Incorporating Local Police Agencies into a National Intelligence Network

Michael E. Buerger
Karen E. Gardner
Bernard H. Levin
John A. Jackson

Futures Working Group White Paper Series:

Vol. 1 No. 1 July 2008

Foreword

This work represents the first offering in what is planned to be a continuing series of white papers authored by members and affiliates of the Futures Working Group. These papers are intended to spark ideas and incite creativity in responding to the future challenges and opportunities that the law enforcement and criminal justice community must confront. As with most white papers, this is not intended to be the final word or definitive perspective concerning the topics discussed. Rather, these papers are designed to foster further discussion and consideration of possible, probable, and preferable future directions for law enforcement. In this vein, the current paper offers a perspective on the critical issue of harnessing the intelligence capabilities that local law enforcement uses on a daily basis. We hope you find this and the future white papers of the Futures Working Group to be useful.

John P. Jarvis, Ph.D.
Chair

Suggested Citation:

Incorporating Local Police Agencies into a National Intelligence Network. By Michael E. Buerger, Karen E. Gardner, Bernard H. Levin, and John A. Jackson. Futures Working Group White Paper Vol. 1. No. 1. July 2008.

Contents

Acknowledgments

The authors and the Futures Working Group express their deep thanks to the Federal Bureau of Investigation, the FBI Academy, and the Behavioral Sciences Unit for their continued intellectual and material support of the Futures Working Group. We are also indebted to the Society of Police Futurists International for its sponsorship of the group. The opinions expressed in this document are those of the authors alone and do not purport to represent either the Federal Bureau of Investigation, the U.S. Department of Justice, or the Society of Police Futurists International.

The authors are also indebted to Marilyn Peterson, a nationally recognized leader in the criminal intelligence community. This working paper proceeds in large part from the May 2004 Intelligence Training Summit held at the FBI Academy in Quantico, Virginia. She was an invited speaker at that meeting, and her work, along with that of her colleagues, provided a starting point for that discussion. Their book (published under the title Intelligence 2000: Revising the Basics) is referenced throughout this paper.

Special thanks go to Mary O'Dea of the Futures Working Group. She undertook the challenging task of editing this work for publication, and her many incisive and insightful contributions have made this a far more coherent and readable document.

Executive Summary

The challenge of incorporating intelligence from the wide array of local agency intelligence into a national network is one of converting from a "need to know" mind-set to one directed by "need to share." Such a paradigm shift requires the intelligence collection process to be redefined from the current system of passive compilation to active information seeking. This paper highlights the complexity, limits, and potential for tapping into our nation's existing state and local law enforcement intelligence collection apparatus, which is decentralized, localized, and dramatically different in form than that used in the federal intelligence community. If a national-level threat intelligence collection tool is to be created, it requires a seamless interface among state and local entities that does not presently exist. Issues regarding law, culture, and capacity will need to be addressed before the desired changes are effected.

The overhaul of the intelligence function also reaches into smaller cities, towns, and rural communities, attempting to incorporate local police agencies into a now informal, but increasingly formalized, national network to identify new threats. There are three primary components of such an outreach. The first is organized coordination between the federal intelligence community and local police and safety agencies, an effort that is well underway. The second is the development of functional intelligence capacities in smaller jurisdictions, a process already addressed by Carter (2004). The third element, to which this paper is primarily devoted, is implicit in the first two: the development of a versatile, multi-tiered system that can assess crime and terrorist threats in local, area, regional, national, and international settings, particularly from reports scattered across geographic and temporal divides.

Proactive collection of intelligence information is a valuable resource for protecting the homeland against terrorists. That effort, however, is of radically different

character than, and must be grafted onto or melded with, the existing and emerging criminal intelligence communities. The change at the local level constitutes nothing less than a shift away from passively recording accidental, random, and occasionally targeted bits of information toward a proactive system that actively reads the environment for changes, anomalies, and new factors. This may be an understatement: outside of a small number of local agencies with active intelligence units, most police records are incident and investigation driven only. The needs of the new system are at odds with the requirements of the existing criminal intelligence establishment, which will necessitate a more complex structure of data cleaning, verification, storage, and analysis than now exists.

The charge to "discover what we do not know" is structurally different from the classic model's task of collecting information and evidence. A threat articulation mission requires a broader vision across time and space, looking for elements that may not proceed from known targets or enterprises, but will intersect with them in the future. Maintaining much larger amounts of information in useful form to be available for constant or periodic reassessment against emerging patterns is a herculean data management endeavor.

A new intelligence model will make a different set of demands of generalist officers than the traditional intelligence endeavors do of intelligence specialists. Both those demands and the dramatically increased quantum of information will create new, as-yet-untested dimensions in domestic intelligence analysis. We can reasonably anticipate that among those demands will be the following changes:

1) the distance between source and analysis will be considerably greater geographically, temporally, conceptually and will involve multiple stakeholders;

2) the resulting "noise" factor will place new strains on the collation and analysis functions of the intelligence community;
3) management of input, evaluation, and dissemination of information will be altered qualitatively and quantitatively by factors of magnitude; and
4) the sum of those changes will also require a directed effort to redefine the fundamental role of the local police officer.

This paper examines some of the preliminary issues related to expanding intelligence functions into traditionally underserved areas. It briefly addresses the proposals for intelligence reorganization occasioned by the Senate 9/11 Commission's July 2004 Report. While the paper mainly discusses issues in terms of generalist officers in small agencies without dedicated intelligence units, some of the issues are pertinent to generalist officers employed in larger urban and state agencies and otherwise isolated from their agency's intelligence unit.

The intelligence system discussed here is a *desired* system with wide-net capabilities that would fundamentally be different from the current systems used by the police criminal intelligence community. Today's police intelligence practices focus on known targets within specific prosecutorial frameworks and -as such- are subject to strict rules governing the information collected. Implementing a wide-net intelligence system will not simply be a matter of expanding or enhancing existing intelligence capacities; rather, the new model requires creating and maintaining a hybrid form of intelligence, perhaps better described as an information-*seeking* product and process.

Introduction

The September 11, 2001, attacks against the American homeland revealed weaknesses in the existing structure of intelligence endeavors: stovepipes of agency-specific vertical communications, information hoarding, and political competition for scarce resources. The USA PATRIOT Act of 2001 and subsequent developments tasked the intelligence community with overcoming institutional barriers to information exchange among federal agencies and improving the quality of information development and networking. The 2008 Annual Threat Assessment of the Director of National Intelligence identified the need to "transition the IC [Intelligence Community] from a federation of independent intelligence organization to a more integrated enterprise" (McConnell, 2008:4). Part of the domestic needs include the increased potential for "home-grown" militants who adopt the ideology and tactics of the radical Islamist movement represented by al-Qaeda and other jihadist entities or who use violent tactics in the furtherance of single-issue causes (McConnell, 2008; Associated Press, 2008a). The July 2007 National Intelligence Estimate noted that Al-Qaeda in Iraq (AQI) advocates attacks on the American homeland (National Intelligence Council, 2007) and that Hezbollah may adopt a similar stance (McConnell, 2008; Associated Press, 2008b).

Perhaps more important, the radicalization process is creating new *ad hoc* groups outside the domain of current intelligence targets. New start-up groups lie within the new charge to "discover what we do not know" that is the driving mandate of the domestic intelligence endeavors. While the FBI has made remarkable strides in this direction, in its role as the nation's primary domestic intelligence-gathering agency, it is still constrained by resources. "Forward-thrown" intelligence can only be enhanced by incorporating the widespread capacities of local agencies and officers into a intelligence – gathering network.

Forward- thrown intelligence at the local level is also an explicit element of the *Prevent Mission* of the Department of Homeland Security's Target Capabilities List (DHS 2006; see Appendix A), the document addressing our ability to deal with terrorist incidents and threshold-incident conditions. Local, county, tribal, and state agencies will have two roles in the intelligence-gathering network. The first is a pass-through role in which they will receive and verify reports of suspicious activity from private citizens and private-sector entities (see DHS 2006:127-129). That role is already being structured by federal authorities, and will be coordinated at the national and regional levels through Fusion Centers, Field Intelligence Groups (FIGS), Regional Intelligence Groups (RIGS), and Joint Terrorist Task Forces (JTTFs).

The second role is the focus of this paper: drawing the intellectual capitalizing of the line officers' local knowledge and acuity of observation into the intelligence network. That requires instilling a line-level awareness of and commitment to the intelligence gathering process in local agencies. Such a charge creates a new mission for already burdened local forces and officers, whose perceptions of the threat and the process will be considerably different than those of dedicated intelligence officers. Past experiences of creating change in police agencies strongly suggests that resistance will be high (in the simplest case, ignoring the new mandate entirely), and new rationale will be bent to the existing mission as defined by the culture, or to familiar structures.

Four main problem areas need to be addressed: the important distinctions of definition and practice of intelligence at various levels; the fragmented nature of institutional and technological capabilities at the local and regional levels; the more consistent, but still variable, network of legal constraints extant within state and local agencies; and a host of cultural issues that constitute potential stumbling blocks to a national endeavor.

