The Intelligence Fusion Process for State, Local and Tribal Law Enforcement

David L. Carter, Ph.D.[1]
Michigan State University

Jeremy G. Carter
Indiana University – Purdue University Indianapolis

Abstract
Intelligence fusion centers have grown rapidly in the last few years as state, local and tribal law enforcement agencies have attempted to find the best way to share information about threats to their communities. The Department of Homeland Security and the Information Sharing Environment of the Office of the Director of National Intelligence embraced the fusion centers as being an important mechanism to aid them in their missions to share terrorism information among law enforcement, the private sector and the intelligence community. The development and management of fusion centers has received significant guidance from the Justice Department, via the Global Intelligence Working group, by developing standards for structure and processes. Critics, however, are concerned the centers have inadequate protections for privacy and civil rights. This paper examines the issues in the centers' development and provides an examination of the support and criticisms of fusion centers.

Keywords*:* law enforcement; intelligence; terrorism; fusion centers

Carter, D. L. & Carter, J. G. (2009). The intelligence fusion process for state, local and tribal law enforcement. *Criminal Justice and Behavior*, 36(12), 1323-1339

[1] Author Correspondence: School of Criminal Justice, Michigan State University, East Lansing, MI 48824-1118, (517) 355.6649, carterd@msu.edu

The Intelligence Fusion Process for State, Local and Tribal Law Enforcement

Over the last several years the U.S. Department of Homeland Security (DHS) has committed millions of dollars to help state and local law enforcement agencies develop intelligence fusion centers (Allen, 2008). While the funds have been readily accepted, concerns have been expressed about the efficiency of intelligence fusion centers (General Accountability Office, 2007), their effectiveness (Masse & Rollins, 2007) and whether there are adequate protections in place to protect citizens' privacy and civil rights (German & Stanley, 2007).

The fusion process represents a new generation for the intelligence function and a new structure for most state, local and tribal law enforcement agencies to understand. Contrary to intuition, the fusion process (analyzing information from diverse resources) and the creation of fusion centers (the physical plant) are more complex than merely changing organizational functions for an existing law enforcement intelligence unit. It typically involves either the re-engineering of the entire conceptual framework of the intelligence function in an agency or the creation of an entirely new entity. It requires engaging a wide array of people and organizations to be both contributors and consumers of the intelligence function; it involves changing attitudes and processes of personnel; it requires establishing new functional and information sharing processes among state, county, municipal, tribal and federal law enforcement partners; it involves the development of new agreements and functional relationships; the development of new policies and processes; and the inculcation of the Intelligence Led Policing[i] philosophy.

As a result, the challenges are multifold, not the least of which is opening oneself and one's agency to the challenges of organizational change. Most humans are dogmatic,

resisting change. However, if incongruent past practices and erroneous assumptions are not eliminated from the development processes of fusion centers, the likelihood of success is diminished. The following discussion is intended to provide insight about the intelligence fusion process by providing a perspective on its role and the challenges posed by the process.

Historical Perspective

Initially, intelligence fusion centers were referred to as Regional Intelligence Centers (RIC). They took different forms throughout the United States with no "single model" for what the intelligence center did or how it should be organized. They evolved largely based on local initiatives as a response to perceived threats related to crime, drug trafficking, and/or terrorism within a geographic region (Carter, Forthcoming). The intent was to marshal the resources and expertise of multiple agencies within that region to deal with cross-jurisdictional crime problems. In some cases, a region was defined as a county (e.g., Rockland County, New York Intelligence Center); as the area surrounding a major city (e.g., Los Angeles Joint Regional Intelligence Center); a portion of a state (e.g., Northern California Regional Intelligence Center), or it may encompass an entire state (e.g., Minnesota Joint Analysis Center) (Carter, Forthcoming).

Most of the earliest RICs began as the product of counterdrug initiatives starting in the 1980s. Indeed, the High Intensity Drug Trafficking Area (HIDTA) intelligence centers[ii] served as models for successful structures and initiatives as well as identifying systemic issues that needed to be overcome.[iii] The HIDTA centers embraced federal, state and local partnerships and focused on developing the expertise of their analysts to

provide intelligence to their operational consumers. Interestingly, the HIDTA Centers are organized under the Office of National Drug Control Policy (ONDCP) yet have personnel assigned from the Drug Enforcement Administration (DEA). Since they are organizationally separate from DEA they provide greater support to local task forces and agencies than the broader DEA operational missions. As time passed, DEA operations relied much more heavily on the El Paso Intelligence Center (EPIC) than on the HIDTA Intelligence Centers, although there is regional variation. As a result of this unique organizational framework and their unitary mission of drug control, the HIDTA Intelligence Centers, while effective in counterdrug operations, did not evolve into the "all crimes" fusion center model.

In the late 1990s, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) developed a number of new programs designed to reduce gun violence. Emerging from these initiatives were ATF Regional Crime Gun Centers. The centers, in some cases co-located with the HIDTA RIC, had a number of intelligence-related roles including "…analyzing trace data to identify gun traffickers, disseminate investigative leads, and coordinate with the HIDTA RIC to identify drug traffickers and their sources of guns" (ATF, 2008). In virtually all cases, both the HIDTA and ATF intelligence centers had a great deal of interaction with state, local and tribal law enforcement agencies. The intent was to integrate – i.e., "fuse" – information from diverse sources to better understand and prevent multi-jurisdictional crime problems.

Hence the foundation was laid for intelligence fusion centers. However, beyond idiosyncratic local crime issues, there was little incentive to expand the centers. Of course, this changed after September 11, 2001.

Because of the RICs demonstrated successes and the information sharing challenges of counterterrorism, additional state and local entities embraced the concept and began developing their own centers. The federal government, at first by the Department of Homeland Security (DHS), saw the value of these initiatives and began providing funding support. Fusion centers were about to experience an expanding role.

> Recognizing that state and local fusion centers represent a critical source of local information about potential threats and a mechanism for providing terrorism-related information and intelligence from federal sources, the Program Manager for the ISE (PM-ISE), the Department of Homeland Security (DHS), and the Department of Justice (DOJ) are taking steps to partner with and leverage fusion centers as part of the overall information sharing environment (General Accountability Office, 2007:2).

