NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

UNLEASHING OUR UNTAPPED DOMESTIC COLLECTION IS THE KEY TO PREVENTION

by

Nestor Duarte

September 2007

Thesis Co-Advisors: Robert Simeral
James J. Wirtz

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Unleashing Our Untapped Domestic Collection is the Key to Prevention		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Nestor Duarte			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Justice, Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Human intelligence from informants, criminals, good-Samaritans and cooperative individuals is the key to neutralizing major terrorist plots. The need for domestic intelligence collection in the United States is supported by a review of the national strategies and data collected from statements of Federal Bureau of Investigation and Department of Homeland Security officials. Unfortunately, scholarly articles and commentaries point to an inadequate human intelligence program five years after the events of September 11, 2001.

This thesis presents a community based exploitation strategy for the expansion of domestic collection through the leveraging of state and local law enforcement, public and private collection. The strategy would take advantage of the significant untapped law enforcement resources available to state and local law enforcement, public and private entities by encouraging sharing and discouraging hoarding. The technology would do the heavy lifting of sifting through the vast amounts of available information to find the key piece of data. Technology can assist analysts by allowing them to exploit the semantic process of the Global Justice Extensible Markup Language (XML), a computer language. Together, this exploitation strategy and technology will become part of new homeland security doctrine that could unleash the full potential of domestic collection and provide the missing pieces of the intelligence puzzle.

14. SUBJECT TERMS Domestic intelligence, intelligence collection, human intelligence, fusion centers, state and local law enforcement intelligence, Data platforms, GJXML			**15. NUMBER OF PAGES** 107
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

UNLEASHING OUR UNTAPPED DOMESTIC COLLECTION IS THE KEY TO PREVENTION

Nestor Duarte
Assistant Special Agent in Charge, Federal Bureau of Investigation
B.A., Wake Forest University, 1985

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2007**

Author: Nestor Duarte

Approved by: Captain Robert Simeral (ret.)
Co-Advisor

James J. Wirtz, PhD.
Co-Advisor

Douglas Porch,
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Human intelligence from informants, criminals, good-Samaritans and cooperative individuals is the key to neutralizing major terrorist plots. The need for domestic intelligence collection in the United States is supported by a review of the national strategies and data collected from statements of Federal Bureau of Investigation and Department of Homeland Security officials. Unfortunately, scholarly articles and commentaries point to an inadequate human intelligence program five years after the events of September 11, 2001.

This thesis presents a community based exploitation strategy for the expansion of domestic collection through the leveraging of state and local law enforcement, public and private collection. The strategy would take advantage of the significant untapped resources available to state and local law enforcement, public and private entities by encouraging sharing and discouraging hoarding. The technology would do the heavy lifting by sifting through the vast amounts of available information to find the key piece of data. Technology can assist analysts by allowing them to exploit the semantic process of the Global Justice Extensible Markup Language (XML), a computer language. Together, this exploitation strategy and technology will become part of new homeland security doctrine that could unleash the full potential of domestic collection and provide the missing pieces of the intelligence puzzle.

.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my wife Lynda and my sons, Vincent, Antonio and Christopher, for supporting me in this endeavor. This program's most significant sacrifice was my time away from them. I am humbled by their steadfast support and confidence. I would also like to thank the instructors, staff, and fellow students at the Naval Postgraduate School, Center for Homeland Defense and Security, for their relentless pursuit of knowledge and their unflinching patriotism. The richness of the experience has been mind expanding and I will cherish it for the rest of my life. I would particularly like to thank my advisors Captain Robert Simeral (ret.) and James J. Wirtz, PhD. for their guidance, wisdom and expert advice.

Also, I wish to thank the Federal Bureau of Investigation and Department of Homeland Security for supporting this program. Particular thanks go to Special Agent in Charge, Michael J. Folmar and Ms. Carolyn McCormick of the FBI Jacksonville Division who provided me with the time, support and reassurance needed to complete this project. Most importantly, I wish to dedicate this work to the men and women of the FBI, who strive every day to make America safe in spite of untold numbers of pitfalls, obstacles and challenges. This thesis is dedicated to their sacrifices and successes.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

The thesis explores leveraging state and local human intelligence (HUMINT) to increase collection data and expand overall domestic intelligence. Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) efforts to expand domestic intelligence, including coordination of state and local HUMINT, are reviewed. Impediments to the expansion of HUMINT include organizational, budgetary, technological and cultural roadblocks. Data sharing technology is evaluated as a possible mechanism to enable law enforcement sharing of the information that has already been collected by existing law enforcement systems and processes.

B. PROBLEM STATEMENT

Domestic intelligence collection in the United States, specifically state and local HUMINT, is uncoordinated and inefficient to support the terrorism prevention mission.

After the events of September 11, 2001, President Bush stressed the need for military, intelligence, law enforcement, and first responder efforts to focus on the prevention of future terrorist acts. Homeland security leaders recognized that timely and well-synthesized intelligence provided operators with the ability to interdict terrorists before they accomplished their mission. Because intelligence is the centerpiece of prevention, intelligence agencies have labored to enhance their intelligence capabilities in the aftermath of September 11.

Intelligence requires identifying information requirements, collecting information, analysis, dissemination of finished intelligence products and reevaluation. Efforts are underway throughout the United States to enhance analysis and dissemination through fusion centers and intelligence units in virtually every community. Federal, state and local agencies have recognized the importance of increased analytical and information-sharing capabilities to enhance the intelligence cycle. While each of the intelligence

cycle steps provides its own challenges, domestic HUMINT collection has proved to be the limiting factor for domestic intelligence production.

While combined federal, state and local efforts continue to expand the analytical and information-sharing components of the intelligence cycle through increased technology and training, HUMINT production continues to be hampered by inefficient domestic collection. Evidence suggests law enforcement consumers are frustrated with the lack of actionable intelligence reported by domestic fusion centers. This frustration is due in large part to the lack of domestic collection material for analysis and the reliance on open source information by analytical centers. Without a concomitant increase in domestic collection, expanded analysis and dissemination mechanisms at fusion centers is limited to open source and foreign intelligence conclusions, which often lack actionable intelligence necessary for the prevention of major terrorism attacks.

C. METHODOLOGY

1. Interviews

Interviews of federal, state and local intelligence executives were undertaken to establish the current environment in domestic intelligence collection activities and discuss future strategy and implementation. Special emphasis was placed on identifying the challenges and obstacles incurred in the expansion of domestic HUMINT activities. For example, what are the personnel and budget resource issues faced by agencies regarding HUMINT collection? What are the legal impediments to domestic collection? How are the federal agencies utilizing state and local resources in support of HUMINT? The thesis hypothesis regarding leveraging state and local HUMINT will be evaluated. The critique will focus on the acceptance of an improved HUMINT acquisition strategy, especially the budgetary, organizational and cultural impediments that stand in the way of a national strategy to exploit existing collection capabilities.

Selected chiefs and representatives of police were interviewed to evaluate local law enforcement efforts in domestic collection, use of local HUMINT in support of the war on terrorism, acceptance and cultural issues regarding a national HUMINT strategy

and other possible solutions to HUMINT expansion. Law enforcement interviews were solicited from small, medium and large departments to represent the state and local law enforcement community as a whole.

2. Case Study

A case study of the fusion process in the North Florida area was conducted to depict a typical effort at domestic intelligence fusion occurring at the state and local level. The case study illustrates the process, goals, achievements, challenges, and obstacles from the state and local perspective.

3. Technology Studies

Brief studies regarding several data exchange platforms being constructed by the FBI, DHS, and U.S. Navy are discussed to ascertain if these platforms could facilitate a national domestic HUMINT strategy. An analysis of the suitability of the national data platforms as vehicles for leveraging state and local information are discussed. A study of the U.S. Navy's Law Enforcement Information Exchange (LiNX) system is shown to illustrate an example of current technology being used to link law enforcement collection information across department lines in an analytical and sharing environment.

D. DATA

The data surrounding domestic intelligence encompasses four categories of information: the national strategies and policies framing the situation; statements, articles and comments regarding the current and future state of domestic HUMINT collection; the adoption of Community Oriented Policing and Intelligence Led Policing by state and local law enforcement in America; and new intelligence sharing technologies to assist with collaboration.

First, the need for domestic intelligence collection in the United States is supported by a review of the national strategies regarding intelligence expansion after the attacks of September 11, 2001. An analysis of these intelligence milestones forms the

backdrop of the problem, namely the necessity for expansion of domestic collection, specifically in the area of HUMINT in support of the war on terrorism.

Second, data collected from statements of FBI and DHS officials indicate that HUMINT needed to be expanded and that there were challenges involved in the expansion.[1] After the events of September 11th, many improvements to the intelligence production cycle occurred. For example, many intelligence agencies created new and detailed collection requirements designed to address the terrorist threat.[2] Similarly, many agencies increased their analytical capabilities through additional resources and technology in an effort to boost intelligence analysis and production.[3] Furthermore, resources were and continue to be expended in the expansion of law enforcement sharing initiatives to expand the dissemination function.[4]

Scholarly articles and commentaries, however, point to an inadequate HUMINT program five years after the events of September 11, 2001. The 9/11 Commission Report, for example, was critical of the FBI's status of HUMINT expansion and doubtful of its abilities to achieve significant results in this area.[5] Moreover, a collaborative writing by former FBI and Central Intelligence Agency (CIA) executives concluded that intelligence was lacking HUMINT and not adequately addressing the issue of domestic

---

[1] Federal Bureau of Investigation, *Statement of Robert S. Mueller III, Director Federal Bureau of Investigation before the Senate Committee on Appropriations Subcommittee on Commerce, Justice and Science*, 109th Congress, 1st Session, 2005. Available Online: http://www.fbi.gov/congress/congress05/mueller052405.htm (accessed November 24, 2006); *Federal Bureau of Investigation, Statement of Willie T. Hulon, Deputy Assistant Director, Counterterrorism Division Federal Bureau of Investigation, before the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census*, 109th Congress, 2nd Session, 2006. Available Online: http://www.fbi.gov/congress/congress04/bald071304.htm (accessed December 2, 2006); *Federal Bureau of Investigation, Statement of John S. Pistole before the House Judiciary Committee*, 108th Congress, 2nd Session, 2004. Available Online: http://www.fbi.gov/congress/congress04/pistole082304.htm (accessed November 24, 2006); Office of Homeland Security, *Department Six Point Agenda* (Washington, DC: DHS, 2006), 1. Available Online: http://www.dhs.gov/xabout/history/editorial_0646.shtm (accessed November 24, 2006.)

[2] Statement of John S. Pistole, FBI Deputy Director,1.

[3] Ibid.

[4] Office of Homeland Security, *Department Six Point Agenda* (Washington, DC: DHS, 2006). Available Online: http://www.dhs.gov/xabout/history/editorial_0646.shtm (accessed November 24, 2006).

[5] National Commission on Terrorist Attacks upon the United States (Washington, DC: Government Printing Office, 2004) 4, Available Online: http://www.911commission.gov/staff_statements/staff_statement_12.pdf (accessed November 24, 2006).

intelligence.[6] Finally, commentators point to the relative size of the federal domestic effort in comparison to the overall intelligence community as an issue in collection efforts.[7] The resulting conclusion is that federal domestic agencies are committing resources to analysis and dissemination, but are not increasing HUMINT on a nationwide scale. The conclusion is that if federal agencies rely solely on their own collection efforts they will be at risk of not having the necessary information to predict and prevent the next major act of terrorism.

Third, the literature on Community Oriented Policing and Intelligence Led Policing by state and local law enforcement and interviews of selected law enforcement representatives is used in this thesis. Journal articles and reports after September 11, 2001, look to intelligence fusion and analysis as the way for police units in the United States to support the war on terrorism.[8] For example, in 2005, the International Association of Chiefs of Police (IACP) issued their report regarding law enforcement's role in the war on Terrorism. The report included a strategy of expansion of fusion centers and the integration of law enforcement information through increased analysis that "connects the dots" and prevents the next attack.[9] These strategies are based on the premise that "all terrorism is local" and that local law enforcement generates the type of information to thwart an attack. [10]

Fourth, national and regional data platforms capable of digitally incorporating the sharing of law enforcement information were studied. These platforms include the FBI's

---

[6] Robert Bryant, et al., "America Needs More Spies," *The Economist*, July 10, 2003. Available Online: http://www.economist.com/world/na/displayStory.cfm?story_id=1907776 (accessed November 26, 2006.).

[7] David E. Kaplan and Kevin Whitelaw, "Remaking U.S. Intelligence – Part II: the Money," *U. S. News and World Report*, November 11, 2006. Available Online: http://www.usnews.com/usnews/news/articles/061103/3dni.money.htm (accessed November 24, 2006).

[8] Department of Justice, *Intelligence Led Policing: the New Intelligence Architecture* (Washington, DC: DOJ, 2005). Available Online: http://www.ncjrs.gov/pdffiles1/bja/210681.pdf (accessed December 2, 2006).

[9] International Association of Chiefs of Police, *From Hometown Security to Homeland Security* (Washington, DC: IACP, 2005). Available Online: http://www.theiacp.org/leg_policy/HomelandSecurityWP.PDF (accessed December 10, 2006).

[10] Ibid.

National Data Exchange,[11] DHS' Homeland Security Information Network and Homeland Security Data Network, the Regional Intelligence Information System and the U.S. Navy's Law Enforcement Information Exchange.[12] Agency website information and executive statements provide technical and operational information regarding these initiatives. The data platforms provide nationwide accessibility to all law enforcement and promise the ability to exchange law enforcement information on a real time and in a collaborative environment.

E. LIMITS AND SIGNIFICANCE

1. Limits

A review of police intelligence literature reveals many strategies to increase analysis and law enforcement sharing, but there is little literature available regarding the use and leveraging of police informers or police overt intelligence gathering in support of the war on terror. In fact, the topic of domestic collection is addressed only as to the impact on civil liberties. The literature is lacking research regarding new forms of domestic HUMINT collection.

Because of the confidential nature of police informant operations and the need to restrict access, the literature is lacking research and scholarly articles on the topic of exploitation of existing collection resources. The thesis addresses the issue via selected interviews of law enforcement representatives; however, additional research is needed to identify gaps in collection efforts at the state and local level. Furthermore, data regarding HUMINT reporting at the state and local level is unavailable or irretrievable for academic analysis.

---

[11] Department of Justice, *EGovernment Act Implementation Update* (Washington, DC: Budget Data Request May 8, 2004). 3 Available Online: http://www.usdoj.gov/jmd/ocio/egovactreport2004.pdf (accessed October 8, 2006).

[12] Department of Homeland Security, *Information Sharing and Analysis* (Washington, DC: DHS, 2006). Available Online: http://www.dhs.gov/xinfoshare (accessed November 26, 2006).

2. Literature

The thesis brings together various literatures in an effort to answer the research question. The literature encompasses four separate topics describing: a. the framework for the current state of domestic intelligence; b. the need for expansion of domestic HUMINT; c. law enforcement and policing in the war on terrorism; and d. the technology capable of supporting a national HUMINT strategy. These topics are woven together to answer questions not covered in the current literature. The thesis synthesizes the available literature and provides the reader with insight into an emerging threat, namely, the lack of retrievable domestic HUMINT. Furthermore, the interviews provide additional data regarding the use of police informers in support of domestic collection. Therefore, the thesis advances the literature regarding domestic HUMINT and provides insight into future challenges regarding domestic collection requirements.

3. Future Research Efforts

As a public policy document, the thesis suggests a possible national strategy for leveraging domestic collection at the state and local level. Future research is needed regarding the acceptance of such a policy by law enforcement and the relative success such a policy would have on the expansion of domestic HUMINT. Additional research regarding organizational and cultural bias toward the use of domestic collection is also needed. The thesis does not address the issue of civil liberty concerns associated with all domestic collection.

4. Immediate Consumer

The thesis is designed to serve the Department of Justice and Department of Homeland Security, which are responsible for national domestic collection activities and intelligence strategy. Currently, the FBI is responsible for domestic intelligence investigations and the primary federal collector of domestic HUMINT information. DHS is responsible for analysis of domestic information in an "all-hazards" approach. Both the FBI and DHS are primary consumers of such a policy and would ultimately be responsible for promulgation and implementation.

F. ROAD MAP

Chapter II – The Need for Better Collection

Chapter II provides information regarding general intelligence knowledge, terms and methodologies necessary for the formulation and advancement of the thesis. Specifically, the chapter addresses the importance of collection and HUMINT. Challenges to HUMINT collection are discussed as they relate to the lack of HUMINT available to analysts at state and regional fusion centers.

Chapter III – The Current Domestic Intelligence Environment

Chapter III provides the reader with a snapshot of current federal, state and local domestic intelligence efforts. The chapter highlights changes and developments by the FBI and DHS with respect to their intelligence operations after September 11, 2001. State and local law enforcement intelligence operations are also described, including the emergence of Community Oriented Policing and Intelligence Led Policing in American law enforcement.

Chapter IV – The Future in Domestic Intelligence

The future of domestic intelligence in the United States is discussed as it relates to HUMINT collection and analysis at state and local fusion centers. The issue of stove piped information and knowledge management limitations is presented as an obstacle to transmittal of collection data to fusion centers. Data platforms and technology that may affect future aggregation of domestic intelligence information are reviewed.

Chapter V – Obstacles to National Collection and Analysis

Chapter V addresses the obstacles to collection and analysis including legal restrictions, cultural issues, funding restraints and recalcitrant bureaucracies. A change methodology including change agents and the need for leadership is addressed.

Chapter VI – Strategy and Conclusion

The final chapter provides a strategy for unleashing stove piped domestic collection including an adaptation of W. Chan Kim's and Renee Mauborgne's *Blue Ocean Strategy*. The conclusion advocates the need for accessing and exploiting state and local domestic collection using analytical technology instead of costly and intrusive expansion of federal collection programs. Recommendations include cultural, funding, technological and bureaucratic changes to federal, state and local intelligence programs.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE NEED FOR BETTER COLLECTION

After the events of September 11, 2001, the George W. Bush Administration adopted a strategy to expand domestic intelligence to prevent the next act of terrorism. In 2004, the president of the United States issued Executive Orders 13355 and 13356, which restructured, delineated and expanded intelligence management and dissemination within the Intelligence Community (IC).[13] That same year, Congress passed the Intelligence Reform and Terrorism Prevention Act, which established the Office of the Director of National Intelligence (DNI).[14] In 2005, the DNI office issued a formal strategy outlining the new course for domestic intelligence.[15] The DNI's strategy called for the establishment of a "National Clandestine service to integrate all elements of human source collection."[16] This strategy also called for the expansion of an integrated intelligence process that conformed to existing legal and civil liberty protections.[17] To implement the domestic parts of the new intelligence model, the Federal Bureau of Investigation (FBI) issued a strategy to augment intelligence by creating the Directorate of Intelligence.[18] The FBI strategy included the prevention of terrorism through the "expansion of robust human source reporting."[19] On April 28, 2005, the Department of Homeland Security (DHS) issued its Intelligence and Information Sharing Initiative,

---

[13] U. S. President Executive Order, *Strengthening Management of the Intelligence Community, Executive Order 13355* (Washington, DC: Government Printing Office, 2004). Available Online: http://www.fas.org/irp/offdocs/eo/eo-13355.htm (accessed November 29, 2006); U.S. President Executive Order. *Strengthening the Sharing of Terrorism Information to Protect Americans, Executive Order 13356* (Washington, D.C.: Government Printing Office, 2004). Available Online: http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html (accessed November 29, 2006).