Definitions and Practice. The concept and practice of intelligence is fragmented. At least three primary groups use the same title for different functions: the federal-level intelligence community, the still relatively select criminal intelligence community scattered among state and local police agencies, and a broader network of crime analysis units operating in local police departments. Each of these communities has a slightly different model of intelligence, geared toward its specific mission and jurisdictional legal constraints. Each also has its own internal language; even the most basic terms, like "agent" and "officer", have different meanings in the different communities. As a result, initial consultations to draw them together may well illustrate the old bromide about "nations separated by a common language."

Institutional and Technological Capacity. The records systems of the nation's police range from paper-driven systems with file cabinets and paper boxes to state-of-the-art integrated systems and analytic software. The single most important characteristic of American policing is that it is locally based: the concept of local control is ingrained in the psyche of the police and the civil governments to which they answer.

All purchasing decisions are based upon a combination of local budgets and local politics, accented by the persuasiveness of the salesman. There is no industry standard for data collection, evaluation, storage, or analysis. There is no common structure for reporting (below that of the *Uniform Crime Report*, which is itself an abstract of the myriad local forms). The institutional capability of retrieval and interpretation is often vested in persons, rather than systems. Often, those persons are civilian employees with no police experience, much less intelligence or analysis experience. In short, there are innumerable gaps in and variations on the data that exist at the local level. We cannot assume that extraction and transmittal will be easy even when cooperation exists.

Legal Constraints. Police records in general, and intelligence files in particular, are subject to a wide range of restrictions imposed by state legislatures, state courts, and federal appellate divisions. The American legal system is premised upon a presumption of innocence to be overcome by the state only by evidence obtained by legal means. While the definition of what is legal is malleable, the political environment governing the police still clings to bedrock ideas about privacy and civil liberties that do not exist in all intelligence community theaters. Recognition of the immediacy of the threat to the nation is not universal, nor is there common agreement about the trade-off of privacy for security even among those who acknowledge the threat. Local officials are held to strict civil and criminal accountability for violations of statutory requirements, with no leeway for duress of imminent threat. These and other issues shape the domain of cultural concerns as mission drives culture.

Cultural Issues. Some nominal intelligence partners have internalized civil liberties issues. Local police serve multiple constituencies, and there have been conflicts between local mandates and federal initiatives. Current and past efforts to enlist local police into the enforcement of immigration laws have foundered in some cities because they threatened the agencies' long-term ability to serve the larger immigrant community in their jurisdictions. The priorities of local agencies are local.

Moreover, the lengthy memories of past conflict between federal and local jurisdictions remain barriers that must be overcome. Despite concurrent jurisdiction and strong interpersonal relations between individuals working across agency boundaries, an image persists that federal *agencies* encroach upon locals' turf.

Past initiatives at sharing information have a reputation for being a one-way street from local jurisdictions into the federal agency, from whence it is never seen or heard from again. Communications have been cursory and peremptory in far too many cases,

giving the impression of federal high-handedness. While relationships have been improving, these are lingering sensibilities that continue to affect agency coordination.

The locally-oriented culture that maintains what can appear to be parochial myopia is actually cued to an entirely different set of rules and demands. Most agencies are underfunded and resource limited, stretching to cover the demands of their local activity. Participation in extra jurisdictional activities is seen as an important but ultimately nonessential part of the police mission. Local police are answerable to local authorities and communities for local conditions and events.

Current Practices

Creating a broad intelligence capability will redefine the existing intelligence practices of the police intelligence community, which is highly disciplined, concerned with criminal enterprises, subject to specific legal requirements and controls, and focused on identified targets. The emerging model of intelligence-as-desired is more free-form, casting a wide net of street-sense inquiry in an effort to identify emerging threats and support efforts to control the nation's border.

The elements of the police intelligence community are aggressive, purposive hunters. At best, members of local agencies are passive grazers, whose attention is drawn to the unusual. Different cultures arise from their different missions, and there are locally specific variations on cultural themes beyond the main divisions. The result is disparate understandings of threat, need, and purpose. Efforts to build a comprehensive national intelligence collection enterprise must recognize the implications of those differences and develop appropriate strategies for stimulating interest and participation.

Roles of Generalist Patrol Officers

Generalist patrol officers will most likely be generators of information for the intelligence cycle in one of two ways. They may be the proverbial canaries in the mine shaft, alerting investigators and policy makers to emerging elements in the field. Alternatively, they may produce useful fragments that fit into or advance a known scenario or investigation, perhaps becoming incidental players in a larger investigative effort, aware of at least some elements that are focused on a specific target or threat. Both of those scenarios hinge upon timely recognition, either an ongoing project or a new but recognizable trend. More problematic is the handling of information that does not have an immediate anchor, the first hints of an emerging threat pattern that will not be identified for some time.

Canaries in the Mine Shaft. Not every target or threat is known in its full dimensions at the start. Among local police agencies, some patterns are identified through informal comparison of experiences or from observation of aberrant patterns of coincidence. The spread of urban gangs to suburban and small-city venues was one such observation; so, too, were the spread of methamphetamine use and the emergence of small-scale local meth production facilities. Whether either trend could have been stopped or reduced through timely intelligence is unknown, but the potential for mitigating other emerging threats by early identification and intervention stands as a grail for wide-net intelligence work. Once social problems reach the public stage and come to the attention of administrators, they are usually too well entrenched to yield to simple interventions, and the quantum of available resources often is inadequate to meet the new challenge. This argues for standing intelligence requirements, communicated openly, as well as easy reporting channels. The job of defining the requirements is already

underway; the creation of easy reporting channels may prove to be more problematic, for reasons outlined below.

Accidental Fragments. The nature of patrol and investigative work is to notice things that are out of place and to be suspicious. At times, officers are moved to report suspicious events to someone within or outside of their organization who will recognize the significance of the information. The famous 1957 meeting of the crime families in Apalachin, New York, is perhaps the most well-known example of serendipity; it is also an extremely rare gem.

A number of obstacles exist that can thwart serendipity.

- *Inexperience*: The officer is unable to recognize a potentially important fact, event, or development.
- *Uncertainty*: The officer is uncertain about the significance of an anomaly or whether or not to report an observed anomaly.
- *Role definition*: We have no real measure of how much important information is lost simply because police officers do not identify themselves as collectors. Role identification contributes to a "not our job" attitude based on the perception that intelligence development lies outside the law enforcement mission parameters.
- *Active discouragement*: Superiors or local culture discourages reporting, including disbelief that "it could happen here," disdain for the intelligence enterprise generally (and extension of "not our job"), or antipathy toward the particular receiving agency or its representatives.
- *Lack of a meaningful identification with any larger homeland security efforts*: Even in the absence of inter-agency alienation or role-definition distances, line officers may simply be intellectually or emotionally isolated from the goals of homeland security.

- *Inconvenience*: Shift changes, the onset of vacations, having to deal with unpleasant intermediaries, and the desire to avoid paperwork prevent reporting.
- *Intra- and inter-organizational roadblocks*: These include personnel shortages, local crises, vacations, special events, backlogs, and personalities.
- *Lack of or ignorance of a reporting medium or procedure.*
- *Lack of adequate and appropriate information storage and processing facilities* to handle and preserve inputs over time and severe shortfalls in retrieval and analysis capacities.
- *Laziness*.

The current initiatives promulgated by the FBI and the Department of Homeland Security should eventually eliminate the reporting obstacles. Training and indoctrination may help overcome the limitations of ignorance and uncertainty. Neither should be considered effective antidotes to disdain, opposition, or sloth.

Even in the best of circumstances, most police intelligence retention is that of human memory. Officers' activities and, thus, their records systems are incident driven and far more dependent upon citizen initiation than officer initiation of an inquiry. Important facts that should be part of the organizational memory are, thus, scattered in isolated formats; making connections between two salient facts is a matter of serendipity, and making connections across jurisdictional boundaries is even more rare because of the lack of opportunities for contact. Perhaps the most vivid example of this can be found in the opening chapters of Helter Skelter, prosecutor Vincent Bugliosi's account of the investigation of the Tate-LaBianca murders (Bugliosi, 1975).

Some improvements are evident in locales with a strong community policing ethos, where officers maintain an ongoing domain knowledge that is not call-dependent. Those are relatively rare locations, and domain knowledge is still more likely to reside

with the officer, rather than within any systematic set of records kept by the agency. As a general rule, the police have little or no capacity for acquiring and maintaining threat-based intelligence other than that which is incidental to criminal investigations.

The creation of collection, reporting, and storage mechanisms for a national intelligence network requires a multi-layered capacity. Herein lies the crux of the hybrid system matter: to create a system that would better "connect the dots," filling in gaps in the intelligence picture. A national system would require several elements that lie outside the mandate and restrictions that govern the existing criminal intelligence endeavor. In a perfect world, the data would be accessible to local, area, state, border-state, regional, and national authorities. This accessibility would require some form of long-term storage of data beyond the current parameters set for criminal intelligence work under 28 Code of Federal Regulations (hereafter 28 C.F.R.; see Carter 2004, Appendix D). This issue is explored at greater length in the Storage section, below.

