



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**DETECT AND DEFEAT — THE COMPLEXITIES OF  
ACCOMPLISHING THE HLS MISSION WITH EXISTING  
INTELLIGENCE COLLECTION PRACTICES**

by

Jeffrey Robertson

September 2007

Thesis Advisor:  
Second Reader:

Robert Simeral  
Richard Bergin

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
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.				
<b>1. AGENCY USE ONLY</b>		<b>2. REPORT DATE</b> September 2007	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE</b> Detect and Defeat — The Complexities of Accomplishing the HLS Mission with Existing Intelligence Collection Practices			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR</b> Jeffrey T. Robertson				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b> A	
<b>13. ABSTRACT</b> <p>Since the tragic events of 11 September 2001, it has been argued that accurate and well-vetted intelligence is critical to securing the Homeland; but over five years after the historic day, the realm of creating an “effective” domestic intelligence platform falls short of meeting desired milestones. The distinct threat of radicalism incubating within our smaller communities (townships, rural community) still exists and the lack of intelligence collection efforts at the local level may be fueling this threat.</p> <p>As a result of interviewing small townships and rural communities dispersed across the United States, it was discovered that though law enforcement resources of our smaller populations have been recognized as critical assets in the realms of Homeland Security (HLS), small townships and countryside communities still experience shortfalls in available resources and HLS related training. More times than none, these deficits revolve around domestic intelligence collection, processing, and dissemination.</p> <p>This research project will review the shortfalls plaguing the environment of intelligence collection and sharing. This project will also offer a cost effective strategy to mitigate the identified intelligence discrepancies and propose a solution to improve information sharing between Homeland Security stakeholders.</p>				
<b>14. SUBJECT TERMS</b> Domestic Intelligence; Law Enforcement; Local Government; Community; Intelligence Cycle; National Guard; Surveillance; Homeland Security; Information Sharing			<b>15. NUMBER OF PAGES</b> 89	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UU	

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**DETECT AND DEFEAT — THE COMPLEXITIES OF ACCOMPLISHING THE  
HLS MISSION WITH EXISTING INTELLIGENCE COLLECTION PRACTICES**

Jeffrey T. Robertson  
Civilian, United States Air Force  
Bachelor of Science in Electrical Engineering, University of Colorado, 1999  
Master of Science in Electrical Engineering, University of Colorado, 2002

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: Jeffrey T. Robertson

Approved by: Robert Simeral  
Thesis Advisor

Richard Bergin, Ph.D.  
Second Reader

Douglas Porch  
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Since the tragic events of 11 September 2001, it has been argued that accurate and well-vetted intelligence is critical to securing the Homeland; but over five years after the historic day, the realm of creating an “effective” domestic intelligence platform falls short of meeting desired milestones. The distinct threat of radicalism incubating within our smaller communities (townships, rural community) still exists and the lack of intelligence collection efforts at the local level may be fueling this threat.

As a result of interviewing small townships and rural communities dispersed across the United States, it was discovered that though law enforcement resources of our smaller populations have been recognized as critical assets in the realms of Homeland Security (HLS), small townships and countryside communities still experience shortfalls in available resources and HLS related training. More times than none, these deficits revolve around domestic intelligence collection, processing, and dissemination.

This research project will review the shortfalls plaguing the environment of intelligence collection and sharing. This project will also offer a cost effective strategy to mitigate the identified intelligence discrepancies and propose a solution to improve information sharing between Homeland Security stakeholders.

THIS PAGE INTENTIONALLY LEFT BLANK



## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>PROBLEM STATEMENT .....</b>	<b>1</b>
<b>B.</b>	<b>RESEARCH QUESTION .....</b>	<b>2</b>
<b>C.</b>	<b>SPECIFIC RESEARCH OBJECTIVE .....</b>	<b>2</b>
<b>D.</b>	<b>SIGNIFICANCE OF RESEARCH .....</b>	<b>2</b>
<b>E.</b>	<b>REVIEW OF RELEVANT LITERATURE.....</b>	<b>3</b>
<b>F.</b>	<b>HYPOTHESIS.....</b>	<b>7</b>
<b>G.</b>	<b>METHODOLOGY AND RESOURCES .....</b>	<b>8</b>
<b>II.</b>	<b>THE REALM OF INTELLIGENCE.....</b>	<b>11</b>
<b>A.</b>	<b>COLLECTION .....</b>	<b>11</b>
1.	SIGINT.....	11
2.	HUMINT.....	12
3.	OSINT .....	13
4.	GEOINT.....	14
5.	MASINT.....	16
<b>B.</b>	<b>ESSENTIAL ELEMENTS OF INFORMATION .....</b>	<b>16</b>
<b>C.</b>	<b>INTELLIGENCE CYCLE.....</b>	<b>17</b>
1.	Planning, Direction, Needs, and Requirement .....	18
2.	Collection .....	18
3.	Process Exploitation.....	18
4.	Analysis .....	19
a.	<i>Current Intelligence</i> .....	19
b.	<i>Estimative Intelligence</i> .....	19
c.	<i>Warning Intelligence</i> .....	19
d.	<i>Research Intelligence</i> .....	20
e.	<i>Technical Intelligence</i> .....	20
f.	<i>Dissemination</i> .....	20
<b>D.</b>	<b>FUSION .....</b>	<b>20</b>
1.	Collection and Correlation.....	21
2.	Fusion.....	22
3.	Analyzed.....	22
4.	Dissemination .....	22
<b>E.</b>	<b>SUMMARY .....</b>	<b>23</b>
<b>III.</b>	<b>ANALYSIS OF CURRENT HLS ISSUES – ADAPTIVE ADVERSARIES.....</b>	<b>25</b>
<b>A.</b>	<b>TERRORIST CELL OPERATIONS: ADAPTIVE COMMUNICATIONS AND COLLABORATION.....</b>	<b>25</b>
<b>B.</b>	<b>TECHNOLOGY .....</b>	<b>26</b>
1.	Mail Systems.....	26
2.	Amateur Radio.....	27
3.	Cell Phones .....	28
4.	Encryption .....	29

5.	Internet.....	29
C.	HUMAN SMUGGLING – ILLEGAL IMMIGRATION: LEVERAGING CLANDESTINE ORGANIZATIONS.....	31
D.	SUMMARY .....	33
IV.	ANALYSIS OF COMMUNITIES.....	35
A.	TONAWANDA, NY.....	37
B.	VOLUSIA COUNTY .....	38
C.	NASSAU COUNTY, NEW YORK.....	39
D.	CITY OF BATAVIA, NEW ORK.....	39
E.	SUMMARY .....	44
V.	DISCUSSION .....	47
A.	OPERATIONS.....	47
1.	Leveraging the National Guard.....	47
2.	Intelligence, Surveillance and Reconnaissance (ISR).....	49
a.	<i>IMINT</i> .....	49
b.	<i>MASINT</i> .....	50
c.	<i>HUMINT</i> .....	52
3.	Partnerships.....	53
B.	TRAINING .....	54
1.	Language and Culture Differences.....	55
2.	Information Technology .....	56
C.	SUMMARY .....	57
VI.	RECOMMENDATIONS AND FINAL THOUGHT .....	59
A.	AVAILABLE ISR RESOURCES.....	59
B.	MANNING.....	60
C.	TRAINING .....	61
D.	INFORMATION SHARING .....	61
E.	FINAL THOUGHT .....	62
	BIBLIOGRAPHY .....	65
	INITIAL DISTRIBUTION LIST .....	73

## LIST OF FIGURES

Figure 1.	Intelligence Cycle .....	17
Figure 2.	Intelligence fusion environment. ....	21
Figure 3.	Effectiveness of current configuration.....	40
Figure 4.	Organizational value for intelligence investments.....	43

THIS PAGE INTENTIONALLY LEFT BLANK

## **EXECUTIVE SUMMARY**

### **A. PURPOSE**

This thesis will define and discuss the shortfalls in the current intelligence collection and information sharing structures respective to the local (small municipality and rural community) Homeland Security effort. It will also suggest recommendations for local law enforcement agencies to enhance their presence in the national intelligence process.

### **B. DISCUSSION**

(1) Since the tragic events of 11 September 2001, it has been argued that the accurate and well vetted intelligence is critical to security the Homeland; but over five years after the historic day, the realm of creating an “effective” domestic intelligence platform falls short of meeting desired milestone; many of which can be mitigated at the local level.

(2) This thesis introduces the five disciplines of intelligence collection, the intelligence cycle, and provides a baseline understanding of the realms of intelligence. It also explores the adaptive techniques of the modern adversary.

(3) This research primarily focused on local level law enforcement intelligence efforts in relation to their contribution to the overall Homeland Security objective. The communities of Tonawanda, NY; Nassau County, NY; Valusia County, FL; and Batavia, NY agreed to participate as research subjects for this thesis. To collect information for analysis, a survey consisting of questions pertaining to intelligence collection and information dissemination was disseminated to each of the participating communities. The information collected was used in the analysis phase of this thesis and was used when crafting recommendations.

(4) The immediate consumers for this research will be federal, state, and local decision makers of the intelligence, inter-agency, law enforcement, command and control (C2) communities. The recommendations incorporated within this thesis may contribute to the development and execution of future domestic intelligence architectures.

THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

First and foremost, I would like to express my gratitude to my wife Lisa and daughter Abaigeal for their support and patience while I ventured through this academic trek. I also would like to thank my parents David Robertson, Lt Col, USAF (ret) and Chu Mann Robertson for their support, guidance, and encouragement in my early years and through my past academic endeavors.

Special thanks also go to my fellow cohort members (Cohort 601/602), my thesis advisors, and the Center for Homeland Defense and Security (CHDS) faculty, to include the support staff. With out this top-notch crowd, my academic experience would not have been as enjoyable, memorable, and challenging.

I also want to acknowledge my Headquarters United States Northern Command Standing Joint Forces Headquarters North (USNORTHCOM/SJFHQ-N) teammates who contributed to the drafting of this thesis by providing guidance based on their professional experience and vast understanding of the worlds of the National Intelligence Community, Homeland Security, and Homeland Defense.

THIS PAGE INTENTIONALLY LEFT BLANK



# I. INTRODUCTION

## A. PROBLEM STATEMENT

Since the tragic events of 11 September 2001, it has been argued that accurate and well-vetted intelligence is critical to securing the homeland; but over five years after the historic day, the realm of creating an “effective” domestic intelligence platform falls short of meeting desired milestones. The distinct threat of radicalism incubating within our communities still exists and the topic is often addressed by decision makers; however, very little action has been taken.<sup>1</sup> In the case of current Homeland Security (HLS) issues related to the activities of individuals with ties to Al Qaeda and illegal immigration, persons of interest operating in small municipalities and rural communities can easily evade detection.<sup>2,3</sup> Evasion can be achieved by the terrorist cell cautiously adapting to the intelligence collection and monitoring methods bestowed upon them and, if detected, reverting to using alternative technologies and operational techniques, thereby minimizing their operations and planning signature.<sup>4,5</sup> An intelligence environment with a nominal number of signatures creates an atmosphere where accurate collection becomes difficult, thereby hindering the overall effectiveness of HLS operations.

---

<sup>1</sup> Larry Copeland, “Domestic Terrorism: New Trouble at Home,” *USA Today*, 14 November 2004, [http://www.usatoday.com/news/nation/2004-11-14-domestic-terrorism\\_x.htm](http://www.usatoday.com/news/nation/2004-11-14-domestic-terrorism_x.htm) [last accessed 26 January 2007].

<sup>2</sup> In his 22 July 2007 interview with MSNBC Meet the Press, Admiral Mike McConnell made it clear that the DNI is not aware of any sleeper cells residing within the U.S. Borders. However, ADM McConnell did state that there are individuals within the United States with ties to Al Qaeda senior leadership. <http://www.msnbc.msn.com/id/19850951> [last accessed 23 July 2007].

<sup>3</sup> Dan Verton, *Black Ice: The Invisible Threat of Cyber –Terrorism* (New York: McGraw-Hill 2003), 82, 88.