Building on this observation, the General Accountability Office (GAO) went on to document a number of federal efforts underway designed to support fusion centers and address challenges or obstacles identified by fusion center directors (General Accountability Office, 2007: 23-39).

The first effort cited by the GAO is that the DHS, FBI and the PM-ISE have taken actions to assist fusion centers in gaining access to and managing multiple federal information systems, including classified systems. This means that state, local and tribal fusion center personnel have access to information that may have been collected by the intelligence community and/or information that was collected via less stringent legal standards than is required for law enforcement agencies. Access to these systems is

viewed by law enforcement as an important factor in helping to "connect the dots" about threats, thereby more effectively protecting the community. Conversely, the American Civil Liberties Union (ACLU) is concerned that efforts such as this will turn "local police officers into national domestic intelligence agents" (German & Stanley, 2008:2).

The second effort is that both the DHS and FBI have committed to providing security clearances to state, local and tribal fusion center personnel and reducing the time it takes for a clearance to be processed. This has been a significant issue for law enforcement executives because they believe that state, local and tribal law enforcement personnel responsible for counterterrorism cannot be effective if they do not have routine access to classified information which reflects the most comprehensive information about threats. Once again, concern has been expressed by civil rights advocates that the widespread granting of security clearances to state, local and tribal law enforcement personnel is evidence that fusion centers and their personnel are becoming federalized. In turn, it is argued, that this will reduce privacy protections as well as reduce accountability of the fusion center to state and local governments (German & Stanley, 2007; German & Stanley, 2008; Electronic Privacy Information Center, 2008).

The next federal initiative is that the DHS and FBI are assisting fusion centers in obtaining and retaining qualified personnel, both through assignments of federal employees to state fusion centers and through some DHS funding support. The major concern on this issue relates to sustainability. Federal funding to state and local government is virtually always limited to a few years. If the fusion center is relying on federal support to operate, then its sustainability is tenuous. The *Fusion Center Guidelines* state that while federal funding can be important for fusion center

development, that the center's operation should rely on standard appropriated funds to help ensure sustainability (Global Intelligence Working Group, 2005:79). The other concern on this initiative is that fusion centers will rely on federal employees who will likely be reassigned when another problem or crisis takes precedence over the fusion centers.

The final two federal initiatives identified by the GAO are less controversial. The penultimate initiative is that federal funds in support of fusion centers have become more readily available and streamlined in operation to make grant awards faster and easier. Finally, both DOJ and DHS have provided training and technical assistance in support of fusion center development and maturation. On this last point, while the availability of training programs have increased, there are still comparatively limited offerings of these programs due largely to funding limitations. It is a massive task to provide law enforcement training throughout the United States. With comparatively small training staffs, the new intelligence training efforts have significant challenges to overcome.

While progress has been made in the evolution of fusion centers in a comparatively short amount of time, many observers and fusion center governing officers appear to believe that there is still a "long way to go" before fusion centers will seamlessly fulfill their envisioned role.

REFINING THE FUSION CENTER CONCEPT

It was clear after the 9/11 terrorists' attacks that there had been poor information sharing among and between all levels of law enforcement and the Intelligence Community (9/11 Commission, 2004). As more information was learned about the

terrorists and their minor encounters with state and local law enforcement in the weeks and months before the attacks, it was painfully evident that current information systems and processes were simply inadequate to deal with threats of this nature. It was also evident that if a diverse array of raw information was collected by different agencies, it would be essential to have a mechanism to provide data integration and analysis so its meaning would be of value to operational law enforcement personnel.

Increasingly, state and local law enforcement leaders recognized that the experiences of the HIDTA's and RIC's could be applied to counterterrorism. Because of the need to have two-way information sharing directly with federal law enforcement and indirectly with the Intelligence Community, the fusion centers, the FBI and DHS reached out to each other in order to develop fusion centers more holistically. Indeed, "federal departments and agencies—including DHS, FBI, and DOD—launched efforts to develop strategies to incorporate these fusion centers into their information and intelligence activities" (PM-ISE, 2006:18).

Masse and Rollins (2007) note that fusion centers represent a vital part of our nation's homeland security and rely on at least four presumptions. The first of which is that intelligence, and the intelligence process, play a vital role in preventing terrorist attacks. Second, it is essential to fuse a broader range of data, including nontraditional source data, to create a more comprehensive threat picture. Third, state, local, and tribal law enforcement and public sector agencies are in a unique position to make observations and collect information that may be central to the type of threat assessment referenced above. Lastly, having fusion activities take place at the sub-federal level can benefit state

and local communities, and possibly have national benefits as well (Masse & Rollins, 2007:3).

The initial focus of many new fusion centers was exclusively on terrorism – indeed, that still remains the case for a few of the centers such as the Georgia Information Sharing and Analysis Center (GISAC)[iv]. However, most of the centers broadened their focus to embrace "all crimes and all threats". The reason was twofold: First, it was recognized that most terrorist acts had a nexus with other crimes. Hence, focusing exclusively on terrorism may miss some important "indicators". Second, because there is a wide variety of crime, notably criminal enterprises, that were trans-jurisdictional and involved in complex criminality[v], it was recognized that the fusion process would be of value in dealing with these crimes also.

Further evolution of fusion center responsibilities has moved into the arena of an "all hazards" focus (in addition to "all crimes, all threats"). Inclusion of the "all hazards" approach has come from two sources: One is a result of the special conditions on some DHS grants to fusion centers that specify "all hazards". The second source is from state or fusion center governing board mandates. Moreover, given DHS's responsibility to "protect the homeland", their reach extends beyond terrorism to include natural disasters, chemical weapons, weapons of mass destruction and basic law enforcement (Harris, 2008).

Recognizing fusion centers were increasingly integrating the concepts of established law enforcement intelligence activities with the "all crimes, all threats, all hazards" model of intelligence, the Homeland Security Advisory Council (HSAC) observed:

> Although the primary emphasis of intelligence/information fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to state, tribal and local entities is that it will support ongoing efforts to address non-terrorism related issues by…allowing State and local entities to better identify and forecast emerging crime, public health, and quality-of-life trends…supporting targeted law enforcement and other multidisciplinary, proactive, risk-based and community-focused, problem-solving activities; and…improving the delivery of emergency and nonemergency services (HSAC, 2005:2).