Intelligence as Practiced: Focused-Target Collection

This section is a synopsis of the predominant criminal intelligence framework used by local and state police agencies. The prevailing intelligence model for state and local law enforcement is that of criminal investigation intelligence. It is primarily a stand-alone model, though in practice there are important ongoing linkages with regional task forces. More important, it is created upon premises substantively different from the foundational assumptions that drive anti-terrorism intelligence.

While the criminal intelligence model is well-suited to building a case for RICO prosecution, it does not encompass threat requirement and intelligence gap components crucial to the national intelligence model. Criminal intelligence investigation is further

bound by the requirements of 28 C.F.R., which embody civil liberty concerns predicated upon ordinary criminality.

The threat of international terrorism presents a new theater of operation. Terrorists have the potential of inflicting mass casualties through a range of assaults, possibly using weapons of mass destruction (WMDs), creating wide-scale disruption of the economy, and suborning the social order. Since 9/11, the FBI has moved beyond the original framework of criminal intelligence. The new mission for the FBI is "to know what is unknown," recognizing that the scope of its responsibilities now transcends the borders of the nation. The FBI is the only national agency charged with domestic intelligence collection and the primary interface between local agencies and the other members of the intelligence community.

Other models are promulgated from other sources. Among the most important is RAND Corporation's examination of the current state of domestic intelligence (Riley, Treverton, Wilson and Davis, 2005) based on a survey of a stratified sample of 209 local law enforcement agencies [LEAs] and the 50 state-level agencies. The major findings of the RAND survey, excerpted here from the introduction, are as follows:

> Most local departments have little capacity to analyze the information they collect or receive... the sheer number of cooperating agencies sometimes inhibits progress responding to the terrorist threat... Federal authorities, the FBI in particular, will naturally lead in intelligence gathering that is not connected to criminal investigation (xiv).... It is imperative to find new ways to share information and to share it more widely.... The local role in the analytic labor would be to take the general guidance provided by federal authorities and relate it to local domain awareness (xv).... [There is] scant doctrine for shaping state and local LEA intelligence. More vigorous use of the Joint Terrorism Task Forces (JTTFs) as a locus for shaping LEA intelligence activities is one way of providing the fundamental principles. Another option is the development of a federal intelligence support program, similar in structure and role to the position of federal security directors at airports, institutions that are typically locally managed. (xvi-xvii)

Additionally, RAND reported that only one-third of the local LEAs had interaction with the FBI during the year following the 9/11 attacks, and most contacts were for information sharing or anti-terrorism training (page 15). Of the sources of information cited by those agencies as "very useful," professional associations and FBI Joint Terrorism Task Forces (JTTFs) led the list at 21 percent and 20 percent respectively. However, the majority of information received across all source categories including FBI reports, was identified as either "never used" or "not at all useful." The notable exception to that general rule was the FBI's unclassified reports; two-thirds of the respondents indicated those reports were "somewhat useful" (19).

Important as the RAND study is, it is framed in terms of the traditional top-down relationship of federal agencies to state and local authorities that assumes compliance and competence at all levels. Their conclusion is sound: "although law enforcement throughout the United States is fundamentally local in structure, there is no reason that law enforcement intelligence needs to be." The roadmap from current conditions to the desired state is far from clear, however.

The cultural frameworks of federal and state/local LEAs are significantly different and their histories are ` tangled and sometimes toxic, though relationships have been much better in recent years. It is also important to remember that relationships among agencies in contiguous and overlapping local jurisdictions also are sometimes strained and occasionally forthrightly hostile. The languages and perspectives of federal, state, and local agencies are fundamentally different. Given the current state of affairs, a robust national intelligence capacity cannot rest upon blind assumptions, but must take a cold, hard look at the existing realities.

Intelligence Frameworks

Some criminal intelligence professionals work within a two-tiered model: tactical and strategic (see, e.g. Morehouse 2000). Others posit three distinct levels of intelligence: tactical, operational, and strategic (McDowell, 1998). The three-tier model essentially divides the two-tiered model's 'strategic' category into two segments, with *operational* intelligence focusing on organizations and enterprises, reserving *strategic* for long-term trends that may have no specific articulated local targets at the time. A working assumption of this paper is that a national intelligence model will exist and perform in a three-tiered mode.

Tactical intelligence provides opportunities for direct action against targets, countering or preventing a particular crime action or event. Morehouse (2000) describes it as information that "gives enforcement authorities a basic understanding of the criminals and their activities." Tactical intelligence is useful at the local level and is usually focused on an investigation or a prosecution. Collated data on the activities at a drug house, for instance, would document the ebb and flow of traffic, the likeliest time for restocking the supply of drugs, possible and probable defensive tactics, and counter-intelligence, etc. in order to plan an effective raid.

Operational intelligence is a broader and longer endeavor, focusing on criminal enterprises. Analysis supports long-term planning and decision making, particularly in terms of where and how to focus scarce enforcement resources (Morehouse 2000). While tactical intelligence is amassed on individual targets as part of a RICO investigation, the action contemplated may be less immediate. The goal is to neutralize the organization, as well as the many ancillary associates and support networks (fences, money launderers, couriers, etc.), and action against individual members may be delayed while a more comprehensive case is built. When the true picture of the threat emerges, use of

operational intelligence may dictate action toward a higher-priority target based on threats or other requirements.

Strategic intelligence in the three-tiered model involves phenomenon research and evaluation of long-term trends (King, 2000). This analysis supports long-term decision making more than operations, although under the proper conditions, phenomenon research may dovetail with operational concerns. In the two-tiered model, these functions are combined with operational concerns under the strategic heading, but the greater emphasis is on operational utility.

The Existing Emphasis

The extant literature on criminal intelligence focuses primarily on intelligence units, a logical component of large municipal and state agencies that routinely deal with enterprise crime groups ranging from street gangs to international criminal organizations. The target cohort has now broadened to include new targets: international terrorist groups and their support networks and emerging single-issue groups.

Known targets of this type are a constant presence in large cities, requiring ongoing attention. The volume of information generated about them creates a need for dedicated data management and analysis of associations as RICO cases are developed. The nature and extent of harm that such organized groups inflict in metropolitan areas more than justifies the dedicated resources of an intelligence unit.

Extending the concept of intelligence to the numerous smaller agencies of the nation poses special problems. There are approximately 18,000 local police agencies, employing just under 800,000 sworn officers (Osborne, 2006). The approximately 12,000 agencies comprised of fewer than 100 officers (Walker and Katz, 2008:64) typically lack the financial, logistical, and personnel resources to sustain a special intelligence unit. Carter (2004) and Peterson (2004) separately lay out guidelines for the

creation of an intelligence capacity in smaller agencies, essentially a scaled-down version of the larger agency functions, but there are additional factors to consider.

The frequency with which small-town and rural officers will cross paths with members of groups that are targets is unknown, but the probability of such an encounter is likely zero for most officers. An important exception to this might be officers in areas under the influence of gangs, such as MS-13, but initially the officers will be much more concerned with the gang members' behavior in the community than their potential links to international terrorism: officers are held accountable for what happens in their jurisdiction, not what occurs outside it.

Nevertheless, the "Smallville" communities outside the urban centers represent soft spots in the intelligence network (RAND 2005; Maguire and King, forthcoming 2009). At least hypothetically, Smallville is a likely location of new initiatives for criminally circumventing law enforcement's existing intelligence network. Smallville represents one of the best places to hide for terrorists and other criminal entrepreneurs. For that reason, Smallville needs to be incorporated into the planning effort, but the planning effort, in turn, must understand and incorporate the special character of the nation's Smallvilles and their police.

Intelligence as Desired: Wide-Net Seeking

The external threats of international terrorism provide impetus and opportunity to expand and improve the criminal intelligence function of the American police, whose responsibilities are much broader than just the threat of al-Qaeda and associated groups. Multi-jurisdictional task forces focus on drug and criminal enterprise organizations in regional and multi-state environments. For decades, the American police have conducted local intelligence operations against organized crime enterprises, drug gangs, and street

gangs. Successful creation of this new intelligence system would benefit all of those endeavors. There is a social push (largely from outside the police establishment) to create what is termed intelligence-led policing (see, e.g., Atkins 2000).

Basic principles of intelligence collection apply alike to criminal intelligence and efforts to thwart international and domestic terrorism. A mounting body of evidence demonstrates that terrorist networks are resorting to a wide range of "ordinary" crimes, drug sales, cigarette tax avoidance, credit card theft and sale, etc. to finance their activities. Events, such as the August 2004 arrest in Chicago of Craig William Nettles for plotting to blow up a federal courthouse, lend credence to the idea that boundaries between American criminal elements and international terrorists are increasingly permeable. Though a lone actor rehearsing a grudge for a counterfeiting conviction, Nettles had attempted to make contact with al-Qaeda or Hamas terrorists, presumably for assistance or advice. The "terrorists" he met with were instead federal undercover agents, but the symbolic weight of the crossover solicitation by a domestic anti-government fanatic to an international enemy group remains a significant warning sign of what could be. Joining the criminal and anti-terrorist intelligence efforts is a vital factor in keeping our homeland safe.