<sup>4</sup> Patrick Keefe, *Chatter* (New York, NY: Random House, 2005), 8.

<sup>5</sup> Mark Krikorian, “The Security Costs of Immigration,” *American Outlook*, February 2003, <http://www.cis.org/articles/2003/msksecurityoped203.html> [last accessed 21 January 2007].

## **B. RESEARCH QUESTION**

Undertaking their part of HLS, how can rural communities and small municipalities enhance their intelligence collection processes and increase their contribution to the domestic intelligence cycle?

## **C. SPECIFIC RESEARCH OBJECTIVE**

In this research, I will identify the shortfalls in the current intelligence collection and information sharing structures. I will also seek to identify a cost effective strategy to mitigate the discovered shortfalls. The recommended solution will include elements that can be applied to small community presence and effectiveness in the realms of domestic intelligence.

## **D. SIGNIFICANCE OF RESEARCH**

The immediate consumers for this research will be federal, state, and local decision makers of the intelligence, inter-agency, law enforcement, command and control (C2) communities. Ultimately, recommendations extending from academic institutions will circulate through the hallways of national and state level decision makers. The recommendation incorporated within this thesis may contribute to the development and execution of future domestic intelligence architectures which will enhance the efficiency of the national intelligence community. In addition, this thesis will illustrate a method for HLS to seek a balance between intelligence collection via the different collection disciplines, exploit the collected data, analyze it, provide all source intelligence assessment, and disseminate the intelligence down to the streets at the appropriate classification level.

As stated in the literature review, accessible literature respective to domestic intelligence reform is limited. The discussions incorporated in this thesis will contribute to defining the evolution of the core functions, processes, and partner relationships associated with collecting intelligence on subjects of interests residing internal to the Homeland. In addition to addressing historical and current intelligence collection

platforms, this thesis will briefly discuss contributing elements of intelligence sharing respective to the multi-agency HLS intelligence community and will propose a effective solution to items mentioned in the problem statement.

## **E. REVIEW OF RELEVANT LITERATURE**

There is a vast collection of literature oriented towards the realms of foreign intelligence that can be broken down into several types of literature: Academic, Legislation, Insider Intelligence (field-agents, analysts), and Policies/Official Guidelines. Over the years, many within these disciplines have debated whether technology based intelligence, surveillance, and reconnaissance (ISR) platforms should remain as a key asset in HLS. Experienced analysts and veteran intelligence field agents like Mark Lowenthal and Gary Schroen agree that Human Intelligence (HUMINT) is a more effective method of collecting intelligence than its high tech alternatives. Their arguments stand against the thoughts and guidance of intelligence community (IC) powerhouses such as George J. Tenet and General Michael Hayden USAF.

Mark Lowenthal, the president of the Intelligence and Security Academy and former assistant director of central intelligence for analysis (2002-2005), has provided input in several mass media forums. In his book *Intelligence: From Secrets To Policy*, Dr. Lowenthal argues that HUMINT and open source intelligence (OSINT) are the significant attributes of the intelligence world and that these two ISR collection attributes have proven to be equal to, if not more significant than, their sensor based intelligence collection counterparts such as signals intelligence (SIGINT), measurement and signatures intelligence (MASINT), and Geospatial Intelligence (GEOINT). Sensor based intelligence collection platforms are often heavily dependent on technology and may be collectively termed under the phrase “national technical means” (NTM). Lowenthal emphasizes that on the modern battlefield the adversary fights with guerilla-style tactics. With HUMINT, the United States IC, at all echelons, “can collect certain types of

information (intentions and plans) that technical collection cannot.”<sup>6</sup> With this being said, the further investment in HUMINT assets will allow for better tracking of its adversaries.

HUMINT, also known as insider intelligence, activity has also played a big role in the first stages of the Global War on Terror and securing the Homeland. Prior to the invasion, the United States Government (USG) pre-positioned agents of the Central Intelligence Agency (CIA) within the borders of Afghanistan to build relationships with local tribesmen and develop an alliance. Gary Schroen, a CIA operator assigned lead a team into northern Afghanistan to connect with leaders of the Northern Alliance, also argues that HUMINT assets contribute to the collection of valuable intelligence. The first element of any HUMINT activity is building a relationship and trust with the information source. In one section of his book, Schroen describes the interaction between the CIA and the local Afghan tribes:

We also received, on a daily basis, reports from “human assets” who crossed over from the Taliban positions. These sources were either Taliban soldiers co-opted by the Northern Alliance, or civilians living inside NA lines – who had family or friends on the Taliban side.<sup>7</sup>

The information collected on a daily basis by Schroen and his crew provided a valued insight of locations, operations, and adversarial intent; and in turn saved the lives of U.S. troops in the early hours of Operation Enduring Freedom (OEF).

On the other side of the table, there are arguments that the high-tech ISR platforms are more effective than HUMINT. In their respective 2000 testimonies to the House Permanent Select Committee on Intelligence, George J. Tenet, Director of Central Intelligence (1997-2005), and Michael Hayden, Director of National Security Agency (1999-2005), both emphasized the importance of high-tech surveillance. In his statement, Tenet said that the U.S. relies on SIGINT to collect information regarding the capabilities and intentions of national interests to include foreign states and persons supporting

---

<sup>6</sup> Mark Lowenthal, *Intelligence: From Secrets to Policy* (Washington DC: CQ Press, 2006), 18.

<sup>7</sup> Gary.C. Schroen, *First In: An Insiders Account of How the CIA Spearheaded the War on Terror in Afghanistan* (New York, NY: Ballestine Books, 2005), 111-112.

foreign policy.<sup>8</sup> Tenet went on to declare that SIGINT is critical to the monitoring activities such as arms control compliance, narcotics trafficking, and aspects of terrorist command and control (C2). In his 2002 testimony to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, General, then Lt. General, Hayden argued that SIGINT remains critical to the national security and further investment is required to keep the discipline alive. General Hayden further expands his argument when he declares that the National Security Agency (NSA) provides a valued SIGINT product line to other agencies to include law enforcement agencies (LEA) on a daily basis. He also acknowledges that an amendment to current policies will be required to accommodate electronic searches and put the adversary behind bars.<sup>9</sup> General Hayden now fills the role as Director of the Central Intelligence Agency. Since his transition, General Hayden has redirected his stance on intelligence collection investments. Hayden in his opening statement before the Senate Intelligence Committee declared that human intelligence collection will be the CIA's number one priority and the CIA will "enhance the standards of tradecraft in HUMINT collection across the intelligence community."<sup>10</sup>

Intelligence reform has been a key topic of debate in Washington DC since the events of 11 September 2001. Based on the reform, the fundamentals of running the nation's IC have revolved around redefining the policies and official guidelines of the community.

In October 2005, the Office of the Director of National Intelligence published the United States National Intelligence Strategy (NIS) with a follow on annex defining human capital allocation. The NIS lays out the architecture of the mentioned intelligence reform by defining vision, mission statement, strategy, and objectives.<sup>11</sup> According to the

---

<sup>8</sup> Statement by Director of Central Intelligence George J. Tenet Before the House Permanent Select Committee on Intelligence, 106<sup>th</sup> Congress, 2<sup>nd</sup> Session 12 April 2000, Routine proceedings S2553-S2646, [http://www.odci.gov/cia/public\\_affairs/speeches/dci\\_speech\\_041200.html](http://www.odci.gov/cia/public_affairs/speeches/dci_speech_041200.html) [last accessed 29 January 2007].

<sup>9</sup> Ibid.

<sup>10</sup> John Dwyer, "General Hayden: Man on a Mission," *American Thinker Online*, 29 January 2007, [http://www.americanthinker.com/blog/2006/05/general\\_hayden\\_man\\_on\\_a\\_missio.html](http://www.americanthinker.com/blog/2006/05/general_hayden_man_on_a_missio.html) [last accessed 29 January 2007].

<sup>11</sup> Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of the America: Transformation through Integration and Innovation* (Washington, D.C.: Government Printing Office, 2005), 8.

annex, the IC workforce of skilled human assets has decreased in the past decade because of lower U.S. birthrates, fewer college graduates with foreign language and technical skills, and a competitive open market.<sup>12</sup> With this said, the annex details a strategy to effectively employ its existing and future collection of human asset resources to include linguists, analysts, and field agents.

Before recommendations can be made regarding change to the current policies, the balance between civil liberties and ISR requirements needs to be understood. Richard Posner, a sitting Judge on the U.S. Court of Appeals for the Seventh Circuit, discusses the interpretations of individual Constitutional rights versus HLS related surveillance, detention, interrogation, and profiling.<sup>13</sup> Civil liberties advocates concur with Posner that changes are required; however, the private interest group argues that before civil liberties versus ISR requirements are rebalanced, other factors such as current overt safety and security practices will need to be addressed.<sup>14</sup>

There has been little published concerning domestic intelligence reform in the context of HLS and collection methods on persons of interest residing within the United States. Due to this, literature focused on the HUMINT platforms and NTM used in historic national security campaigns will be reviewed and cited in this thesis. HUMINT and NTM practices used within the realms of foreign intelligence can be integrated into the domestic intelligence reform. However, legal issues regarding the violation of civil rights are critical when exercising any form of intelligence collection internal to the U.S. borders. These issues have been reflected in the literature discussed within this section of the proposal.

---

<sup>12</sup> Office of the Director of National Intelligence, *US Intelligence Community's Five Year: Strategic Human Capital Plan* (Washington, D.C.: Government Printing Office, 2006), 5-6, 8.

<sup>13</sup> Richard Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (New York, NY: Oxford University Press, 2006), 56-57, 84-85, 112, 114.

<sup>14</sup> James X. Dempsey, "Civil Liberties in A Time of Crisis," *Human Rights Magazine Online*, Winter 2002. <http://www.abanet.org/irr/hr/winter02/dempsey.html> [last accessed 2 January 2007].

## **F. HYPOTHESIS**

Though proven valuable in historic campaigns, NTM intelligence collection methods have been unsuccessful when tracking broad networked radical terrorist groups such as al Qaeda. While residing in the United States and its allied nations, the al Qaeda terrorist cells that participated in the 11 September attacks effectively planned and coordinated their sleeper cell operations without raising the attentions of the federal government and local law enforcement authorities. Walead al-Shehri, identified by the FBI as a participant in the 9-11 attacks,<sup>15</sup> lived in Daytona Beach as early as 1993 while attending Embry-Riddle Aeronautical University. According to records and testimony from a Daytona Beach, FL apartment manager, a unit in his complex was rented to Almed al-Ghamdi, another 11 September contributor, in 1995 and later to al-Shehri.<sup>16</sup> In this time, the two individuals coordinated internationally with other al Qaeda cells in the development stages of the 11 September attack. The information regarding this activity was revealed in the extensive interviews and investigations following the attack.<sup>17</sup>

Given the multiple scenarios where individuals with ties to terrorist groups such as Al Qaeda live and operate within our smaller communities, it has become difficult for the federal governments to detect and deter malicious terrorist activities. Discoveries of the alleged terrorist activities in Lodi, CA (2001) or human smuggling operations in Mercer County, PA (2005) represent two cases where illegal operations were taking place within the United States literally undetected for a period of time. These two cases will be further discussed in a later chapter.

---

<sup>15</sup> "Hijack 'Suspects' Alive and Well," British Broadcasting Company (BBC), 23 September 2001, [http://news.bbc.co.uk/2/hi/middle\\_east/1559151.stm](http://news.bbc.co.uk/2/hi/middle_east/1559151.stm) [last accessed 2 January 2007].

<sup>16</sup> Global Security, "Wail al-Shehri," [http://www.globalsecurity.org/security/profiles/wail\\_al-shehri.htm](http://www.globalsecurity.org/security/profiles/wail_al-shehri.htm) [last accessed 26 January 2007].

<sup>17</sup> The 9/11 Commission, *9-11 Commission Report* (Washington, D.C.: Government Printing Office, 2004), 169.

## **G. METHODOLOGY AND RESOURCES**

In search of an answer to the research question, I broke my research into two parts. To begin with, I reviewed published plans, policies, and subject matter literature to identify operational concepts, training efforts, advance technology supporting a solution, and organizational intelligence processes.