Structural Issues

There is no single model for a fusion center because of the diverse needs and environmental characteristics that will affect the structure, processes and products of a center. In states such as Texas and California with their large land mass, large populations and international border, the structure and processes of fusion centers will be significantly different than predominantly "land locked" rural states such as Wyoming or Nebraska.

A Congressional Research Service (CRS) report observed that questions have arisen regarding the current and/or potential efficacy of fusion centers. The report notes that in light of the growth of the fusion centers in state and local jurisdictions without a coordinated national plan, "…there appears to be no 'one-size-fits-all' structural or operational model for fusion centers (Masse & Rollins, 2007:18)." From a centralized

federal perspective – as reflected in the CRS report – the lack of a uniform model is assumed to be a flaw. However, the state and local perspective is somewhat different. Indeed, the ability to build a fusion center around grassroots needs is preferred – this permits state and local agencies to mold the fusion center into a model that best suits the needs and challenges that are idiosyncratic to each jurisdiction. As noted by Johnson and Dorn, describing the New York State Intelligence Center (NYSIC):

> Creating one center for intelligence and terrorism information – to combine and distribute that information to law enforcement agencies statewide – prevents duplication of effort by multiple agencies. Additionally, one state fusion center serving the entire New York law enforcement community provides a comprehensive picture of criminal and terrorists networks, aids in the fight against future terrorists events and reduces crime (Johnson & Dorn, 2008:38).

Within this same line of thought, fusion centers are also structured differently based upon legislative or executive mandates. For example, Montana's fusion center – Montana All Threat Intelligence Center (MATIC) – is mandated to focus on "all threats"; the New Jersey Regional Operations Intelligence Center (ROIC) includes emergency operations as well as fusion; the Massachusetts Commonwealth Fusion Center (CFC) focuses on all crimes; and the Oregon Terrorism Intelligence Threat Assessment Network limits its focus to terrorism. The variability of fusion center structures is broad because of functional necessity and the inherent nature of "local control" and "states' rights" perspectives.

While the structure and operational processes of fusion centers may be different, national professional standards have nonetheless been articulated which outline "good practice" in critical administrative areas regardless of the center's mission. That is the intent of the *Fusion Center Guidelines*.[vi]

Despite some criticisms, the fact that fusion centers are structured differently is not a weakness, but a strength. It exemplifies that each center is designed to meet local and regional needs as well as being able to best integrate the fusion center with existing organizational components and priorities.

For example, the Michigan State Police have widespread responsibility for both traffic and criminal law enforcement throughout the state. As such, the Michigan Intelligence Operations Center (MIOC) is organizationally placed in the state police. However, Florida has two predominant state law enforcement organizations: the Florida Highway Patrol, responsible for traffic law enforcement, and the Florida Department of Law Enforcement (FDLE), responsible for criminal law enforcement. As a result, the Florida Fusion Center is organized as part of the FDLE Office of Statewide Intelligence. Hence, each state structured its fusion center in a manner that best fits existing organizational structures and functional responsibilities.

The point to note is there are different operational and functional models of law enforcement throughout the United States. Fusion centers are no different since they are an element of state or local government and have the challenge to meet the unique needs of the jurisdiction they serve. As observed in one study,

> Fusion centers [must identify] their mission and their customers, at what level of analytic product they will produce, and to whom.

> Not all fusion centers will need the same amount of strategic analysis or tactical analysis, but, in order to determine what to produce, they will have to understand their customers' needs and ensure they are educated so they understand the difference between the two products. Fusion centers will also need to determine how they will integrate the emergency responder community (Nenneman, 2008:109).

It is, perhaps, this last point that will be the most challenging to define since "all hazards intelligence" and "meeting the needs of the emergency responder community" are not traditional roles for the law enforcement intelligence function. Some guidance to assist fusion centers in this area is being developed through the identification of "baseline capabilities".

Baseline Capabilities for Intelligence Fusion Centers

As a result of national plans that seek to increase the efficiency and effectiveness of information sharing efforts, fusion centers serve as the interlink between state, local, and tribal law enforcement and the federal Information Sharing Environment for the exchange of terrorism information. As such, it was recognized that there was a need to define fundamental baseline operational capabilities that should be used by fusion centers, as well as major urban area intelligence units, in order to meet the information needs of all consumers of the various intelligence centers. In practice, the "baseline capabilities" serve as performance standards that can be used to measure effectiveness of the fusion center, of the fusion process and of personnel.

A joint project of the Global Intelligence Working Group, U.S. Department of Justice, U.S. Department of Homeland Security and the Program Manager-Information Sharing Environment, resulted in a companion document to the *Fusion Center Guidelines* that identifies elements that serve as the foundation for integrating state and major urban area fusion centers into the federal Information Sharing Environment. The project is based on the fusion process capabilities outlined in the 2007 Fusion Center Assessment and the 2007 and 2008 Homeland Security Grant Program, Fusion Capability Planning Tool Supplemental Resource (DHS, 2007). In addition to the 2007 Assessment, the baseline operational standards outlined in the project were developed using guidance provided in the *Fusion Center Guidelines*, the *National Criminal Intelligence Sharing Plan* (NCISP), the *Information Sharing Environment Implementation Plan*, and the U.S. Department of Homeland Security's *National Preparedness Guidelines* and *Target Capabilities List* (TCL). Relying on the guidance of these national standards, the baseline capabilities for fusion centers is guided by the requirements of the Presidential *National Strategy for Information Sharing*.

The limitation, however, is that the capabilities are only directed toward "terrorism information" – which includes both terrorism and crimes that have a terrorism nexus – as a result of the ISE's legislative mandate from the Intelligence Reform and Terrorism Prevention Act of 2004. The DHS Intelligence and Analysis Directorate, has completed an appendix to the Baseline Capabilities document which deals with baseline capabilities for Critical Infrastructure/Key Resources (DHS-IAD, 2008). Additional baseline capabilities are being prepared for the fire service and public health as appendices to the baseline capabilities document.