A new intelligence model will make a different set of demands of generalist officers than the traditional intelligence endeavors do of intelligence specialists. Both those demands and the dramatically increased quantum of information will create new, as-yet-untested dimensions in domestic intelligence analysis. We can reasonably anticipate that among those demands will be the following changes:

1) the distance between source and analysis will be considerably greater geographically, temporally, and conceptually – and will involve multiple stakeholders;

2) the resulting "noise" factor will place new strains on the collation and analysis functions of the intelligence community;

3) management of input, evaluation, and dissemination of information will be altered qualitatively and quantitatively by factors of magnitude;

4) the sum of those changes will also require a directed effort to redefine the fundamental role of the local police officer; at the very least, uniforms must understand that the information may have a life, a utility, and a considerable value for policy development far beyond its immediate local interest.

A multitude of potential factors militate against the possibility that a national intelligence network can be created. The sporadic nature of contacts with viable targets is perhaps the greatest strain on the endeavor and is discussed in greater detail below. The variable (and shifting) levels of support within agencies and their jurisdiction's civil government units aggravate endemic structural weaknesses: lack of user-friendly reporting channels; the erratic or nonexistent nature of feedback; and a concomitant lack of understanding of how collection fits into the national "big picture" of homeland security, much of which may be classified. Nevertheless, three things demand that the work be undertaken: the dramatic international terrorist threat, the constant assault on the U.S. economy by increasingly complex international criminal enterprises; and the spread of domestic criminal enterprises into every corner.

The Intelligence Cycle

Intelligence professionals in law enforcement (who operate under different mandates and constraints from those in the international realm) speak of the intelligence enterprise as a closed feedback loop, one that usually focuses on a known target. In the

section below, the cycle outlined by Peterson (2000) provides a basic framework for considering that process; references and vocabulary not ascribed in this work are drawn from that source.

The primary distinction between the classic criminal intelligence model and the emerging model is that the classic model does not articulate specific threats or manage collection. It is case-focused, with the targets already identified on the basis of defined predicate crimes and an external mandate for the maintenance and disposition of intelligence collected within a specific period of time.

The new model requires both threat articulation and data collection management. The charge to "discover what we do not know" is structurally different from the classic model's task of collecting information and evidence. A threat articulation mission requires a broader vision across time and space, looking for elements that may not proceed from known targets or enterprises, but will intersect with them in the future. Maintaining much larger amounts of information in useful form to be available for constant or periodic reassessment against emerging patterns is a herculean data management endeavor.

The neutralization of organizations, a goal of RICO prosecutions, cannot be assumed in the new battlefront of international terrorism. The evolution of al-Qaeda from a centrally controlled organization to a communications-linked network and from a network to a diffused network of spiritual/intellectual guidance presents additional challenges. Combating terrorism requires both criminal investigation techniques and intelligence collection operations. The enterprise theory of crime underlying RICO provides the platform for combining those previously separate missions.

It is necessary to consider terrorism as an ecological niche with special replacement issues. As eliminating one drug organization may simply clear the ground

for competitors to move in or new start-ups to fill the vacant niche, elimination of a terror cell may inspire or make room for others to take up the cause. Unlike market-driven crimes, ideologically driven movements may be enhanced or galvanized by initial enforcement successes against them.

Intelligence operations are coordinated campaigns of surveillance, monitoring communications, tracking finances, developing human intelligence, infiltrating cells and nodes, and a variety of other activities. They are long-term endeavors designed to illustrate the nature and extent of a criminal enterprise, documenting the involvement of all central, associated, and peripheral actors whose actions contribute to the goals of the enterprise. Though labor intensive and complex, the costs of those investigations are justified by preventing a great deal of harm that might be inflicted upon a community or nation by the targets.

For these reasons, the purpose of an intelligence campaign is to know the enemy. The best strategy may not be to target the first appearance or the initial predicate act, but instead to focus intelligence-gathering efforts in order to identify the other elements moving in the background. Where one prairie dog pops up its head, a complex colony is probably nearby.

The first stage of the intelligence process is the **Collection** of information about the targets, including habits, associations, predicate criminal histories, haunts, contacts, and interests. Information can be collected from surveillance (both visual and electronic), culled from public sources and databases, provided by street contacts and insiders, and compiled from "pass-on" contacts referred by patrol officers. For intelligence-as-practiced, Peterson (2004:15) describes collection in terms of a series of questions related to the requirements of the client or customer. What is the desired outcome of the

collection effort? What questions are being asked by the client… the answer for which they need to know?

The new factors that drive intelligence collection are almost certainly not explicit to the patrol officer on the street. Not only are the above questions foreign to street officers and detectives but the clients are all but unknown to them as well. Further, of the subsequent list of "the most common forms of data collection used in intelligence units" (Peterson 2004:15), only the confidential informant is in the current vocabulary of the average street cop. Even that language is changing as the FBI has adopted as a common vocabulary the language of the intelligence community (e.g., "source development" is changing into "HUMINT" shorthand for "Human Intelligence" and similar shifts of definition)**.**

Information collected is not yet intelligence. One of the most difficult training tasks will probably be to get that distinction across to those who tend to use the terms interchangeably. The next steps in the cycle are the **Evaluation** and **Collation** of the evidence collected, leading to **Analysis**. The new threat-detection approach is already broadening the scope of traditional intelligence, leading to additional categories not envisioned in classic intelligence doctrine: collection management and target validation.

The process of **Evaluation** is primarily that of making judgments about the validity and reliability of information, particularly evaluating the credibility of the original sources of the information. With a focused investigation, the resources for that type of vetting are usually available; with a wide-net system, evaluation will be done primarily at the local level, with upper levels hard-pressed to verify the wide array of local inputs. Like Herbert Packer's "Crime Control" model of criminal justice, a wide-

net intelligence gathering system will almost certainly have to operate largely upon a blind trust in the accuracy and validity controls of the previous levels.

Collation combines related information about the target, storing it, and arranging it in such a way that "relationships can be discerned" (Morehouse, 2000). Its primary function is to make pertinent information readily available to investigators; it also serves the function of deleting unconfirmed and non-relevant information from the database (Peterson, 2000). The same process can reveal gaps and inconsistencies in the data and lead to renewed data collection efforts.

Analysis is the core activity that turns collected information into actionable intelligence. It tests newly collected information against other known information and existing intelligence. When a target subject meets with a previously unknown individual in a bar or restaurant, this event may indicate a new player in the criminal enterprise or it may indicate a simple social contact outside the target's criminal activities. Testing that known contact against other information and looking across time to see whether the new individual interacts with the target again or with others associated with the target's group is part of the process that determines whether or not it is intelligence or simply information. The utility of the report is gauged and prioritized: is the new player a potential informant or a new target? Does he or she have vulnerabilities that could be exploited to the degree that it warrants diversion of resources to him or her as a new target? Or, is the individual's involvement so low that the team will note, but otherwise ignore, subsequent observations until more acute information is developed?

After **Analysis**, the refined intelligence is **Disseminated** and then **Reevaluated**. **Dissemination** reports intelligence back to investigators and prosecutors managing the case. The basic criteria for receiving intelligence briefings are "right to know" and "need to know" (Parks, 2000); absent those two criteria, intelligence access is restricted. These

restrictions help refine investigative focus and align resource allocations as necessary while protecting the integrity of the investigation. Theoretically, all individuals involved in the investigation are advised continually of new developments and opportunities for interventions that could enhance the investigation or strengthen the case. The ongoing process of generating, reporting, reassessing, and generating new intelligence simultaneously develops evidence for prosecution and adjusts the scope of the investigation.

Traditionally, intelligence units and enterprise crime investigators are both the generators and receivers of intelligence. This process takes place within the parameters of one or more investigations with which the investigators are familiar and to which they are dedicated. The investigations tend to be their sole or primary responsibility, though they are often expected to be aware of broader trends that are relevant to the investigations. Most important, the core of their work involves a population of previously identified actors: their targets.

Meanwhile, Back In Smallville.…

The situation of a police officer, sheriff's deputy, or state trooper is considerably different from that of an urban intelligence officer or task force investigator. Local officers' primary duties include patrolling proactively and answering calls. Their localized knowledge base is considerably broader and more diverse than those of enterprise crime investigators, though usually not as deep concerning particular targets. In the best case scenario, local and county officers are occasional generators of information and even more occasional consumers of intelligence. In the alternative scenario, they are neither, either through disinterest or lack of opportunity.

Street cops live in a moment-by-moment world. Their information concerns are primarily tactical and bound by concerns specific to the small patch of the world under their authority. Police officers are also community caretakers, social workers of last resort, and catalysts for a wide variety of local, short-term, street-corner psychology events, interpreting the system for the people. In the process, they acquire both knowledge of the community and a soft network of relationships that can be important capital in the collection effort. Whether it can be systematically organized and tapped remains an open question.

Whether local, county, or regional officers are aware of the various intelligence targets within their territory is uncertain. The knowledge they possess is widely variable and probably limited. Some individuals may seek information that is as up-to-date as possible out of an intrinsic sense of mission or a desired career path. They actively acquire information through professional journals, peer groups and associations, and the Internet. Most compile an individually centered, selective cognitive map of their territory, without any comprehensive understanding of the full and shifting nature of the threats facing the nation. Furthermore, many are impervious to extrinsic influences that attempt to elevate their awareness and involvement.