Second, to better understand the problems at the grass root local law enforcement level of intelligence, I created a case study to examine the intelligence processes of smaller municipalities and rural communities. Interviews with law enforcement and intelligence professionals were performed to gain first hand views of the collection process. The questions incorporated within surveys would be oriented around professional experiences of both HUMINT and NTM collection disciplines. Details would include success rates of apprehension of persons of interest versus collection discipline, personal thoughts of each method, and respective organizational budgets. Based on disciplines and experience, it is expected that there will be differences in opinions as to which collection disciplines are effective. The collected information will be consolidated with published research to provide an answer to efficient collection investments. The following samples a series of questions that will be encompassed within the survey:

- 1) What is your agency's annual budget?*
- 2) What is the population of your municipality, community, and/or area of responsibility?*
- 3) How much is allocated to HLS intelligence related collection efforts?*
  - a) How much is given to technology dependent collection platforms?*
- 4) Does your agency have direct access to federally allocated counter-terrorism grants?*
  - a) If yes, which ones? What is the allocated amount?*
- 5) What will improve your agency's information sharing environment with other organizations (federal state, local)?*
- 6) Is your staff trained to identify potential terrorist activity?*
  - a) If no, how much of your future budget is dedicated to terrorist training?*



*7) What are the political, economic, and social dilemmas, challenges, and successes of requiring greater amounts of intelligence collection and analyses for Homeland Security purposes, the areas of potential cooperation and conflicts in agency roles and responsibilities?*

*8) What is your professional experience with HUMINT, OSINT, and technology based (SIGINT, MASINT, and GEOINT) collection platforms. Based on your experience, which of the two do you see being more effective in resolving current intelligence reform issues?*

THIS PAGE INTENTIONALLY LEFT BLANK

## **II. THE REALM OF INTELLIGENCE**

Know the enemy and know yourself; in a hundred battles you will never be in peril. — Sun Tzu <sup>18</sup>

Before the realm of domestic intelligence can be extensively discussed, an understanding of the intelligence cycle, the different disciplines of intelligence, and essential elements of information should be examined. Intelligence provides critical information used by planning cells when developing courses of action (COA) for the decision maker. The decision maker may take suggested COAs into consideration when he or she makes the decisions to defeat the adversary or mitigate vulnerabilities.<sup>19</sup> This said, intelligence disciplines and methods span from heavy dependence on technology to those that are dependent on simply human activity. This chapter provides an overview of five collection disciplines, the intelligence cycle, and provides a baseline understanding of the realms of intelligence.

### **A. COLLECTION**

The realms of intelligence can be broken down into five defined disciplines based on the collection type. These five disciplines are SIGINT, HUMINT, OSINT, GEOINT, and MASINT. Intelligence organizations at all levels of government have systematic approaches to collect information via one or a combination of different intelligence disciplines.

#### **1. SIGINT**

SIGINT is an overarching discipline that encompasses communication based collection platforms such as telemetry intelligence (TELINT), electronic intelligence (ELINT), and communications intelligence (COMINT). TELINT is the form of

---

<sup>18</sup> S. B. Griffith, *Sun Tzu Art of War* (London, England: Oxford University Press, 1971), 84.

<sup>19</sup> Office of the Chief of Naval Operations, “Naval Intelligence – Naval Doctrine Publication (NDP) 2,” Department of the Navy, <http://www.fas.org/irp/doddir/navy/ndp2.htm> [last accessed 19 March 2007].

collection that detects weapons testing. ELINT is used to detect and gauge the adversary's communication capabilities and is dependent on electronic emissions from Command and Control (C2) platforms used in voice communications; and weapons and radar tracking systems. As a sub-category of SIGINT, COMINT involves the gathering and analysis of messages or voice information resulting from the interception of communications. In the past, there have been concerns from the Federal government regarding the sharing of SIGINT products with law enforcement. In a report to the Senate Select Committee on Intelligence, Lieutenant General Michael Hayden, the former Director of the National Security Agency (NSA), stated that though the NSA provides a significant amount of SIGINT to the law enforcement community, the recipients may not realize the product is SIGINT because the material is handled in various ways to protect the sources and methods of collection. There are several questionable areas respective to handling intelligence. In some scenarios, without knowing the details specific to the methods of collection, a "un- authorized" organization holding of SIGINT products may come close to violating federal intelligence oversight policies.<sup>20</sup>

## **2. HUMINT**

HUMINT, also known as espionage, is a low technology solution to intelligence collection and is considered the oldest form of intelligence collection; however it can be considered the most complicated. As with the other collection types, the employment of HUMINT incorporates weighing the risks associated with detection against the value of the intelligence collected. The risk of detection when using HUMINT is significantly high when compared to the other disciplines. The IC trains its HUMINT resources to look for persons who have valuable intelligence, assess the immediate environment for potential vulnerabilities such as alcoholism, stagnating career, and faltering marriage all of which would leave the target more susceptible to USG proposition.

---

<sup>20</sup> United States Congress. *The Statement for the Record By Lieutenant General Michael V. Hayden Before the Joint Inquiry of The Senate Select Committee on Intelligence and the House permanent Select Committee on Intelligence* (107th Congress, 2nd Session. 17 October 2002), 9.

There are advantages to the integrating HUMINT sources into the collection cycle. HUMINT offers a good source of near real-time intelligence, can provide direct and indirect relations between persons of interest, and more important, it can expose adversarial intentions. It is difficult to extract intentions from the other intelligence disciplines. Because of the high risk associated with using HUMINT, the list of disadvantages is extensive. Amongst the disadvantages include political sensitivity, deception, and the time required to infiltrate the adversary's network or organization of interest.

Gaining a HUMINT agent does not occur over night. Because the risk of counter-terrorism is high, bilateral trust and respect needs to be gained between the collection agent and the intelligence community before valued information flow begins. This applies to agents that are recruited by the IC and individuals that voluntarily approach the USG with information. If an agent is tasked to infiltrate an organization, the ease of penetrating a terrorist group is dependent on the type of network the cell forms.

HUMINT has become a critical element when countering terrorist activity and has proven its weight in gold in both the Global War on Terror (GWOT) and securing the Homeland. Overseas, HUMINT directly contributed to the disruption of European based terrorist cell activities to include a London based Islamist cell experimenting with lethal toxins and militants responsible for the 2003 car bombings in Casablanca.<sup>21</sup> Like their European counterparts, U.S.-based law enforcement organizations have integrated HUMINT into their operations and have tailored the discipline to effectively counter illicit activities local to their respective jurisdictions.

### **3. OSINT**

OSINT consists of anything that can be obtained from free press or is publicly available. There are advantages to integrating OSINT data into the collection cycle. In addition to offering more than one perspective of a specific topic of interest, OSINT

---

<sup>21</sup> William Rosenau and Peter Chalk, "Can We Learn From Others?" RAND Corporation article published in the *Wall Street Journal*, 15 April 2004, <http://www.rand.org/commentary/041504WSJ.html> [last accessed 26 April 2007].

offers an environment where the information is broadcasted in a predictable fashion in the form of subscriptions (magazines, journals) or daily publications (newspapers, news reels). However, as with the other collection types there are disadvantages with OSINT as a source of intelligence. Along with the high volumes of data associated with OSINT that makes it difficult to separate the wheat from the chaff, there is a strong risk of informational bias, deception, or elevated promotion of ideas. Additionally if the information source is of foreign nature, translation may be needed which may skew the original context and could lead to misconception.

With this said, because of the volumes of information associated with OSINT, there stands a requirement for a significant amount of time and a team of skilled analysts to produce useful information. Time and a robust labor force strictly allocated to processing OSINT are two luxuries intelligence agencies, especially at the state and local levels, often do not have.

#### **4. GEOINT**

GEOINT refers to the collected and analyzed geospatial imagery. Within the constructs of the United States IC, the National Geospatial Intelligence Agency (NGA) has the primary responsibility to coordinate the collection, processing, and dissemination of GEOINT data. As with the other intelligence disciplines there are advantages and disadvantages to using GEOINT as a collection source.

As the old saying goes, “a picture says a thousand words.” GEOINT is a discipline that affords decision makers and analysts a familiar view of the area of interest. Firstly, there is a vast selection of commercial geospatial resources available when the task of collecting imagery is assigned. If required, governments can request the commercial geospatial imagery world to obligate their resources to provide valued data. The value of using commercial industry has increased over the past couple of decades for the fact that due to the nature of classification, the data collected by commercial geospatial companies may be released to multi-national and interagency partners.<sup>22</sup>

---

<sup>22</sup> United States Army, *Field Manual 2-0 (FM-2-0): Intelligence*, Headquarters Department of the Army, May 2004. Section 7-8.

Secondly, imagery collection platforms can be used to detect, locate, and identify the activities of the adversary. Through imagery, an analyst can extract information such as equipment type, obstacles, and fortifications which can be used to study the adversary's capabilities.

There are two major disadvantages of GEOINT. The first is the quality of the end product versus the area of interest and its surroundings. Variables such as weather, surrounding terrain, or overgrowing vegetation may hide a target of interest or area at hand. This in turn may hamper GEOINT analysis and the progress of the overall intelligence cycle. The second orients itself around understanding intent, and in a case where GEOINT is used to capture the movement of a person of interest, it is extremely difficult to extract information pertaining to the intent of the activity. In a case like this, the analyst can only speculate when studying the images in hand.

Though GEOINT has been predominantly used by federal-level organizations such as the Department of Defense, it also has been utilized by the authorities at the state and local levels of government. In an interview with Robert Zitz, the Deputy Undersecretary for Preparedness with the Department of Homeland Security, the Military Geospatial Technology documented that through the use of unmanned aviation vehicles (UAV) equipped with imagery equipment, law enforcement agencies has been afforded the ability to extract highly accurate data in a near real time fashion.<sup>23</sup> Zitz also mentioned that GEOINT has proven worth in recent multi-organizational Joint Task Force operations supporting National Special Security Events (NSSE) such as President Ford's funeral and during Super Bowl XLI, GEOINT resources were employed providing the "eye in the sky" perspective of the area of responsibility.

---

<sup>23</sup> Harrison Donnell, "Preparedness Leader: Strengthening Homeland Security through Geospatial Information," *Military Geospatial Technology Online*, [http://www.military-geospatial-technology.com/print\\_article.cfm?DocID=198](http://www.military-geospatial-technology.com/print_article.cfm?DocID=198) [last accessed 27 April 2007].

## **5. MASINT**

Measurement and signature intelligence (MASINT) can be considered the “other” intelligence collection environment.<sup>24</sup> MASINT incorporates technology based sensors and collection methods not defined under SIGINT or IMINT. Information collected from MASINT sources often relate to specific events such as a nuclear explosion or describes idiosyncratic characteristics of a subject of interest through means of radar, acoustic, infrared, or seismic sensors.

In a study conducted by the House of Representatives Permanent Select Committee on Intelligence, it was discovered that through MASINT technology, “specific weapon systems, chemical compositions and material content, and potential adversary’s ability to employ these systems” can be identified.<sup>25</sup> There two disadvantages associated with MASINT. The first relates to the lack of external understanding of the discipline. Because MASINT is unique in nature, the discipline is not well understood by those outside the MASINT community. This lack of understanding leads to the under employment of the discipline. The second orients itself around costs and personnel. MASINT is a science intensive discipline and requires specialized well versed personnel to implement. As stated in the Congressional study, “Such scientists can not typically be professionally developed within the IC (Intelligence Community).”<sup>26</sup> This creates additional requirements for the funding lines needed to accommodate the subject matter experts necessary to make MASINT effective.

### **B. ESSENTIAL ELEMENTS OF INFORMATION**

The intelligence cycle begins with the essential elements of information (EEI), also known as a commander’s critical information requirements (CCIR) or in the terms of laymen: “What information does the decision maker require to make his or her decision?”

---

<sup>24</sup> United States Air Force, *Air Force Pamphlet 14-210: USAF Intelligence Targeting Guide*, Headquarters Department of the Air Force, 1 February 1998, 141.