While the structure and processes of baseline capabilities for fusion centers is an important step for increasing efficiency and effectiveness, a significant gap remains. Specifically, most fusion centers will be dealing with "all crimes" – particularly those fusion centers expressly supporting law enforcement agencies that have implemented an intelligence-led policing philosophy – using intelligence analysis to guide day-to-day law enforcement activities (Ratcliffe, 2008). However, there is currently no initiative going forward that will define baseline capabilities for the type of information and analysis that many fusion centers will devote the preponderance of their time to: crimes of violence, drug trafficking, organized crime and other trans-jurisdictional complex criminality.

THE INTELLIGENCE FUSION PROCESS

The fusion process is an overarching methodology of managing the flow of information and intelligence across levels and sectors of government in order to integrate information for analysis (*Local Anti-Terrorism Information*, 2005). That is, the process relies on active involvement of state, local, tribal and federal law enforcement agencies – and sometimes non-law enforcement agencies (e.g. private sector) – to provide the input of raw information for intelligence analysis. As the array of diverse information sources increases, there will be more accurate and robust analysis that can be disseminated as intelligence.

While the phrase "fusion center" has been used widely, often there are misconceptions about the function of the center. Perhaps the most common misconception is that the center is a large room full of work stations where the staff is constantly responding to inquiries from officers, investigators and agents. This vision is

more accurately a "watch center" or "investigative support center" – *not* an intelligence fusion center. Another common misconception is that the fusion center is minimally staffed until there is some type of crisis wherein representatives from different public safety agencies converge to staff work stations to manage the crisis. This is an "emergency operations center", *not* an intelligence fusion center.

The fusion center is not an operational center, but a support center. It is *analysis* driven. The fusion process proactively seeks to identify threats posed by terrorists or criminal enterprises and stop them before they occur – prevention is the essence of the intelligence process. The distinction, however, is that the fusion center is typically organized by amalgamating representatives – ideally, mostly intelligence analysts – from different federal, state, local and tribal law enforcement agencies into one physical location. Each representative is intended to be a conduit of raw information from his/her agency who can infuse that agency-specific information into the collective body of information for analysis. Conversely, when there are intelligence requirements[vii] needed by the fusion center, the representative is the conduit back to the agency to communicate, monitor and process the new information needs. Similarly, the agency representative ensures that analytic products and threat information are directed back to one's home agency for proper dissemination.

According to the *Fusion Center Guidelines*, a fusion center is:

> … defined as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity. The intelligence

> component of a fusion center focuses on the intelligence process, where information is collected, integrated, evaluated, analyzed, and disseminated. Nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information that can be "fused" with law enforcement data to provide meaningful information and intelligence about threats and criminal activity (Global Intelligence Working Group, 2005:8).

Obviously, not every law enforcement agency can contribute a person to work in the fusion center. Hence the fusion center must develop mechanisms for two-way information sharing that captures information from the "nontraditional collectors" and provides threat-based information back to those who have the "need to know". As a result, multiple strategies and technologies need to be developed for diverse two-way information sharing.

For example, electronic two-way information sharing via the various secure electronic information systems – Regional Information Sharing System (RISS.net), Law Enforcement Online (LEO), Homeland Security Information Exchange (HSIN), Anti-Terrorism Information Exchange (ATIX) – can be very effective. In the case of ATIX, individuals beyond the law enforcement community who have a demonstrated need – including private sector persons – may also have access to the system and use it for secure two-way information sharing. Another example is the New York Police Department's "Operation Nexus":

> The New York City Police Department's Operation Nexus is a nationwide network of businesses and enterprises joined in an effort to prevent another terrorist attack against our citizens. Our detectives [visit] firms that have joined us in this mutual effort. Members of Operation Nexus are committed to reporting suspicious business encounters that they believe may have possible links to terrorism. The NYPD believes terrorists may portray themselves as legitimate customers in order to purchase or lease certain materials or equipment, or to undergo certain formalized training to acquire important skills or licenses. … Through Operation Nexus, the NYPD actively encourages business owners, operators and their employees to apply their particular business and industry knowledge and experience against each customer transaction or encounter to discern anything unusual or suspicious and to report such instances to authorities (NYC, 2008).

Another model has emerged and is being increasingly adopted throughout the U.S. Developed in Los Angeles, the Terrorism Early Warning (TEW) group has multiple functions, including supporting the intelligence fusion center.

> The Los Angeles TEW includes analysts from local, state and federal agencies to produce a range of intelligence products at all phases of response (pre-, trans-, and post attack) specifically tailored to the user's operational role and requirements. The TEW bridges criminal and operational intelligence to support strategic

> and tactical users. As part of this process, the TEW seeks to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team. Toward this end, the TEW has developed a local network of Terrorism Liaison Officers at law enforcement, fire, and health agencies, formed partnerships with the private sector to understand threats to critical infrastructure, and has developed and refined processes to analyze and synthesize threat data to support its client agencies (Sullivan, 2005:1).

Regardless of the method of information sharing, the key factors are: there must be diverse raw input, it must be analyzed; and intelligence output must be shared with appropriate consumers.

Why Fusion Centers?

The heart of good intelligence analysis is to have a diverse array of valid and reliable raw information for analysis (Clark, 2007). The more robust the raw information, the more accurate the analytic output (i.e., intelligence) will be. If one thinks of information input in terms of bandwidth, the typical law enforcement intelligence unit has a narrow bandwidth. That is, information is gathered from a fairly narrow array of sources, thereby limiting both the quality of the analysis and the ability to see the "big picture" of a criminal enterprise. Quite simply, the more limited the input of raw information, the more limited the quality of intelligence. However, if the number of sources is broadened to include a wide range of agencies representing much broader

geographic and jurisdictional parameters, then the bandwidth is much wider. With wider bandwidth, there is a greater (and more diverse) information flow. Therefore, with greater information flow, the analysis becomes more accurate and utilitarian. As the quality of analysis increases, the ability to prevent or mitigate the operations of a terrorist or criminal organization increases exponentially.