The above observations may seem to canonize the obvious, but they are integral for moving beyond the current state of intelligence to developing an intelligence-gathering capacity in the law enforcement services of small cities, towns, and rural communities. The template that develops intelligence officers in agencies with dedicated resources is vastly different from, and almost certain to fail in, agencies of general focus and limited capacities.

The best way to explain the differences may lie in the old chestnut, the needle-in-the-haystack metaphor. Intelligence officers and RICO investigators may be looking for

needles in a haystack, but they are looking in a relatively well-defined haystack with at least some assurances that there will be needles. Police officers working in generalist capacities are faced with an entire field of haystacks in which there may be a needle or multiple needles, but more likely there are no needles at all.

Institutional and Technological Capacity

Training. At the most basic level, training must acquaint officers with the needs, rationale, and conduct of the intelligence process. Training will expose officers to the practice of intelligence, the function and needs of analysts, and the rudimentary processes of analysis itself. A prototype of such training already exists in the training designed for full-time intelligence officers and analysts; stimulating broader participation will require adapting that training regimen to the actual work environment of the field officers (the "needle in a haystack" problem).

This type of training will involve helping officers identify potentially useful information and encourage them to maintain a "wide field of vision" of events outside their jurisdiction. In a best-case scenario, it also limits the submission of "dubious value" reports. Realistically, however, any wide-reach system can expect far more chaff than kernels of wheat.

One of the greatest prospective dangers of enlarging the intelligence net is data overload, a flood of irrelevant and extraneous reports that exceed the capacity of organization and analysis. The controlled flow of information sought by professionals will be inundated by "amateur night." The potential for street officers to be producers of "useless, non-relevant, or incorrect information" (Peterson 2004:16) is substantial. Training will need to help officers, supervisors, and analysts make rough-cut

determinations of what information is of purely local interest and which has the potential for broader application.

It is likely that most of the officers trained will have no further contact with an intelligence network after their training. Equally likely, a small group will become high-volume contributors of information. Between these two poles will fall large groups of field officers whose contributions will be sporadic, probably occurring at widely disparate intervals. None of that diminishes the value of what they contribute.

The information we can logically expect field officers to contribute to an intelligence network falls into two categories: suspicious activity and informed observation. There is also a point to encouraging the reporting and addition of field interrogations, arrests, and any negative contact information available from salient incidents. Of these, the "this is suspicious" observation of something out of the ordinary, but not necessarily connected to any larger picture, will probably turn out to be the larger quantum of submissions. The knowledgeable observation of identifiable activity and connections likely will occur as a result of the intelligence information disseminated. Only a few individual officers who go to great lengths to keep themselves informed of larger activities, will contribute ahead of dissemination.

Imposing a new intelligence-reporting system may also produce resistance and non-compliance. We should not assume that police officers would automatically jump at the chance to participate in a large-scale but attenuated effort to improve national security. The concept is too broad and the immediate results too nebulous to speak directly to the hunter mentality of local officers. The National Incident Based Reporting System (NIBRS) provides a useful analogy: while it represents an improvement in crime reporting for those at the national level, its mechanics are a quantum leap in difficulty beyond the more familiar UCR format, and many officers despise it for that reason.

A major ingredient of a training curriculum will involve setting out useful guidelines for initial sifting of observations, decision-making with regard to reporting, and framing details. Ideal intelligence reporting is detailed: it runs contrary to the actual practice of police reporting, which tends to be minimalist. The ideal police report from the field officer's perspective is a single, terse sentence in the half-inch, white-space block at the bottom of the Crime/Incident Report cover sheet.

Transmittal and Evaluation Issues. A national intelligence effort will constitute a different type of intelligence than that currently in practice. Multiple data-collection and display formats will need to be reconciled, much as offenses logged under different state codes must be adapted to the federal definitions of the Uniform Crime Report (UCR). Despite the versatility of computer programs for data mining (such as the embattled MATRIX program), current database screening depends upon larger standard databases than a wide-net collection screen will collect, at least in the initial stages.

In the process, protocols must be articulated for the evaluation of information collected at the local and regional levels. Ideally, this effort should be a process that mutually educates federal, state, regional, and local players on their anticipated needs and capacities. Optimal protocols for developing, screening, and packaging information for the various receiving levels will be a byproduct of a process created in consultation with knowledgeable analysts working in state and local capacities. It would be prudent to set periodic conferences to revisit the issues after program launch as hiccups and other difficulties will inevitably arise.

Storage. Both the serendipitous fragments and the canaries in the mineshaft models will produce a huge load of data to be collated and stored. Some of the material will be of purely local or nearby regional interest, some will have a larger regional application, and some small amount will be important to national security or the control

of transnational crime. At each level, false positives and ambiguities will strain collation and evaluation efforts, and we can predict a tendency toward one of two polar extremes: record everything or record practically nothing.

For local agencies with fewer resources, passing information into the transmittal chain and then washing their hands of it is a predictable form of participation. Though we might wish for a national intelligence initiative to be a jump-start for developing local intelligence capabilities, foreign terrorism threats are the most important developments for the ongoing national efforts of the FBI, NSA, and the Community. Incorporating local collection into the Bureau's and the Community's efforts will be slow, not instantaneous. We should expect greater progress in areas bordering jurisdictions with an established intelligence unit that can help shepherd or mentor the process, and delayed or lagging developments elsewhere.

False negatives are also an inevitable feature of the evaluation process, particularly in the area of emerging trends, but there is at least a quasi-efficient backup system in the human memory. While one ideal might be to have all information preserved at the local level, for retrieval and confirmation when new patterns emerge, it is unrealistic to expect it to develop immediately. Some potential leads will be lost due to lack of verification or authentication, particularly given that local domestic collection efforts probably will be restricted by the stronger ethos of protecting civil liberties.

There is a wedding cake metaphor for data thus collected: the greatest amount, with the broadest reach, will be at the local level. Much of what is deemed "interesting" locally will be discarded at the first regional level and more at the next; only a small portion would be expected to make it to the national level for evaluation.

Those bits and pieces that are sent upward will have the added weight of at least one or more vetting processes. It is likely that those moving up will have a recognized

relevance to ongoing targets: the decision-making in this regard is vested in the Joint Terrorism Task Forces or the FBI Field Intelligence Groups (FIGs).

What is unclear at the front end of system development is whether emerging trends will be more readily discerned or obscured by an inevitable bias toward existing targets. Part of the process must be the development of an ethos that rewards the detection of emergent trends, challenges prevailing orthodoxy, and identifies/articulates gaps and anomalies.

Civil Rights and Civil Liberties. Civil rights concerns will be essential components of the training issue and of operations. The long-standing tension between the rights of citizens to broad access of public space and the notion of "belonging here" (in a prototypical Jane Jacobs [1961] neighborhood sense) will be writ large in any intelligence network. It is human nature to regard "outsiders" of various stripes as inherently more suspicious than neighbors.

It is also probable that persons with long-standing grudges against their neighbors will find ways to couch their complaints in the language of whatever crusade is currently running in the public arena. The moralistic "I'm gonna call the cops on you" last-tag will be immeasurably enhanced if the object of ire can be entered into a criminal intelligence database. Perhaps it is not beyond the pale to suggest that police officers will contrive to register individuals who are their pet peeve, in hopes of striking gold. Both tendencies have the potential to create considerable 'noise' in the system, as will the predictable input from "cranks, buts, and screwballs" (McLean, 1965) already familiar to public service and intelligence agencies. Screening illegitimate reports will be an imperative for both individual officers and supervisors.

Reporting. At the present time, the single largest structural barrier to an intelligence network is the uncertainty about to whom and in what form information

should be reported. This is the area most amenable to top-down instigation, either through the FBI's National Security Branch, the JTTFs, or the FIGs. The irony and the danger, however, is that top-down initiatives fail without local buy-in.

The need for careful, inclusive planning is paramount: despite the patriotic rhetoric of the "defense of the homeland," most local officers will regard the new expectations as an unwarranted imposition. The analysts and the local commander to whom the intelligence function is delegated are critical players, but special and continuous attention needs to be directed to those who, in the first instance, write (and record) what they damn well please (Stamp, n.d.).

Feedback. Feedback presents an enormous logistical problem, with implications for staff resources and thus for budgets. Nevertheless, feedback to contributors is a simple act that should be considered essential to maintaining the network: people like to be acknowledged for their efforts. Field officers are more likely to continue to participate in the network effort if they feel that their efforts are appreciated, and they are not just engaging in an empty ritual. The limitations noted in the Rand report (above) represent a potential obstacle that has repercussions for the entire enterprise.

Feedback is a labor- and time-intensive pursuit. The most natural economy of effort provides feedback in the form of intelligence, rewarding efficiency with information, but we cannot realistically expect that type of system to work for a wide-net intelligence-seeking mechanism. Most feedback will simply reward effort, participation rather than effectiveness. As most contributions will be of no real utility to substantive intelligence, the bulk of the feedback will carry no actual intelligence. Furthermore, since the same economy directs that it is more efficient to communicate to agencies rather than individuals, the same structural barriers obstructing the outward/upward flow of

information are present to affect incoming feedback communications. Nevertheless, we must not lose sight of the fact that feedback is important when it is associated with something of value to the individual officer or the local agency (see also Maguire and King, forthcoming 2009).