[14] U.S. Congress, House, *Intelligence Reform and Terrorism Prevention Act of 2004*, December 7, 2004, 108th Cong, 2d session, House report No. 108-796 (Washington, DC: Government Printing Office, 2004). Available Online: http://www.nctc.gov/docs/pl108_458.pdf (accessed December 2, 2006).

[15] Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America* (Washington, DC: Office of the Director of National Intelligence, 2005). Available Online: http://www.dni.gov/publications/NISOctober2005.pdf (accessed December 2, 2006).

[16] Ibid., 13.

[17] Ibid., 11.

[18] Federal Bureau of Investigation, *Strategic Plan 2004-2009* (Washington, DC: FBI, 2003). Available Online: http://www.fbi.gov/publications/strategicplan/strategicplanfull.pdf (accessed December 2, 2006).

[19] Ibid., Section IIB1.

which highlighted the need for domestic collection of intelligence from information derived from state, tribal, and local government sources.[20]

In addition to the administration's policies and strategies, several government entities critically reviewed the events of September 11, 2001, and provided insight and recommendations regarding intelligence collection, analysis and dissemination. The first major investigation of the intelligence shortcomings of the United States was conducted by a joint inquiry of the Congress of the United States. The report was released on December 10, 2002.[21] The report recommended that the government "establish capabilities for the timely sharing of intelligence within the intelligence community and with appropriate other federal, state, and local authorities." Similarly, the 9/11 Commission Report released on July 22, 2004, found that information was not shared adequately across jurisdictional boundaries and that a national intelligence center was necessary to coordinate domestic intelligence.[22] On July 7, 2004, the Senate's Intelligence Committee released its report on prewar-intelligence calling, for the development and recruiting of sources with direct access to information.[23] The Commission on Intelligence Capabilities of the United States regarding Weapons of Mass Destruction, commonly known as The WMD Commission, issued its report on March 31, 2005, and recommended, among other things, that HUMINT collection should be standardized under one agency, namely the CIA.[24] Together, these strategies and

---

[20] Department of Homeland Security, *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and information Fusion* (Washington, DC: Office of Homeland Security, 2002), 2. Available Online: http://www.dhs.gov/xlibrary/assets/HSAC_HSIntelInfoFusion_Apr05.pdf (accessed, December 2, 2006).

[21] U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001*, unclassified version of report, December 2002, 4.

[22] National Commission on Terrorist Acts upon the United States, *the 9/11 Commission Report* (New York: W.W. Norton & Co., 2004), 353, 411.

[23] Senate Select Committee on Intelligence, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, July 7, 2004, 34. Available Online: http://www.gpoaccess.gov/serialset/creports/intel_reform.html (accessed September 3, 2007).

[24] Commission on Intelligence Capabilities of the United States regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005, 22. Available Online: http://www.wmd.gov/report/ (accessed September 7, 2007).

recommendations demonstrate the consensus behind the expansion of domestic intelligence and the creation of a national strategy for domestic HUMINT within the United States after 2001.

A review of domestic intelligence requires a discussion about the components of intelligence. Efforts at expanding domestic intelligence can be categorized according to each component. Analyzing the intelligence cycle reveals the importance of collection to the process and human intelligence as the key to effective domestic collection.

A. INTELLIGENCE CYCLE

It is important to distinguish intelligence from information. Information sharing, especially in law enforcement circles, is often confused with the dissemination of intelligence. Intelligence can be distinguished from information as a subset. Intelligence is information that has been collected, processed, and narrowed to meet the needs of a policy maker.[25] The process of identifying the requirements of the policy maker, collecting information, analyzing it, and disseminating it to the appropriate consumers is known as the intelligence cycle or intelligence process.[26] The cycle, often described or illustrated as a unidirectional arc, is actually closer to a multidirectional process path with multiple opportunities for feedback and additional analysis.[27]

[25] Mark M. Lowenthal, *Intelligence from Secrets to Policy* (CQ Press, Washington, DC: 2006), 2.

[26] Ibid., 65.

[27] Ibid., 66.

Figure 1. Intelligence Cycle.

B. SIGNIFICANCE OF COLLECTION

Perhaps the most difficult aspect of intelligence within the intelligence cycle is collection. Known as the bedrock of intelligence, collection is the accumulation of information for analysis.[28] Collection can be complicated, depending on the requirement question to be answered, because it often involves the receipt of information not easily or readily obtained through other means. Collection requirements respond to the questions a policy maker needs answered. The questions are often challenging and protected by enemy or criminal opposition. The collector is faced with obtaining information that is difficult to obtain or hidden from plain view. Instead of attempting to answer large intelligence questions outright, intelligence professionals seek to breakdown

[28] Lowenthal, *Intelligence from Secrets to Policy,* 68.

requirements into packets of information that can be analyzed. Known as intelligence requirements, these requests outline specific bits of information to be collected. Together they help the analyst form the answers to the policy questions being investigated.

Within the art of collection are several different collection disciplines known as INTs. The collection disciplines include Signals Intelligence (SIGINT), Geospatial Intelligence (GEOINT), Measurements and Signature Intelligence (MASINT), Open Source Intelligence (OSINT), and Human Intelligence (HUMINT).

Within HUMINT are two broad categories known as overt and covert HUMINT. These categories indicate whether or not the human collector's identity is either known or concealed from the subject of collection. For example, spies operating under cover are referred to as covert collectors, while police officers receiving information from community members can be described as overt collectors. In each case the identity of the individual as collector is either concealed or known respectively. Domestic HUMINT efforts can therefore be described as covert operations, i.e. informants, spies, undercover Agents, or overt intelligence gathering such as community policing, community outreach and other overt law enforcement activities. Both forms of HUMINT play a significant role in the domestic intelligence cycle. While federal, state and local law enforcement utilize both overt and covert collection techniques; these efforts are uncoordinated and lack national strategy.

C. IMPORTANCE OF HUMAN INTELLIGENCE TO COLLECTION

Prior to September 11, 2001, domestic intelligence gathering by state and local law enforcement in the United States had been a function of the analysis of predicated investigative law enforcement information. That is, information which was originally obtained from criminal investigations initiated as a result of probable cause that a crime had been, or was about to be, committed. The post September 11th paradigm called for domestic intelligence gathering, not necessarily predicated on prosecution, but for the prevention of an attack. No longer was there time to wait for the crime to occur and coordinate the intelligence to apprehend the perpetrators, instead efforts were underway to identify the conspirators before they were able to act.

In the FBI, for example, the shift from crime solving to prevention was, and continues to be, a significant challenge after September 11, 2001. [29] The large shift in thinking, as well as resources, evolved into the Directorate of Intelligence (DI) within the FBI, with the mission of "connecting the dots" before the next major attack occurred. Although intelligence units in the FBI were nothing new, the FBI DI was now responsible for the FBI's domestic collection, analysis and dissemination process. The post September 11th collection process, centered on intelligence community collection requirements, directed a Bureau-wide effort of intelligence gathering tailored to specific intelligence needs. The analysis component continued to be expanded as a result of huge increases in analytical resources, allowing the DI to create tactical, strategic and global analysis of information. The dissemination processes, known mostly for its Intelligence Information Reports, began to disseminate thousands of reports to the intelligence community. The HUMINT component also was expanded through recruitment of sources and expansion of community outreach programs.

In spite of the expansions, the HUMINT collection component continues to be the most challenging part of the intelligence cycle. The requirement, analytical and dissemination functions, challenged with many obstacles, are largely a function of resources and new business practices. The requirement and analytical processes are replicated throughout the country in many quality intelligence and fusion centers. Enhanced analytical products are being created throughout the country using expanded analytical resources and better analytical tools. The FBI dissemination process, hampered by information technology short comings and information sharing issues, will eventually benefit from equipment updates and new sharing practices. Although there are many analytical centers around the United States, collectors of intelligence are more limited. While analytical and information sharing concerns often dominate the public discussion, collection limitations ultimately affect the available information to be

[29]Federal Bureau of Investigation, *Statement of Robert S. Mueller III, Director, Federal Bureau of Investigation to Congress*, July 27, 2005. Available Online: http://www.fbi.gov.congress/congress05/mueller072705.htm (accessed May 23, 2006).

analyzed and disseminated. The collection requirement is complicated by the need to cultivate human sources of information, increase liaison activities, and establish technical and electronic collaborative systems.

To provide first responders with actionable intelligence, it is necessary to gather intelligence regarding the activities of individuals who have not yet committed a crime but may be planning to do so. The underpinning of prevention is a robust collection capability. The intelligence base from which the analytical process stems and generates law enforcement sharing depends upon it. The post September 11th environment calls for aggressive collection of overt and covert human intelligence to predict vulnerabilities and identify trends. This will undoubtedly involve significant increases in the domestic collection capability of the law enforcement and intelligence community. For example, data mining techniques designed to cull through millions of records, already used extensively by the private sector and by foreign intelligence collectors, will have to be applied to the domestic arena. Government partnerships with private sector entities capable of providing significant intelligence through increased technology will also increase. These and other new methods will undoubtedly conflict with civil liberty and privacy concerns. Ultimately, a balance of competing interests will be necessary to address the conflicting priorities of legitimate intelligence gathering in support of prevention efforts and protecting individual privacy.

Figure 2. Total HUMINT Base: Overall HUMINT capability increases as covert and overt HUMINT are leveraged through collaboration with state and local entities within the community. The figure depicts HUMINT expanding geometrically as it is aggregated with ever increasing groups of collectors at the federal, state and local level.

III. THE CURRENT DOMESTIC INTELLIGENCE ENVIRONMENT

Since September 11, 2001, governmental bodies, journalists, analysts, academicians and practitioners have recommended sweeping changes to the federal domestic intelligence model of the United States. These observers have focused on reforms to the FBI and DHS. Recommendations for reform of the FBI have included divesting the agency of its intelligence and counterterrorism functions. Known as the "MI-5" model, proponents of a new agency solution suggest such an agency would enhance domestic collection and provide policy makers with better intelligence. Detractors contend that the FBI has long standing infrastructure and investigative skills needed for the intelligence mission, and that reforming the FBI is more efficient.

This chapter addresses these calls for reform by describing changes and developments made to the intelligence programs of the FBI and DHS after September 11, 2001. Specifically, the chapter will discuss expansions of the FBI's Directorate of Intelligence and the DHS Office of Intelligence and Analysis. Additionally, the chapter addresses the growing body of intelligence within the state and local law enforcement community as a result of Community Oriented Policing and Intelligence Led Policing programs.

A. FBI INTELLIGENCE MODEL

Efforts at reforming the FBI have centered on the creation of the Directorate of Intelligence (FBI/DI) and the adoption of the new Model Counterterrorism Investigative Strategy. In July 2003, the FBI issued this strategy to all field offices.[30] The newly created FBI/DI expanded intelligence and analytical resources and was designed to

[30] Federal Bureau of Investigation, "The FBI Counterterrorism Program Since 9/11," Report to the Terrorism Commission on the events of September 11, 2001, 29. Available Online: http://www.fbi.gov/publications/commission/9-11commissionrep.pdf (accessed May 30, 2007).

provide intelligence with independent and highly trained intelligence professionals dedicated to intelligence collection and management. [31]

The Model Counterterrorism Strategy combined the investigative tools available to criminal and intelligence investigations under one new investigative classification. Criminal tools such as Grand Jury Subpoenas, search warrants, Title III wire taps and criminal informants were merged with National Security intelligence and investigative tools such as National Security Letters, Foreign Intelligence Surveillance Act court orders and intelligence asset information. The combined investigative strategy afforded investigators the use of all investigative tools available to the FBI under one investigative classification. This scenario was impossible prior to September 11, 2001, as a result of the infamous "wall" procedure which segregated criminal and intelligence investigations.[32]

Critics of the FBI's new plan, however, were quick to attack its usefulness. For example, John Lehman, of the 9/11 Commission, wrote in an editorial piece in the *Washington Post*, stating that

> Congress sought to remedy this problem by creating a national security service within the FBI to focus on preventive intelligence rather than forensic evidence. This has proved to be a complete failure.[33]

A similar conclusion was offered by Judge Richard Posner on August 6, 2006:

> The bureau is a criminal investigation agency. Its orientation is toward arrest and prosecution rather than toward the patient gathering of intelligence with a view to understanding and penetrating a terrorist network The bureau's tendency, consistent with its culture of arrest and

---

[31] Federal Bureau of Investigation, *Counterterrorism* (Washington, DC: FBI, 2006). Available Online: http://www.fbi.gov/aboutus/transformation/ct.htm (accessed, November 24, 2006).

[32] FBI Report to the National Commission on Terrorist Attacks upon the United States: *The FBI's Counterterrorism Program Since 9/11* (April 14, 2004).

[33] John Lehman, "We're Not Winning This War," *The Washington Post*, August 31, 2006; A25. Available Online: http://www.washingtonpost.com/wp-yn/content/article/2006/08/30/AR2006083002730.html (accessed March 17, 2007).

> prosecution, is to continue an investigation into a terrorist plot just long enough to obtain enough evidence to arrest and prosecute a respectable number of plotters.[34]

The Markle Report, which was also critical of the FBI, cited two flaws in the FBI's approach to Domestic Intelligence. First, the report noted that inviting the FBI to investigate citizens not predicated by criminal activity incurred a conflict of interest for the FBI. Second, the report stated that the FBI was not equipped to provide analytical intelligence reporting to other parts of the federal government.

The premise that the FBI has a conflict of interest has been stated by others to support the opposite conclusion: A stand alone domestic intelligence agency without the concomitant role of enforcing civil rights would be *more* likely to violate privacy issues then a law enforcement agency.[35] The Markle Report's "checkered history" quote refers to the abuses sustained by Dr. Martin Luther King Jr. and his family during the FBI's Counterintelligence Program (COINTELPRO) Era of the 1960s. Significant changes have occurred in the FBI since that era. The 9/11 Commission also tackled the issue of FBI abuses in the 1960s. They concluded that after the criticisms of the FBI by the Church Committee in the 1970s, "the pendulum swung away from those types of investigations in the 1980s and 1990s." The Committee also concluded that "if a new domestic intelligence agency were outside the Department of Justice, the process of legal oversight-never easy- could become even more difficult."[36]

Critics also have suggested that the FBI is too entrenched in police culture and not suited for the intelligence mission. The *Boston Herald* recently wrote "FBI culture is a police culture, not a counter-spy culture. And it's likely it will stay that way. Congress is in a far better position to mobilize a counter-spy culture outside the agency than even the

---

[34]Richard A. Posner, "We Need Our Own MI5," *The Washington Post*, August 15, 2006, A13. Available Online: http://www.washingtonpost.com/wpdyn/content/article/2006/08/14/AR2006081401160.html (accessed March 17, 2007).

[35] National Commission on Terrorist Attacks upon the United States (Washington, DC: Government Printing Office, 2004), 423, Available Online: http://www.911commission.gov/staff_statements/staff_statement_12.pdf (accessed November 24, 2006).

[36] Ibid.

most well-intentioned FBI director could do inside the agency."[37] In response to these criticisms, the FBI has created specific career paths and training programs to make the intelligence programs independent from the criminal side of the house.

The tendency exhibited here is to paint the Bureau with a wide brush and to refer to its history and stereotypes as current fact. In reality, the Bureau has undergone significant changes to adapt to the post September 11th counterterrorism environment. For example, the FBI/DI is now headed by an Assistant Director. The FBI/DI has hired over two thousand analysts and has established Field Intelligence Groups in all 56 FBI field offices. It has a College of Analytical Studies, which is an analytical training program that helps build relationships with numerous other intelligence agencies including the CIA and MI-5. And, although the FBI/DI lacks academic maturity, the program is proceeding quickly and decisively in an independent fashion.

The FBI has retained the responsibility to recruit and task informants in domestic intelligence investigations. An important part of the FBI's Intelligence Program is the expansion of covert HUMINT in all of its programs. While specific figures regarding increases in human sources are classified, the FBI's report to the 9/11 Commission on changes since 2001 stated that one of the "yardsticks" for measuring the effectiveness of a counterterrorism program was the development of human assets. The report stated that an application of these yardsticks demonstrated that progress in expanding the human source program had been achieved since September 11, 2001.[38] The fact that both Agents and analysts in the counterterrorism program have been increased should lead the reader to conclude that the FBI human asset program has been significantly expanded.

Although the FBI has made gains in terms of expansion of its terrorism and intelligence programs, as of 2005, according to the 9/11 Commission Report, the FBI had been unable to expand domestic human intelligence. The report stated that "despite the widespread view that assets and informants are the best source of intelligence," the FBI

---

[37] Boston Herald Editorial Staff, "We Need an American MI-5," *Boston Herald*, August 27, 2006. Available Online: http://news.bostonherald.com/editorial/view.bg?articleid=154613 (accessed April 29, 2007).

[38] *The FBI Counterterrorism Program since 9/11*, 63.

was unsuccessful in recruiting informants into high level terrorist circles.[39] Insomuch as the expansion of intelligence is essential to the prevention of terrorism and an integral part of the national strategy, the FBI's covert resources alone will not adequately expand overall domestic intelligence production.

One way to overcome insufficient covert human collection assets is to expand collection through overt community outreach programs. The FBI had long recognized the importance of community cooperation to fight crime. For many years, the Bureau had operated community outreach programs designed to form relationships with minority, civic, civil rights and other groups. For example, minority groups were contacted to assist with Civil Rights investigations. Civic groups were targeted to enhance corporate fraud and public corruption investigations. And civil rights groups were asked to provide information concerning police abuse and hate crimes. These programs existed in every FBI field office. The role and scope of these units remained essentially the same for decades.

After the events of September 11, 2001, however, the FBI began to shift its efforts to broaden intelligence collection and to expand community enhanced liaison programs. As a result, almost all criminal and intelligence programs in the FBI have seen a surge in community based intelligence gathering. While some of the programs are not termed intelligence gathering per se, all share certain things in common. For instance, counterterrorism programs strive to form positive relationships with members of the Muslim community through meetings and working groups from the area mosques, Islamic centers and clubs. The meetings allow both parties to get to know each other and to break down negative stereotypes.

