recently between the FBI and the NYPD (whose counterterrorism chief is a former CIA official) in the Najibullah Zazi case.[27] Local agencies still think of information sharing as a one-way experience, lacking confidence that state police, fusion centers, or federal agencies will share information with local agencies and officials when they should.

At the state level, it seems absolutely essential in the new information sharing environment that fusion centers learn to function as state-wide entities rather than state police entities. In the former mode, they stand a chance of being perceived as serving all agencies in the state, and if they in fact disseminate useful information and products to all agencies, they should become critical assets for both intra-state and national information sharing.[28] On the other hand, if they come to be seen as glorified state police units serving state police interests first and foremost, then they will provide little added value and will not substantially improve information sharing. Local agencies will tend not to participate, they will create their own fusion centers when possible, and they

will continue to create their own individual relationships with federal agencies in an ad hoc manner. This seems to be a very crucial distinction that is still being worked out around the country, with no guarantee of success.

Beyond the state level, it is interesting that only two of the respondents consistently referred to the NCTC and information sharing environment throughout the scenarios, and none referred to the ITACG. The NCTC was established in 2004 and includes federal law enforcement agencies, national intelligence agencies, and the military among its partner organizations. As described on the NCTC website:

> NCTC serves as the primary organization in the United States Government for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the United States Government (except purely domestic terrorism); serves as the central and shared knowledge bank on terrorism information; [and] provides all-source intelligence support to government-wide counterterrorism activities.[29]

The NCTC is assisted by the ITACG, which specifically represents the interests of state and local law enforcement and related officials. Its purpose is to enable and facilitate the production of "federally-coordinated" terrorism-related information and products that are shared "through existing channels" with state and local agencies. The ITACG is billed as a temporary step in coordinating federal law enforcement and national intelligence communication with state and local agencies, "until such time as the ISE matures organizationally and culturally to satisfy those needs as a normal part of doing business."

Together, these new entities, along with the 2007 *National Strategy for Information Sharing* and the *Intelligence Community Information Sharing Strategy*,[30] are supposed to assure that terrorism-related information and intelligence are shared more effectively among all the counterterrorism players, including state and local police, federal law enforcement, federal and state homeland security operations, the national intelligence community, and the military. The fact that much of this new architecture and strategy was not cited by most project respondents may reflect its newness, or it may indicate that old habits have yet to be replaced by new ones.[31]

RECOMMENDATIONS

This small exploratory study is not a firm foundation from which to offer any strong recommendations for improving intelligence and information sharing. Moreover, the complexity of the inter-organizational environment of law enforcement-related and homeland security-related information sharing is daunting, comprised as it is of thousands of local, state, and federal agencies, plus the military. One would be hard pressed to design a more complicated or challenging system. Fundamentally, of course, it is a system intended to limit the power of the government rather than maximize its effectiveness.

A 2001 Government Accountability Office (GAO) report on information sharing for critical infrastructure protection emphasized the importance of building trust between officials and agencies.[32] Recommended techniques for building trust included regular interaction, consistent representation, appropriate vetting of participants, creation of an

atmosphere of mutual respect, and enforcement of information sharing norms. Additional recommendations included timely and secure communication, top management support, leadership continuity, penalties for failing to share information, and rewards for sharing.

Beyond these basic principles, a few specific intelligence-sharing suggestions can be offered:

- State fusion centers have to figure out how to serve their entire state, not just the state police. DHS might insist that these centers have governing boards with majority local representatives. That would help get local law enforcement buy-in and participation. State police could still house or run the centers, but they would have to be responsive to local interests in order to maintain the support of their governing board.
- Model agreements between local law enforcement agencies and state fusion centers should be developed and implemented. These agreements could stipulate that the local agency will complete and submit SAR in a systematic and timely manner, but also mandate the fusion center to report back on SAR utilization and generally obligate the fusion center to operate on a "need to share" basis.
- All agencies should adopt the "tear line" practice as a means of implementing "need to share." This practice puts non-classified information found in intelligence reports below a "tear line" so that it can be disseminated more quickly and more broadly. Information that would compromise intelligence sources and methods remains "above the tear line" and still does not get disseminated except to qualified recipients who "need to know."
- JTTF meetings need to be held with reasonable frequency to keep local chiefs and commanders in the intelligence loop and to build and maintain the trust needed to encourage information sharing. If these meetings are held frequently, and if "need to share" is the operating philosophy, then local law enforcement suspicion and resentment can easily be minimized.

As simplistic as some of these recommendations sound, they would probably be sufficient to resolve much of the gridlock associated with local law enforcement's participation in counterterrorism intelligence and information sharing. That is because, with the exception of the NYPD and a very few other big city agencies, local police agencies do not see themselves in competition with each other or with state and federal agencies in the intelligence game. Most of them would like to play their role and do their part, as long as state and federal agencies cooperate and treat them fairly.