<sup>25</sup> Committee on Intelligence, “IC2: The Intelligence Community in the 21<sup>st</sup> Century,” US House of Representatives, (104<sup>th</sup> Congress, November 2004), [http://www.fas.org/irp/congress/1996\\_rpt/ic21/ic21007.htm](http://www.fas.org/irp/congress/1996_rpt/ic21/ic21007.htm) [last accessed 23 March 2007].

<sup>26</sup> Ibid.



The EEI may vary between separate operations depending on the threat scenario, the adversary, and the coalition partners at hand. For example, in the sense of a Homeland Security operation, the EEI can relate to the environment immediate to an area of interest (AOI), the effects surrounding the AOI, the threat (adversary action, weather, etc.), and the list of courses of actions available to the adversary. During a disaster consequence management scenario, a decision maker may task his intelligence assets to collect and analyze intelligence pertaining to a city's infrastructure services (utilities, transportation, physical composition) and local culture (religious beliefs, local governments, cultural norms, local population demographics).

### C. INTELLIGENCE CYCLE

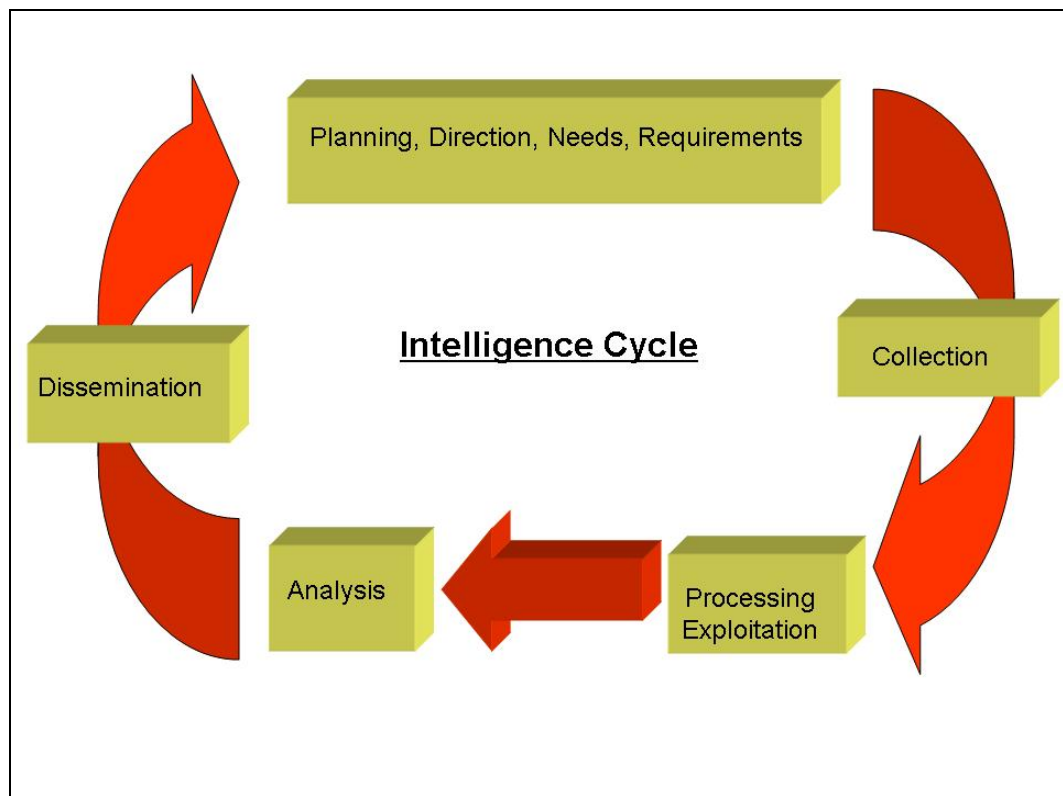


Figure 1. Intelligence Cycle

The intelligence cycle can be broken into five stages: planning, direction, needs, and requirement; the collection; process exploitation; analysis; and dissemination as shown in Figure 1. Each stage will be discussed in this section.

### **1. Planning, Direction, Needs, and Requirement**

The intelligence cycle begins and ends with the operational requirement generated by the user community's respective decision makers. The final product of the intelligence cycle will provide these user community with the information needed to effectively conduct their duties and fulfill their mission requirements. Often the requirements include a set of EEIs respective to the specific mission set.

As the completion stage of the intelligence cycle, the end customer may assess the intelligence product and determine whether or not the data provided meets the original intelligence requirement or fulfills the expanding requirements evolving with the ongoing scenario. If the requirements are not fully met, the intelligence cycle is re-executed and further employed until all requirements have been met or until the operation has come to a close.

### **2. Collection**

Once the requirements are passed, the collection community will employ their respective collection platforms to gather the intelligence relevant to the operation. The collection process is continuous and may continue through the lifecycle of the operation. The various types of collection methods are detailed in Section 1 of this chapter.

### **3. Process Exploitation**

The information collected from the various intelligence disciplines is processed, evaluated for relevance (e.g., separating the wheat from the chaff), and consolidated into an "all source" more manageable package. Once assembled, the package is passed on for analysis.

#### **4. Analysis**

The analysis of information is in a sense, the transformation stage; through analysis, information is transformed from semi-processed information into exploitable intelligence. Analysts take the provided “all source” data and implement a more thorough evaluation process which leads to an intelligence product ready for dissemination to the end user. With this said, there are five categories of a finished intelligence product: current intelligence, estimative intelligence, warning intelligence, research intelligence, and technical intelligence.<sup>27</sup>

##### ***a. Current Intelligence***

Current intelligence incorporates day-to-day events seeking to apprise the user community with ongoing developments respective to global, national, or local area of concern. Current intelligence can cover evolving subjects related to politics, military, and economics. Such reports may be generated and published on a daily, weekly, or monthly basis.

##### ***b. Estimative Intelligence***

Estimative intelligence assesses potential developments that could directly affect the Decision maker’s area of responsibility. Estimative intelligence provides the decision maker an environment where he or she can begin crafting near or long term decisions regarding potential threats or activities.

##### ***c. Warning Intelligence***

Warning intelligence provides the decision maker with a notice of concern. Warning includes recognizing or predicting events that can be detrimental to the decision maker’s area of responsibility. Warning intelligence also incorporates alternative outcomes of the anticipated scenarios and rates each scenario based on probability and impact to the area of concern.

---

<sup>27</sup> United States Intelligence Community, “Intelligence Cycle,” [http://www.intelligence.gov/2-business\\_cycle1.shtml](http://www.intelligence.gov/2-business_cycle1.shtml) [last accessed 26 March 2007].

*d. Research Intelligence*

Research intelligence strengthens both the current and estimative intelligence for the fact that detailed research methods are encompassed when generating an end product. Based on this, all aspects related to elements such as the adversary is published within the intelligence report.

*e. Technical Intelligence*

Technical intelligence is based on the technological resources of the adversary and includes information pertaining to existing technical capabilities, research and development efforts, weapons systems, etc. Technical intelligence is often presented to the user community in media such as detailed system handbooks, white papers, and detailed system assessments and briefs.

*f. Dissemination*

Efficient delivery of intelligence is critical to the success of an operation. Historically dissemination has been implemented by means of hard print and shredded upon receipt and review; however, in the modern age, intelligence reporting can be executed in digital format via email or through the use of web portal technology. This thesis advocates the sharing the information through means of electronic mediums by employing cross-security enclave information technology information sharing platforms.

**D. FUSION**

Intelligence fusion is the process of managing the flow of information or intelligence as it is transformed into a form useful to the decision maker. As shown in the following figure, intelligence fusion is a cyclic process and be broken into four phases: collection and correlation, fusion, further analysis transforming the intelligence into a format that is of value to the end-user, and dissemination.<sup>28</sup> In the events after

---

<sup>28</sup> Homeland Security Advisory Council, "Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion," US Department of Homeland Security, 28 April 2005. 5-7.

dissemination, the end product may have not answered all questions due to an evolving scenario. This causes an environment where the customer may submit additional requests for intelligence collection.

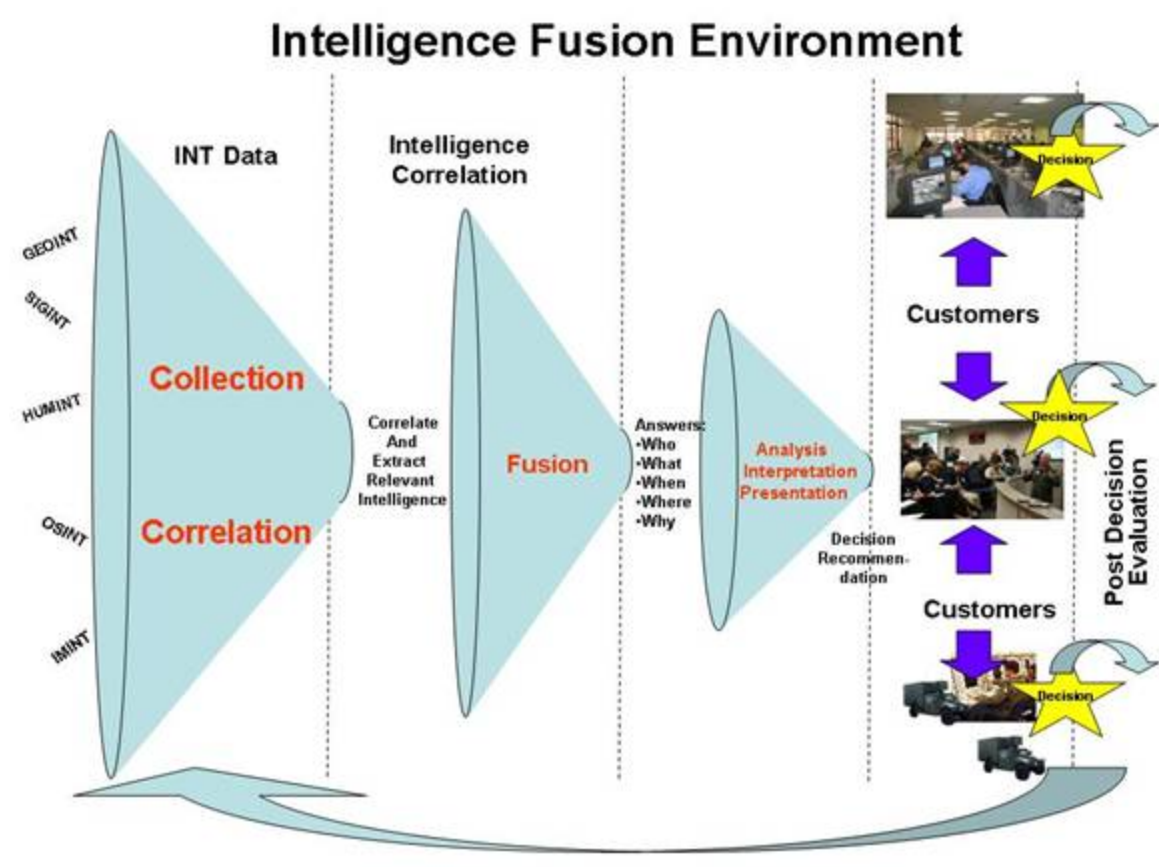


Figure 2. Intelligence fusion environment.

## 1. Collection and Correlation

With the collection phase of the fusion process, EEI requirements are communicated to a collection and correlation cell. Based on the classification level assigned to the incoming data, the information is sorted into defined “piles” and in turn, integrated with intelligence relevant to fulfilling the decision maker’s EEI requirement.

## **2. Fusion**

In the fusion phase, intelligence is taken from the collection agents, blended, and validated for credibility.

## **3. Analyzed**

In the analysis process, subject matter experts are employed to further analyze the processed intelligence. Value added intelligence that can be used in the development of COA respective to risk based prevention, crisis action response, and consequence management.

## **4. Dissemination**

Within the dissemination stage, the processed intelligence is delivered to the end user in a timely manner and may support the decision process. Further, with dissemination, the processed intelligence may be archived for use in future operations. In this phase, feedback may be issued by the end user. Feedback, caused by an updated threat, vulnerability, or effect-based assessment may generate the initiative to reevaluate the originally issued EEI.