Information Management. At the local level, preservation of information is subject to the vagaries of local budgets. Although computer systems have largely replaced the older paper records system, the structure of databases limits their versatility. Even the creation of a single field to note that information was forwarded to a network contact means a substantial commitment to programming, testing, and debugging; in systems operating with flat files instead of relational databases, such a change will demand enormous amounts of (mostly empty) storage space.

An unknown factor is the integration of 9-1-1 call data and hotline reports with the largely incident-driven formal records system. Police reporting systems are by nature incident-driven; the sheer volume of calls to the police precludes making an official record of small reports. The aversion of police culture to "making paper" also weighs against formal treatment of potentially important information.

In some jurisdictions actual practice still discourages the sort of eclectic reporting by citizens that an intelligence network would hopefully feed upon, the gossipy fragments of "someone doin' somethin' dirty/ decent folks can frown on" (Kristofferson, 1972) that might also betoken deeper involvement in criminal or terrorist activities. The effectiveness and sustainability of a wide-net seeking mechanism will depend upon our collective ability to create a culture change in this regard.

Information management will also involve decisions about shelf life and long-term analysis. Civil liberties issues related to gang databases provide an early glimpse into some of these difficulties, as do the more dramatic problems illuminated by the

Innocence Project. Some degree of police information is simply wrong, and some of it is a bad-faith form of wrong.

Linking disparate fragments of information over time is the responsibility and the art of the intelligence analysts, though data-mining techniques will undoubtedly continue to evolve to enhance that skill. Some provisions need to be made for the contributions of field officers who also make those connections by serendipity, dogged digging, and flash-of-insight inspiration. Managing resentment over free lance analysis will be a supervisory issue within the upper echelons of the network. It would be advisable to treat all such contributions as new information, with professional feedback, even if only a small proportion of them actually make a contribution.

Dissemination. Unlike feedback, dissemination of intelligence sends out actionable information. "Actionable" should be treated as a phrase of art: its primary purpose will most likely be to heighten field officers' scanning for specific activities identification of threats and intelligence gaps -- rather than providing the basis for interventions by local authorities (see also Maguire and King, forthcoming 2009).

Aside from locally analyzed information, most downward disseminated intelligence will probably serve to inform field officers of broad trends and developments, without any target-specific mandate. Intelligence that has target-specific implications will be acted upon by task forces and federal agencies, as determined by the content and the target. The action itself may occur in locations geographically distant from the source of the information, effectively eliminating the source agency or officers from any but vicarious participation.

Legal Constraints

The single greatest external challenge to the wide-net collection effort is the patchwork system of statutes and case law governing the use of intelligence data. While 28 C.F.R. provides a general guideline, there are 50 separate legal codes governing the conduct of state and local police officers and other peace officers. In addition, case law from the state courts and the federal district courts overlay another level of patchwork restrictions that will differ from state to state and region to region. These restrictions are not trumped by 28 C.F.R. or other federal rules. The silver platter doctrine of *Elkins v. U.S* will likely retain its force even when the direction of information and evidence transmittal is reversed.

The procedural rules that govern state and local police actions are predicated upon the presumption of innocence, and an expectation that The State will not move against its citizens without a level of just cause that is both articulable and open to examination. The lower threshold of "reasonable, articulable suspicion," which authorizes brief *detention* and inquiry, is also incorporated into 28 CFR 23:20. *Arrest* is justified by the higher standard of probable cause, a combination of facts and circumstances that would lead a reasonable person (under some circumstances, a "reasonable and experienced police officer") to believe that a crime was, is, or is about to be committed.

Case law refines these two broad standards on a case-level basis, but the standard is specific to the court's jurisdiction. For instance, under some decisions, a vehicle stopped for a traffic violation may be held only until that traffic matter is resolved by warning or ticket. No further inquiries about criminal matters may be made by an officer after the traffic portion of the stop has been concluded by the return of license, registration, and warning or citation paper. On the other hand, courts have ruled that a 45-minute wait for the arrival of a drug-sniffing dog falls within the category of

"threshold detention" rather than "arrest," inserting administrative convenience (or practicality) into the mix.

Perhaps the most stringent set of rules is found in Pennsylvania, which does not permit its officers to audiotape conversations between the officer and a stopped driver, even though the stop may be recorded by video camera. Criminal intelligence files must be purged within one year if there is no action on the information provided. Though information may be shared with other agencies during the course of an investigation or inquiry, the original agency is responsible for the purging of any such transmittal and may be held civilly or criminally liable for downstream use of purge-required information (CHRIA Handbook, 2001; Olligschlaeger, 2005).

Many states are more tolerant of legitimate intelligence files, but there is no national standard at the present time. Federal rules always apply to federal cases, but state actors will be reluctant to participate if they are still subject to potential action under state codes and regulations.

The full range of this material is not fully documented at this time, but it constitutes a structural barrier to threat-based intelligence until it can be resolved by legislation or other means. While it is certainly possible to distinguish criminal intelligence efforts from national threat-based intelligence, until there is a clear ruling from the Supreme Court, courts have demonstrated a tendency to draw analogies to what is known and established on order to determine the rules for new elements. The point of reference is likely to be the criminal intelligence protocols in whatever jurisdiction challenges are raised.

Secondary Concerns

Several additional concerns will attend the enterprise as well. Though they are new manifestations of problems that affect other police operations, they have a more acute focus when applied to intelligence efforts. It is one thing to lose a criminal case; it is quite another to see the accumulated efforts of a long-term investigation get wiped out by error, dereliction, or criminal activity on the part of agency members. It would be worse by far to suffer additional damage and casualties as a result of intelligence failures due to faulty implementation of so ambitious a scheme.

Police intelligence work has been a "closed shop" for all intents and purposes, guided by a relative handful of professionals deeply immersed in the endeavor and highly cognizant of the rules and strictures governing it. Such enterprises are well defended against (though not impervious to) infiltration and suborning. The wider the net being cast, however, the more points of vulnerability are created, and the greater the chance the effort will be accidentally or deliberately compromised.

Corruption and Wrongful Dissemination. The possibility of critical information being leaked or sold to targets -- or simply to others with no "need to know" status is already an episodic problem with criminal histories. The problem concerns sworn and civilian personnel alike, and need not be a product of outright corruption (though certainly many high-profile cases fall into the corruption category).

Purposeful infiltration is also a threat, particularly from enterprise crime groups native to this country, whether for their own purposes or as part of a broader network of alliances with foreign groups. While the screening process for intelligence units is rigorous and highly selective, the hiring process for those with access to a wide-sweep network will be highly variable throughout the nation (as widely disparate as the current selection standards and processes for sworn officers). Access to the core of the

intelligence function almost certainly will not be possible merely through infiltration of third-tier reporting stations, but there exists the possibility that disseminated intelligence may be compromised, creating a potential counterintelligence capacity for groups under surveillance.

There is an outside chance of corruption of the system via false leads introduced into the system by infiltrated employees. Given the intelligence community's dedication to verification, this would be a remote possibility under normal circumstances. It is perhaps a greater threat in the event of successful multiple purposeful infiltration, which itself is admittedly an even greater outside chance, though the Aldrich Ames and Robert Hanssen scenarios in the CIA and FBI, respectively, lend themselves to exploitation for such purposes. These concerns crop up periodically in the existing efforts against traditional organized crime, and they should be anticipated in a variety of aspects for the new intelligence missions.

We should also note that in the wake of earlier scandals, strong countervailing forces have developed: increased numbers of audits, greater penalties for violations, and the like. Not only are these developments not inimical to the national effort, they should be viewed as important tools to maintain the integrity and capacity of the effort. They are costly, however, and will place additional strain on budgets and internal capacities.

Blabbermouths. Intentional infiltration is not the only way in which intelligence can be compromised and months of careful work undone. While any agency can be vulnerable to an employee who "goes over to the dark side" (an Ames or a Hanssen), carelessness and egotism --operationally manifest as boasting or loose radio chatter, policing's equivalent to the old "Loose Lips Sink Ships" admonition of WWII can be equally devastating. The smaller the proportion of an officer's workload the intelligence network is, the less important it is to him or her, and the less likely to be

thought of from an information-security perspective. Outside the intelligence community and the regional task forces, the proportion of officers who are security-conscious will likely be small indeed.

Even casual disregard for scanner-land can be deadly to an operation. One of the most salient war stories of recent years (post-1995) is that of a drug operation that was canceled when the agents were stopped by a patrol officer. The agents had drugs to sell to a criminal enterprise under controlled circumstances. After the agents identified themselves and the vehicle stop concluded, the officer joked by radio to another colleague that s/he had "just stopped three kilos of heroin"... and proceeded to explain the circumstances (though fortunately without specific details) over the air. A third officer heard the transmission and was alert enough to notify the drug agent's command, which aborted the buy for purposes of officer safety.