Cyber programs have likewise initiated "Infragard" chapters all over the country. These working groups target information technology professionals in major commercial

[39] National Commission on Terrorist Attacks upon the United States, *Staff Statement No. 12* (Washington, DC: Government Printing Office, 2004), 4. Available Online: http://www.911commission.gov/staff_statements/staff_statement_12.pdf (accessed November 24, 2006).

and industrial applications who might be targets of computer intrusions or internet fraud. These working groups also provide training and intelligence bulletin information to the members.

Another recently expanded outreach program is the Field Intelligence Groups (FIG), which undertake mapping and threat assessment initiatives.[40] FIGs, as the field extension of the FBI's Directorate of Intelligence, are producing programmatic threat assessments for locations all around the country. These assessments are based on aggressive mapping and surveying regional areas known as domains. Surveys include area law enforcement at all levels, open source information, and analysis of FBI information. Liaison, working groups and relationships are the key to the success of these programs. Broad based knowledge from multiple sources is intended to provide detailed, specific domain mapping.

Legacy community outreach programs such as the Civil Rights and minority programs also have seen an upsurge in tempo and scope. Civil Rights programs are now encouraged to establish working groups and task forces with all significant minorities, civic and non-governmental organizations in a region, instead of only the predominant or large group. This has resulted in an increase in meetings and liaison with groups throughout the country.

Traditional task group operations in the criminal arena continue to expand and concentrate on force multiplication and increased use of civilian partnerships. Each FBI field division also is expected to conduct yearly Citizens' Academies in their respective cities. The Citizens' Academy affords participants an up close view of the FBI and its operations. The FBI in turn is building a cadre of civilian ambassadors to promote cooperation and civic involvement. The alumni assist with recruiting, community awareness, business liaison and promotion of the FBI's overall mission. Mission awareness and personal relationships with agency representatives increases the effectiveness and efficiency of the FBI.

[40] *The FBI Counterterrorism Program since 9/11*, 28.

The next step in the expansion of community outreach process is the national coordination of these programs. Coordination increases the productivity of the FBI's overt collection operations. Many of these programs overlap or produce information of interest to more than one kind of investigation. By coordinating these efforts, the programs are more responsive to their members. Moreover, civilians tend to be associated with multiple groups and societies which lend themselves to multiple collection efforts and disciplines. The coordination of these programs gives the FBI the ability to take advantage of the scope of its liaison and jurisdiction on a national scale.

B. DEPARTMENT OF HOMELAND SECURITY INTELLIGENCE MODEL

The DHS Office of Intelligence and Analysis (OI&A) was formed in the aftermath of September 11, 2001. It is dedicated to the analysis of all government related intelligence pertinent to the homeland security of the United States.[41] The OI&A was intended to act as a one stop shopping point for all domestic analysis. DHS is responsible for the analysis of all matters pertaining to the nation's current or future vulnerabilities.[42] To accomplish this, DHS must collect, analyze and disseminate intelligence that may have an impact on the protection of national infrastructure. While the OI&A does not have specific collection authority itself, it is mandated to receive domestic collection intelligence from other collection agencies within and outside the Department, including Customs and Border Protection, Immigration and Customs Enforcement, United States Secret Service, United States Coast Guard, Department of Defense agencies, FBI, CIA and others.[43] The OI&A also receives terrorism specific data from the National Counterterrorism Center, which is comprised of all intelligence agencies collecting on terrorism related matters.

---

[41] Peter Chalk and William Rosenau, "Intelligence, Police and Counterterrorism: Assessing Post 9/11 Initiatives," *Rand Reports*, October 30, 2003, 12. Available Online: http://www.rand.org/nsrd/terrpanel/additional/intelinputv2.pdf (accessed August 19, 2007).

[42] Department of Homeland Security, "DHS webpage," Available Online: http://www.dhs.gov/xinfoshare (accessed June 3, 2007).

[43] Ibid.

The DHS Intelligence Section's priorities include improving the quality of intelligence analysis across the Department, integrating the DHS intelligence enterprise, strengthening support for state and local authorities, ensuring DHS takes its full place in the intelligence community and solidifying the DHS relationship with Congress.[44]

The first three priorities are embedded in the Department's efforts to fund, establish, guide and leverage the fusion centers around the country. Central to the DHS' efforts to collect intelligence is the emergence of the state fusion centers. DHS considers the fusion center network to be an essential component of the national intelligence architecture.[45] The state and Local Fusion Center Program is a direct outgrowth of the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004.[46] Both pieces of legislation have called for a more robust national intelligence picture able to draw upon federal, state, local and tribal assets.[47] By establishing a robust fusion center network, DHS improves intelligence analysis, collection and dissemination.

The fusion centers also provide DHS with a crucial platform for "push and pull" of information from the state and local arena. The state and local threat information is considered vital to the overall threat matrix and vulnerability assessment mission. By investing in the fusion centers, DHS not only gains connectivity but also strengthens state and local departments' intelligence efforts simultaneously. DHS analysts and intelligence officers assigned to state fusion centers are able to leverage intelligence vital to this process, and act as force multipliers of scarce DHS intelligence resources.

---

[44] *Statement of Assistant Secretary Charles E. Allen to the U.S House of Representatives*, May 24, 2006, 2. Available Online: http://homeland.house.gov/SiteDocuments/20070413143439-12273.pdf (accessed June 6, 2007).

[45] Telephonic Interview of Jack Tomarchio, Deputy Chief intelligence Officer, Office of Intelligence and Analysis, Department of Homeland Security, by the author on February 27, 2007.

[46] *Statement of Assistant Secretary Charles E. Allen to the Subcommittee on Intelligence Information Sharing and Terrorism Risk Assessment, House Homeland Security Committee*, February 14, 2007, 4. Available Online: http://hsc.house.gov/SiteDocuments/20070314172258-47553.pdf (accessed August 19, 2007).

[47] Ibid.

The fusion centers' ability to serve as a two-way street of information allows DHS to collect and disseminate information with up to 70 regional and state intelligence centers.[48] The Homeland Security Data Network, (HSDN) is a classified data platform capable of transmitting classified information between these fusion centers. DHS has budgeted $110,000 per fusion center for the purposes of wiring HSDN into each center. DHS plans to have "tailored, multi-disciplinary teams of intelligence and operational professionals in major fusion centers nationwide by the end of fiscal year 2008."[49] This is an ambitious plan that will require deploying over 200 highly trained and skilled intelligence officers/analysts by 2008. DHS has currently deployed 16 officers to various fusion centers around the country.[50]

Between the National Counter Terrorism Center representation and the fusion center network of networks, DHS envisions a national intelligence picture capable of detailed threat assessments. The OI&A will receive the data and "use this data to 1) map potential threats against existing vulnerability assessments, 2) take and recommend responses to identified challenges contingencies; and 3) set national priorities for critical infrastructure protection."[51]

According to the FBI, DHS plays a crucial role in "assessing and protecting vulnerabilities in our national infrastructure and at the borders."[52] Coordination is achieved through the sharing of databases at the headquarters level and through task force collaboration at the field level.[53] Analysts from both departments hold weekly briefings regarding pertinent intelligence and executives from both departments are exchanged to foster better understanding of the culture and products of other organizations.[54]

---

[48] *Statement of Assistant Secretary Charles E. Allen.*

[49] Department of Homeland Security, "DHS webpage." Available Online: http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm (accessed May 30, 2007).

[50] Ibid.

[51] Chalk and Rosenau, "Intelligence, Police and Counterterrorism: Assessing Post 9/11 Initiatives,"14.

[52] *The FBI Counterterrorism Program since 9/11*, 45.

[53] Ibid.

[54] Ibid.

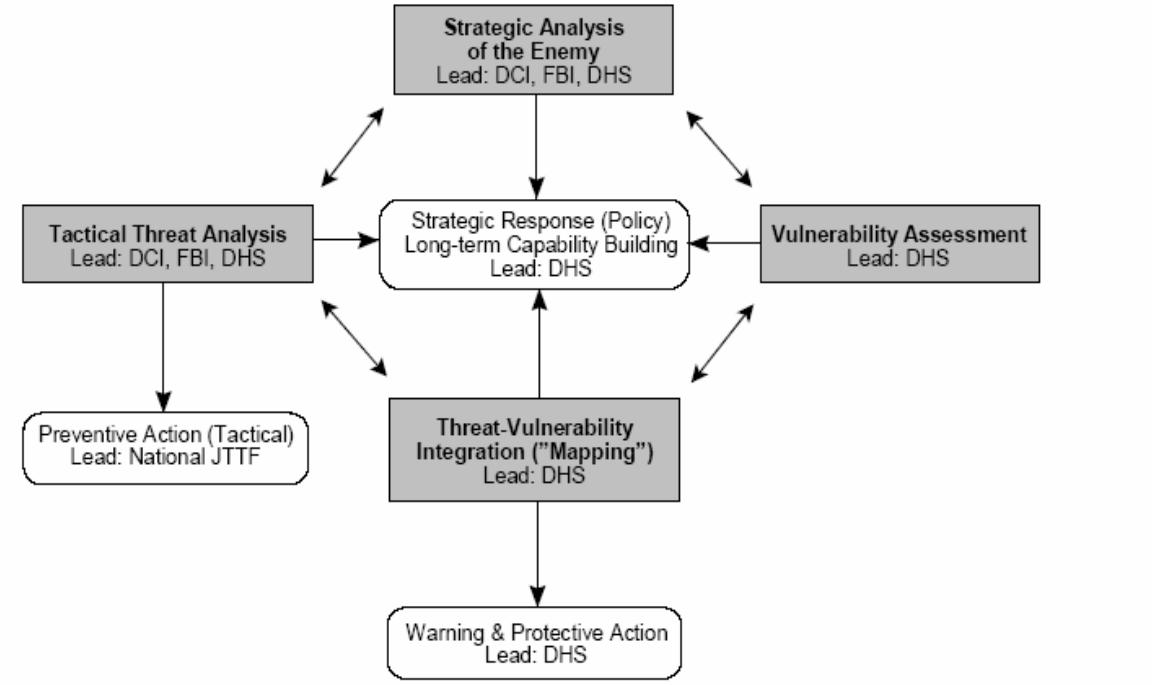


Figure 3. Roles and responsibilities of Homeland Security Intelligence and Information Analysis.[55]

C. THE STATE AND LOCAL LAW ENFORCEMENT INTELLIGENCE MODEL: AN UNTAPPED INFORMATION BONANZA

This section discusses the emergence of state and local law enforcement domestic intelligence as a result of community oriented and intelligence led policing programs. The section describes the evolution of intelligence in policing and the increasing volume of intelligence data being collected. The section also discusses obstacles in accessing data that is non electronic or file data that is not easily retrievable.

[55] Todd Masse, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches* (Congressional Research Service, August 18, 2006), Figure 2, CRS-10.

1. Community Oriented Policing

Approximately 30 years ago, basic policing philosophy began to shift from patrol and response to gaining awareness on the ground by engaging the community.[56] Law enforcement began to work closely with communities and officers transitioned from squad cars to bicycle patrols. As police officers interacted more and more with the public, police departments gained valuable intelligence. Across the country, police departments slowly began to see the wisdom and effectiveness of engaging the public. In the ensuing years, a majority of departments adopted the model and adapted it to their own particular needs. By 1997, 98% of departments with over 500 officers had adopted Community Oriented Policing (COP) in America.[57] 80% of the large departments had created Neighborhood Watch programs, 85% held police community meetings and 97% said COP had improved cooperation between police and citizens.[58] As of 2003, 82% of all departments were utilizing COP, including 50 departments with more then 1000 officers and 61% of departments who employed at least 100 officers.[59] The shift to COP created safer neighborhoods and better relations between police and the community.

The close relationship with the public created more information about the community, its players and the social environment. Police departments were more attuned to the problems of the community and were able to prevent crime by interdicting situations before they resulted in violations of the law. A by-product of COP was increased intelligence and information about the community.

---

[56] Department of Justice, "Community Oriented Policing Services, Protecting Your Community from Terrorism: Strategies for local Law Enforcement, The Production and Sharing of Intelligence," *Volume 4*, February 2005, VII. Available Online: http://www.cops.usdoj.gov/default.asp?Item=143 (accessed August 19, 2007).

[57] National Institute of Justice, "Community Policing: 1997 National Survey Update of Police and Sheriff's Departments," September 22, 2000, iii. Available Online: http://www.securitymanagement.com/library/ncj_police0601.pdf (accessed August 19, 2007).

[58] Ibid, iv, v.

[59] Department of Justice, *Law Enforcement Management and Administrative Statistics, Local Police Departments, 2003*, May 2006, 7. Available online: http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed August 19, 2007).

After September 11, 2001, law enforcement professionals began advocating the COP model as an intelligence vehicle for preventing terrorism.[60] The challenge therefore was to understand the terrorism intelligence gap in terms of community policing and apply the lessons from past successes without violating individual's civil liberties.[61] The idea that information sharing alone could solve the intelligence gap became a misconception.[62] It became apparent that collecting the right information, at the right time, and sharing it, was the goal. Because police officers involved in COP can be viewed as overt collectors, they can be the crucial pieces of the puzzle that detect anomalies in the community.[63] According to Peter Modaferri, Chief of Detectives, Rockland County, NY, "we need a generation of police officers who know how to identify, collect, and use information before we can ensure legitimately productive information sharing."[64]

2. Intelligence Led Policing

The conceptualization of the patrol officer as overt collector led to crime fighting via intelligence gathering and analysis.[65] The next generation in police philosophy became known as Intelligence Led Policing (ILP). ILP, which emerged in the 1990s, was defined as a collaborative enterprise that relied on improved intelligence gathering and community oriented policing.[66] Police Chief William J. Bratton described ILP as, "the collection and analysis of information to produce an intelligence end-product designed to

---

[60] Heather J. Davies and Gerard R. Murphy, "Protecting Your Community from Terrorism," *Police Executive Research Forum*, Washington, DC: March 2004, 1. Available Online: http://www.mipt.org/pdf/Protecting-Your-Community-From-Terrorism-Vol2.pdf (accessed August 19, 2007).

[61] Ibid.

[62] Ibid.

[63] Ibid., 23.

[64] Ibid., 31.

[65] George L. Kelling and William J. Bratton, "Policing Terrorism," *Manhattan Institute*, No. 43, September 2006, 5. Available Online: http://www.manhattan-institute.org/html/cb_43.htm (accessed June 6, 2007).

[66] Marilyn Peterson, "Intelligence Led Policing: The New intelligence Architecture," Department of Justice, Bureau of Justice Assistance, NCJ 210681, VII, September 2005. Available Online: http://www.ncjrs.gov/pdffiles1/bja/210681.pdf (accessed June 6, 2007).

inform police decision making at both the tactical and strategic levels."[67] ILP combined the strengths of COP and leveraged it by adding the analysis of key data. Instead of wasting personnel resources on areas devoid of crime, ILP concentrated COP on those communities that analysis indicated would benefit from a greater police presence. Mapping and police statistical analysis provided hard data for police managers to use in assigning resources and creating strategy. Popularized by the New York Police Department in the 1990s, intelligence led policing was able to drastically reduce crime in New York City by adjusting an existing COP program according to intelligence and analytical data.[68]

Since September 11, 2001, ILP has been suggested as the model for terrorism policing. The theory, much like that of COP, is that ILP can be applied to terrorism by adjusting the data collection points and focusing the resources on terrorist related indicators.

Intelligence operations by state and local departments, however, have been hindered by lack of policies, procedures and training.[69] Most law enforcement departments do not have intelligence units; only 100 of the larger departments have established intelligence units.[70] The majority of law enforcement has not been able to realize the potential of ILP. While COP was inherent in smaller departments as a function of the relative size of the community and the department, ILP is dependant upon analytical resources and information technology. This is important because the success of fusion centers depends on the free flow of reporting from the vast array of law enforcement departments throughout the United States. Without the benefits of ILP and the intelligence units to guide them, the 91% of departments with fewer then 50 officers

---

[67] *Protecting Your Community from Terrorism*, 19

[68] Ibid., 2.

[69] *Intelligence Led Policing – The New Intelligence Architecture*, VII.

[70] David E. Kaplan, "Spies Among Us," *U.S. News and World Report*, April 30, 2006, 3. Available Online: http://www.usnews.com/usnews/news/articles/060508/8homeland.htm (accessed May 6, 2007).

are relied upon to relay information to the fusion centers through informal channels. This puts a tremendous responsibility and burden on patrol officers from smaller departments and rural America.

Prompting individual officers to recognize, collect and disseminate information is a function of training. Many larger departments are creating training regimens for their smaller department colleagues to expand their collection capabilities. For example, the Los Angeles Police Department, through its training officer program, conducts terrorism and cultural awareness training for multiple jurisdictions and organizations to increase overall collection of information flowing to the Terrorism and Early Warning Center and the Joint Regional Intelligence Center (JRIC).[71] The JRIC then is able to concentrate on tips, leads and indicators of threat information and run them against trend analysis programs to conduct prevention activities.[72]

While the trained police officer continues to be a vital part of domestic intelligence in the war on terror, the requirement to collect information places the burden on the individual police officer to recognize the abnormal behavior and report it to the appropriate entity. This technique also is dependent on training and the availability of appropriate and convenient reporting channels. If COP is to be leveraged for domestic collection, police reports and communications need to be leveraged with analytical technology.

Information garnered by a community based police officer needs to be recorded and uploaded to local databases regardless of the officer's training or expertise. Raw data transmitted to the fusion network can be accessed by trained analysts using state of the art analytical technology to link information across jurisdictional and state lines. This information could prove to be the key piece of information needed to prevent a terrorism attack. There is always a risk that a piece of information which may have seemed insignificant or not worth reporting to anyone outside the department might be discarded. By compiling all information and using technology to sift through it, collection is

[71] Interview of Robert V. Fox, Lieutenant, LAPD JRIC by the author on May 7, 2007, Destin, Florida.

[72] Ibid.

maximized and analytical products are expanded. The analytical product, therefore, becomes significantly greater then the sum of what might appear to be seemingly insignificant parts.

Relying on self reporting by police officers affects many police units. When officers do not have the time or inclination to recognize trends, anomalies or indicators outside their specific bailiwick, this is termed the "bloodhound" effect.[73] Police officers, like bloodhounds, can be so focused on their specific duties, that they seem oblivious to other concerns. While this may appear as a negative attribute of the officer, focus and concentration are often the difference between a good investigator and a great one. It also may be the difference between life and death when focusing on staying alive and protecting oneself is tantamount. Attention to detail is, therefore, necessary in police work if we desire complicated investigations and safe investigators. The bloodhound effect also may explain why less potential terrorism reporting occurs. The officers in question may have focused on following leads relevant to a particular investigation and consciously or subconsciously avoided other distractions. A collection system that relies on individuals from varied disciplines to self-report information may unnecessarily limit itself to only the most egregious or obvious terrorism information.