The modern concept of correlating intelligence into a manageable and understandable form has been executed through the creation of fusion centers. The fusion center concept, originally engineered to be intelligence clearing houses promoting information sharing between all levels of government, have evolved into a smaller unconnected fusions centers scattered across the nation; a configuration that has defeated the initial intent of information sharing across all enclaves of government. State and local officials have taken action into their own after they received poor quality and quantity of service from the federal level fusion centers. As an example, with the information provided by the federal level fusion centers, Boston Police argues that it often employed its resources chasing down “ghost” targets and often received a list of

critical infrastructure subjects to protect without explanation.<sup>29</sup> Because of this, the trust between federal government and local governments decreased causing an environment where information exchanged between federal, state, and local intelligence organizations, as described in the Homeland Security Act of 2002, is minimal.<sup>30</sup>

## **E. SUMMARY**

In closing, the success of an operation requires knowledge and understanding of the tactics of the enemy in relation to a decision maker's area of responsibility. Though each collection discipline plays a significant role within of the IC, each has its advantages and disadvantages. A seasoned decision maker will not depend on a single collection discipline, but will leverage the available collection capabilities to his or her advantage. In due course, the collected intelligence will distill through the organization's intelligence cycle and, in the end, will contribute to the decision making process.

---

<sup>29</sup> Shane Harris, "Expansion of local intelligence-sharing centers sparks controversy," *Government Executive*, 13 February 2007. [http://www.govexec.com/story\\_page.cfm?articleid=36121](http://www.govexec.com/story_page.cfm?articleid=36121) [last accessed 27 April 2007].

<sup>30</sup> Democratic Staff of the Committee on Homeland Security, "The State of Homeland Security 2006: Annual Report Card," US House of Representatives, 35-37.

THIS PAGE INTENTIONALLY LEFT BLANK



### **III. ANALYSIS OF CURRENT HLS ISSUES – ADAPTIVE ADVERSARIES**

Terrorist organizations currently have the luxury of adapting to the ISR methods targeted against them and, if detected, can revert to using alternative technologies and stand operating procedures in mid-operation reducing their ISR signature.<sup>31-32</sup> To be effective in deterring these organizations from operating within its borders, the USG will literally have to disrupt all realms of command, control, and communications (C3) and establish a robust domestic ISR platform to be fully effective; however, under current policy, this approach will be unlikely because the actions taken to meet the goal may violate the civil liberties of the common law abiding citizen. This thesis argues that individuals and groups of interest (e.g., radical fundamentalists, individuals with ties to known terrorist cells, international terrorist groups) have capitalized on the fact. This chapter will discuss the adaptive techniques that such groups exploit when operating within the United States to include operations and implemented technology.

#### **A. TERRORIST CELL OPERATIONS: ADAPTIVE COMMUNICATIONS AND COLLABORATION**

Whether we are turning on a light, opening the refrigerator, talking to Aunt Sue who lives a hundred miles away, or driving a car the modern world has been shaped by technologies designed in the nineteenth and twentieth centuries. Further advancements in technology have diminished the barriers associated with time and space causing modern civilization to become reliant on instant access to the information super-highway; ease and speed in computation; and lighter and smaller portable communication devices. Groups with ties to Al Qaeda residing within the United States are not any different. These groups have adopted technology into their day-to-day operations; they also understand that the USG has become limited in its ability to monitor domestic

---

<sup>31</sup> United States Department of State, “Funding Terror Becoming Costlier, Riskier, U.S. Official Says,” <http://usinfo.state.gov/ei/Archive/2004/Sep/30-755521.html> [last accessed 28 April 2007].

<sup>32</sup> Gordon Corera, “Al-Qaeda undimmed by sanctions,” British Broadcasting Company, 27 August 2004, <http://news.bbc.co.uk/1/hi/world/americas/3606384.stm> [last accessed 28 April 2007].

communications. In 2005, it was publicly announced that a federal court revoked the USG's authority to freely monitor communications within the United States;<sup>33</sup> however, in 2007 it was proposed that amendments to the Foreign Intelligence Surveillance Act (FISA) be addressed in an effort to modernize the policies referencing surveillance.<sup>34</sup> The proposed amendments authorize the re-instatement of electronic surveillance as long as there is a defined oversight system in place.

Further, in their past campaigns against the United States, terrorist groups have shown that they are well versed in a broad range of communications processes such as the low-tech conventional "snail-mail" system and high frequency (HF) radio to the more modern email, cell phones, web development, encryption, and steganography.<sup>35</sup> Based on the knowledge that their activities are painted on the USG's radar, terrorist groups have the option of exchanging their tools of the trade in mid-operation; therefore, making it extremely difficult for the USG to detect and continuously track terrorist planning and coordination activities.

## **B. TECHNOLOGY**

Because technology is readily available in the commercial market; relatively low in cost and reliable, terrorist groups have adopted methods of incorporating technology into their day-to-day operations and planning cycles. The following cases illustrate how technology has been integrated into the operating procedures of terrorist organizations:

### **1. Mail Systems**

When the mail system and terrorism are used in the same sentence, one pictures the "Unabomber" Theodore Kaczynski. Kaczynski, a former math professor, used the mail system to his advantage, and, in at least sixteen cases, mailed letter bombs to his

---

<sup>33</sup> Mary Lou Seymour, "Fed court limits power to monitor cell phones," *Bloomberg*, 29 November 2005, <http://www.rationalreview.com/content/4416> [last accessed 17 April 2007].

<sup>34</sup> American Bar Association, "Anti-Terrorism and Preservation of Civil Liberties: Electronic Surveillance Activities in the 109<sup>th</sup> Congress," American Bar Association, [http://www.abanet.org/poladv/priorities/elec\\_surveill/109th\\_elecsurv.pdf](http://www.abanet.org/poladv/priorities/elec_surveill/109th_elecsurv.pdf) [last accessed 28 April 2007].

<sup>35</sup> Sharon Gaudin, "The Terrorist Network," *Network World*, 26 November, 2001, <http://www.networkworld.com> [last accessed 16 February 2007].

victims, killing three people and injuring twenty-three others between 1978 and 1995.<sup>36</sup><sup>37</sup> The US Postal Service (USPS) and private parcel carriers (UPS, DHL, FedEx) combined create one of the world's largest postal systems in the world. The USPS alone handles over 200 billion letters per year.<sup>38</sup> However, it is one of the least secure systems because of the fact that it remains a system based on speed, low cost, trust, freedom, and privacy.<sup>39</sup> If a sender wishes to remain anonymous, he or she has the option of either excluding a return address or, if the package is sent via a postal box, can use a false return address. This leaves the system a favored medium for terrorist activity because the sender can not be verified or identified beyond a return address.<sup>40</sup> Once in the system, a piece of mail or parcel goes through up to twenty-six separate steps in the process of collection, processing, and delivery of the package. Security measure additions at each of the stage of the process can significantly increase the door-to-door time and the cost of postage. Based on this, terrorist groups can capitalize on the openness of the mail system to their advantage and use the environment to collaborate and transport materials with minimal chance of detection.

## **2 Amateur Radio**

Amateur radio, also known as HAM Radio, is a social and public service hobby that spans the entire world. In the late nineteenth century, Guglielmo Marchese Marconi circumvented the limitations of the hard wire telegraph and created the wireless radio technology. This technology is currently used in emergency management and for communication during the deployment of military assets. Modern terrorist groups, such as Al Qaeda, have integrated amateur radio as a median to pass information and have

---

<sup>36</sup> Associated Press, "Kaczynski Pleads not guilty to Unabomber Charges," *USA Today*, 10 December 2006, <http://www.usatoday.com/news/index/una77.htm>. [last accessed 24 February 2007].

<sup>37</sup> Court TV Online – The Unabomber, <http://www.courtTV.com/trials/unabomber/bombings.html> [last accessed 21 January 2007].

<sup>38</sup> "Postal Terrorism White Paper," Peter C. Lytle, The Business Development Group, 15 October 2001, <http://www.bdgpartners.com/postalterrorism.htm> [last accessed 25 February 2007].

<sup>39</sup> Ibid.

<sup>40</sup> Ibid.

adopted HF (3-30MHz) as a primary frequency band. With HF, a terrorist organization in Iraq or Afghanistan can talk to or email terrorist support groups embedded within the United States with nothing more than a simple transceiver, a car battery, and an equally simple wire antenna. Because of the mobility aspects, this configuration leaves the terrorist organization less vulnerable to tracking than using modern telecom architectures such as cell-phone repeater antenna arrays, permanent stationed satellite ground stations, and conventional land-line telephones.

### **3. Cell Phones**

Cell phones have become a day-to-day necessity. In less than two decades, the cell phone has evolved from a communications tool of the socially elite to being a low cost personal item. It is said that, mobile phones now outnumber land-line telephones in some places, with most adults and many children now owning mobile phones.<sup>41</sup>

Cell phones have become a tool of the trade for terrorist groups. They use the technology to assist direct collaboration and planning while enhancing real time situational awareness.<sup>42</sup> Disposable cell phones do not require the purchaser to produce a credit card or sign a contract, leaving very little evidence for law enforcement. According to Jack Cloonan, a former FBI official, “there is very little audit trail assigned to this phone”<sup>43</sup> Disposable cell phone technology helps create an environment where terrorist organizations are less vulnerable to radio frequency (RF) tracking than they would be if they used modern telecom architectures such as fixed cell-phones and conventional land-line telephones.

---

<sup>41</sup> Central Intelligence Agency web site, <http://www.cia.gov/cia/publications/factbook/geos/uk.html#Comm> [last accessed 29 December 2006].

<sup>42</sup> Ron Suskind, “The Untold Story of Al-Qaeda’s plot to Attack the Subways,” Time Magazine, 26 June 2006, <http://www.time.com/time/magazine/article/0,9171,1205478,00.html> [last accessed 26 February 2007].

<sup>43</sup> Ross and Eposito, “Surge in Sale of Disposable Cell Phones May Have Terror Link,” ABC News, 12 January 2006. <http://abcnews.go.com/WNT/Investigation/story?id=1499905> [last accessed 24 February 2007].

#### **4. Encryption**

Encryption software is easy to obtain providing an advantage for terrorist groups. When and if a message is intercepted, authorities have to guess which ciphering algorithm was used prior to the extraction of the message. Terrorist groups have also added steganography as an additional layer of security allowing for data to be transmitted in the clear. Steganography is the embedding of images, text, audio files, or a combination of each within another media form, for example, normally digitized pictures or text. If the host image is large enough, the impact of embedding files is virtually undetectable via the human senses. Because of the fact that it is difficult for intelligence collection resources to keep track of all the images floating around on the internet, terrorist groups reserve the option to use steganography as a supplement to encryption or when encryption devices are not available.

#### **5. Internet**

The lack of regulation, vast audiences, and the ease of access has made the internet a choice tool for modern terrorism. From the information gathered after the September 11 attacks, it was discovered that Al Qaeda relied heavily on the internet in the planning process.<sup>44</sup> The post-9-11 Internet still offers the same freedom and terrorist organizations of today exploit the fact in their activities. Terrorist groups use the Internet to gather information related to targets of interest, real time news, Government counter-terrorism practices potential targets, and “how-to” manuals defining methods of attack. To remain unidentified, terrorist organizations have the option of collaborating using free web based email accounts (Yahoo, MSN, and Google) and computers provided by public establishments such as libraries and Internet cafés.

---

<sup>44</sup> Steven Cherry, “Terror Goes Online,” *IEEE Spectrum*, <http://www.spectrum.ieee.org/pring/2472> [last accessed 29 December 2006].