Whether the ill-advised radio message was overheard by anyone outside the police network, much less by the targets, remains unknown. All the same, the carelessness of an officer not attuned to the dangers and requirements of undercover drug work jeopardized not only the safety of the undercover officers, but also months of painstaking investigation and potentially the lives of unknown informants. Those risks will attend the national security intelligence effort as well.

In the rush to coordinate antiterror initiatives, the original reasons for the development of stovepipes, and the firewalls between federal agencies and state and local agencies, has been overlooked. Turf battles, the popular villain of the media accounts, are only part of the story. Measures that restrict intelligence to the agency that develops it are inherently defensive, protecting the organization's investment in the investigation.

So many avenues of communication are available to the bad guys that police have a powerful incentive to keep them working in the channels where we can keep tabs on

them: the most vivid example is the Ultra/Enigma code-breaker advantage held by the British in WWII. Had the Nazis had even one whiff of suspicion that their code had fallen into enemy hands, they would have changed the code immediately. Protecting that secret forced Winston Churchill to allow the bombing of Coventry: protecting the city might have tipped the Nazis to the fact the code was broken and endangered the planned D-Day landings.

A contemporary illustration is available: the al-Qaeda network was vulnerable to tracking as long as they used the same cell phones more than once. When our ability to track them was made public, they switched to one-time-use phones.

On a different scale, and without the ethical dilemma of having to trade Coventry for Overlord, police intelligence efforts follow a similar path. In that context, agencies know their own people (or at least have much more knowledge about them). They have at best only once-removed assurances about the employees of other agencies. The default mode is not quite active distrust, but a presumptive absence of outsiders.

Partnerships and Allies. The community policing movement has placed great emphasis on police working in partnership with multiple agencies and non-governmental organizations (NGOs) as well as with individual citizens and neighborhood groups. Progressive police leaders have long recognized that they have a client group in common with social services and other NGOs, and they usually employ that knowledge to good effect on behalf of those clients and the community at large.

Allied agencies could have information about Persons of Possible Interest to the intelligence effort. Those agencies (and their employees, the street-level bureaucrats who are the counterparts of the patrol officer) have neither the operational charge nor necessarily the same philosophical understanding of the War on Terror, as do enforcement and intelligence officers. There exists a broad general condemnation of the

9/11 attacks and a generic agreement that we ought to prevent future attacks, but once those bromides are operationalized in terms of the agency mission, agreement will likely cease, or at least fragment, into domains of limited subscription. The furor over scrutiny of library and bookstore records under the Patriot Act is but a small taste of the reaction we can expect to attempts to undermine client confidentiality.

Attempting to incorporate or co-opt allied agencies that might have access to information about intelligence targets runs two risks. The first is the alienation of the agency from cooperative ventures of any sort, since it will be uncertain what of the information sharing is legitimate and what is the "camel's nose" of intelligence gathering. The second is the inadvertent release of some information, perhaps in the form of asking an unusual question that arouses suspicion, that tips the target to the possibility of scrutiny. The former is partly a matter of political ideology, but primarily a matter of professional orientation. The latter can occur deliberately, motivated by a personal opposition to government intrusions, or accidentally regardless of political orientation.

Members of helping organizations do not necessarily share the mindset of the police, much less the intelligence community, and may not understand the operational concerns and limits. A blundering attempt to be helpful, by asking a freelance question that exposes the surveillance, can be as catastrophic as blabbermouthing or subversion.

Future Possibilities

Thus far, the examination of the intelligence network issue has focused solely on law enforcement agencies. The first two levels have defined themselves in terms of the Joint Terrorism Task Forces (a multi-jurisdictional model familiar from intelligence work against enterprise crime), Field Intelligence Groups, and most recently Fusion Centers for regional intelligence sharing. Additional efforts have been directed at replicating the

crime analysis unit model of large agencies in medium-sized and smaller police organizations. This work has concerned itself with field officers working in police agencies. All of these models assume that the work of developing intelligence is a hermetically sealed function of the police. Other models exist.

In its previous publications, the Futures Working Group has offered net-centric organization as a prescriptive approach to improving the performance of policing institutions (Cowper, 2005; Myers, 2007; Myers and Cowper, 2007). Most often, the authors have focused their discourse at the scale of the agency. These descriptions have emphasized the internal dynamics of the enterprise and its external relationship with the general community and its political leaders.

The net-centric analytical frame can also be employed with the agency as one of the components (a node) of a larger system. This approach is particularly useful in describing police agency involvement in the interagency intelligence structures discussed in this monograph. Peer-to-peer, cooperative relationships can be leveraged into small-world networks involving the government (police), academia, and private enterprise.

Traditional methods of police-private sector information exchange rely upon the subpoena, an instrument of coercion. Such methods place the public and private sectors in conflict. Considering the volume of identity theft, credit card fraud, spamming, and phishing schemes, complete cooperation confronts a corporation with potentially devastating financial burdens. Consequently, businesses rationally develop utility thresholds that must be passed before cooperation can be justified. Businesses have very real concerns that may be at odds with the objectives of law enforcement.

Government holds most of the legal and enforcement authority necessary to interdict criminal activities. However, government is normally missing two other capacities: analytic resources and relevant information. Academia possesses significant

capacities of young and developing analytic talent. Because of the nature of western economies, private sector enterprises own most of the intelligence and investigatory information relevant to crime. This is particularly so in the realm of cyber crime, where the requisite information is contained on the servers, data arrays, and workstations of numerous corporations, internet service providers, intermediaries, and victims. Successful intelligence models will increasingly draw upon all the resources.

The object of net-centric design is the creation of small-world or "mesh" networks, primarily in a peer-to-peer architecture. In the world of policing, many such networks have evolved outside agency boundaries already; Levin and Jensen (2005) have dubbed the phenomenon "the electronic donut shop," and noted the inherent power to develop and share information ahead of the formal recording curve. Like the window-to-window conversations at jurisdictional boundaries, the electronic meeting formats contain a considerable amount of chaff surrounding the useful nuggets of information. They tend to be directed by line-level concerns (and forms of expression), but they represent a resource available to be tapped and given greater purpose.

Police agencies also can utilize the net-centric principles to engineer peer networks with the private sector and academia. In doing so, the peer nature of the relationships must be respected. The needs of private and academic sector partners must be measured and met by the network. Proprietary information must be treated with respect and confidentiality. In an environment of equity, the private sector will be encouraged to bring critical information and contribute its resources to the analysis of the information. With the assistance of scholars from academia, new insights and analytic skills can be added, though experience suggest they will serve strategic ends better than tactical ones. Traditional organizational settings still militate against rapid exploitation of serendipity and time-sensitive materials.

The National Cyber-Forensics and Training Alliance (NCFTA), headquartered in Pittsburgh, exemplifies this model. Initially developed at the Pittsburgh Field Office of the FBI, the NCFTA serves as a "neutral, meet-in-the-middle hub" for law enforcement, private industry, and academia (Larkin, 2007). According to its Mission Statement:

> The NCFTA provides a neutral, collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia and law enforcement. The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations. These activities are intended to educate organizations and enhance their abilities to manage risk and implement strong security practices. (NCFTA, 2007)

The scope of the NCFTA's work is clearly more than simply intelligence gathering, but one of the byproducts of this multi-tiered approach is an exchange of pertinent intelligence information that would be unlikely to be developed by traditional means.

One pillar of this approach is sharing information about potential cyber threats across corporate boundaries. The Alliance's approach assures confidentiality of each member's proprietary information from its competitors. At the same time, the neutral environment allows Alliance members to simulate how newly-discovered techniques of cyber-raiding might appear on and affect their own systems, sharing information ahead of actual attack. Where actionable criminal information is a product of the forensic analysis, the FBI or the Postal Inspectors are free to open an investigation.

Critical to the model is a suspension of the enforcement-only mindset of the investigators. There is an awareness that the interests of the corporate partners lie in several different areas: first and most important, they wish to neutralize the new threat. Second, they desire recovery of lost assets, if possible, a priority, which often leads to civil rather than criminal law avenues of redress. Third, they benefit by being able to re-

tool their defenses against the threat. Fourth, they are able to retain those measures that have been proven to work. The final benefit is a basis for retraining their staff.

The NCFTA developed out of the traditional enforcement-oriented mission, as an attempt to bridge the wide gap of information known to criminal investigators and that known to corporate risk managers and security experts. While investigations and prosecution have been important products of the cooperative approach, another byproduct has been the development of new intelligence sources.

Criminal and terrorist groups rarely discriminate in their targets. They engage in multiple activities across the artificial boundaries of crime-recording categories, committing whatever crime harvests the most money. As a result, the corporate sector is often the canary in the mineshaft for new forms of criminality: new fraud schemes, variations on hacking and phishing techniques, and the like. Their analysts see patterns in data that are not apparent to criminal investigators, and their data typically span multiple jurisdictions and geographic regions. Even when prosecution is not sought by the corporate partner, the knowledge of the criminal enterprise that results from the forensic analysis can be invaluable to law enforcement.