3. Knowledge Management in Policing

Another rapidly growing trend in policing is the recognition that an agency must know what it knows. Law enforcement departments recognize that as a result of COP and ILP, they are becoming accumulators of vast amounts of data which they are unable to process quickly and efficiently. Knowledge management is the management of the department's intellectual assets held by its employees, databases, corporate history, and expertise.[74] Knowledge management in policing recognizes that police culture

[73]Phillip Leggiere, "The Fusion Revolution," *Homeland Security Today*, April 2007, 26. Available Online: http://www.fas.org/irp/agency/ise/guidelines.pdf (accessed June 6, 2007).

[74] T. Dave Chavez Jr., "Knowledge Management in Policing," *Department of Justice, Community Oriented Policing Services*, October 25, 2005, 3. Available Online: http://www.cops.usdoj.gov/mime/open.pdf?Item=1615 (accessed June 6, 2007).

emphasizes individual knowledge collection as experience and expertise.[75] Knowledge management therefore can be the untapped reservoir of information within police departments. This reservoir could represent the intelligence base of the department and the vital clues needed to unravel the next plot. Leveraging that reservoir requires tapping into the knowledge base of the individuals and managing that information in an efficient and effective manner. The study of knowledge management is uniquely suited to the challenge of focusing this reservoir toward fusion centers in an effort to leverage the collection information.

To assist in retrieving information, software designers have created programs to manage information and catalog it for retrieval. Technology solutions, however, presuppose the existence of information technology systems and automation. This continues to be an issue for smaller police departments and is a reoccurring theme throughout this paper. While the majority of departments embraced COP as a practical way to connect with the public they serve, resource and funding limitations have stymied smaller departments from taking advantage of ILP and the ensuing dilemma of knowledge management. Insomuch as this situation effects up to 91% of the law enforcement departments with officers numbering fewer then 50, the lack of ILP and knowledge management will have a significant effect on the overall amount of collection data reaching the fusion centers.

To tap into the reservoir of intelligence locked up in these police departments across the country, officials must create avenues for them to connect to the fusion centers. Many of these departments have dated technology systems from the 1980s and 1990s which limit their ability to access their own intelligence base. Some of the departments require policy and procedural changes to increase record keeping and documentation. Still others simply need resources to advance police operations into intelligence operations and analytical record keeping.

To increase connectivity and standardization, the Department of Justice established the Information Systems Technology Enhancement Project (ISTEP) to assist

[75] Chavez, "Knowledge Management in Policing," 5.

departments with knowledge management. ISTEP suggests three areas of guidance: 1) reconsider the domain of police related information; 2) collect new types of data; and 3) limit analysis to data that is timely and relevant.[76] Without standardization of data and digitization of information, smaller departments will be left out in the cold when it comes to data fusion.

[76] Department of Justice, Office of Community Oriented Policing Services, *Police Department, Information Systems Technology Enhancement Project, 17.* Available Online: http://www.cops.usdoj.gov/files/ric/Publications/e09990004_small.pdf (accessed September 3, 2007).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE FUTURE OF DOMESTIC INTELLIGENCE

A. FUSION CENTERS

There is evidence of a fledgling national intelligence fusion process. At least forty two of the fifty states have created state fusion centers.[77] The concept of information fusion has emerged as the fundamental process to facilitate the information sharing between federal, state and local entities.[78] These centers are attempting to link and exploit information gathered by state and local organizations.

The Department of Justice has defined fusion centers as an "effective and efficient mechanism to exchange information and intelligence."[79] Phillip Leggiere describes fusion centers as "a way to enable law enforcement, public safety, emergency management, and other partners to mutually aggregate, analyze, and disseminate criminal and terrorist related information."[80]

The goal of fusion centers, according to Leggiere, is to "provide a mechanism through which government law enforcement, public safety, and the private sector can come together with a common purpose and improve the ability to safeguard our homeland."[81] Fusion centers are expected to allow federal, state and local entities to better prevent acts of terrorism and provide necessary data for the preparation of natural disasters.[82] Fusion is envisioned as a collaborative process of combining data and

---

[77] Eben Kaplan, "Fusion Centers," *Council on Foreign Relations,* February 22, 2007, 1.

[78] Department of Homeland Security, Homeland Security Advisory Council, *Intelligence Information Sharing Initiative: Homeland Security Intelligence & Information Fusion,* April 28, 2005, 2.

[79] Department of Justice, Bureau of Justice Affairs, *Fusion Center Guidelines*, 3. Available Online: http://www.fas.org/irp/agency/ise/guidelines.pdf (accessed August 19, 2007).

[80] Phillip Leggiere, *The Fusion Revolution,* 28.

[81] Ibid., 4.

[82] Ibid., 11.

expertise from homeland security, public safety, private sector, law enforcement, critical infrastructure and intelligence entities.[83] Information from these entities improves the situational awareness picture.

Fusion centers work by inputting data sets from a broad spectrum of information encompassing the varied disciplines described above.[84] The idea, according to Eben Kaplan of the Council on Foreign Relations is that "the next time a would-be terrorist on a government watch list is pulled over for speeding, the officer at the scene will have the information he needs."[85]

[83] Leggiere, *The Fusion Revolution*, 13.

[84] Eben Kaplan, "Fusion Centers," 2.

[85] Ibid.

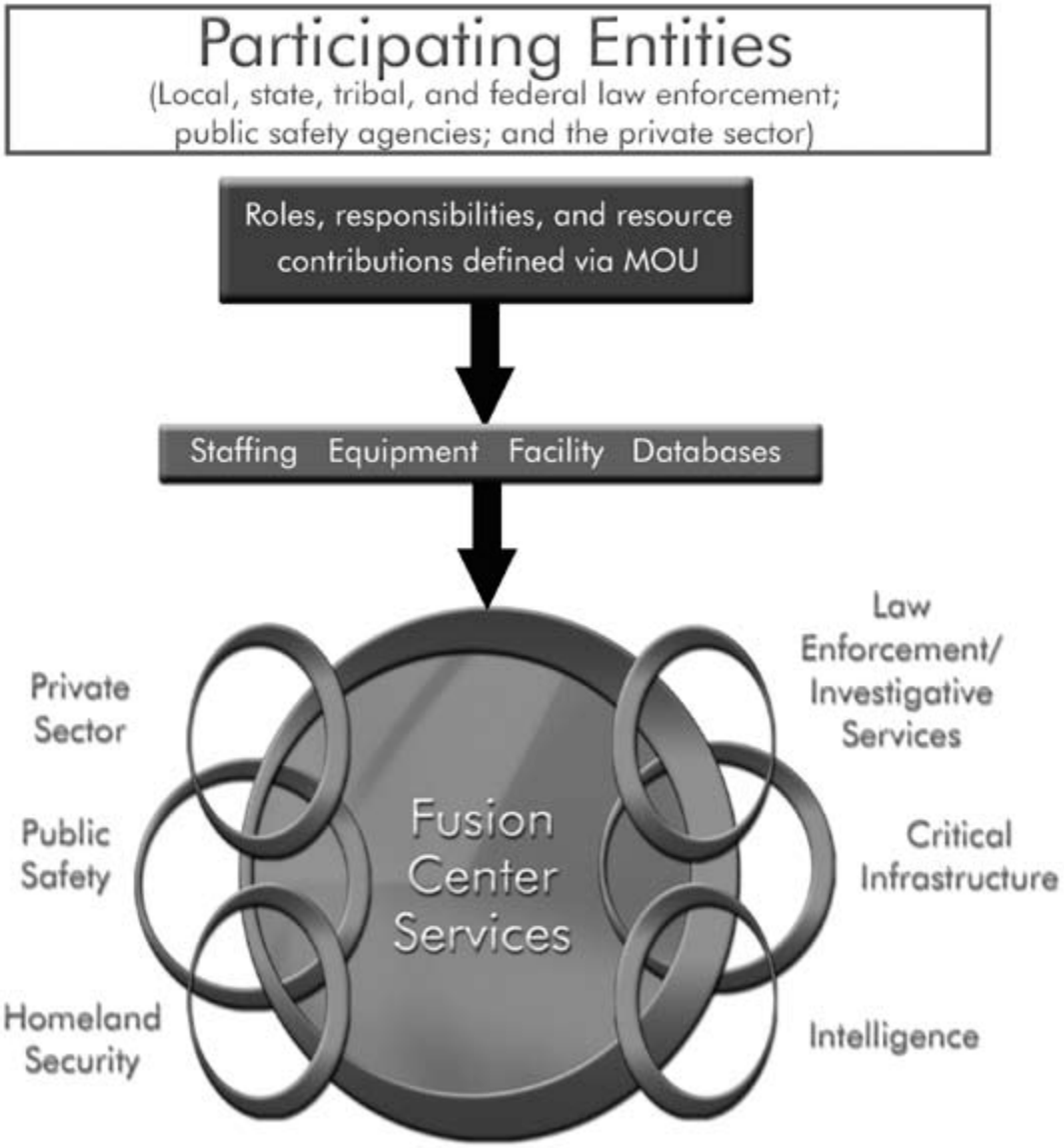


Figure 4. Fusion Center participant interaction diagram.

Fusion centers could be the key conduit or critical node for sharing federal information to the local level.[86] Charlie Allen, Chief Intelligence Officer for DHS describes fusion centers as a "co-equal network, not just computers and wires, but a rapid analytic movement."[87] Eventually, DHS envisions a "network of networks" that would function as a virtual national fusion center. A virtual fusion center, linking the country's fusion centers through technology and standardization.[88] This virtual fusion center, network of networks, will be able to push and pull information between federal, state and local players.[89] DHS has devoted over $380 million dollars to the project and expects to place intelligence officers and analysts in every fusion center to assist in the process.[90] Hoping to foster up to 70 fusion centers across the United States, DHS envisions every major urban and metropolitan area, including every state, to be represented.[91] The concept is for each individual fusion center to serve the community it represents by addressing the needs and requirements unique to that community. To qualify for grants however, the fusion centers must conform to certain requirements designed to achieve connectivity and networking capabilities.[92]

While most parties agree that much has been achieved at the federal, state and local level with respect to fusion centers, Ambassador Thomas McNamara, Program Manager, Information Sharing Environment (ISE), Office of the Director of National Intelligence, concludes that although much has been accomplished, much has to be done.

---

[86] Kaplan, "Fusion Centers," 2.

[87] Statement of Assistant Secretary Charles E. Allen, National Fusion Center Conference, Destin Florida, March, 6, 2007.

[88] Statement of Secretary Michael Chertoff, National Fusion Center Conference, Destin Florida, March 6, 2007.

[89] Ibid.

[90] Ibid.

[91] Interview of Deputy Assistant Secretary Jack Tomarchio by the author, Destin, Florida, March 6, 2007.

[92] *Fusion Center Guidelines*, 3.

According to McNamara, "We have in 5 years reached the end of the beginning."[93] Obstacles remain a constant reminder of the challenge ahead. For instance, in spite of the significant investment by DHS and state and local entities, funding continues to be a problem. Capital investments by DHS does not guarantee maintenance and daily expenses will be sustained by cash strapped state and local governments. Training also is an issue. Most fusion centers are technology intensive, requiring highly trained personnel.[94] Information sharing efforts also suffer from constant turf wars amongst the agencies. These battles hamper the collaborative environment and stymies analytical work product.[95] Also, analytical cadres require advanced education and years of experience to become subject matter experts. Expert analysts take years to mature. Expanding national analytical resources will take many years. According to Ambassador McNamara, fusion centers are also not envisioned as part of the intelligence community.[96] This could prove to be confusing, since fusion center information is vital to the domestic intelligence analysis used in a national domestic intelligence estimate. If the fusion centers are to be rapid analytic centers capable of information sharing greater then that of the computers and wires as DHS envisions, federal, state and local entities will have to overcome these obstacles.

B. STATE AND LOCAL HUMINT IN FUSION CENTERS

While the role of the federal government in providing funding, creating guidelines and national strategies is clear, the role of state and local partners in the fusion center process is less defined. Comments from state and local experts provided to the Lessons Learned Information Sharing project sponsored by DHS showed that there was a perception by state and locals that they were receiving information from the federal

---

[93] Statement of Ambassador Thomas McNamara, Program Manager, ISE, ODNI, National Fusion Center Conference, Destin, Florida, March 6, 2007. Available Online: http://www.ise.gov/docs/Amb%20McNamara%20Remarks%20at%20Fusion%20Conference.pdf (accessed August 23, 2007).

[94] *The Fusion Revolution*, 32.

[95] Ibid.

[96] Statement of Ambassador Thomas McNamara, 6.

government without being asked for information in return.[97] Also, the survey showed that in the absence of clear guidance from the federal government, state and locals were developing their own networks to share information among themselves.[98] The report concluded that DHS should "focus on leveraging existing programs and seek to integrate those programs into a cohesive, national information and intelligence sharing architecture."[99]

Since reports have concluded that state and local information is vital to predicting future attacks, fusion centers lacking this type of information is a threat to national security. State and local information provide the indicators needed for tactical warning currently unavailable to national intelligence assessments. The "push and pull" effect described by Secretary Chertoff at the moment seems to be more push and less pull. This is further supported by the report issued by the International Chiefs of Police in 2005. The Chiefs concluded that the federal Government had not coordinated its information sharing policies with state and local officials.[100] The now famous quote that "All terrorism is local" was born of this report.[101] The need for fusion center information to contain more state and local data is obvious and yet both data and anecdotal information suggests adequate state and local information is not reaching the fusion centers.

One possible explanation for the lack of critical law enforcement collection information in fusion centers is that most law enforcement is comprised of small departments which are not fully computerized. In 2000, there were 17,784 departments, including 12,666 police departments and 3,070 sheriff's departments.[102] According to the Department of Justice, Bureau of Justice Assistance, 75% of the state and local law

---

[97] Department of Homeland Security, *Lessons Learned information Sharing, LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process*, December 2005, 5. Available Online: http://www.dhs.gov/xlibrary/assets/Final_LLIS_Intel_Reqs_Report_Dec05.pdf , (accessed August 19, 2007).

[98] Department of Homeland Security, *Lessons Learned information Sharing*, 2.

[99] Ibid., 3.

[100] IACP, From Hometown Security to Homeland Security, 2.

[101] Ibid., 3.

[102] Department of Justice, Bureau of Justice Statistics, *Law Enforcement Statistics, Summary Findings, BJS Homepage*, 1. Available Online: http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed May 14, 2007).

enforcement departments had fewer then 24 officers.[103] In 1994, 91% of departments employed fewer then 50 sworn police officers.[104] Most local police departments, therefore, are small: 50% employ fewer then 10 commissioned officers.[105] Since small departments are plagued by funding limitations which prevent wide usage of computer systems, automation and intelligence specialization, it is logical to assume most of these smaller departments are isolated from the urban, technology driven fusion centers.[106]

Much of the information needed by fusion centers, specifically the community oriented policing information from small town America, is housed in these small departments that do not have technological access to fusion centers. Unfortunately, informant tips, field investigation reports, lead and community liaison information is trapped in paper-driven, informal law enforcement networks throughout small town and rural America. Information from these departments must be relayed by traditional methods such as direct telephone contact, law enforcement liaison activities or intra-department threat assessment and survey channels. Absent specific analytical systems and processes, the majority of law enforcement collection data is stove piped within the departments themselves.

Interviews of law enforcement executives representing 27 small, medium and large agencies revealed varied collection and intelligence dissemination programs throughout the United States. [107] For example, data suggests that large law enforcement departments, defined as those comprised of 1000 officers or more, have adopted community oriented policing programs, have moved to intelligence led policing

---

[103] Department of Justice, Bureau of Justice Assistance, *The National Criminal Intelligence Sharing Plan*, October 2003, 1. Available Online: http://www.fas.org/irp/agency/doj/ncisp.pdf (accessed August 19, 2007).

[104] Ralph A. Weisheit, et al., "Rural Crime and Rural Policing," *National Institute of Justice*, September 1994, 8. Available Online: http://www.ncjrs.gov/pdffiles/rcrp.pdf (accessed August 19, 2007).

[105] Ibid.

[106] *The National Criminal Intelligence Sharing Plan*, 1.

[107] Information is based upon the author's interviews of law enforcement executives from representative samples of large, medium and small departments from throughout the United States. The author conducted interviews of chiefs, sheriffs, and agency representatives from 27 departments during the period November 2006–June 2007. Interviews sought to identify each department's level of human intelligence gathering process including analytical and data sophistication.

strategies, have created intelligence units to support the strategies and may engage in criminal intelligence gathering activities as permitted by their respective state and local laws.

Medium-sized departments, defined as those comprised of more then 100 sworn officers, but less then 1,000, have adopted community oriented policing programs, but are struggling with intelligence led policing because they do not for the most part have the resources for intelligence units and analytical cadres. Medium-sized departments rarely conduct intelligence operations outside of support of special events in their area.

Small to medium departments, defined as having less then 100 sworn officers, have or are in the process of adopting community oriented policing programs, but have little or no intelligence function whatsoever and are dependent on their colleagues for intelligence.

Smaller departments, defined as those with 24 sworn officers or less, may use community oriented policing programs, have little or no digitized intelligence information outside of simple report writing and criminal record information, and rely almost exclusively on other departments for intelligence and analytical products.

The above analysis suggests that a significant amount of information is stove piped among medium and small police departments that may contribute to the overall intelligence and analytical picture needed to thwart the next major terrorist attack. The information is trapped in department records, unit reports, paper reporting systems, individual officer records, and the officers themselves. Releasing this information will require organizational, cultural, technological and budgetary solutions.

For this reason, the Department of Justice's Intelligence Sharing Plan recommends all departments automate incident based record keeping, join regional information systems such as the FBI Law Enforcement Online and utilize the latest version of the Global Justice Extensive Markup Language Data Model. In this way, small departments can digitize their information in the most modern data standard, capable of interoperability with other participating agencies, and thereby connect to the

fusion network of networks. Although DOJ has invested significant funds to create the XML format and provide software, funding is not yet available for hardware at the local level.

The International Association of Chiefs of Police (IACP) recognizes the challenges of smaller departments. The IACP has teamed up with the Department of Justice's Bureau of Justice Assistance to create the Smaller Police Department Technical Assistance Program (SPTAP). The SPTAP provides services, support and training to smaller police departments. The SPTAP also publishes Best Practices Guides to assist the Chiefs of smaller departments. In spite of these efforts, funding and resource shortfalls continues to hamper intelligence gathering and sharing at the smaller department level.