As for operational planning, also known as Cyber planning<sup>45</sup>, terrorist groups have avoided detection by capitalizing on the flexible characteristics of the internet to their advantage. In the form of web pages that contain dynamic content (e.g., images, text, form fields, etc) and that can be produced on-the-fly, terrorist groups use the internet for the dissemination and collection of information. Terrorist groups have full control of their respective web pages by defining the dynamics of a web-page lifecycle (i.e., when the page is inserted and removed from the internet) passing command and control information to its operatives with little chance of detection. The life-cycle of a dynamic web page can last as little as a couple of hours to several days. As an example, an end user, provided a timeline, can access a dynamic web-page and download several steganographed images to a local workstation. Assuming that the end user or sleeper cell has deciphering tools in hand, the hidden message can be extracted and operational action can be taken. The color, size, and placement of web parts on a web page, such as pictures and text, can also relay hidden information to the end user (e.g., a web page host header text that is red, in font size 19, and placed on the right of center). The end user can interpret the message as “move the sleeper cell into attack position no later than 1900 on a predetermined date.”

The difficulty of detecting terrorist activities increases as the communication mediums available to terrorist cells expands. This section introduced only a couple technological tools terrorist groups use to their advantage and will continue to evade the monitoring activity of authorities. Terrorist groups have the luxury of using any one or a combination of the mentioned technologies above in their planning of the next 11 September 2001 like attack. How does the USG gain an advantage in the technological cat and mouse game? As a possible start, in addition to modifying current laws, the USG should increase its efforts in better understanding of the tactics, techniques, and procedures of terrorist organizations in given scenarios.

---

<sup>45</sup> Timothy L. Thomas, “Al Qaeda and the Internet: The Danger of ‘Cyberplanning,’” *Parameters – US Army War College Quarterly*, Spring 2003, <http://www.carlisle.army.mil.usawc/Parameters/03spring/thomas.htm> [last accessed 29 December 2006].

### **C. HUMAN SMUGGLING – ILLEGAL IMMIGRATION: LEVERAGING CLANDESTINE ORGANIZATIONS**

Over the past couple decades, human smuggling has become an extremely profitable business. Along the U.S.-Mexico border alone, human smuggling rings gross around \$4.75 billion a year.<sup>46</sup> Because of the increased U.S. effort to secure its borders, it has become more difficult to cross the borders. Because of this, the smaller organizations that smuggled one or two persons in the past, have joined forces and have evolved into a well-structured organized crime network. Based on the increased U.S. vigilance on its borders, in order to remain undetected, these human smuggling networks are forced to search for more remote routes and to become more creative in their ways to transport their “clienteles”; as a result, the cost for service has increased from the fee of \$50-100 per trip (1980) to \$1000-2000 (2003).<sup>47</sup> Though this value may be a large sum for a common Latin American émigré searching for the “American Dream,” this amount is not significant to well funded terrorist organizations. Terrorist groups have taken advantage of the porous borders of the United States and, as a form of evasion have incorporated illegal migration into their workforce logistics operations. As a result of the contravention of smuggling rings, it has been revealed that terrorist cells, through the abundant routes used by human smugglers that specialize in moving Middle Eastern and Islamist clientele, have successfully moved personnel into the United States potentially increasing the personnel strength of their sleeper cells.<sup>48</sup>

One transportation means used by terrorist groups to move personnel is air travel. Because of the current tactics, techniques, and procedures (TTP) of its air travel security personnel, U.S. authorities have tended to direct their focus on the travelers traveling to and from nations of predominantly Islamic influence. Terrorist cells have learned, understand, and have adapted to these procedures and have employed South and Central

---

<sup>46</sup> Kris Axtman, “Changing landscape of an underground trade,” *The Christian Science Monitor*, 17 July 2003, <http://csmonitor.com/2003/0717/p03s01-usgn.htm> [last accessed 20 February 2007].

<sup>47</sup> Ibid.

<sup>48</sup> Davick Services, “Increasing Coordination Between Mexican Drug Cartels, Human Smuggling Networks, and U.S. Based Gangs,” *News For Public Officials Newsletter*, February 2007, [http://www.davickservices.com/line\)in\\_sand3.htm](http://www.davickservices.com/line)in_sand3.htm) [last accessed 20 February 2007].

American based human smuggling rings.<sup>49</sup> Upon arriving to these countries, the hired smuggling ring will provide the “traveler” with a new identity and travel documents that appear to be legitimate. By entering the U.S. by way of nations such as Argentina and Peru, such terrorists will tend to be less scrutinized than if they were traveling from Muslim based countries.<sup>50</sup>

Occasionally, the organized human smuggling rings associated with moving immigrants via forged documents and air travel are intercepted by the intelligence and law enforcement communities joined to protect the United States. Following their discovery, these rings will often face the repercussions associated with their illegal activity and will tend to research other immigration avenues with less of a significant profile. Rather than assuming the risk of detection by flying into the United States from the Americas, terrorist groups are assumed to be taking advantage of the nation’s porous borders and overworked Border Patrol agents, and have added the movement of personnel into the United States by means of ground transportation and human smugglers to their portfolio of adaptive techniques.

Adnan Shukrijumah, suspected Al Qaeda lieutenant, has been known meet with transnational gangs such as the El Salvador based Mara Salvatrucha, also known as MS-13, to potentially recruit the organization’s assistance in moving personnel northward from a point of origin in South or Central America into the United States.<sup>51</sup> MS-13, a group that does not have an alliance to any nation state is one of many human smuggling groups that specialize in assisting the masses of illegal immigrants on their northbound trek.<sup>52</sup> One of the group’s favored means of transportation is the train routes that span along both Mexican coasts. Historically, these routes have been the primary method of

---

<sup>49</sup> Thomas Davidson II, “Terrorism and Human Smuggling Rings in South and Central America,” *Terrorism Monitor*, Volume III, Issue 22, 17 November 2005, 6.

<sup>50</sup> *Ibid.*, 6.

<sup>51</sup> Middle American News, “Al Qaeda Seeks Ties to Latin Gangs,” *Middle American NewsOnline*, <http://www.manews.org/1104alqaeda.html> [21 February 2007].

<sup>52</sup> Thomas Davidson II, “Terrorism and Human Smuggling Rings in South and Central America,” *Terrorism Monitor*, Volume III, Issue 22, 17 November 2005, 8.



travel for illegal immigrants on their journey to the United States.<sup>53</sup> Once the individuals reach a designated Mexico border town such as Matamoros, Mexico, the travelers will join an illegal immigrant group and will move across the border with the assistance of an assigned coyote. Once cleared of all debt to the smuggling chain, the individual will then assimilate into the communities of the United States and potentially join the ranks of Al Qaeda supporters residing in the United States.

#### **D. SUMMARY**

The United States historically has been successful in battlefield campaigns where tactics of the enemy were well known and understood; however, the United States is fighting a complexly networked adversary and does not have the luxury of applying the lessons learned from past campaigns against conventional enemies. Unlike historical U.S. adversaries, the modern foe plans and operates under the shadows of the suburbs and big cities of the United States only to raise its head when the attack occurs. With this being said, though policies concerning domestic intelligence have changed since the modern concept of Homeland Security began, more revision is required if the enemy is to be defeated. Five years after the tragic events of the 11 September 2001, the United States continues to chase its enemy with technological advancements. In doing so, the terrorist cells have grown to understand the counter-terrorism methods of operations used against them and will continue to effectively plan for the next attack while minimizing the organizations' signatures that are vulnerable to ISR techniques. In our efforts to defeat the modern adversary, the decision makers of the United States should re-assess current domestic intelligence capabilities and produce a more effective collection strategy that yields improved ISR methods.

---

<sup>53</sup> Davidson II, "Terrorism and Human Smuggling Rings," 7.

THIS PAGE INTENTIONALLY LEFT BLANK

## IV. ANALYSIS OF COMMUNITIES

As a result of the multiple HLS driven exercise scenarios oriented around potential terrorist cells covertly operating within the nation's smaller communities and municipalities, issues regarding intelligence processes and counter-terrorism strategies have often been revealed and discussed within the offices of our nation's decision makers since 11 September 2001.<sup>54</sup> Further, in contrast to popular belief, it can be assumed that terrorist cells are not only operating and planning abroad, but may be collaborating with terrorist support groups operating in the nations large metropolitan areas and smaller communities dispersed across the heartland.<sup>55</sup> In December of 2001, it was brought to the attention of the USG that an alleged sleeper cell was operating in the small California agriculture community of Lodi. In this setting, Naseem Khan, a Pakistani immigrant, approached authorities and volunteered information pertaining to Ayman al Zawahiri, al Qaeda's number two, visiting the local mosque and the fact that the resident imam, Mohammed Adil Khan, was linked to radical Islamist organizations in Pakistan.<sup>56</sup> Because of further intelligence gathering activities, it was discovered that there were several individuals residing in the area of Lodi that may have been operating under the al Qaeda jihad movement.

In another case, the Mercer County Sheriff Department implemented a procedure to check for identifications of not only the driver of a vehicle, but also of the passengers as part of their efforts to detect potential illegal activities and minimize human trafficking through its area of responsibility.<sup>57</sup> As a result, in March 2006, Pascual Elias Diego-

---

<sup>54</sup> This thesis is not expressing that all spending directed to securing the nation has not gone to waste; however, it is addressing the fact that various resources required to detect malicious terrorist activities internal to its borders may be unreadily available.

<sup>55</sup> Alexandra Marks, "Are terrorist cells still in the US?" *The Christian Science Monitor*, 10 August 2005. <http://www.csmonitor.com/2005/0810/p02s01-ussc.html> [last accessed 10 July 2007].

<sup>56</sup> Lowel Bergman, "The Enemy Within," Transcripts from the Public Broadcasting System (PBS) Frontline, 10 October 2006, <http://www.pbs.gov/wgbh/pages/frontline/enemywithin/etc/script.html> [last accessed 26 January 2007].

<sup>57</sup> Mark Houser, "Illegal Immigration face crackdown in Pennsylvania," *Pittsburgh Tribune – Review*, 23 July 2006.

Pablo was taken into custody by Pennsylvania State Patrol for human trafficking after a patrol officer became suspicious during a routine traffic stop. Diego-Pablo was pulled over for simply speeding and only after a discussion with patrol officer was it discovered that he was transporting undocumented riders across the nation. The passengers of Mr. Diego-Pablo were assumed to be harmless migrants searching for the “American Dream,” were taken into custody, and were processed through the respective HLS channels; however, there is a great threat that terrorist cells are exploiting similar immigration channels to move their resources into the nation undetected.<sup>58</sup>

Based on the two described cases, local law enforcement resources have increasingly become significant assets in the nation’s HLS efforts.<sup>59</sup> It can be assumed that because of their interactions with their respective communities, these local law enforcement assets have the capability to detect minor changes and abnormalities within their areas of responsibilities. An intelligence environment with vested local community resources, also known as community lead policing, will create an atmosphere where intelligence collection is enhanced thereby escalating the overall effectiveness of HLS operations. A robust domestic intelligence collection environment will contribute to reducing illegal immigration and may contribute to the future discovery of terrorist sleeper cells residing in the United States.

There is a wide range of opinions regarding the extent of terrorist activities occurring within the United States. On one of the spectrum, the individuals that debate that because very few terrorist cells have been detected within the U.S., the United States is secure and the USG is effective in its HLS efforts. Others that reside on the other end of the opinion spectrum argue the U.S. remains un-secure and there stands a great risk that U.S. based terrorist cells remain undetected and are actively planning the next attack. Regardless of the partisanship, there is a concurrence that government action towards deterring terrorist activities does not stop at the level of international policy, but also

---

<sup>58</sup> Steven A. Camarota, “Census Bureau: Over 100,000 Illegal Aliens from the Middle East,” Center for Immigration Studies, 22 January 2002 <http://www.cis.org/articles/2001/censusillegalsme.html> [last accessed 11 July 2007].