These observations are reinforced by recent analyses of both law enforcement and national security intelligence operations found a problem that has been referred to as the "stovepipe" of information in agencies (Kindsvater, 2003). That is, each agency would develop a large body of information and analytic products that would be retained within the agency and rarely shared with other agencies. Analysis was generally limited to the information that came from internal sources and dissemination of information was also largely internal. As a result, while agencies were developing information it was simply being stacked, metaphorically like a stovepipe. Current thought recognizes that far more value can be derived from information that is widely shared for analysis – information from one agency may be a key in learning about a threat when integrated with information another agency. Hence, there was a need to "fuse" as much information as possible. As noted in a report from the Heritage Foundation, the fusion center would not simply duplicate the activities of existing agencies, but would enhance and improve their efforts by providing a service that does not yet exist (Dillon, 2002).

A Reorientation from the Current Intelligence Model

Law enforcement intelligence at the state, local and tribal levels has been organizationally and operationally haphazard at best. Most of America's law

enforcement agencies had no intelligence capacity at all. Many that did have an "intelligence unit" of some form were doing little, if any, analysis. In reality, most were investigative support centers where officers could call and get various types of information about investigations and cases. Often the personnel staffing the units, while perhaps having the title of "analyst" were typically clerical people who had been promoted, often with little if any training in formal intelligence analysis techniques.

Some agencies had formally trained analysts; however their analytic products were frequently inconsistent and were often "stove piped". One reason for the lack of information sharing was that the predominant philosophy was that of "operations security" for intelligence reports. This fundamentally meant that because of concern that information from intelligence reports may be "leaked", very rigid "right to know" and "need to know" dissemination standards were used. Essentially, this meant that an officer typically would not see an intelligence report unless he or she was working on the inquiry.

Fusion centers, and the NCISP, have changed many of these traditional characteristics. Having multiple agencies participate in a center means that there is less likelihood the intelligence will be "stove piped" and will, conversely be more widely disseminated. On this last point, the philosophy of intelligence has also changed. While operations security remains a concern, the predominant approach is to disseminate intelligence to as many law enforcement officers as possible. The rationale is that the more officers who have information about threats, the more likely that threat will be identified and mitigated.

Human Resource Issues

Staffing the fusion centers is obviously a critical responsibility. Because they take different forms, staffing patterns vary, however there are certain trends that have emerged. The "lead agency"[viii] for the fusion center will have primary staffing responsibility and typically will provide the center's management personnel, most operational staffing and employ new staff, such as intelligence analysts. Larger agencies within the fusion center's service area will be asked to contribute staff, typically on a "temporary duty" status with assignment and duty responsibilities articulated in a Memorandum of Agreement (MOA) between the fusion center and the contributing agencies.

Beyond these staff members, the FBI is assigning at least one agent, and sometimes analysts, to each fusion center. In addition, the Department of Homeland Security Intelligence and Analysis Directorate (I&A) is assigning at least one person to most of the primary state fusion centers. In many cases, the National Guard assigns analysts and different federal agencies – such as the Drug Enforcement Administration (DEA) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) – will assign personnel. Once again, there is no explicit model for assignment – it is usually based on local needs and often personal relationships.

In reality, there is a limited supply of professional law enforcement intelligence analysts in the U.S. largely because most law enforcement agencies did not want to budget for professional positions. Many analysts were clerical personnel with limited knowledge, skills, abilities and training in intelligence – an issue compounded by a lack of recognized professional standards for intelligence analysts (Marin, 2008). Rather they

were reliable employees who were given expended duties. One major reason this occurred was that many law enforcement executives felt they could not justify paying high salaries to non-sworn analysts – they would opt to hire sworn officers instead. Some executives, however, saw the value of intelligence analysts and ensured they had the "best and brightest" people whom they could pay competitively.

One example of this is former Spokane, Washington Police Chief Roger Bragdon. When faced with a multimillion dollar budget reduction, Chief Bragdon faced the realization that it was inevitable that some Spokane police employees would lose their jobs. When faced with this difficult decision Chief Bragdon elected to furlough a number of sworn officers, however, none of his department's crime analysts or intelligence analysts lost their jobs. His reasoning, based on his experience, was simple: Using the analysts' reports, Spokane officers "worked smarter" (Bragdon, 2008). It was, in Chief Bragdon's view, the most reasonable alternative. The investment in analysts permitted the department to continue maintaining a safe community by focusing operational activities to crime and threat priorities.

COLLATERAL ISSUES

Beyond questions related to the efficacy of the intelligence fusion process, a number of issues have emerged about the operations of fusion centers. There are sharply diverse perspectives of these issues between advocates and critics.

Is There a Role for the Private Sector?

The Program Manager-Information Sharing Environment observed that the private sector can be a rich resource of information that adds a broadened dimension to information collection. Many large corporations have sophisticated security operations that monitor global threats to their facilities, products and personnel posed by organized crime and criminal extremists as well as predatory criminals (NIAC, 2006). This type of information is often different than that collected by law enforcement organizations and can add a unique, and more insightful, component to the body of information being analyzed by the fusion center.

Similarly, the private sector is often a legitimate consumer of law enforcement intelligence meeting the "right to know" and "need to know" information sharing standards. For example, 85% of the U.S. critical infrastructure is owned by the private sector (National Preparedness Directorate, 2006). Moreover, the private sector has a large personnel force who, if given the proper information, can significantly increase the "eyes and ears on the street" to observe individuals and behaviors that pose threats. As noted in one the "Best Practices" papers produced by the Department of Homeland Security, "a jurisdiction's analysis and synthesis entity, [such as a fusion center], should also establish processes for sharing information with the local private sector" (*Local Anti-Terrorism Information,* 2005). However, critics have expressed the concern that there is information in fusion centers that private sector personnel should not have access to (German & Stanley, 2007). The caution goes on to note that the inclusion of the private sector represents "…the creation of a 'Surveillance-Industrial Complex' in which security agencies and the corporate sector join together in a frenzy of mass information gathering, tracking and routine surveillance" (German & Stanley, 2007:11).

Of course, there are information sharing issues that need to be resolved. For example, certain types of personal information may be inappropriate for law enforcement to release to the private sector. Similarly, many in the private are concerned that proprietary information related to corporate products may be inappropriately released. Despite these limitations and concerns, there appears to be a legitimate role for the private sector in fusion centers. Just as in the case of law enforcement partners, Memoranda of Understanding and Non-Disclosure Agreements need to be in place that includes provisions on information sharing processes and restrictions.