C. THE XML REVOLUTION

The Global Justice Extensible Markup Language (XML) Standard is a computer language designed to encode each item of the language with the meaning of the item itself. The markup language is a mechanism that allows the object to be coded with a tag that identifies the meaning of the object to the computer thereby providing "smart" capabilities.[108] These capabilities provide extensive options including search, relational and content specific programming. The XML standard is sanctioned by World Wide Web consortiums and compatible with Internet protocols.[109] The Global Justice XML Data Model (GJXDM) was designed for law enforcement and public safety professionals to share information using a common data language, and thereby remove the burden from each individual agency of creating or adopting standards.

There are three primary components of GJXDM including the Data Dictionary, Data model and Component Reuse Repository.[110] The Data Dictionary contains language definitions which standardize their use in the schema. The Data Model organizes data

---

[108] Department of Justice, Bureau of Justice Affairs, *DOJGJ website*. Available Online: http://www.it.ojp.gov/topic.jsp?topic_id=43 (accessed August 19, 2007).

[109] Ibid.

[110] Ibid.

schema for use by multiple agencies. And, the Component Reuse Repository database houses the data to be accessed by all authorized users.[111] These tools eliminate the need for agencies to create interfaces for data sharing. It is the vocabulary for law enforcement to communicate with each other technologically. According to the Department of Justice, the ensuing database is designed to "arm everyone across the justice and public safety communities with the most accurate and up-to-date data to make the very best decisions."[112]

Combining XML technology with the Department of Justice's Global Justice XML Data Model gives law enforcement a common language standard and system for communicating effectively. The XML technology facilitates metadata acquisition and relational analysis necessary for sophisticated intelligence products. The Data Model protocol advances the technology and makes it accessible to smaller departments which lack the resources to create and finance expensive analytical software technology. Used in tandem, the law enforcement community has a software standard for communicating together and linking criminal justice information.

While the XML and GJXDM provide the "rules of the road" for collaboration communication, they are not the road itself. Data platforms have been created to provide users with portals that serve as "ramps" to get on and off the intelligence information super-highway. These platforms include the FBI's National Data Exchange, DHS's Homeland Security Information Network (HSIN), Regional Information Sharing System (RISS) and others.

---

[111] *DOJ* Department of Justice, Bureau of Justice Affairs, *DOJGJ website*.

[112] Ibid.

1. National Data Exchange

According to the FBI, The National Data Exchange (NDEx) is tasked with "providing local, state, tribal and federal law enforcement with a system to collect, process, and disseminate criminal and investigative data to be used for law enforcement sharing."[113]

To accomplish this mission, the FBI is developing a system that will collect and process crime data in support of investigations, crime analyses, law enforcement administration, strategic and tactical operations, and national security responsibilities. An important feature of the project is that NDEx will be built on existing FBI run infrastructure supporting the National Crime Information Center and the Law Enforcement Online (LEO) programs already functioning successfully and widely accepted by law enforcement.[114]

The goals of the NDEx program are to "design and implement an information sharing system, enhance partnerships, provide increased access to information, provide a one-stop-shopping capability for law enforcement information sharing, provide access to more sophisticated tools to a wide spectrum of law enforcement, become a predictive crime modeling tool, provide link analysis capabilities, and transcend local, state, tribal and federal jurisdictions." [115]

NDEx's little brother and regional component, RDEx, has been piloted in four areas including Seattle, St Louis, Jacksonville, and Washington, D.C. The RDEx system deploys several technologies to the federal, state, local and tribal agencies participating in the network. RDEx includes the ability to search full text, unstructured criminal data (Google type searches), link analysis tools, and geospatial mapping functionality. According to GovExec.com, "Information on the system includes the identities of

---

113 Federal Bureau of Investigation, *Federal Bureau of Investigation, NDEx Program Overview* (Criminal Justice Information Services publication), 1. Available Online: http://www.fbi.gov/hq/cjisd/ndex/ndex_overview.htm (accessed October 8, 2006).

114 Department of Justice, *EGovernment Act Implementation Update* (Budget Data Request 05-08), 2004, 2. Available Online: http://www.usdoj.gov/jmd/ocio/egovactreport2004.pdf (accessed October 8, 2006).

115 Federal Bureau of Investigation, *NDEx overview*, 1.

vehicles and weapons, addresses and phone numbers. The program allows cases to be plotted on maps so geographical patterns can be identified."[116]

The outcome of NDEx is still in question. The program is a multiyear phased project in three installments. The first phase involved modeling and prototypes which could be tested and evaluated. That phase was completed in 2005. Phase 2 is a 28 month incremental phase which involves feedback and pilot implementation. The program is in the midst of Phase 2. Phase Three is designed to provide additional capabilities and scope to the program. Phase Three hopes to expand the program into new and yet to be determined aspects of law enforcement sharing. The program platform is designed to accept additional aspects and capabilities. Phase Three is scheduled to be completed in the 2008–2009 time frames.

The NDEx program, including Phase Three, has plans for developing a systems approach to the operation, and maintenance of several interconnected IT and supporting applications. The program, as envisioned, will also be a "fusion point for the correlation of nationally-based criminal justice information with certain national security data."[117]

To assess the effectiveness and expansion potential for the program, the following criteria were analyzed.

a. Scalability

To promote a national program capable of interconnecting tens of thousands of law enforcement agencies, NDEx will have to incorporate scalability to its expansion plans. In this regard, the project relies on two important features. First, the system is built upon the CJIS infrastructure which is the largest crime database network

---

[116] Daniel Pulliam, *FBI Launches Regional Data Sharing System*. Available Online: http://www.govexec.com/dailyfed/0605/062805p1.htm (accessed October 8, 2006).

[117] Statement of Willie T. Hulon, Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, before the, House Government Reform Subcommittee on, Technology, Information Policy, Intergovernmental Relations and the Census, *"Facilitating an Enhanced Information Sharing Network That Links Law Enforcement and Homeland Security for federal, state and Local Governments*, July 13, 2004, 10. Available Online: http://reform.house.gov/UploadedFiles/Hulon%20Testimony.pdf (accessed October 8, 2006).

system in the world.[118] The CJIS platform already supports the National Crime Information Center (NCIC), Uniform Crime Reporting (UCR), and Integrated Automated Fingerprint Identification System (IAFIS) fingerprint identification systems used by the majority of law enforcement nationwide.[119] Second, the system is designed to accept expansion including local systems, regional systems such as Law enforcement Information Exchange (LiNX), and LEO. Phase Three envisions specific additions of components and IT systems. The infrastructure has been designed to accept modular expansion and therefore scores high on scalability.

b. Interoperability

As a result of several drivers after the events of September 11, 2001, including Presidential Executive Orders, Congressional legislation, FBI initiatives and post 9/11 recommendations, the Department of Justice created the Law Enforcement Information Sharing Program (LEISP).[120] The key strategy of the LEISP was to promote uniformity and accessibility through a "One DOJ" policy of standardized IT information sharing network.[121] The system provides law enforcement with one entry point via the LEISP Exchange Specification (LEXS).[122]

As a result of this network interface, law enforcement has ease of access and interoperability via internet connectivity. Using various portals such as LEO or RISS, law enforcement can access the RDEx network of shared data including text searches, link analysis and geospatial analysis.[123]

---

[118] EGovernement Act Implementation Update, 3.

[119] Ibid.

[120] Federal Bureau of Investigation, NDEx Power Point Presentation (Washington, DC: March, 2007), 1.

[121] Ibid., 2.

[122] Ibid., 5.

[123] Ibid., 5.

c. Open vs. Proprietary Technology

Another benefit of the LEISP is the use of open standards such as XML, Web Services and NIEM schema (version 0.3). These open standards allow any law enforcement system to participate in the RDEx portion of the information sharing environment. This has resulted in a common language for sharing information among differing computer systems, such as the Global Justice XML Data Dictionary described above. This standard was developed with information sharing in mind, in collaboration with state and local law enforcement and participation from the IT industry.[124]

d. Variables

Variables include the costs, governance issues, the technology itself and perhaps more importantly, the acceptance by the law enforcement community. Because the system relies on voluntary participation by law enforcement to upload their proprietary reports and access the system, the program's success relies on the degree to which it is accepted.

To contend with these issues associated with data collections, the FBI turned to the leading law enforcement partnerships for guidance in developing governance and acceptance conventions. These organizations include: International Association of Chiefs of Police, the National Sheriffs Association, the Major Cities Chiefs Association, and the Major County Sheriff's Association. A joint Position Statement dated August 15, 2005, was released by these organizations, which set forth three requirements for success:

Development of a Statement of Requirements designed with local law enforcement input and utilization in mind. It recommends that the requirements should be validated through representatives of their associations and coordinated by the FBI CJIS Advisory Board (APB)

[124] EGovernment Implementation Update, 4.

After an agreed upon Statement of Requirements is completed, a Funding Projections document that reflects the costs for each phase of the project to the agencies needs to be prepared

Based upon the Statement of Requirements and Funding Projections, the FBI and the Department of Justice will need to formalize a process that will result in a consistent message about the Project's mission, goals, strategy, and status.[125]

The CJIS Division of the FBI is responsible for the NDEx/RDEx program. CJIS, along with the CJIS Advisory Board, have committed to working with the joint advisory law enforcement panels and are implementing their recommendations. Representatives from CJIS are currently conducting presentations to state and local law enforcement entities throughout the United States in an effort to educate the community and obtain feedback. Consequently, there is an effort underway to provide a consistent message about NDEx's mission, goals, strategy and status.

The NDEx/RDEx project was born out of the intelligence chaos of 9/11. The project was designed specifically as a national law enforcement sharing mechanism. To benefit from consistent feedback and modification, it was designed as a multi-phased, long term project. The project is enhanced by intentional scalability and open standards, with off-the-shelf software such as link analysis and iMap features. The project is vulnerable, in that it is completely susceptible to variables which affect law enforcement acceptance of the program. Lack of acceptance by the state and local law enforcement community would render the system useless. Additional obstacles include funding for connectivity and user equipment costs and governance issues. To overcome these issues, the FBI is promoting the project, created advisory panels to assist with user issues regarding costs and governance and initiated pilot projects in various parts of the country to establish a successful track record. While the potential for the program is significant, the ambitious scale and goals of the project remain as yet unfulfilled.

[125] Neil Kurlander, "Out of Step," *XML Journal*, January 25, 2006, 2. Available Online: http://xml.sys-con.com/read/175403.htm (accessed August 19, 2007).

2. Homeland Security Information Network

The Homeland Security Information Network (HSIN) is a computer based system platform designed to increase information sharing between federal, state, local and tribal entities. The HSIN systems link state and urban areas with DHS intelligence systems. The network helps provide situational awareness, collaboration, analytical capabilities and real time information sharing.[126] HSIN is used by DHS' Office of Intelligence and Analysis to post intelligence related products.[127] DHS has created several sub systems including HSIN-Intel designed to share unclassified intelligence to consumers already using the HSIN network.[128] The HSIN-S, a secret network, provided a classified avenue for network sharing. The HSIN-S eventually transitioned into the Homeland Security Data Network (HSDN) providing additional classified capabilities and modeled after the military Secret Internet Protocol Network.[129]

In February 2004, Groove Networks announced they had partnered with DHS to use Groove Networks Collaboration Technology to power the HSIN network.[130] Groove Networks, a leading office software producer, is best known for their collaboration software which facilitates multiple users in a virtual work environment. At the time, then Secretary Ridge predicted that the HSIN/Groove system would allow ever increasing expansion of federal, state and urban area information sharing through sophisticated technology.[131]

---

[126] Department of Homeland Security, "Homeland Security Information Network Webpage," https://www.dhs.gov/xinfoshare/programs/gc1156888108137.shtm (accessed May 29, 2007).

[127] U.S. House of Representatives, Committee on Homeland security, Subcommittee on Intelligence Sharing, and Terrorism Risk Assessment, Statement *of Charlie Allen, The Homeland Security Information Network: An Update on DHS Information Sharing Efforts*, September 13, 2006, 4. Available Online: http://www.hlswatch.com/category/events/ (accessed August 19, 2007).

[128] *Statement of Charlie Allen, The Homeland Security information Network*, 5.

[129] Ibid., 7.

[130] Groove Network, "Groove software is core component of HSIN; Demo at Homeland Security Conference Today" (Beverly, Mass., February 26, 2004). Available Online: http://www.groove.net/release.cfm?pagename=press_feb26_2004 (accessed August 19, 2007).

[131] Ibid.

In June 2006, the DHS Inspector general released a report critical of the implementation of HSIN.[132] The report concluded DHS had failed to take into account several important steps in the effective planning and implementation of HSIN.[133] The report recommended communication with HSIN users to clarify mission and vision; provide clear guidance regarding data flow; standard operating instructions; obtain system requirements from users and create performance metrics for the system. [134]

Similarly, in May 2007, The Government Accounting Office (GAO) also criticized DHS for not coordinating the design and implementation of HSIN with already existing platforms such as Regional Information Sharing System (RISS).[135] The GAO report concluded a major factor in HSIN's flaws was the Department's rush to get the system operational. As a result, the report concluded DHS runs the risk of duplicating or interfering with effective existing information sharing systems.[136]

Since the reports, several entities have criticized HSIN and other platforms such as the RISS and the FBI's Law Enforcement Online (LEO) for targeting the same state and local audience thus creating confusion through duplication.137 The threat is that individual departments are sharing information with various uncoordinated systems with the mistaken belief that the information is being aggregated. Ironically, the initial impetus for the creation of the system was to eliminate stovepipes in departmental databases. In the rush to stand up systems as quickly as possible, competing systems such as HSIN, RISS and LEO are creating the stovepipes they endeavored to eradicate.

---

[132] Department of Homeland Security, Office of the Inspector General, *Homeland Security Information Network Could Support Information Sha*ring More Effectively, Office of Information Technology OIG-06-38, June 2006. Available online: http://www.washingtonpost.com/wp-srv/nation/documents/OIG_06-38_Jun06.pdf (accessed August 19, 2007).

[133] Ibid., 3.

[134] Ibid., 4.

[135] Government Accounting Office, Statement of David A. Powner, Director Information Technology Management Issues, *Homeland Security Information Network Needs to Be Better Coordinated with Key state and Local Initiatives*. Available Online: www.gao.gov/cgi-bin/getrpt?GAO-07-822T (accessed May 29, 2007).

[136] Ibid.

[137] Jim Kouri, "Homeland Security Information Network Needs to be Better Coordinated." *Canada Free Press*, May 16, 2007, 2. Available Online: http://www.canadafreepress.com/printpage.php (accessed June 3, 2007).

DHS contends that by "increasing program management, making greater use of existing systems to avoid duplication and providing more usable content, the department can fix the problem."[138]

3. Regional Information Sharing System Program

The Regional Information Sharing System (RISS) Program was created in 1974 to support state and local law enforcement intelligence needs through an initial grant from the U.S. Department of Justice.[139] The program has expanded over the years to include six regional intelligence centers which provide a variety of intelligence functions. The backbone of the program is RISS.net, a secure web-based network accessible to members through telephone or internet.[140] RISS.net provides users with a network for communicating law enforcement information across jurisdictional lines. Riss.net offers resources such as the RISS bulletin board, databases, RISS center web pages, RISS search engine, and other center resources. RISS also provides analytical services including telephone, financial and data analysis in the form of analytical products to its members via the RISS.net.[141] Other services offered by RISS include investigative support, specialized equipment loans, covert purchase funding, technical assistance and training.[142] RISS centers are located in Newtown, Pennsylvania, Springfield Missouri, Franklin, Massachusetts, Nashville, Tennessee, Phoenix, Arizona and Sacramento, California.[143] Typical targets of RISS members are terrorism, drug trafficking, violent crimes, and organized crime.[144]

---

[138] Mary Mosquera, "DHS vows to fix information network," *FCW.COM*, May 28, 2007, 1. Available Online: http://www.fcw.com/article102798-05-28-07-PrintandprintLayout (accessed, June 3, 2007).

[139] Department of Justice, Bureau of Justice Assistance, *Program Brief: Regional Information Sharing Systems Program*, April 2002, 2. Available Online: http://www.ojp.usdoj.gov/BJA accessed 6/9/07 (accessed June 3, 2007).

[140] Department of Justice, Bureau of Justice Assistance, *Program Brief: Regional Information Sharing Systems Program*, 3.

[141] Ibid, 3.

[142] Ibid, 3.

[143] Ibid., 4.

[144] Department of Justice, Regional Information Sharing System, *RISS Overview*. Available Online: http://www.rissinfo.com/overview.htm (accessed June 9, 2007).

Since the initiation of RISS, membership has grown to almost 7,100 law enforcement agencies spanning the entire United States.[145] Recently, in 2002, RISS added the Automated Trusted Information Exchange Network (ATIX) designed to link agencies and other data platforms. RISS-ATIX is offered as a platform to connect fusion centers to the RISS network. Also, the FBI's LEO network was recently linked to the RISS network further expanding the program.[146]

Speaking before the House of Representatives, Captain William Harris of the Delaware State Police stated that the "system (RISS) is both robust and user friendly, and contains more relevant, reliable, and timely law enforcement and homeland security information that is actionable for the line level law enforcement personnel."[147] Harris criticized the bureaucracy of multiple systems as confusing and inefficient for law enforcement. RISS has the benefits of long time credibility with law enforcement, far reach through its extensive network and extensive capabilities and varied products. Detractors of the RISS network argue that it is law enforcement centric. RISS-ATIX, however, has been able to link the RISS network with non-law enforcement systems giving the RISS program more information depth and reach into the community.

D. DATA WAREHOUSES-LAW ENFORCEMENT INFORMATION EXCHANGE

The Law Enforcement Information Exchange (LInX) system is an example of a regional data warehouse that unites several separate law enforcement data sets using common communication standards. The original contract was awarded to Northrop Grumman Corporation in 2004 and built upon an early FBI and St. Louis law enforcement model of data sharing.[148]LInX is a series of data warehouses obtained from

---

[145] Department of Justice, Regional Information Sharing System, *RISS Overview*, 2.

[146] William Harris, "Homeland Security Information Network: Moving Past the Missteps Toward Better Information Sharing," May 10, 2007, 2. Available Online: http://homeland.house.gov/SiteDocuments/20070510132121-04354.pdf (accessed June 9, 2007).

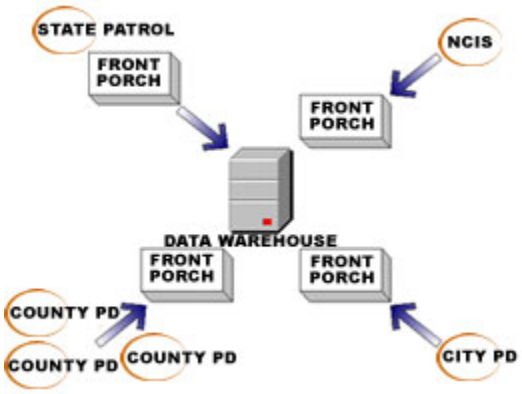
[147] Ibid., 2.