<sup>59</sup> RAND Corporation, *When Terrorism Hits Home – How Prepared Are State and Local Law Enforcement?* (Santa Monica, CA: RAND Corporation, 2004), 28.

expands to the various governments residing internal to the borders of the United States. By the nature of geographic locality, individual budgets, and available resources, it is expected that the governments of respective communities, counties, and townships local to the United States have a diverse range of approaches when contributing their piece to securing the homeland. The demographics of the communities surveyed in the research and analysis phase of this thesis can be described as follows:

- Budget range: \$3.5M to \$600M
- Surface area range: 9 to 1,103 sq. miles
- Populations range: 15,500 to 1.3M citizens

#### **A. TONAWANDA, NY**

After the Tonawanda Board of Commissioners discovered that the township housed seven of the top twenty Erie County critical infrastructure targets assessed by the Department of Homeland Security, it took action to enhance its security infrastructure. Like most small communities across the nation, the Township of Tonawanda does not have the budgetary and personnel resources to dedicate assets to specific tasks and duties such as intelligence analysis or collection; yet, the town has many available resources that could be used to establish and maintain community policing. Tonawanda recognized this trait and instituted an environment where its citizens have the ability to contribute to securing their community eliminating some of the issues and conflicts associated with being understaffed.

As part of its effort, the Township government adopted the Responding Efficiently and Aggressively to Counter Terrorism (REACT), a program originally designed to raise the terrorist activity awareness level of patrol officers by the means of integrating vital community resources into the local Homeland Security effort.<sup>60</sup> Rather than specifically allocating one-hundred percent of their HLS training on the local law

---

<sup>60</sup> Interview with Dennis Carson, Town of Tonawanda Police Department, 14 February 2007.

enforcement community, the Tonawanda Township council distributed its training program educating not only its law enforcement community, but also its water department personnel, building inspectors, emergency medical services (EMS), and local sanitation workers.

The Township recognized that these resources, like their law enforcement patrol officer counterparts, integrate themselves in the community everyday and may notice abnormalities respective to their area of operation. This program has since evolved to include the common citizens of community through Neighborhood Watch Groups and Community Emergency Response Teams (CERT). Because of its limited revenue and its mentioned efforts, the Township of Tonawanda has very little vested in technology-based systems used in collecting and analyzing intelligence.

## **B. VOLUSIA COUNTY, FLORIDA**

Volusia County, Florida, has taken a different approach in securing its area of responsibility. The county is more focused on restructuring its organizational operating procedures and technology than enlisting its resident population as peripherals of its HLS network.<sup>61</sup> Prior to 11 September 2001, an infrastructure consisting of counterterrorism policies and procedures was literally nonexistent with the organization. Since then, rather than focus on including the community in its HLS efforts like Tonawanda, the county adopted a plan to re-structure its organization and formed a unit which specifically participates in HLS related investigations, exercises, operations, and policy development. Unlike the Township of Tonawanda, Volusia County found importance in integrating technology into its intelligence collection and analysis efforts. Volusia County invested in the development of an intelligence database to store raw and processed intelligence. The database, proprietary to Tiburon Incorporated, allows for department employees to access data while resident to the halls of the department or external if the user is mobile while on patrol.

---

<sup>61</sup> Interview with Mike Coffin, Volusia County Sheriff's Office, 10 February 2007.

### **C. NASSAU COUNTY, NEW YORK**

Nassau County, New York, is the most populated of the four communities discussed in this paper. Nassau County, a county with a consolidated budget of \$2.4B,<sup>62</sup> appeared to have consolidated the strategies of Batavia, NY; Tonawanda, NY; and Volusia County in its effort to establish a homeland security posture. Nassau County not only has employed an effort referred to as the Security/Police Information Network (SPIN), a successful community focused program that integrates local commercially owned security entities into its information sharing environment, but also invests in technologies and has restructured its organization and operating procedures to better enhance communications with its staff in addition to state and federal intelligence agencies. The Nassau County government created the Nassau County Regional Intelligence Center (NRIC); a center that often interacts with state and federal Joint Terrorist Task Forces (JTTF) while maintaining information sharing relationships with law enforcement agencies of all government levels to include Interpol and U.S. Military Intelligence organizations.

### **D. CITY OF BATAVIA, NEW YORK**

Batavia, New York, is the least populated and smallest of the four communities discussed in this thesis. Batavia, a city with a consolidated budget of \$22.4M,<sup>63</sup> appeared to have adopted the strategies typical of a small community in its effort to establish a homeland security posture. Like Tonawanda, the Batavia Police Department lacks the budget (\$3.5M) and staffing (thirty-three sworn officers, zero volunteers) to dedicate its personnel to specific tasks and duties such as intelligence analysis, intelligence collection, or information dissemination. As a result, the Batavia PD has turned to depending on external law enforcement based agencies such as the NY State Information Center (NYSIC) and community organizations to fill the internal resource void.

---

<sup>62</sup> Associated Press, "My Agitator's Agitator," [newsday.com](http://newsday.com), 15 June 2006, [http://weblogs.newsday.com/news/local/longisland/politics/blog/2006/06/my\\_agitators\\_agitator.html](http://weblogs.newsday.com/news/local/longisland/politics/blog/2006/06/my_agitators_agitator.html) [last accessed 5 March 2007].

<sup>63</sup> City of Batavia Web site, [http://www.batavianewyork.com/new\\_forms/Batavia%20Facts3.pdf](http://www.batavianewyork.com/new_forms/Batavia%20Facts3.pdf) [last accessed 6 June 2007].

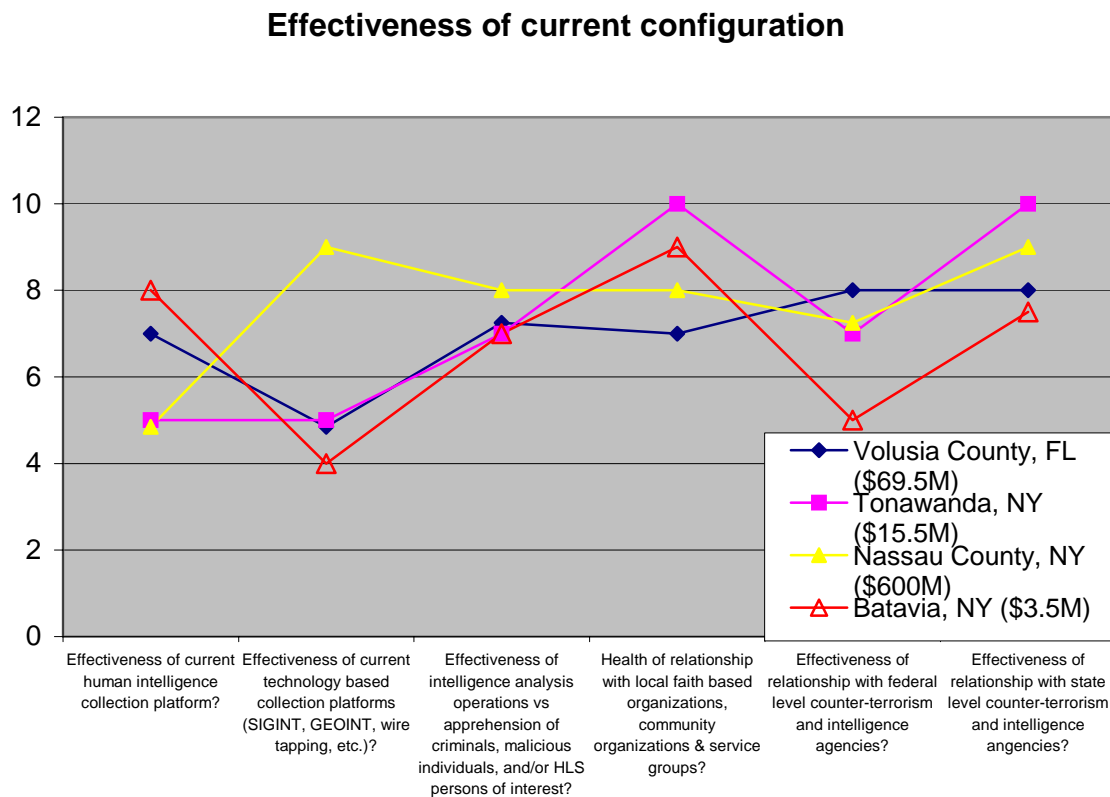


Figure 3. Effectiveness of current configuration

Additionally, like Nassau County, the Batavia decision makers have also successfully adopted a SPIN like program integrating commercially owned security resources into its information- sharing environment as a solution towards filling its personnel void. Though the Batavia City government recognizes information sharing as a critical requirement in doing its part in securing the homeland, it has refrained from investing in advanced technologies supporting intelligence dissemination and collection. The decision to direct funding to other organizational priorities is partly due to the city's limited budget.

As stated in the introduction, this thesis addresses the current collection and information sharing structures of local communities. In the process to collect information to support research, a survey was sent to the predominant law enforcement agency of each community. The premise of this survey was to assess how each



enforcement agency viewed the effectiveness of their intelligence capabilities. Based on the responses, the chart depicted in Figure 3 was generated and used for analysis. The measurement of effectiveness can be broken down as such: 10 – Exceeds requirements; 7 – Meets requirements; 5 – Needs Improvement; 3 – Needs significant revision; 1 – Fails, is not effective in supporting the nation’s HLS efforts. Based on the provided feedback, the conclusions were drawn:

- 1) Human and Technology Intelligence based Collection — A community with a significant budget, such as Nassau County, can afford to invest in technology and may depend less on human based collection. In response to the survey, Nassau County stated that they actively utilize technology in their intelligence collection efforts as it has proven to be effective for intelligence gathering. Countering this, communities with less of a budget, like Tonawanda and Batavia, have answered that they have minimal experience with technology-based collection systems and depend on external sources (e.g., state or regional fusion centers) for information acquired by means of technology.

With the notion that the studied organizations have executed effective work force assessments and the mitigated the issues associated with the findings, it can be assumed that each organization that has sufficient staffing and budget will freely seek a robust technology intelligence collection, analysis, and dissemination environment while those with less, will adapt to their resource conditions and turn to low technology alternatives..

- 2) Intelligence analysis operations versus apprehension of criminals, malicious individuals, and/or HLS persons of interest: Local law enforcement communities, regardless of size and revenue, have confidence in their intelligence cycle and effectively employ intelligence in their efforts to survey the community for illegal activities and when taking crime off the street as shown in Figure 3. In their survey responses, all four municipalities stated that their current intelligence analysis operations either meets or exceeds requirements.
- 3) Relationship with local faith based organizations, community organizations & service groups: Through federal grant programs communities have access to the

funds needed to enhance their staffing, pay overtime to existing personnel, and procuring equipment and technology related to basic law enforcement functions.<sup>64</sup> However through the distributed survey, it was discovered that, at times, the funds are not readily available for the smaller communities spread across the nation. To fill the void smaller communities may turn to local organizations (churches, homeowners association, and neighborhood watch groups) to support the local law enforcement agency. The support may come in form of volunteers augmenting office administrative staff, volunteers filling the role of ride-along patrol officers, or neighborhood watch groups monitoring activities in their respective areas of responsibility. In turn, the sense of community pride increases while the relationship between local government and citizens is enhanced.

- 4) Relationship with state and federal level counter-terrorism and intelligence agencies: Regardless of revenue and size, communities have developed strong relationships with both state level counter-terrorism and intelligence agencies; however, there were mixed results when it comes to relationships with federal agencies. Based on the survey results, one can conclude that community size may contribute to the strength of relationships between local and federal intelligence organizations. Since 11 September 2001, it has been discussed at all levels of government that strong inter agency relationships are critical to the defense of this nation.<sup>65</sup> Many local and state organization tasked with enforcing domestic security have taken the message to heart and established coalitions designed to secure their areas of responsibilities. From a strategic planning standpoint, states such as Florida have created regional domestic security task forces that meet regularly, exercise together, and jointly execute domestic security related operations.<sup>66</sup>

---

<sup>64</sup> Lynn Bauer, "Local Law Enforcement Block Grant Program, 1996-2004," *US Department of Justice - Bureau of Justice Statistics Technical Report NCJ 203096*, September 2004, 3.

<sup>65</sup> Daniel W. Fisk, "Top Priorities For Improving Intelligence and Law Enforcement Capabilities," *A Report of the Working Group on Intelligence and Law Enforcement Capabilities* (Washington DC: The Heritage Foundation, 2002), 53-55.