While the current model emerged as a result of a law enforcement initiative, it need not be the only model. The NCFTA has succeeded because law enforcement partners have stepped back from the field's traditional assertion that law enforcement and prosecution must drive any such partnership. By accepting the legitimate needs of their corporate partners, and to a lesser extent the academic partners, the NCFTA process has been able to lower or bypass traditional barriers of cooperation. In the process, both sides have discovered the value of the synthesis in their respective realms.

Future developments may proceed from this initial effort, using NCFTA as a template and beginning with an equal footing for all sides. Law enforcement should be

aware that a third model may arise from the same template: an entirely private-sector intelligence network, for which law enforcement is only a peripheral, and occasional, client. In an era in which more and more government functions are being shared with or returned to the private sector, some of the traditional expectations of the law enforcement community may no longer be viable.

Summary and Conclusion

Attempts at implementing an "intelligence-as-desired" system should not be approached as just a matter of expanding existing intelligence capacities. Neither should it be assumed that implementation can be accomplished by edict. The mission is so different from the current target-focused practice of intelligence that it will require the creation of a new type of quasi-intelligence, an information-*seeking* process. That process is active hunting, aggressive collection of information against known and emerging threats.

Such a mechanism will have to be integrated with the existing and emerging criminal intelligence communities, an uphill task on both sides of the current dividing line. Not only will the information network have to operate across very different operational mandates, it will have to work up and down a complex network of jurisdictional differences and geographical distance. We need to encourage multiple opportunities for both structural and informal venues that encourage systematic exchange and maximize opportunities for serendipitous discovery and "eureka" moments.

The needs of the new system are at odds with the requirements of the existing intelligence establishment. It will necessitate a more complex structure of data cleaning, verification, storage, and analysis than now exists. It will also require a different legal mandate, since the current time and verification restrictions on intelligence data for active

investigation will be essentially fatal to the wide-net, slow-time endeavor. While it might be best in an ideal world to separate national-import observations from local concerns, at least for archiving, the inherent bias is toward intelligence that is of local utility. Attempting to establish a dual reporting system will increase system costs prohibitively, and much of the potential benefits of the wide net lost. It is also likely that the attenuated buy-in that would result would undercut both efforts; it is probable that even a multiple-efficiency system will yield results so rarely that active participation will be very limited, but we should not write off the potential for such a system on the basis of that possibility alone.

Improving and enhancing the intelligence capacity, whether against terrorist groups or against enterprise crime, will be a difficult task. The distinction between the two threats seems to be receding rapidly as "network" replaces "organization" in the globalized economy, and both groups work sporadically with each other for mutual benefit.

While the creation of a national intelligence network may start with the intent of adapting existing entities and modifying functions, the greater probability is that ultimately it will require a fresh start. A national intelligence network under any name or guise raises red flags to those concerned about privacy, civil liberties, and checks and balances against errors. Enhancing, modifying, or building a wide-net intelligence-gathering faces an uphill climb against the recent public relations disasters of facial recognition software, Carnivore, Matrix, and the rash of wholesale thefts of personal data from data processors. It will be better to conduct the attempt in an open forum than behind the scenes so that those concerns may be addressed.

Though there is a tendency to present any new operation as just an extension of current capacities, in order to protect it with the justification of accepted practices and

existing laws. That may be counterproductive in this case. We are adding an entirely new, architecturally distinct, wing to the intelligence community by tapping into latent capacities of those closest to the collection: the 800,000 canaries in the mineshaft. The specter of Big Brother will not be banished with simple entreaties to "trust us," and the structural differences described above, particularly those of enabling legislation for the preservation of the data collected, are of sufficient magnitude to justify thinking of any wide-net capacity as a new entity.

References

Associated Press (2008a). Damage From U.S. Extremists a Concern. Accessed 02/27/08: http://www.nytimes.com/aponline/us/AP-Domestic-Extremists.html.

Associated Press (2008b). McConnell: Hezollah Threat "Serious." Accessed 02/27/08: http://www.nytimes.com/aponline/us/AP-US-Threats.html.

Atkin, Howard N. (2000). Applications of Intelligence. Pp. 13-21 in Peterson, Morehouse, and Wright (eds), Intelligence 2000: Revising the Basic Elements. Sacramento, CA and Lawrenceville, NJ: L.E.I.U. and IALEIA.

Bugliosi, Vincent, with Curt Gentry (1975). Helter Skelter: the True Story of the Manson Murders. New York: Bantam.

Carter, David L. (2004). Law Enforcement Intelligence: A Guide for State, Local, and Tribal Enforcement Agencies. Washington, D.C. National Institute of Justice. November.

CHRIA Handbook (2001). Criminal History Record Information Act Handbook. Third edition, summarizing Commonwealth of Pennsylvania statute 18 PA C.S.A. section 9101 *et. seq*. Accessed 02/19/08: http://attorneygeneral.gov/uploadedFiles/Crime/chria.pdf

Cowper, Thomas J. (2005). Network Centric Policing: Alternative or Augmentation to the Neighborhood-Driven Policing (NDP) Model? In C.J. Jensen and B.H. Levin (Eds.), Neighborhood Driven Policing. *Proceedings of the Futures Working Group*, Vol. 1, pp. 18-20. Washington DC: Federal Bureau of Investigation.

Elkins v. United States 364 U.S. 206 (1960).

Hall, Mimi (2007), "State-run sites not effective vs. terror." USA Today. 23 July. Accessed 07/23/07: http://www.usatoday.com/news/nation/2007-07-23-intel-centers_N.htm

Harris, Don R. (1976). The Basic Elements of Intelligence, 2nd edition. Washington, D.C.: Law Enforcement Assistance Administration.

Jacobs, Jane (1961). The Death and Life of Great American Cities. New York: Basic Books.

King, John W. (2000). Collection. Pp. 79-85 in Peterson, Morehouse, and Wright (eds), Intelligence 2000: Revising the Basic Elements. Sacramento, CA and Lawrenceville, NJ: L.E.I.U. and IALEIA.

Kristofferson, Kris (1972). Jesus Was A Capricorn (Owed to John Prine). Song track on Jesus Was A Capricorn album. Columbia Records.

Larkin, Daniel J. (2007). Personal communication. 26 September.

Levin, Bernard H. and Carl J. Jensen III (2005). The electronic donut shop: Networking in the information age. The National Academy Associate 7(2), 14-15, 20-21, 23.

Maguire, Edward R. and William R. King (2009). Federal-Local Coordination in Homeland Security. Forthcoming in Forst, B., J. Greene, and J. Lynch (eds.), Security and Justice in the Homeland: Criminologists on Terrorism. Cambridge.

McDowell, Don (1998). Strategic Intelligence: A Handbook for Practitioners, Managers and Users. Cooma, Australia: Istana Enterprises Pty. Ltd.

McLean, David R. (1965) Cranks, Nuts, and Screwballs. Studies in Intelligence 9:79-89. Summer. Central Intelligence Agency. Accessed 02/18/08: http://www.foia.cia.gov/browse_docs_full.asp.

Meyers, Richard (2007). From Pyramids to Network: Leadership and Structure in 2020. In Joseph A. Schafer, Ed. Policing 2020: The Future of Crime, Communities, and Policing. Washington, DC: Federal Bureau of Investigation.

Meyers, Richard, and Thomas Cowper (2007). Net-Centric Crisis Response. In Joseph A. Schafer and Bernard H. Levin (Eds.), Policing and Mass Casualty Events. *Proceedings of the Futures Working Group*, Vol. 3, pp. 56-77.

Morehouse, Bob (2000). The Role of Criminal Intelligence in Law Enforcement. Pp. 1-12 in Peterson, Morehouse, and Wright (eds), Intelligence 2000: Revising the Basic Elements. Sacramento, CA and Lawrenceville, NJ: L.E.I.U. and IALEIA.

National Cyber-Forensics and Training Alliance. (2007). http://www.ncfta.net/about.asp

National Intelligence Council (2007). National Intelligence Estimate. July. Washington, DC.

Olligschlaeger, Andreas (2005). Personal communication.

Osborne, Deborah (2006). Out of Bounds: Innovation and Change in Law Enforcement and Intelligence Analysis. Joint Military Intelligence College: Washington, DC: JMIC Press.

Parks, Dean (2000). Dissemination. Pp. 113-119 in Peterson, Morehouse, and Wright (eds), Intelligence 2000: Revising the Basic Elements. Sacramento, CA and Lawrenceville, NJ: L.E.I.U. and IALEIA.

Peterson, Marilyn B. (2004). Address to the IACP.

Peterson, Marilyn B., Bob Morehouse, and Richard Wright (Eds.) (2000) Intelligence 2000: Revising the Basic Elements. Sacramento, CA and Lawrenceville, NJ: L.E.I.U. and IALEIA.

Riley, K. Jack, Gregory F. Treverton, Jeremy M. Wilson, and Lois M. David (2005). State and Local Intelligence in the War On Terrorism. Santa Monica: RAND.

Stamp, Sir Josiah (n.d.) Attributed aphorism.

USA PATRIOT ACT (2001). H.R. 3162, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. Passed 24 October 2001. 107th Congress, 1st session.

Walker, Samuel, and Charles M. Katz (2008) The Police in America: An Introduction. Sixth edition. Boston: McGraw Hill.