[148]Naval Criminal Investigative Service, Law Enforcement Information Exchange, *About LInX*, 1. Available Online: http://www.ncis.navy.mil/linx/about_linx.html (accessed June 2, 2007).

participating law enforcement agencies providing unprecedented access by agency users. LInX has been implemented in five regions including Florida/Georgia, Hawaii, Texas, Virginia and Washington.[149]

The data sent to the LInX warehouse is comprised of incident reports, case records, computer aided dispatch events, citations, mug shots, pawn data, and free text investigative notes.[150] The information provided by participating agencies is processed and normalized. The information is then ready for retrieval by authorized users. In the case of the FBI, the RDEx platform described above is used to transmit FBI data from FBI servers to the LInX warehouse. The warehouse provides federal, state and local investigators with fingertip access to each others investigative information heretofore unavailable in any one location.

The LInX data warehouse is comprised of data sets from various levels of law enforcement.



[151]

Figure 5. Law Enforcement Information Exchange Data Warehouse.

[149] *About LInX*.

[150] Naval Criminal Investigative Service, Law Enforcement Information Exchange, Technical Overview, 1. Available Online: http://www.ncis.navy.mil/linx/technical.html (accessed June 2, 2007).

[151] Naval Criminal Investigative Service, Law Enforcement Information Exchange, *About LInX*, Technical Data (diagram.). Available Online: http://www.ncis.navy.mil/linx/about_linx.html (accessed June 2, 2007).

The data warehouse becomes a tool for breaking down barriers and creating trust. Information housed in individual department record stores is difficult to access through informal networks. By storing information in common data warehouses, individual officers can access stove piped information previously inaccessible. Successes associated with the system help break down walls of mistrust and encourage collaborative activity. Cases which have utilized the system create investigative connections and leads that would have been impossible without the collaborative power of the system.[152]

The above described information sharing systems are just a few of the platforms and warehouses available to law enforcement and the public safety community. Each system offers users specific capabilities. In each case, the stated goal of the platform is the broad exchange of information. Users report, however, that competing systems hamper information sharing and obstruct the very premise of the system. Standards, such as the Global Justice XML Standard, emphasize the necessity to create technologies which communicate with each other and avoid duplication of effort. Governance and coordination bodies such as the Information Sharing Environment (ISE) Working Group are necessary to ensure that platforms created to maximize sharing conform to existing strategies and protocols. Without governing bodies, departments risk implementing costly systems which may hamper instead of expand information sharing.

E. CASE STUDY: FUSION CENTER PROCESS IN NORTH FLORIDA

Recently, individuals from various law enforcement and intelligence agencies met and formed an intelligence exploratory committee to study the fusion process in North Florida. During the spring of 2007, intelligence practitioners from federal, state and local departments studied the intelligence flow and sharing process between the agencies. As a result, the exploratory committee created a document outlining a proposed future information and intelligence system in anticipation of a formal regional strategy.[153] The

[152] Alan Joch, "Long Arm of the Law," *FCW.COM*, August 29, 2005, 4. Available Online: .http://www.fcw.com/article90468-08-29-05-Print&printLayout (accessed June 2, 2007).

[153] North Florida High Intensity Drug Trafficking Area (HIDTA), Intelligence Exploratory Committee, *Information and Intelligence Sharing Strategy for Northeast Florida* (May 2007), Jacksonville, Florida.

purpose of the document was described as the formulation of a "general plan to increase communication between numerous information and intelligence resources within the Northeast Florida Region."[154]

The exploratory committee recognized that intelligence sharing had occurred in North Florida at various levels between varying entities for many years.[155] The Committee identified sharing mechanisms in place which had served specific historical intelligence requirements. For example, in the late 1990s, the High Intensity Drug Trafficking Area (HIDTA) program had funded and created the North East Florida Investigative Support Center (NeFISC) to analyze and promote criminal intelligence sharing amongst law enforcement agencies, specifically in drug related investigations. Also, in the 1990s, the FBI had created the Jacksonville Joint Terrorism Task Force to address terrorism related investigations in the Division. Similarly, after the events of September 11, 2001, the State of Florida created the Regional Domestic Security Task Force to assist with Homeland Security law enforcement and security related information sharing. These entities were created to increase information sharing and in reaction to specific historical threats to the area.

The Committee also recognized that while these groups were designed to serve varying purposes, they comprised key elements of intelligence gathering in the region. Other groups, such as the Intelligence Unit of the Jacksonville Sheriff's Office (JSO), the Jacksonville Port's Joint Maritime Advance Scheduling and Targeting Team (JMASTT), the FBI Field Intelligence Group (FIG), and the newly created Regional Intelligence Fusion Center (RIFC) rounded out the intelligence and analysis entities in the region. The study, therefore, sought to identify a fusion plan that would coordinate all these entities and thereby leverage their joint capabilities.

Originally, the Committee had envisioned recommending a consolidation of resources and capabilities under one roof in a centrally located fusion center. Logistical obstacles such as long term leases, varying security and protocols, and resource shortfalls

---

[154] *Information and Intelligence Sharing Strategy for Northeast Florida*, 3.

[155] Author serves as the HIDTA Executive Board Vice-Chairman and member of the North East Florida Intelligence Steering Committee.

made this option unrealistic. The Committee instead, created a virtual fusion system plan to unite the entities under a virtual roof comprised of steering and governance oversight. The plan calls for a Steering Committee, Fusion System Working Committee and a centralized point for dissemination of joint products and intelligence. [156]

Although the fusion system is still in progress, the plan calls for a strategy to facilitate the sharing of criminal intelligence, define ways to increase coordination, enable unified sharing of information and produce topic specific threat assessments for all member agencies in the area.[157] The plan suggests the unification of technology through the LInX system of data warehousing and a centralization of intelligence through the Northeast Florida Investigative Support Center (NeFISC). Each of the other intelligence centers will feed the virtual warehouse and be able to retrieve from it. The resulting system will have the benefits of expanded intelligence access while respecting the limited resources and flexibility of the component entities.

By emphasizing information sharing over construction of additional centers, and technology sharing over acquisition of new computers and wires, the proposed fusion system promotes effective intelligence sharing within the boundaries of limited government. This is accomplished through information management and collaborative governance. Central to the process is the cooperation and vitality of the interested parties. The key to success therefore, revolves around the group's commitment and desire to achieve mutual information sharing versus a mandated process forced upon unwilling or disinterested parties. Without the willingness of the partners to engage and commit in a collaborative process, which emphasizes voluntary sharing of key data, the committee concluded that fusion could not be reached through any amount of technology, resources or authority.

---

[156] *Information and Intelligence Sharing Strategy for Northeast Florida*, 10.

[157] Ibid, 3-4.

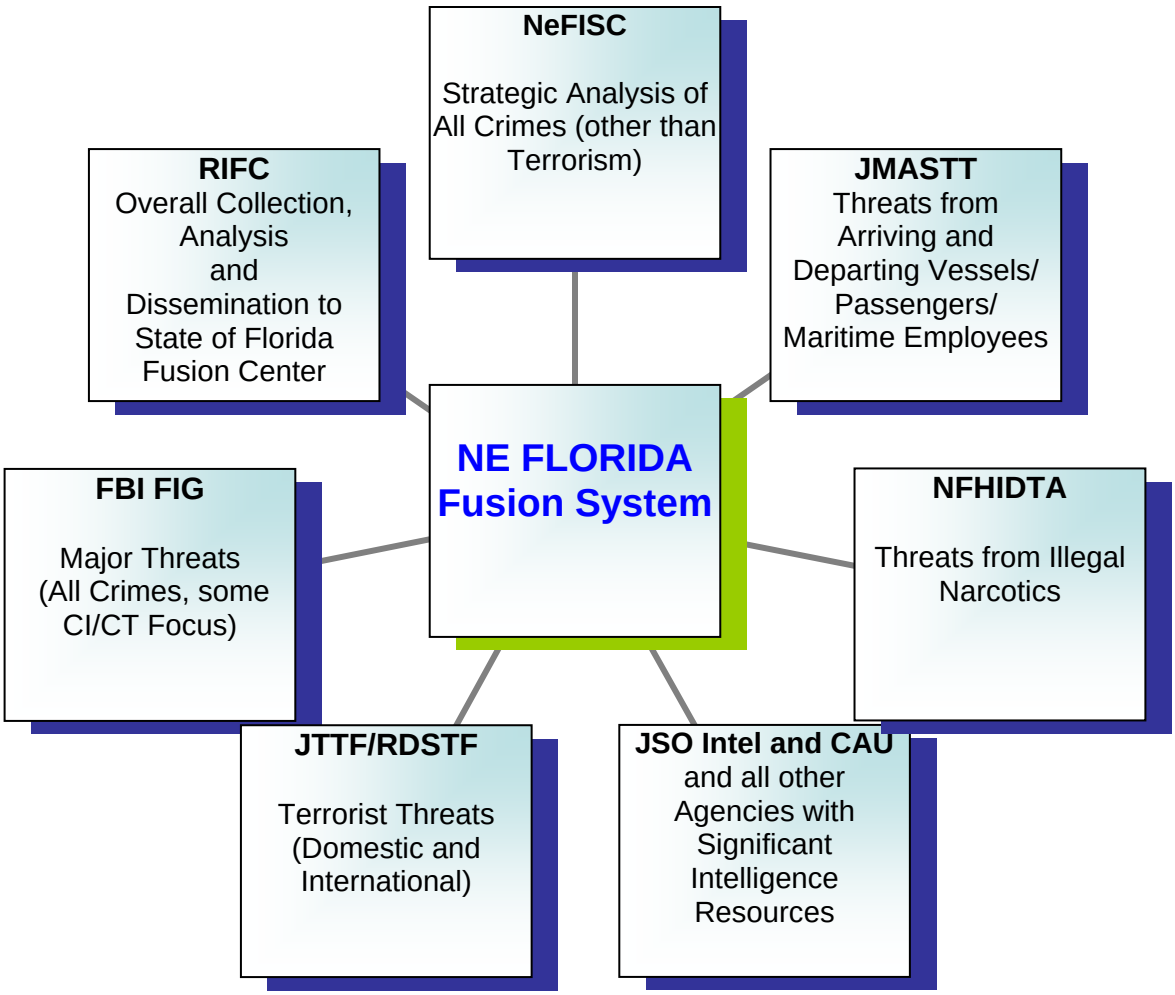


Figure 6. North East Florida Fusion System. [158]

[158] *Information and Intelligence Sharing Strategy for Northeast Florida*, 9.

V. OBSTACLES TO DOMESTIC COLLECTION AND ANALYSIS

A. OBSTACLES

Expansion of covert HUMINT is time consuming and manpower intensive. In 2004, then Director of the CIA, George Tenet, commented that even with his ambitious plan to rebuild the clandestine service, it would take the CIA at least five years to grow its spy program.[159] Furthermore, even with ambitious new programs, there are no guarantees that expanded budgets and long-term plans will produce timely and relevant HUMINT. Some observers even suggest that no amount of money or time will generate sources that can report on the most difficult targets, such as the Al Qaeda inner circle.[160] Domestic agencies are faced with a similar challenge in penetrating cells operating within the United States. Despite the expansion in human source programs, federal authorities may still lack the ability to significantly increase HUMINT.[161]

Unfortunately, domestic collection expansion has lagged behind for several reasons. First, the majority of the intelligence community was designed and concentrated on foreign collection. Only a small part of the overall intelligence community capability is devoted to domestic collection. For example, at least 85% of the intelligence budget is controlled by the Department of Defense.[162] This includes the National Security Agency, the National Reconnaissance Office and the Defense Intelligence Agency. As described above, under existing legislation, none of these agencies is permitted domestic collection outside of Department of Justice and DHS involvement. The Central Intelligence

---

[159] George Tenet, *Address on U.S. Prewar Intelligence on Iraqi Weapons of Mass Destruction* (Washington, DC: 2005). Available Online*:* http://www.cnn.com/2004/US/02/05/tenet.transcript.ap/index.html (accessed December 10, 2006).

[160] Susan Taylor Martin, "Old Fashioned Spying is a Hard Thing to Find," *St. Petersburg Times,* May 20, 2006, 2. Available Online: http://www.sptimes.com/2006/05/20/Worldandnation/Old_fashioned_spying_.shtml (accessed December 10, 2006).

[161] Ibid., 3

[162] David E. Kaplan and Kevin Whitelaw, "Remaking U.S. Intelligence – Part II: the Money," *U.S. News and World Report*, November 11, 2006. Available Online: http://www.usnews.com/usnews/news/articles/061103/3dni.money.htm (accessed November 24, 2006).

Agency is similarly prohibited.[163] The remaining domestic intelligence branches, which have responsibility for domestic collection, share less than 15% of the overall intelligence budget.

Second, domestic laws and procedures restrict domestic collection in support of civil liberty protections. As a result of 1960s era intelligence abuses, the Church Committee in 1975 recommended significant restrictions to domestic collection investigations.[164] In response, in 1978, the Congress passed the Foreign Intelligence Surveillance Act to restrict domestic intelligence wiretapping by the FBI.[165] The National Security Act of 1947 and the Intelligence Reform Act of 2005 also provided specific delineation of domestic and foreign collection.[166] These acts specifically restricted Department of defense agencies and the CIA from domestic collection activities except under limited circumstances. Taken as a whole, these legislative acts significantly restrict domestic collection for intelligence purposes and delineated the FBI as primarily responsible for intelligence investigations in the United States. None of this legislation however, affects the criminal jurisdictions of any agency to conduct criminally predicated investigations using authorized evidence-gathering tools.

Third, since only a small portion of the intelligence community engages in domestic collection, these efforts have a comparatively small effect on the increase in overall collection. For example, only a portion of the FBI is dedicated to intelligence collection activities within the National Security Branch of the agency.[167] Likewise, the

---

[163] *National Security Act of 1947*, 50 U.S.C. 401. Available Online: http://www.intelligence.gov/0-natsecact_1947.shtml (accessed September 3, 2007).

[164] U.S. Congress, Senate, *United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, Congress 94, Session 1, 1975. Available Online: http://foia.state.gov/Reports/ChurchReport.asp (accessed January 25, 2007).

[165] *Foreign Intelligence Surveillance Act*, 50 U.S.C. 36 §1801 (1978). Available Online: http://uscode.house.gov/download/pls/50C36.txt (accessed September 3, 2007).

[166] U. S. House of Representatives, House Report 108-796, *Intelligence Reform and Terrorism Prevention Act of 2004.* Available online: http://www.gpoaccess.gov/serialset/creports/intel_reform.html (accessed September 3, 2007).

[167] Federal Bureau of Investigation, *National Security Branch Overview* (Washington, DC: FBI, 2006). Available Online: http://www.fbi.gov/hq/nsb/whitepaper.htm (accessed November 26, 2006).

DHS Intelligence Section is relatively new and still in the formative stages.[168] The combined effort of these branches is still relatively small in comparison to the Department of Defense and CIA resources devoted to foreign collection. The relative expansion of these branches, however ambitious, remains a small percentage of the overall intelligence community effort.

Fourth, agencies with domestic collection responsibilities have invested their scarce resources on analysis and dissemination, the segments of the intelligence cycle where they are most likely to achieve results. For instance, since September 11, 2001 the FBI has doubled the number of its analysts and tripled its linguists.[169] Yet, the 9/11 Commission found that although the FBI had made progress in redirecting its efforts at analysis, "systemic collection work is left undone." [170] Also, in an article titled *America Needs More Spies*, published July 10, 2003, a group of six FBI and CIA intelligence experts collaborated to discuss the lack of domestic human intelligence collection.[171] They concluded that to prevent terrorism, terrorist organizations must be penetrated and that the United States did not have adequate human intelligence to do the job.[172] While they recognized that efforts were underway to increase analysis, they concluded more HUMINT was not forthcoming.[173]

For all these reasons, the intelligence community has seen a comparatively small increase in domestic collection, while other segments of the intelligence production cycle have been expanded. Since overall intelligence production relies on collection as one of its most important aspects, the lack of expansion in domestic collection will have a bottle neck effect on efforts to increase domestic intelligence production.

---

[168] Department of Homeland Security, *Information Sharing and Analysis* (Washington, DC: DHS, 2006), 1. Available Online: http://www.dhs.gov/xinfoshare (accessed November 26, 2006).

[169] Federal Bureau of Investigation, *Counterterrorism* (Washington, DC: FBI, 2006). Available Online: http://www.fbi.gov/aboutus/transformation/ct.htm (accessed November 24, 2006).

[170] *Staff Statement No. 12*, 4.

[171] "America Needs More Spies," 1.

[172] Ibid., 2.

[173] Ibid., 2.

B. OUTLOOK

One mechanism for increasing domestic collection is to exploit the existing state and local HUMINT resources described above. This strategy benefits from several advantages. For example, local law enforcement already operates tens of thousands of criminal informants who would be enormously expensive and time consuming to develop and recruit from scratch. These informants are operated within existing legal guidelines and do not require new or expansive legal authorities to create. While state and local jurisdictions might limit non-predicated intelligence gathering, predicated information could still be very useful in terrorist related investigations.

Moreover, the growing trend of Community Oriented Policing in American law enforcement, which by some estimates is used in over 80% of police departments, is a form of overt collection. Law enforcement has adopted these techniques for engaging the community in dialogue and communication in an effort to identify and reduce crime at the neighborhood level. As a result, police officers are becoming overt collectors of intelligence in their communities. Recently, the International Association of Chiefs of Police concluded in their annual report that their efforts at community policing was the answer to policing terrorism in America since at its core terrorism is a local problem and could be identified through community policing techniques.[174] By leveraging the covert and overt collection capabilities of state and local law enforcement overall domestic collection could be expanded without creating new federal agencies and programs.

Furthermore, the state and local law enforcement community scale is huge compared to the existing federal domestic resources; i.e., over 800,000 state and local law enforcement officers versus a few thousand Agents assigned to the FBI's National Security Branch and the DHS Intelligence Section.[175] The ability to leverage the entire law enforcement community would instantly have a significant impact on federal resource issues. This effect, on a much smaller scale, can already been seen in the JTTF

---

[174] *From Hometown Security to Homeland Security*, 4.

[175] Department of Justice, *Bureau of Justice Statistics, Law Enforcement Statistics* (Washington, DC: DOJ, 2006) 1. Available Online: http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed November 27, 2006).