Resistance to the Fusion Center Concept

Law enforcement agencies have historically been resistant to information sharing for several reasons. One of the concerns has been that when information is shared, the original agency loses control of future dissemination. This is a legitimate concern because of privacy and liability issues, notably if there is no guarantee that the information would be controlled (FCW, 2008). Another reason for poor information sharing was agency ego – information is power and those who have more information can have more influence (Beare & Murray, 2007). While this appears to represent a minority of cases, it nonetheless exists. A final, somewhat mundane, reason for poor information sharing is that it was not convenient because of technological or logistical reasons (Slayton, 2000).

It was recognized post-9/11 that not only did the intelligence community need to become more adept at information sharing, so did the law enforcement community. With policy recommendations established in both the NCISP and the *Fusion Center*

Guidelines, many of the logistical issues were resolved. Similarly with growing access to secure information systems that were based on Internet protocols – RISS.net, LEO, and HSIN – the technology was enhancing more widespread information sharing to agencies of all sizes.

This enhanced information sharing was not welcomed by all. In a statement released by the American Civil Liberties Union (ACLU), concern was expressed by civil libertarians that intelligence fusion centers may jeopardize civil rights. The ACLU stated,

> The establishment of a single source intelligence center raises important issues concerning the scope of its operations and need for safeguards to ensure that its operation do not violate civil liberties or intrude on personal privacy (ACLU, 2005).

Continuing on this theme, the ACLU explicitly stated questions it wanted answered about fusion center operations.

> We need a lot more information about what precisely the fusion center will do, what information it will be collecting, who will have access to the information, and what safeguards will be in place to prevent abuse (ACLU, 2005).

Every fusion center commander should be able to answer those questions – if not; the policy and process infrastructure of the center needs to be re-examined.

Fusion Centers and Civil Rights Issues

There is a concern among many privacy advocates that the growth of fusion centers will increase the jeopardy to citizens' civil rights and privacy (Rossler, 2003; Sullivan, 2003; Dinh, 2004, House of Representatives, 2008). As noted in a National Governor's Association "Best Practices" paper, "The risks to individuals' privacy begin when personal information of any kind is entered into criminal justice information systems" (MacLellan, 2006:4). Complicating this issue is the fact that not understanding the concept of the fusion process, many privacy advocates fear that the centers are the next iteration of centralized surveillance of citizens.

One of the greatest concerns about fusion centers in this regard is participation of federal law enforcement agencies and National Guard personnel whose jurisdictions for information collection and retention are different than state, local and tribal law enforcement agencies. Certainly, when a state, local or tribal law enforcement agency is the custodian of an intelligence records' system, care must be taken to exclude information from the fusion center that does not meet the standards of information collection, retention, dissemination, and purging as articulated in the federal regulation 28 CFR Part 23[ix], as per the recommendations in the *Fusion Center Guidelines* and the NCISP.

Fundamentally, the privacy and civil rights issues of citizens related to fusion centers are the same as any other aspect of the intelligence process. Those relevant standards of the NCISP apply in the same manner and should be fully adhered to. Further, Guideline 8 of the *Fusion Center Guidelines* states that the management of the fusion center should, "Develop, publish, and adhere to a privacy and civil rights policy"

(Global Intelligence Working Group, 2005:49). Commentary on this guideline goes on to note that…

> …one of the critical issues that could quickly stop intelligence sharing is the real or perceived violation of individuals' privacy and constitutional rights through the use of intelligence sharing systems. In order to balance law enforcement's ability to share information while ensuring that the rights of citizens are upheld, appropriate privacy policies must be in place (Global Intelligence Working Group, 2005:49).

As a consequence, civil rights issues for fusion centers have components related to policy, training, supervision and public information that must be addressed in the development and implementation stages.

Fusion Centers and the Information Sharing Environment (ISE)

The ISE *Implementation Plan* embraced the growth of fusion centers as a critical linchpin to serve as information clearinghouses between federal entities (both federal law enforcement and the Intelligence Community), non-federal law enforcement and the private sector.

> [M]any States and localities emphatically moved to create and invest in fusion centers in the post-9/11 environment. These fusion centers now play a prominent role in collecting, analyzing, and sharing terrorism information. Individually, these centers represent vital assets for collecting terrorism-related information.

> Collectively, their collaboration with the Federal government, with one another (state-to-state, state-to-locality), and with the private sector represents a tremendous increase in both the nation's overall analytic capacity and the multi-directional flow of information. It is important to note that these centers are not homogenous—considerable variations exist in terms of operations and mission focus (e.g., homeland security, law enforcement, emergency response). To date, more than 40 such centers have been established across the United States, and significant effort has gone into developing and adopting standards to facilitate easier information access, sharing, and use (PM-ISE, 2006: 7-8).

To further this plan, the PM-ISE has established a National Fusion Center Coordination Group (NFCCG), led by DHS and DOJ, to identify federal resources to support the development of a national, integrated network of fusion centers (General Accountability Office, 2007:12). Moreover, the ISE…

> …recognizes the "all-crimes and all-hazards" nature of state and local sharing, where state, local and tribal organizations may share and fuse together multiple types of information to address a variety of needs including law enforcement, preparedness, and response and recovery. In many instances, this information may not initially be recognized as terrorism information, but may be information that could ultimately prove crucial in preventing, preparing for, or responding to terrorism. The ISE focus on terrorism information

> will not impede or interrupt these additional fusion center functions (PM-ISE, 2006:11).

EFFECTIVENESS OF FUSION CENTERS

For the most part, fusion centers are so new that there has been no empirical assessment of their effectiveness. There is some anecdotal evidence that suggests "success" in four ways (Carter, Forthcoming). In the experience of the authors who have worked with agencies in all regions of the U.S., the fusion centers that are currently operating have dramatically increased the amount of information shared among law enforcement agencies. Most have developed explicit "intelligence products" and have proactively engaged agencies in their service area to join their networks.

The first measure of success is whether more information is being shared between law enforcement agencies at all levels of government. There is significant evidence to suggest that information sharing has increased (McNamara, 2008), however there are factors beyond the creation of fusion centers that have contributed to broader information sharing. These include the creation of the Criminal Intelligence Coordinating Council (CICC), overt initiatives by the FBI Directorate of Intelligence to create discernable intelligence products that are "written for release"[x] to state, local and tribal law enforcement agencies, and widespread adoption of the NCISP that inherently enhances information sharing.