At the federal level, the situation is different. Federal law enforcement and intelligence agencies often do seem to regard each other as the competition. They also seem to regard local law enforcement agencies as inferior or perhaps untrustworthy (or, in the case of the NYPD, as competition). Beyond systematic and persistent efforts at trust building, forceful action by the president, attorney general, DHS secretary, and Congress would seem necessary to overcome longstanding traditions and the political/bureaucratic pathologies that currently inhibit significant improvement in information sharing among the heavyweight agencies in the national intelligence

community, and between those agencies and their more humble counterparts in state and local law enforcement.

Gary Cordner *is professor of criminal justice at Kutztown University in Pennsylvania and a commissioner with the Commission on Accreditation for Law Enforcement Agencies (CALEA). Previously, he was police chief in St. Michaels, Maryland and Dean of the College of Justice & Safety at Eastern Kentucky University. Dr. Cordner earned his PhD from Michigan State University. He may be contacted at cordner@kutztown.edu.*

Kathryn Scarborough *is on leave from her position as professor in the Department of Security, Safety, and Emergency Management at Eastern Kentucky University. She is co-author of textbooks on police administration and women in law enforcement and has directed several projects focused on law enforcement technology, cyber crime, and police intelligence. Dr. Scarborough worked as a police officer in Virginia and earned her PhD in criminal justice from Sam Houston State University.*

Acknowledgments: This article is derived from a study funded by the Homeland Security Defense Education Consortium (now the Homeland Security Defense Education Consortium Association). Any errors or misrepresentations in the paper are solely the responsibility of the authors. Points of view expressed in the paper are the authors' and do not represent the views of HSDEC or the Department of Defense. The authors are grateful for the support of HSDEC and specifically for encouragement and assistance provided by Houston Polson and Lance Robinson.

---

[1] Gary Cordner and Kathryn Scarborough, "Connecting Police Intelligence with Military and National Intelligence," in Keith Logan, ed., *Homeland Security and Intelligence* (New York: Praeger, forthcoming 2010).

[2] The terms "police" and "law enforcement" are used interchangeably in this article. Neither is meant to exclude sheriffs/deputy sheriffs, sworn investigators, or other similar officials.

[3] Brian A. Reaves, *Census of State and Local Law Enforcement Agencies* (Washington, DC: Bureau of Justice Statistics, 2007), http://www.ojp.usdog.gov/bjjs/pub/pdf/csllea04.pdf.

[4] The relative strength and roles played by municipal police, sheriffs, state police, and federal law enforcement vary from state to state. Louisiana is the most sheriff-dominated state (sheriffs as a proportion of all police), Delaware is the most state police dominant, and Arizona is the most federal law enforcement dominant. See Gary Cordner, "The Architecture of U.S. Policing: Variations Among the 50 States," *Police Practice and Research: An International Journal* (forthcoming, 2010) for more detailed description of this variation.

[5] Half of the 18,000 police agencies in the United States have ten or fewer sworn officers.

[6] Federal and/or state law sometimes assigns lead responsibilities and specific jurisdictions, as in the case of National Special Security Events (NSSEs). In most cases, though, the law does not specify who is in charge, and the relative standing of various agencies with concurrent jurisdiction is unspecified or at least ambiguous.

[7] Peter K. Manning, "Information Technologies and the Police," in Michael Tonry and Norval Morris, eds., *Modern Policing* (Chicago: University of Chicago Press, 1992), 370.

[8] David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (Washington, DC: Office of Community Oriented Policing Services, 2004).

[9] "Reopen SFPD's Intelligence-Gathering Unit," *San Francisco Examiner*, October 15, 2009, http://www.sfexaminer.com/opinion/Examiner-Editorial-Reopen-SFPDs-intelligence-gathering-unit-64317377.html#.

[10] Jerry H. Ratcliffe, *Intelligence-Led Policing* (Devon, UK: Willan Publishing, 2008).

[11] Lydia Khalil, "Is New York a Counterterrorism Model?" *Expert Brief* (New York: Council on Foreign Relations, September 10, 2009), http://www.cfr.org/publication/20174/counterterror_model_in_progress.html?breadcrumb=%2F; "NYPD Holds Security Briefing Ahead of High Holy Days," New York Police Department Press Release, September 14, 2009, http://www.nyc.gov/html/nypd/html/pr/pr_2009_ph22.shtml; Sullivan, John P. Sullivan and James J. Wirtz, "Global Metropolitan Policing: An Emerging Trend in Intelligence Sharing," *Homeland Security Affairs* 5, no. 2 (May 2009), http://www.hsaj.org/?fullarticle=5.2.4.