Program. The JTTFs, which currently number approximately 108, employ approximately four thousand task force officers which more then doubles the FBI Agent complement.[176]

The exploitation of this network, however, does not come without its own challenges and roadblocks. For example, most local law enforcement informants are operated by individuals who maintain the majority of the informant's information. To benefit a national audience, the information would have to be captured electronically. Similarly, community policing efforts are often not oriented toward intelligence gathering per se and therefore are not well documented. Consequently, both covert and overt HUMINT efforts at the state and local level tend to be focused on specific crime problems and may overlook the intelligence windfall potential of collection activity. This is particularly evident in smaller departments which do not have the resources for specifically dedicated intelligence units or sophisticated analytical operations

Unfortunately, information sharing and more importantly intelligence sharing at fusion centers, continues to be hampered by classification issues, technology hurdles and law enforcement cultural impediments. Jurisdictional overlap and turf wars have always hampered law enforcement information sharing, and continues to frustrate efforts to enhance intelligence production at fusion centers. American law enforcement is categorized by many departments at various governmental levels, each with its own funding and mission requirements. These differences often cause difficulties for fusion centers. Varied missions create differing requirements for fusion centers which are pulled in different directions trying to satisfy their customers.[177]

The conflicting missions and jurisdictions force fusion centers to produce "generic" products which appeal to a broad constituency. The lack of focus associated with the process diminishes the value of the products and causes the products to lack actionable intelligence. [178] Moreover, fusion centers lack collection managers with the authority to task collection and therefore are unable to tailor specific products for the

[176] FBI Director Robert S. Mueller III, Testimony, 3

[177] Interview of FBI Supervisory Special Agent Christopher Piersza, former Supervisor from the FBI Directorate of Intelligence, by the author, June 21, 2007, Jacksonville, Florida.

[178] Ibid.

same reason. Also, fusion centers lack production standards and policies. Therefore, each center has adopted its own standards according to the community's particular needs and capabilities. Although some centers have matured their analytical capabilities, linking them on a nationwide basis is hampered by the lack of standardization.

C. EMBRACING CHANGE AND ACCEPTANCE

If acceptance is a key component of the enhanced intelligence process, how do we encourage our nation's law enforcement and domestic intelligence community to change the way they look at domestic collection? The concept of organizational change is a well-known discipline within the business and government community. For example, John P. Kotter discusses several stumbling blocks which cause change to fail.[179] Among these is 1) the necessity to establish urgency for the change; 2) establish and communicate a vision; 3) remove obstacles and plan short term wins; and 4) do not prematurely declare victory without anchoring the changes.

The idea of initiating a new frontier of change must be sold to the troops by an eager and committed leader.[180] Executives often view change as positive improvements to the business operation, while employees view change as complicating their lives.[181] Strebel describes the relationship as a personal contract between the employer and employee in which reciprocal obligations and mutual commitments are shared.[182] In the case of domestic collection, law enforcement has certain perceptions regarding intelligence and the role of state and local law enforcement. A central premise to the change needed in domestic collection involves altering the perceived reciprocal obligations between federal, state and local law enforcement. Leaders must establish the priority for all law enforcement, from Agents and detectives, to cops on the beat, to view themselves as collectors of national security information.

---

[179] John P. Kotter, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review on Leading through Change* (March-April 1995):3-18.

[180] Paul Strebel, "Why Do Employees Resist Change?" *Harvard Business Review on Leading through Change* (May-June 1996):45-62.

[181] Ibid., 47.

[182] Ibid., 48.

Successful change occurs when leaders are able to redefine the personal contracts and include the changes as beneficial to both parties. Undefined contract changes invariably fail.[183] Redefining contracts usually entail significant commitment by the leaders, described by Kim and Mauborgne[184] as "unforgettable calls for change." The leaders must establish the urgency of the agenda and maintain the energy and force behind its necessity. If changes in domestic collection are to succeed, law enforcement leaders must energetically accept their roles as leaders of national security intelligence collectors through out the country.

A common misperception regarding change is that workers, or in this case law enforcement and public safety officers, are recalcitrant and will not change voluntarily. Research shows, however, that organizations have change agents within them, which Steven Kelman describes as "change vanguards," who will push for changes they perceive solve problems.[185] Committed and motivated leaders who engage change vanguards find partners who can initiate rapid change within an organization. State and local law enforcement appear eager to take a greater role in the fight against terrorism and are ready for properly articulated, intelligence gathering strategy. For example, comments by state and local experts in the Lesson Learned Information Sharing project stated that local law enforcement was not being asked enough for information by federal authorities.[186] This suggests that there are change vanguards within state and local law enforcement ready to be tasked for collection information.

Leaders also must declare the vision with enough clarity to inspire the change agents to follow.[187] Failure to "set the stage," as Garvin and Roberto describe, can lead to failure.[188] It is important to frame the messages and "manage the mood" if change is

---

[183] Strebel, "Why Do Employees Resist Change?" 51.

[184] W. Chan Kim and Renee Mauborgne, "Tipping Point Leadership," *Harvard Business Review on Leading through Change* (April 2003):19-44.

[185] Steven Kelman, *Unleashing Change* (Washington, DC: Brookings Institution Press, 2005), 39.

[186] Department of Homeland Security, *Lessons Learned Information Sharing, LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process*, December 2005, 5.

[187] John P. Kotter, "Leading Change: Why Transformation Efforts Fail," 7, 8.

[188] David A. Garvin and Michael A. Roberto, "Change through Persuasion," *Harvard Business Review on Leading through Change* (February 2005):85-104.

to be sustained.[189] Leadership roles and authorities in domestic intelligence are unfortunately not well defined. Federalism causes confusion between the roles of the federal, state and local government entities. Insomuch as local collection efforts are being targeted in this strategy, local leaders must accept their role as collection managers and create the environment described above to initiate change. Federal intelligence leaders will not possess the authority or credibility to reach change vanguards in the state and local system. This mantra must be carried by local leaders, who need to conduct an "effective persuasion campaign" as described by Garvin and Roberto, focused at the change vanguards within their agencies. It must be clearly articulated, energetically advanced and unequivocally supported, if change is to be achieved.

Kotter also describes the necessity to remove obstacles and plan short term wins. Fusion centers continue to be hampered by classification issues, technology hurdles and law enforcement cultural impediments. If change is to be initiated, pre-requisite hurdles such as classification and cultural issues that hamper information flow must be alleviated. Resolving classification issues could be seen as both removal of obstacles and a short term win. Also, local intelligence successes in fusion center operations, where federal, state and local collectors have successfully fused intelligence should be touted and used as catalysts for the change process. Examples of terrorist plots averted or criminal investigations solved through collection fusion could also serve in this regard.

Additionally, Kotter emphasizes the importance of cementing positive changes before prematurely declaring victory. Currently, there is a movement to anoint fusion centers as the final solution and declare intelligence sharing solved. While fusion centers show great promise for the future, they have only begun to initiate a national intelligence process and require substantial improvement before declaring the job done. Moreover, the lack of domestic collection reaching the fusion centers has not been widely discussed and requires additional research and study. Changes to overall information sharing and the intelligence process should not be confused with expanding domestic collection and the strategy to coordinate same.

---

[189] Garvin and Roberto, "Change through Persuasion," 96.

A strategy to coordinate national collection efforts will require energetic leadership, especially at the local level, and change agents willing to initiate the changes. It will require buy-in from leaders at all levels and the empowering of frustrated state and local patriots slogging through the current inefficient and marginally effective intelligence system. There is evidence of these individual's existence in many articles and journals which cry out for intelligence reform. And, there is untapped leadership in the ranks of federal, state and local public servants. This type of change is possible if the clear articulated strategy evokes promise for the fulfillment of mutual obligations for both the leaders and the led.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. A COORDINATED NATIONAL COLLECTION AND ANALYSIS STRATEGY TOWARD A NEW HOMELAND SECURITY DOCTRINE

A. STRATEGY

A successful **s**trategic plan requires a vision and mission statement supported by goals and objectives. Situational analysis combined with strategic thinking produces a plan of attack.[190] A strategy must also take into account limited resources which ultimately dictate the capability of the endeavor. Maximizing the resources in a prioritized fashion increases the likelihood of success. [191] The strategy, to be effective, must be achieved within available resources and within cost parameters.

The vision for domestic collection in the United States is to provide detailed situational awareness of domestic threats to the policy makers in a timely and efficient manner. The strategic action envisions fusion of federal, state, local, tribal, public and private intelligence collection to create a detailed threat picture. This can be accomplished by recording, digitizing and transmitting all federal, state, local, tribal, public and private intelligence collection to state and regional fusion centers. Fusion centers would then have the capability to create detailed regional threat assessments. In turn, the regional assessments could be used at the national level to achieve the stated vision of national situational awareness.

The intelligence would encompass granular detail from even the smallest communities in the country, instead of current efforts that lack detail due to knowledge management limitations. To achieve the stated vision, it will be necessary to invest in training, technology and knowledge management software and techniques capable of unleashing collection currently stove piped at the local level. Cultural and bureaucratic

---

[190] Bill Birnham, *Strategic Thinking* (Douglas Mountain Publishing, Costa Mesa, CA, 2004), 190.

[191] Willie Pietersen, *Using Strategic Learning to Create and Sustain Breakthrough Performance* (John Wiley and Sons Inc., New York, 2002), 40.

changes will require change agents and leadership at all levels of government. Funding for these enhancements will be crucial to the strategy's success.

STRATEGIC VISION CONCEPT FOR DOMESTIC COLLECTION

Vision: A national intelligence entity provides detailed situational awareness of domestic threats to policy makers to prevent major terrorist attacks.

Strategic Actions: Leverage Domestic state and local law enforcement HUMINT to enhance national collection coverage. Create threat assessments using national leveraged HUMINT to predict major terrorism events

Goals: 1. Record all HUMINT collection data.
2. Digitize all HUMINT collection data.
3. Transmit HUMINT collection data to regional fusion centers.
4. Create threat assessments using expanded collection of HUMINT.
5. Share assessment products nationally.

Objectives: 1. Funding, training, acceptance of HUMINT recording.
2. Knowledge Management training, software for enhanced digitization.
3. Governance and training in support of sharing regionally.
4. Analytical resources and funding in support of regional threat assessments.
5. Leadership and commitment in support of national sharing of threat products.

Table 1. Strategic Vision Concept for Domestic Collection.

1. Blue Ocean Strategy for Domestic Collection Coordination

Blue Ocean Strategy is a corporate manual designed to describe ways in which corporations can expand into uncharted markets and uncontested space. The bestselling book by W. Chan Kim and Renee Mauborgne introduces the concept of corporate expansion through the development of innovative ideas that allow corporate entities to

rise above current market limitations. The idea is to create a strategy which simultaneously raises value while lowering costs in an uncontested environment. [192]

The vision of raising state and local collection efforts to new levels is dependent upon eliminating cultural issues such as intelligence hoarding and classification hurdles. Digitization of information and transmittal of intelligence must be completed if information sharing is to be increased. Inefficiencies, such as stove piping and duplication of effort must be reduced. The goal of this new homeland security doctrine is to create detailed analytical products that adequately describe the threat domain to the policy makers.

ELIMINATE	**RAISE**
1. Information Hoarding 2. Intelligence Gaps 3. Intelligence failures	1. Information Sharing 2. HUMINT at Fusion centers 3. Electronically recorded HUMINT 4. Situational and Domain Awareness 5. Community involvement
REDUCE	**CREATE**
1. Stove Piping 2. Inefficiencies, duplication of collection 3. Costs	1. Analytical Threat Assessments with granular detail 2. Opportunities for Law Enforcement to interdict or prevent terrorism 3. Synergistic intelligence which encompasses Community Policing information

Table 2. EMS Grid adapted from *Blue Ocean Strategy.*

[192] W. Chan Kim and Renee Mauborgne, *Blue Ocean Strategy* (Boston, MA: Harvard University Publishing Corporation, 2005).

The Blue Ocean Strategy Canvas, as described by Kim and Mauborgne, is an analytical framework that is both diagnostic and action oriented. The authors argue the value of a strategy canvas is its ability to capture the current state, provide an understanding of various factors impacting the current state and suggest alternatives.[193]

The strategy canvass diagram for domestic collection expansion envisions information isolated at the state and local level released through knowledge management techniques and transmitted to regional fusion centers for use in analysis. The leveraging of state and local collection information by fusion centers expands collection and provides analysts with the detailed collection information needed to create threat assessments.

[193] Kim and Mauborgne, *Blue Ocean Strategy*, 25.

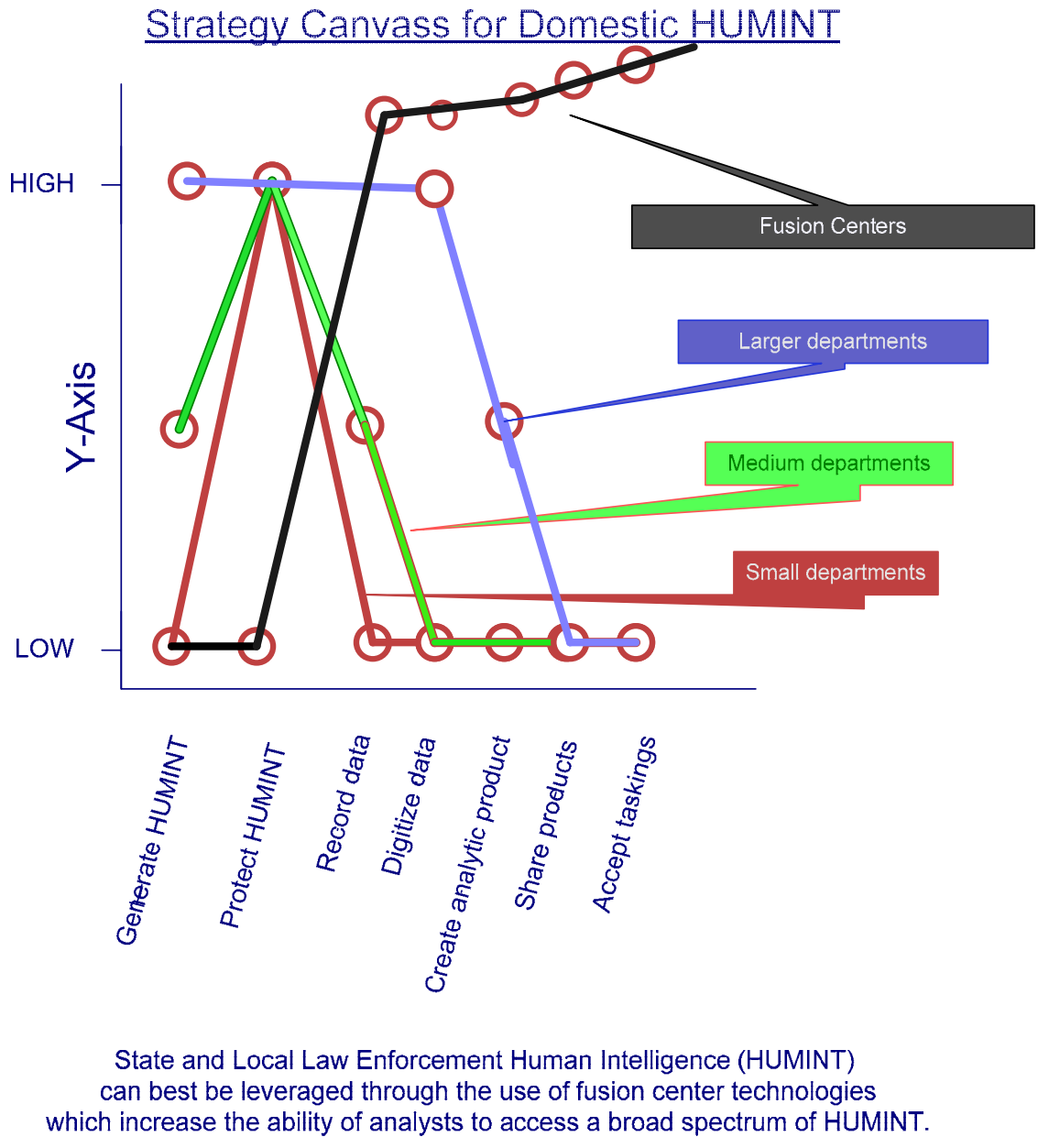


Figure 7. Strategy Canvass for Domestic HUMINT, adapted from *Blue Ocean Strategy*.

A comparison of the current environment versus the Blue Ocean Strategy for leveraging of state and local collection at the regional and national level reveals the advantages of the strategy.

Organization	Current Environment	Blue Ocean Strategy
Federal Domestic Intelligence Agencies	Produce Intelligence based on limited collection, including open source and intelligence community information. Shares information via formal and informal mechanisms.	Detailed threat assessments produced using intelligence gleaned from regional fusion centers including granular detail from all communities.
Large State and local law Enforcement Departments	Produce Intelligence based on limited metropolitan intelligence gleaned from local collection and limited federal input. Share products on a limited basis through formal and informal mechanisms.	Gain access to detailed National, state and local threat intelligence from regional fusion centers. Share intelligence with fusion centers.
Medium sized State and local law Enforcement Departments	Produce case specific intelligence using local criminal HUMINT and investigative information in support of local investigations. Occasionally share information via formal and informal mechanisms, including task forces and conferences.	Gain access to detailed National, state and local threat intelligence via fusion centers. Provide local data to fusion centers for aggregation analysis.
Small law Enforcement Departments	Do not produce intelligence. Do not generally have access to intelligence outside of informal networks. Share information predominantly through informal networks and individual to individual.	Gain access to detailed threat intelligence via fusion center. Gain access to analytical capabilities via fusion centers. Provide local data to fusion centers for aggregation analysis.

Table 3. Head-to-Head Comparison of Current Collection versus Proposed Strategy.[194]

[194] Adapted from Kim and Mauborgne's *Blue Ocean Strategy*.

B. CONCLUSIONS

Recent headlines illustrate the threat of Islamic extremists and that terrorism will be with us for many years to come. Human intelligence from informants, criminals, good-Samaritans and cooperative individuals is the key to neutralizing major terrorist plots. Coordinated terrorism investigations such as the Lackawanna Six and the Fort Dix Six demonstrate that HUMINT is vital to the prevention mission. Up to this point, however, law enforcement has relied on personnel training, recruiting of informants and appeals to the public for the expansion of our HUMINT collection. While these efforts have been laudable and effective thus far, officials must leverage all of their resources if the United States is to defeat a more stealthy and cunning enemy.

Post September 11th studies, such as the National Commission on Terrorist Acts upon the United States (The 9/11 Commission Report) confirm that the Al Qaeda hijackers came into contact with law enforcement at various stages of their plot. No one will ever know if these brief contacts could have led to preventing the attack, since the hijackers were careful to insulate themselves as much as possible. Without a concerted strategy to leverage *all* of our domestic HUMINT, however, we are at risk of repeating history.

It is now evident that information sharing alone will not prevent the next major act of terror. Most intelligence entities in government claim they are overwhelmed with the volume of information available. For the same reason, is also not enough to merely share random information. What is required is a strategy to coordinate HUMINT collection and use the increasingly awesome power of technology to sift through and analyze it.