The second measure of success deals with the ability to collect, retain and disseminate information while protecting the civil rights and privacy of citizens. Once again, anecdotal experiences of the authors indicate that the fusion centers carefully

adhere to policy and legal standards for maintaining their intelligence records systems. None of the centers have been sued for civil rights violations, although several have been the subject of Freedom of Information Act (FOIA) requests to determine the types of information they are collecting and retaining (Electronic Privacy Information Center, 2008). Moreover, training programs for fusion center commanders and personnel all contain components of civil rights issues.

The third measure of effectiveness is more elusive – whether the information and intelligence disseminated by the fusion centers have resulted in the prevention, mitigation and control of crime and terrorism. Once again, some anecdotal evidence from different fusion centers suggests some successes (Carter, Forthcoming) – largely due to better communications between agencies – but it is far too early for a definitive conclusion or any type of empirical assessment of success.

The fourth measure is whether a fusion center is cost-effective. This will be extremely difficult to measure and will involve some value judgments. Inherently, the intelligence process is inefficient; however, it currently appears to be the best methodology to employ for preventing complex, multi-jurisdictional criminality and terrorism. It would seem logical that the amalgamation of intelligence resources in a single fusion center would help increase the cost-effectiveness of the process; however, empirical assessment of these factors after a "track record" has been established will provide better insight. A final difficult factor to determine in cost-effectiveness is how to balance the monetary investment in a fusion center against the fiscal and emotional costs that are spared from a terrorist attack. The answers will not be easy.

A joint report prepared by the U.S. House of Representatives, Committee on Homeland Security and Committee on Foreign Affairs (2008), view the status of determining fusion center effectiveness rather critically, mentioning the lack of identification of stakeholders and quantitative instruments to determine the extent to which their needs are being met has yet to occur (House of Representatives, 2008). Moreover, this report questions the quality and value of the intelligence produced by fusion centers to provide actionable intelligence to those who need it most. In reality it is far too early to evaluate the effectiveness of fusion centers; however, these variables provide guidance for important factors to measure in the near future.

CONCLUSION

The intelligence fusion process holds a great deal of promise for effective intelligence operations. This is particularly true given the multi-jurisdictional character of terrorists' operations and criminal enterprises. The three greatest challenges are (1) to develop a cooperative and committed relationship between all stakeholders; (2) to establish policies and processes that support efficient, effective and lawful intelligence operations; and (3) for fusion centers to "stay on message" as an analytic center.

As with any organization or aspect within society, transformation and reform will not occur overnight. Law enforcement intelligence personnel are continually learning and developing best practices to both protect the American people from foreign and domestic threats while simultaneously observing the rights afforded to those who are being protected. Fusion centers are diverse and still evolving and present a new type of institution into American life (German & Stanley, 2007:22). The individuals involved

and the organization as a whole are responding to meet the current needs of law enforcement and as a result, are learning to perform in a manner consistent with the post-9/11 environment.

BIBLIOGRAPHY

Allen, Charles. (2008). *Information Sharing and the Federal State and Local Levels.* Testimony before the Senate Committee on Homeland Security and Governmental Affairs. July 23, 2008. Washington, DC. Retrieved from http://www.dhs.gov/xnews/testimony/testimony_1216992676837.shtm.

American Civil Liberties Union. (2005). Press Release. *ACLU of Massachusetts Questions Scope of fusion center Activities.* May 11th.

Beare, M. E. & Murray, T. (2007). *Police and Government Relations: Who's Calling the Shots?* Toronto. University of Toronto Press.

Bureau of Alcohol Tobacco, Firearms and Explosives. (2008). *Crime Gun Center (CGC).* Retrieved from http://www.atf.gov/field/newyork/rcgc/.

Carter, David L. (Forthcoming). *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies*. 2d ed. Washington, DC: Office of Community Oriented Policing Services.

Bragdon, Roger. (August 10, 2008). Personal interview with retired Spokane, WA Chief of Police Roger Bragdon in Richmond, VA.

Clark, R. M. (2007). *Intelligence Analysis: A Target-Centric Approach.* 2nd ed. Washington, DC. CQ Press.

Department of Homeland Security. (2007). *FY 2007 Homeland Security Grant Program.* Supplemental Resource: Fusion Capability Planning Tool.

Department of Homeland Security Intelligence and Analysis Directorate. (2008). Critical Infrastructure and Key Resources Support Annex. January 2008.

Dillon, Dana R. (2002). Breaking Down Intelligence Barriers for Homeland Security. Backgrounder, *1536*. Washington, DC: Heritage Foundation.

Dinh, V. D. (2004). Freedom and security after September 11. In *Civil Liberties vs. National Security: In a Post-9/11 World.* M. Katherine B. Darmer, Robert M. Baird, & Stuart E. Rosenbaum. (eds). Amherst, NY. Prometheus Books.

Electronic Privacy Information Center. (2008). *Project on Information Fusion Centers and Privacy*. Retrieved online from http://epic.org/privacy/fusion/.

Federal Computer Week. (2008). *A New Threat, A New Institution: The Fusion Center. Retrieved online at http://www.fcw.com/specials/fusioncenter/.*

General Accountability Office. (2007). *Homeland Security: Federal Efforts are Helping Alleviate Some Challenges Encountered by State and Local fusion centers*. Washington, DC: General Accountability Office, GAO-08-35 Homeland Security.

German, M & Stanley, J. (2008). *Fusion Center Update.* New York, NY: American Civil Liberties Union.

German, M & Stanley, J. (2007). *What's Wrong With Fusion Centers?* New York, NY: American Civil Liberties Union.

Global Intelligence Working Group. (2005). *Guidelines for Establishing and Operating fusion centers at the Local, State, Tribal and Federal Level*. Washington, DC: U.S. Department of Justice. U.S. Department of Homeland Security.

Global Intelligence Working Group. (2005). *Recommendations for Intelligence Requirements for State, Local and Tribal Law Enforcement Agencies*. An

unpublished report of the Intelligence Requirements Subcommittee of the Global Intelligence Working Group.