[12] Bureau of Justice Assistance (BJA), *Nationwide Suspicious Activity Reporting (SAR) Initiative* (Washington, DC: Bureau of Justice Assistance, 2009), http://www.iacptechnology.org/LEIM/2009Presentations/Nationwide%20SAR%20Initiative.pdf

[13] John Rollins and Timothy Connors, "State Fusion Center Processes and Procedures: Best Practices and Recommendations," *Policing Terrorism Report No. 2* (New York: Manhattan Institute for Policy Research, 2007), http://www.manhattan-institute.org/html/ptr_02.htm.

[14] U.S. Department of Homeland Security, "DHS Announces New Information-Sharing Tool to Help Fusion Centers Combat Terrorism," Press Release, September 14, 2009, http://www.dhs.gov/ynews/releases/pr_1252955298184.shtm.

[15] Chad Foster and Gary Cordner, *The Impact of Terrorism on State Law Enforcement: Adjusting to New Roles and Changing Conditions* (Lexington, KY: Council of State Governments, 2005).

[16] ISE, *Information Sharing Environment* (2008), http://www.ise.gov/; White House, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington, DC: White House, 2007), http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf.

[17] Kevin D. Eack, "State and Local Fusion Centers: Emerging Trends and Issues," *Homeland Security Affairs*, Supplement No. 2 (2008), http://www.hsaj.org/pages/supplement/issue2/pdfs/supplement.2.3.pdf; Jerry Markon, "FBI, ATF Battle for Control of Cases," *The Washington Post,* May 10, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/05/09/AR2008050903096.html; Richard B. Schmitt, "FBI is Called Slow to Join the Terrorism Fight," *Los Angeles Times,* May 9, 2008, http://www.latimes.com/news/nationworld/nation/la-na-intel9-2008may09,0,7865641.story; Nancy Bernkopf Tucker, "The Cultural Revolution in Intelligence: Interim Report," *The Washington Quarterly* (Spring 2008): 47-61.

[18] Carter, *Law Enforcement Intelligence*.

[19] Police Executive Research Forum (PERF), *Local Law Enforcement's Role in Preventing and Responding to Terrorism* (Washington, DC: Police Executive Research Forum, 2001), http://www.policeforum.org/upload/terrorismfinal%5B1%5D_715866088_12302005135139.pdf; Matthew Scheider and Robert Chapman, "Community Policing and Terrorism," *Journal of Homeland Security* (April 2003), http://www.homelandsecurity.org/newjournal/articles/scheider-chapman.html; International Association of Chiefs of Police (IACP), *From Hometown Security to Homeland Security* (Alexandria, VA: International Association of Chiefs of Police, 2005), http://www.theiacp.org/leg_policy/HomelandSecurityWP.PDF.

[20] George L. Kelling and William J. Bratton, "Policing Terrorism," *Civic Bulletin* No. 43 (New York: Manhattan Institute for Policy Research, 2006), http://www.manhattan-institute.org/html/cb_43.htm.

[21] White House, *National Strategy for Information Sharing,* 10.

[22] Devlin Barrett, "Law Enforcement Feuding Persists: Efforts to End FBI-ATF Disputes Unsuccessful, Mueller Says," *The Washington Post,* September 17, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/09/16/AR2009091603211.html; Theo Emery, "It's Official: The ATF and the FBI Don't Get Along," *Time,* October 24, 2009, http://www.time.com/time/nation/article/0,8599,1932091,00.html.

[23] The term "state police" is used to refer to each state's primary state law enforcement agency. Actual names include state police, state patrol, highway patrol, and department of public safety. The jurisdiction

and responsibility of these agencies varies from state to state. See Foster and Cordner, *The Impact of Terrorism*.

[24] Eack, "State and Local Fusion Centers."

[25] ISE, *Information Sharing Environment*.

[26] Kelling and Bratton, "Policing Terrorism."

[27] Michael A. Sheehan, "The Hatfields and McCoys of Counterterrorism," *The New York Times*, September 26, 2009, http://www.nytimes.com/2009/09/27/opinion/27sheehan.html?_r=1&th&emc=th.

[28] Rollins and Connors, "State Fusion Center Processes and Procedures;" Eileen R. Larence, "Federal Efforts Are Helping to Address Some Challenges Faced By State and Local Fusion Centers," Testimony before the Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland security and Governmental Affairs, U.S. Senate, GAO-08-636T (Washington, DC: Government Accountability Office, 2008).

[29] Information available at http://www.nctc.gov/.

[30] Director of National Intelligence, *Intelligence Community Information Sharing Strategy* (Washington, DC: Office of the Director of National Intelligence, 2008), http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf.

[31] Schmitt, "FBI is Called Slow to Joint the Terrorism Fight"; Tucker, "The Cultural Revolution in Intelligence."

[32] Government Accountability Office (GAO), *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, DC: GAO, 2001), http://www.gao.gov/new.items/d0224.pdf. The authors are indebted to one of *Homeland Security Affairs'* manuscript reviewers for suggesting this source.