The public expects law enforcement, intelligence and first responder entities to keep them safe. It also expects government to protect individuals' civil liberties and privacy. It is now evident that an expansion of both overt and covert HUMINT is necessary if we are to prevent major acts of terrorism. Before officials set out to create new agencies, new laws and a new domestic HUMINT network, they should take advantage of every bit of HUMINT collection available today. Law enforcement already

has the infrastructure in place and collectors embedded in the communities across the nation. What is needed now is the implementation of a coordination strategy including the exploitation of technology.

A coordination strategy will unite the varied and disperse collection efforts throughout the United States. It would also take into account the enormous untapped law enforcement resources outside the urban areas and not represented by larger inner-city departments. The strategy would encourage sharing and discourage hoarding, at a cultural and technological level. The technology will do the heavy lifting of sifting through the enormous amounts of information to find the key piece of information. It also will free the individual collector from the burden of deciding what is and is not important to report. Finally, it will assist analysts with link technology that can take advantage of the semantic process of the XML computer language. Together, the strategy and technology will become part of new homeland security doctrine that could unleash the full potential of domestic collection and provide the missing pieces of the intelligence puzzle. Perhaps most importantly, all this will be accomplished in an efficient way, using existing domestic collection and within existing federal, state and local laws, thereby protecting civil liberties from more intrusive methods of domestic collection.

C. RECOMMENDATIONS

1. Adoption of Global Justice XML Data Standard as intelligence collaboration "coin of the realm."

2. National coordination of collaborative platforms such as NDEx, HSIN, RISS and LEO in conjunction with regional warehouse systems such as LiNX for extraction of stove piped state and local collection information.

3. National Domestic HUMINT Collection Requirements and Standardized HUMINT Reporting Guidelines, including domestic Collection Managers with the authority to task domestic collection.

4. Expansion of Fusion Center Guidelines to include fusion center process and networking of HUMINT from outside urban areas.

5. Grant process for the expansion of state and local HUMINT including training, technical upgrades, and knowledge management software in support of strategy implementation.

6. Expanded fusion intelligence process to include all public and private sector community groups engaged in overt HUMINT.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allen, Charles, Assistant Secretary. *Statement to the Subcommittee on Intelligence Information Sharing and Terrorism Risk Assessment*. House Homeland Security Committee. February 14, 2007, 4. Available online: http://hsc.house.gov/SiteDocuments/20070314172258-47553.pdf (accessed August 19, 2007).

——— U.S. House of Representatives. May 24, 2006. Available online: http://homeland.house.gov/SiteDocuments/20070413143439-12273.pdf (accessed June 6, 2007).

Birnham, Bill. *Strategic Thinking* (Douglas Mountain Publishing, Costa Mesa, CA, 2004. 190.

Boston Herald Editorial Staff. "We Need An American MI-5," *Boston Herald*. August 27, 2006. Available online: http://news.bostonherald.com/editorial/view.bg?articleid=154613 (accessed April 29, 2007.)

Bryant, Robert et al. "America Needs More Spies," *The Economist*. July 10, 2003. Available online: http://www.economist.com/world/na/displayStory.cfm?story_id=1907776 (accessed November 26, 2006).

Chalk, Peter, and William Rosenau. "Intelligence, Police and Counterterrorism: Assessing Post 9/11 Initiatives," *Rand Reports*. October 30, 2003, 12. Available online: http://www.rand.org/nsrd/terrpanel/additional/intelinputv2.pdf (accessed August 19, 2007).

Chan Kim, W., and Renee Mauborgne. "Tipping Point Leadership," *Harvard Business Review on Leading through Change*. April 2003. 19-44.

———. *Blue Ocean Strategy* (Boston, MA: Harvard University Publishing Corporation. 2005).

Chavez, Dave T. Jr. "Knowledge Management in Policing," Department of Justice, Community Oriented Policing Services. October 25, 2005. 3. Available online: http://www.cops.usdoj.gov/mime/open.pdf?Item=1615 (accessed June 6, 2007).

Chertnoff, Michael, Secretary. Statement to National Fusion Center Conference, Destin, Florida. March 6, 2007.

Commission on Intelligence Capabilities of the United States regarding Weapons of Mass Destruction. *Report to the President of the United States*. March 31, 2005. 22. Available online: http://www.wmd.gov/report/ (accessed September 7, 2007).

Davies, Heather J. and Gerard R. Murphy. "Protecting Your Community from Terrorism," Police Executive Research Forum, Washington, DC: March 2004, 1. Available online: http://www.mipt.org/pdf/Protecting-Your-Community-From-Terrorism-Vol2.pdf (accessed August 19, 2007).

Department of Homeland Security. "DHS webpage." Available online: http://www.dhs.gov/xinfoshare (accessed June 3, 2007).

———. "Homeland Security Information Network Webpage." https://www.dhs.gov/xinfoshare/programs/gc1156888108137.shtm (accessed May 29, 2007).

———. *Information Sharing and Analysis* (Washington, DC: DHS, 2006). Available online: http://www.dhs.gov/xinfoshare (accessed November 26, 2006.).

———. Lessons Learned information Sharing, LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process. December 2005. 5. Available online: http://www.dhs.gov/xlibrary/assets/Final_LLIS_Intel_Reqs_Report_Dec05.pdf (accessed August 19, 2007).

———. Office of the Inspector General, *Homeland Security Information Network Could Support Information Sharing More Effectively*, Office of Information Technology OIG-06-38. June 2006. Available online: http://www.washingtonpost.com/wp-srv/nation/documents/OIG_06-38_Jun06.pdf (accessed August 19, 2007).

———. *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and information Fusion* (Washington, DC: Office of Homeland Security, 2002). 2. Available online: http://www.dhs.gov/xlibrary/assets/HSAC_HSIntelInfoFusion_Apr05.pdf (accessed, December 2, 2006).

Department of Justice. "Community Oriented Policing Services, Protecting Your Community from Terrorism: Strategies for local Law Enforcement, The Production and Sharing of Intelligence," Volume 4, February 2005, VII. Available online: http://www.cops.usdoj.gov/default.asp?Item=143 (accessed August 19, 2007).

———. Bureau of Justice Affairs. DOJGJ website. Available online: http://www.it.ojp.gov/topic.jsp?topic_id=43 (accessed August 19, 2007).

———. Bureau of Justice Affairs. *Fusion Center Guidelines*, 3. Available online: http://www.fas.org/irp/agency/ise/guidelines.pdf (accessed August 19, 2007).

———. Bureau of Justice Assistance. *Program Brief: Regional Information Sharing Systems Program.* April 2002, 2. Available online: http://www.ojp.usdoj.gov/BJA (accessed June 3, 2007).

———. Bureau of Justice Assistance. *The National Criminal Intelligence Sharing Plan.* October 2003, 1. Available online: http://www.fas.org/irp/agency/doj/ncisp.pdf (accessed August 19, 2007).

———. Bureau of Justice Statistics. *Law Enforcement Statistics, Summary Findings*. BJS Homepage, 1. Available online: http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed, May 14, 2007).

———. *Law Enforcement Statistics* (Washington, DC: DOJ, 2006) 1. Available online: http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed November 27, 2006).

———. *EGovernment Act Implementation Update* (Budget Data Request May 8, 2004. Available online: http://www.usdoj.gov/jmd/ocio/egovactreport2004.pdf . 2 (accessed October 8, 2006).

———. *Intelligence Led Policing: the New Intelligence Architecture* (Washington, DC: DOJ, 2005). Available online: http://www.ncjrs.gov/pdffiles1/bja/210681.pdf (accessed December 2, 2006).

———. *Law Enforcement Management and Administrative Statistics.* Local Police Departments, 2003, May 2006, 7. Available online: http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed August 19, 2007).

———. *Regional Information Sharing System, RISS Overview*. Available online: http://www.rissinfo.com/overview.htm (accessed June 9, 2007).

Federal Bureau of Investigation. *Report to the National Commission on Terrorist Attacks upon the United States: The FBI's Counterterrorism Program Since September 2001* (April 14, 2004).

———. "The FBI Counterterrorism Program Since 9/11," *Report to the Terrorism Commission on the events of September 11, 2001, 29.* Available online: http://www.fbi.gov/publications/commission/9-11commissionrep.pdf (accessed May 30, 2007).

———. *Counterterrorism* (Washington, DC: FBI, 2006). Available Online: http://www.fbi.gov/aboutus/transformation/ct.htm (accessed November 24, 2006).

———. *NDEx Program Overview* (Criminal Justice Information Services publication), 1. Available online: http://www.fbi.gov/hq/cjisd/ndex/ndex_overview.htm (accessed October 8, 2006).

———. *National Security Branch Overview* (Washington, DC: FBI, 2006). Available online: http://www.fbi.gov/hq/nsb/whitepaper.htm (accessed November 26, 2006).

———. *Strategic Plan 2004-2009* (Washington, DC: FBI, 2003). Available Online: http://www.fbi.gov/publications/strategicplan/strategicplanfull.pdf (accessed December 2, 2006).

Foreign Intelligence Surveillance Act, 50 USC 36 §1801 (1978). Available online: http://uscode.house.gov/download/pls/50C36.txt (accessed September 3, 2007.)

Garvin, David A., and Michael A. Roberto. "Change through Persuasion," *Harvard Business Review on Leading through Change* (February 2005):85–104.

Government Accounting Office. Statement of David A. Powner, Director Information Technology Management Issues, "Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives." www.gao.gov/cgi-bin/getrpt?GAO-07-822T (accessed May 29, 2007).

Groove Network, "Groove software is core component of HSIN; Demo at Homeland Security Conference Today" (Beverly, MA, February 26, 2004). Available online: http://www.groove.net/release.cfm?pagename=press_feb26_2004 (accessed August 19, 2007).

Harris, William. "Homeland Security Information Network: Moving Past the Missteps Toward Better Information Sharing," May 10, 2007, 2. Available online: http://homeland.house.gov/SiteDocuments/20070510132121-04354.pdf (accessed June 9, 2007).

Hulon, Willie T., Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation. Statement before the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "Facilitating an Enhanced Information Sharing Network That Links Law Enforcement and Homeland Security for federal, State and Local Governments," July 13, 2004, 10. Available online: http://reform.house.gov/UploadedFiles/Hulon%20Testimony.pdf (accessed October 8, 2006).

International Association of Chiefs of Police. *From Hometown Security to Homeland Security* (Washington, DC: IACP, 2005). Available online: http://www.theiacp.org/leg_policy/HomelandSecurityWP.PDF (accessed December 10, 2006).

Joch, Alan. "Long Arm of the Law." FCW.COM, August 29, 2005. 4. Available online: .http://www.fcw.com/article90468-08-29-05-Print&printLayout (accessed June 2, 2007).

Kaplan, David E. "Spies Among Us," *U.S. News and World Report*. April 30, 2006, 3. Available online: http://www.usnews.com/usnews/news/articles/060508/8homeland.htm (accessed May 6, 2007).

——— and Kevin Whitelaw. "Remaking U.S. Intelligence – Part II: the Money," *U. S. News and World Report*. November 11, 2006. Available online: http://www.usnews.com/usnews/news/articles/061103/3dni.money.htm (accessed November 24, 2006).

———. "Remaking U.S. Intelligence – Part II: the Money," *U.S. News and World Report*. November 11, 2006. Available online: http://www.usnews.com/usnews/news/articles/061103/3dni.money.htm (accessed November 24, 2006).

Kelling, George L. and William J. Bratton. "Policing Terrorism," *Manhattan Institute,* No. 43. September 2006, 5. Available online: http://www.manhattan-institute.org/html/cb_43.htm (accessed June 6, 2007).

Kelman, Steven. *Unleashing Chang*e (Washington, DC: Brookings Institution Press, 2005), 39.

Kotter, John P. "Leading Change: Why transformation efforts fail," *Harvard Business Review on Leading through Change* (March–April 1995).

Kouri, Jim. “Homeland Security Information Network Needs to be Better Coordinated.” *Canada Free Press*. May 16, 2007, 2. Available online: http://www.canadafreepress.com/printpage.php (accessed June 3, 2007).

Kurlander, Neil. “Out of Step,” *XML Journal*. January 25, 2006, 2. Available online: http://xml.sys-con.com/read/175403.htm (accessed August 19, 2007).

Leggiere, Phillip. “The Fusion Revolution,” *Homeland Security Today*. April 2007, 26. Available online: http://www.fas.org/irp/agency/ise/guidelines.pdf (accessed June 6, 2007).

Lehman, John. “We’re Not Winning This War,” *The Washington Post*. August 31, 2006; A25. Available online: http://www.washingtonpost.com/wp-yn/content/article/2006/08/30/AR2006083002730.html (accessed March 17, 2007.).

Lowenthal, Mark M. *Intelligence from Secrets to Policy* (CQ Press, Washington, DC: 2006), 2.

Martin, Susan Taylor. “Old Fashioned Spying is a Hard Thing to Find,” *St. Petersburg Times*. May 20, 2006. 2. Available online: http://www.sptimes.com/2006/05/20/Worldandnation/Old_fashioned_spying_.shtml (accessed December 10, 2006).

Masse, Todd. “Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches” (Congressional Research Service, August 18, 2006), Figure 2, CRS-10.

McNamara, Thomas, Ambassador, Program Manager, ISE, ODNI, National Fusion Center Conference. Destin, Florida. March 6, 2007. Statements available online: http://www.ise.gov/docs/Amb%20McNamara%20Remarks%20at%20Fusion%20Conference.pdf (accessed August 23, 2007).

Mosquera, Mary. “DHS vows to fix information network,” FCW.COM, May 28, 2007, 1. Available online: http://www.fcw.com/article102798-05-28-07-PrintandprintLayout (accessed June 3, 2007).

Mueller, Robert, Director FBI. Statement to Congress. July 27, 2005. http://www.fbi.gov.congress/congress05/mueller072705.htm (accessed May 23, 2006).

National Commission on Terrorist Acts upon the United States. *The 9/11 Commission Report* (New York: W.W. Norton & Co., 2004), 353, 411, 423. Available online: http://www.911commission.gov/staff_statements/staff_statement_12.pdf (accessed November 24, 2006).

National Institute of Justice. “Community Policing: 1997 National Survey Update of Police and Sheriff’s Departments.” September 22, 2000, iii. Available online: http://www.securitymanagement.com/library/ncj_police0601.pdf (accessed August 19, 2007).

National Security Act of 1947, 50 U.S.C. 401. Available online: http://www.intelligence.gov/0-natsecact_1947.shtml (accessed September 3, 2007).

Naval Criminal Investigative Service, *Law Enforcement Information Exchange, About LInX*, 1. Available online: http://www.ncis.navy.mil/linx/about_linx.html (accessed June 2, 2007).

———. Technical Overview, 1. Available online: http://www.ncis.navy.mil/linx/technical.html (accessed June 2, 2007).

———. About LInX, Technical Data (diagram.). Available online: http://www.ncis.navy.mil/linx/about_linx.html (accessed June 2, 2007).

North Florida High Intensity Drug Trafficking Area (HIDTA), *Intelligence Exploratory Committee, Information and Intelligence Sharing Strategy for Northeast Florida* (May 2007), Jacksonville, Florida.

Office of Homeland Security, *Department Six Point Agenda* (Washington, D.: DHS, 2006). Available online: http://www.dhs.gov/xabout/history/editorial_0646.shtm (accessed November 24, 2006).

Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America* (Washington, DC: Office of the Director of National Intelligence, 2005).Aavailable online: http://www.dni.gov/publications/NISOctober2005.pdf (accessed December 2, 2006).

Peterson, Marilyn. “Intelligence Led Policing: The New intelligence Architecture,” Department of Justice, Bureau of Justice Assistance, NCJ 210681, VII, September 2005. Available online: http://www.ncjrs.gov/pdffiles1/bja/210681.pdf (accessed June 6, 2007).

Pietersen, Willie. *Using Strategic Learning to Create and Sustain Breakthrough Performance* (John Wiley and Sons Inc., New York, 2002), 40.

Posner, Richard A. "We Need Our Own MI5," *The Washington Post*. August 15, 2006; A13. Available online: http://www.washingtonpost.com/wpdyn/content/article/2006/08/14/AR2006081401160.html (accessed March 17, 2007.)

Pulliam, Daniel. "FBI launches regional data sharing system." Available online: http://www.govexec.com/dailyfed/0605/062805p1.htm (accessed October 8, 2006).

Senate Select Committee on Intelligence. *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*. July 7, 2004, 34. Available online: http://www.gpoaccess.gov/serialset/creports/iraq.html (accessed September 3, 2007).

Strebel, Paul. "Why do employees resist change?" *Harvard Business Review on Leading through Change* (May-June 1996):45–62.

Tenet, George. *Address on U.S. Prewar Intelligence on Iraqi Weapons of Mass Destruction* (Washington, DC: 2005). Available online: http://www.cnn.com/2004/US/02/05/tenet.transcript.ap/index.html (accessed December 10, 2006).

U.S. Congress, House, Intelligence Reform and Terrorism Prevention Act of 2004. December 7, 2004, 108th Cong, 2d session, House report No. 108-796 (Washington, DC: Government Printing Office, 2004). Available online: http://www.nctc.gov/docs/pl108_458.pdf (accessed December 2, 2006).

———. Senate, United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Congress 94, Session 1. 1975. Available online: http://foia.state.gov/Reports/ChurchReport.asp (accessed January 25, 2007).

U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Intelligence Sharing, and Terrorism Risk Assessment, Statement of Charles Allen, The Homeland Security Information Network: "An Update On DHS Information Sharing Efforts." September 13, 2006, 4. Available online: http://www.hlswatch.com/category/events/ (accessed August 19, 2007).

———. House Report 108-796. Intelligence Reform and Terrorism Prevention Act of 2004. Available online: http://www.gpoaccess.gov/serialset/creports/intel_reform.html (accessed September 3, 2007).

U. S. President Executive Order, *Strengthening Management of the Intelligence Community*, Executive Order 13355 (Washington, DC: Government Printing Office, 2004). Available online: http://www.fas.org/irp/offdocs/eo/eo-13355.htm (accessed

November 29, 2006); U.S. President Executive Order. *Strengthening the Sharing of Terrorism Information to Protect Americans,* Executive Order 13356 (Washington, DC: Government Printing Office, 2004). Available online: http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html (accessed November 29, 2006).

U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001*, unclassified version of report, December 2002, 4.

Weisheit, Ralph A. et al. "Rural Crime and Rural Policing." National Institute of Justice, September 1994, 8. Available online: http://www.ncjrs.gov/pdffiles/rcrp.pdf (accessed August 19, 2007).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Training Division
   Federal Bureau of Investigation
   Washington, D.C.

4. FBI Jacksonville
   Federal Bureau of Investigation
   Jacksonville, FL