Harris, B. (2008). Fusion centers may strengthen emergency management. *Government Technology*, August 2008.

Homeland Security Advisory Council (HSAC). (2005). *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*. Washington, DC: Department of Homeland Security.

Johnson, B. R. & Dorn, S. (2008). Fusion centers: New York state intelligence strategy unifies law enforcement. *The Police Chief*, 75(2), 38.

Kindsvater, Larry C. (2003). The need to reorganize the intelligence community. *Studies in* Intelligence, 47(1). Retrieved from http://www.cia.gov/csi/studies/vol47no1/article03.htm.

Local Anti-Terrorism Information and Intelligence Sharing: Information Sharing Overview. (2005) Lessons Learned Information Sharing, U.S. Department of Homeland Security. Retrieved from http://www.LLIS.gov.

MacLellan, T. (2006). *Protecting Privacy in Integrated Justice Systems*. Washington, DC: National Governors' Association Center for Best Practices.

Masse, T & Rollins, J. (2007). A Summary of fusion centers: Core Issues and Options for Congress. *CRS Report for Congress*. Washington, DC: Congressional Research Service, United States Congress. September 19th.

Marrin, S. (2008). Intelligence analysis: Turning a craft into a profession. *University of Virginia*. Retrieved from

https://analysis.mitre.org/proceedings/Final_Papers_Files/97_Camera_Ready_Paper.pdf.

McNamara, T. (2008). *Annual Report to the Congress on the Information Sharing Environment*. Washington, DC: Program Manager-Information Sharing Environment.

National Commission on Terrorists Attacks Upon the United States. (2004). *9/11 Commission Report*. Retrieved from http://govinfo.library.unt.edu/911/report/index.htm.

National Preparedness Directorate. (2006). *National Infrastructure Preparedness Plan*. Washington, DC: U.S. Department of Homeland Security.

National Infrastructure Advisory Council. (2006). *Public-Private Sector Intelligence Coordination*. Final Reports and Findings. July 11, 2006.

National Institute of Justice. (1985). *Hallcrest Report I*. Washington, D.C. U.S. Department of Justice.

Nenneman, M. (2008). *An Examination of State and Local fusion centers and Data Collection Methods*. Monterey, CA. A thesis prepared for the Naval Post Graduate School.

New York City. (2008). Operation Nexus. NYPD Shield Initiative. Retrieved from http://www.nypdshield.org/public/nexus.nypd.

Program Manager-Information Sharing Environment (PM-ISE). (2006). *Information Sharing Environment Implementation Plan*. Washington, DC: Office of the Director of National Intelligence.

Ratcliffe, J. (2008). *Intelligence-Led Policing*. Portland, OR. Willan Publishing.

Rossler, T. (2003). New mission and new challenges: Law enforcement and intelligence after the USA Patriot Act. *Journal of the Institute of Justice and International Studies*, 3, 70-79.

Slayton, J. (2000). Establishing and Maintaining Interagency Information Sharing. JAIBG Bulletin. U.S. Department of Justice.

Sullivan, J. P. (2005). *Terrorism Early Warning and Co-Production of Counterterrorism Intelligence*. A paper presented at the Canadian Association of Security and Intelligence Studies. Montreal, Canada.

Sullivan, K. (2003). Under the watchful eye: Incursions on personal privacy. In *The War on Our Freedoms: Civil Liberties in an Age of Terrorism*. R. Leone & G. Anrig, Jr. (eds). New York, NY. The Century Foundation.

United States House of Representatives. (2008). *Wasted Lessons of 9/11: How the Bush Administration has Ignored the Law and Squandered its Opportunities to Make our Country Safer*. Prepared by the Majority Staffs of the Committee on Homeland Security and the Committee on Foreign Affairs. Washington, D.C.

ENDNOTES

[i]See http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf and http://www.cops.usdoj.gov/mime/open.pdf?Item=1395

[ii]http://www.whitehousedrugpolicy.gov/hidta/ny-nj-content.html

[iii]The Counterdrug Intelligence Executive Secretariat (1331 F Street, NW, Suite 700, Washington, DC 20530; Telephone: (202) 353-1875/Fax (202) 353-1901) has an insightful unpublished report on *Metropolitan Area Consolidation/Collocation of Drug Intelligence Elements* that describes success and challenges for Regional Intelligence Centers.

[iv]https://www.llis.dhs.gov/channel/channelContentListing.do?channelId=90287&categoryId=5546

[v]"Complex criminality" refers to criminal enterprises that are involved in a wide range of criminal activities in support of their core enterprise. For example, a drug trafficking organization may be involved in drug production, drug trafficking, money laundering, smuggling, corruption of public officials, fraud and other offenses.

[vi]The *fusion center Guidelines* are often referred to as "federal guidelines" because they are a product of the Global Intelligence Working Group (GIWG) of the Global Justice Information Sharing Initiative (Global) which is funded by and advisory to the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. However, it should be noted that the vast majority of GIWG members are from state, local and tribal law enforcement agencies. Similarly, the group of Subject Matter Experts assembled to develop the *fusion center Guidelines* was also predominantly state, local and tribal representatives.

[vii]"Intelligence requirements" are information that is needed to help make a comprehensive and accurate analysis of a threat. *See*: (GIWG, October, 2005).

[viii]The "lead agency" is that organization which has primary responsibility for creating and operating the fusion center. On a state level it is typically either the state police (such as in Michigan) or the state Office of Homeland Security (such as in Kentucky). In other cases a city police department may be designated the lead agency (such as in Indiana). There is no definitive model beyond the fact that one agency must have primary responsibility.

[ix] 28 Code of Federal Regulations (CFR) Part 23 is a guideline for law enforcement agencies. It contains implementing standards for operating federally grant-funded multijurisdictional criminal intelligence systems. It specifically provides guidance in five primary areas: submission and entry of criminal intelligence information, security, inquiry, dissemination, and the review-and-purge process. As taken from http://www.iir.com/28cfr/Overview.htm

[x]"Writing for release" means that the intelligence products are prepared in a "Sensitive But Unclassified" form permitting more widespread distribution among law enforcement.