<sup>66</sup> Florida Domestic Security Oversight Council, "Domestic Security in Florida: Making Florida Safer," *2005 Domestic Security Annual Report*, December 2005, 5.

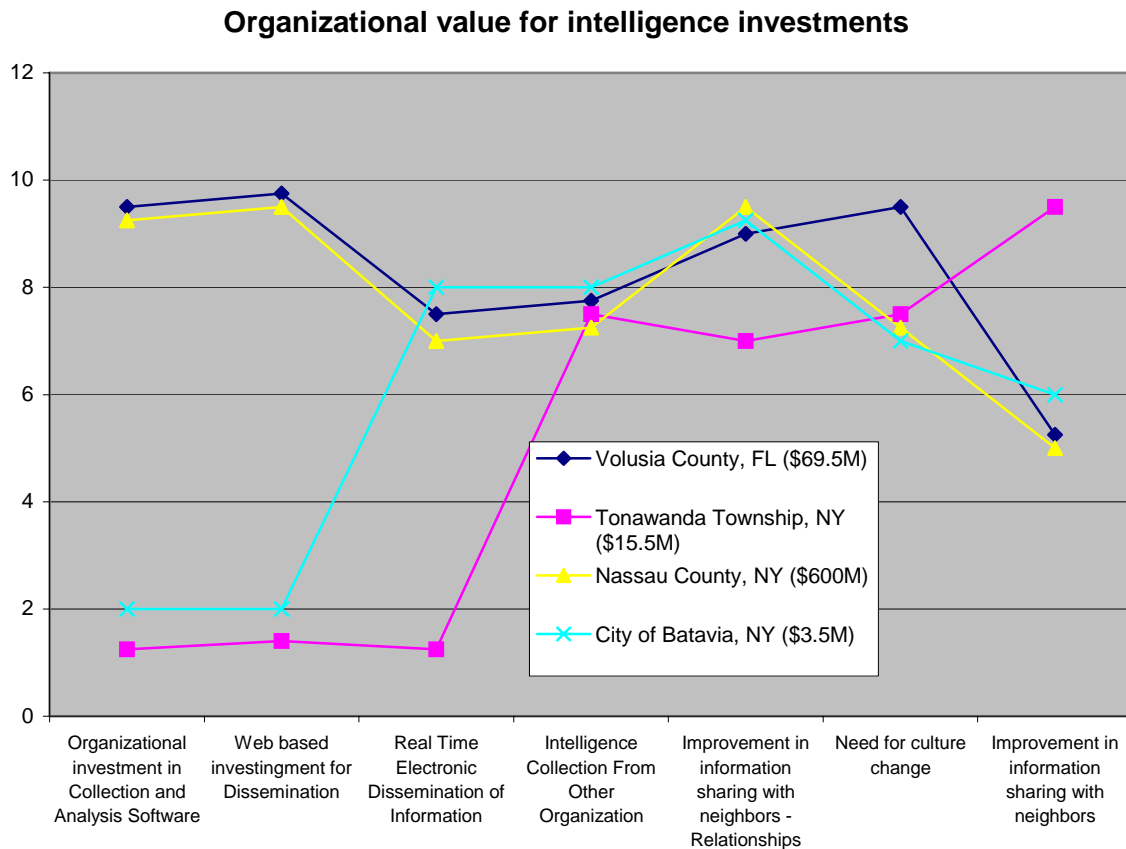


Figure 4. Organizational value for intelligence investments.

A second survey was designed to measure how organizations value critical elements of Homeland Security based their respective investments. This survey was also sent to Volusia County, Tonawanda Township, Nassau County, and Batavia. The result of the survey is reflected in Figure 4 with 10 representing a “HIGH” value (organization believes the element is significant to the HLS effort) while 1 equates to “LOW” (organization believes the elements is not significant to HLS effort). Based on the results of the survey, the following three conclusions were established:<sup>67</sup>

<sup>67</sup> The conclusions were drawn based on the short answer questions issued to the participating organization. As an example, if the organization has implemented an extensive information-sharing environment based on web interfaces, it can be assumed that the organization has placed high value in web-based technologies.

All four communities have investments, some more heavily than the others, in a form of technology to assist in intelligence collection, analysis, correlation and dissemination. The survey results show that the Counties of Nassau and Volusia, the two counties with larger budgets, both place a higher value on technology based intelligence capabilities than the communities of Batavia and Tonawanda. Though the survey results of four of the many thousands of communities disbursed across the nation does not paint the whole picture, a noticeable trend has formed. Based on the survey results, it can be concluded that communities with limited budget have invested their resources (time and work force) in establishing human relationships than modern technology to process intelligence into a useable format.

All four surveyed communities stated that they desire improvements in information sharing and culture change. Further, taking the lessons learned from post-11 September 2001 assessments versus issues such as information sharing challenges, the smaller organizations made mention that they have adapted to working with very little, with respect to available resources, to secure their areas of responsibility. Based on the discussions with the surveyed local law enforcement agencies, it could be concluded that communities, regardless of size and revenue, believe that culture change is critical in the evolution of organizations charged to secure the homeland.

As the two more populous and profitable of the four surveyed communities, Nassau and Volusia Counties placed moderate importance towards the need to improve information sharing capabilities with external organizations while the remaining two placed higher worth in this field. Based on the mixed survey results, it was difficult to draw a defined conclusion. However, it is understood that communities, regardless of size and revenue, believe that information sharing with other organizations is critical in securing their areas of responsibility and desire change in existing processes when applicable.

## **E. SUMMARY**

In summary based on the direct affects of 11 September 2001, all four communities have the common interest of detecting, deterring, and defeating the current

adversary. Like governments at an international level, these local governments have created localized strategies based on their geographic locality, individual budgets, and available resources. If these resources were to be combined into a unified network, they will enhance their value in the value in the realms of Homeland Security.

THIS PAGE INTENTIONALLY LEFT BLANK

## V. DISCUSSION

Law enforcement resources local to our communities are critical assets to securing the nation and are valued partners in the realms of intelligence collection and dissemination.<sup>68</sup> Through training, patrol officers in our larger metropolitans (e.g., New York City, Boston, and Los Angeles) have gained the knowledge and capability to detect terrorist related malicious activities and share their intelligence with other members of the national intelligence community through state and regional intelligence fusion centers. Under the same construct, it also can be assumed that the same law enforcement organizations have the capability of receiving federally produced intelligence products as means of situational awareness. However, it has been expressed in a Department of Justice report that occurrences of smaller community law enforcement agencies either receiving federally produced intelligence products or directly contributing critical information into the intelligence cycle are very limited.<sup>69</sup> Limited distribution of intelligence and information can easily translate into substandard, blemished, and potentially perilous decision-making at all levels of government.<sup>70</sup>

In addition to referencing the results of the thesis research survey mentioned in Chapter IV, this chapter will discuss a few intelligence community issues pertaining to operations and training.

### A. OPERATIONS

#### 1. Leveraging the National Guard

Amongst the communities surveyed in Chapter IV, it was discovered that organizational personnel strength was a common concern. Many rural communities

---

<sup>68</sup> RAND Corporation, *When Terrorism Hits Home*.

<sup>69</sup> Office of the Inspector General, "The Federal Bureau of Investigations Efforts to Improve the Sharing of Intelligence and Other information," US Department of Justice, Report No. 04-10, December 2003. <http://www.usdoj.gov/oig/reports/FBI/a0410/findings.htm> [last accessed 26 July 2007].

<sup>70</sup> Steven Ptark, Charles Webster, and Tony Wilson, "Effective Decision-making Processes for the Joint Force Commanders," *Air Land Sea Bulletin at the Air Land Sea Application Center*, [http://www.au.af.mil/au/awc/awcgate/dod/effective\\_decision.htm](http://www.au.af.mil/au/awc/awcgate/dod/effective_decision.htm) [last accessed 26 July 2007]

simply don't have the manpower to meet day-to-day operational requirements let alone the additional operational demands associated with participating in HLS efforts. As an example, the city of Batavia, NY, often tasks its officers with additional duties, which take away from primary duties of patrolling the community, analyzing intelligence, or disseminating processed information. As an example, Batavia has a strong concern that their operations will be severely impacted if they lose county funded billets to a county level coordinated center. With one particular Batavia office, the loss of a single individual will create a void in the flow of information (inbound/outbound) from the department. Such a void may allow a terrorist cell or human smuggling ring to operate undetected within the respective jurisdiction.<sup>71</sup> How can the HLS Community fill this void? Some would argue that the local National Guard Office acting as an augmenting force might be a suitable solution in terms of mitigating some of the personnel concerns expressed by the smaller communities.

The values of employing the National Guard to mitigate personnel shortfalls in various State Intelligence Fusion centers has been debated in many forums since 11 September 2001;<sup>72</sup> however very little has been discussed with respect to potentially using National Guard assets in local governments as part of the HLS effort. As stated in the literature review section in Chapter I, there is very little published with respect to Domestic Intelligence and the possibilities of integrating National Guard assets into local law enforcement roles under state active duty (SAD) status. This reluctance to publish such information may be based on the legislative disagreement of existing statutes, the fear of misinterpreting existing laws, or localized political sensitivities, or a combination of the three.<sup>73</sup>

---

<sup>71</sup> Derek J. Marsh, Issues Impacting Human Trafficking Collaborations: A Local Law Enforcement Perspective," Orange County Human Trafficking Task Force Westminster Police Department, March 20, 2007, 4-6. <http://homeland.house.gov/SiteDocuments/20070321101447-62337.pdf> [last accessed 26 July 2007].

<sup>72</sup> Grace Jean, "Guard Balancing Emerging Roles in Homeland Defense," *National Defense Magazine*, September 2005. [http://www.nationaldefensemagazine.org/issues/2005/sep/guard\\_balancing.htm](http://www.nationaldefensemagazine.org/issues/2005/sep/guard_balancing.htm) [last accessed 26 July 2007].

<sup>73</sup> Kate Folmar, "California Bill Proposed to Limit Activity of National Guard," *San Jose Mercury News*, 26 April 2006. [http://www.constitutioncenter.org/education/TeachingwithCurrentEvents/ConstitutionNewswire/16083\\_print.shtml](http://www.constitutioncenter.org/education/TeachingwithCurrentEvents/ConstitutionNewswire/16083_print.shtml) [last accessed 29 June 2007].



According to the National Guard Bureau, National Guard elements under SAD status need not comply with federally regulated policies such as Posse Comitatus Act (PCA) and Intelligence Oversight regulations.<sup>74</sup> If such regulations were applicable to the National Guard under SAD status, these policies would restrict Guard members from participating in law enforcement activities and localized intelligence activities (even in times of crisis). With this said, the National Guard brings various capabilities to assist with the day-to-day operations, counter-terrorism intelligence support, and disaster response (as required).<sup>75</sup> Properly leveraged, these capabilities may free up local law enforcement assets to perform other duties.

## **2. Intelligence, Surveillance and Reconnaissance (ISR)**

### ***a. IMINT***

Aerial surveillance: Consider a human smuggling group is conducting illegal activities on a border-town farm in rural United States (see Chapter III – pages 52-54):

Based on given US Constitutional rights, a respective landowner (or farmer) may assume that because their activities (malicious or not) is occurring on private land, they have the rights to privacy and the local law enforcement is not authorized to conduct ISR without a valid warrant.

In this scenario, the farmers adjacent to the property in question have become suspicious of the activities occurring on the neighboring property and placed an anonymous telephone call to the local sheriff. Based on the information provided, the local sheriff placed the residence under ground based surveillance (e.g., strategically placed vehicles, law enforcement officers with binoculars). The surveillance activities occurred over a couple of days, but turned up nothing with respect to illegal activities. But the complaints continued.

---

<sup>74</sup> John Dixon and Chris Rofrano, “Intelligence Operations Briefing,” National Guard Bureau Briefing for a Joint Staff conference, slide 18. [http://www.ngb.army.mil/jointstaff/pslja/conference/2007/intelligence\\_oversight.ppt](http://www.ngb.army.mil/jointstaff/pslja/conference/2007/intelligence_oversight.ppt) [last accessed 28 June 2007].

<sup>75</sup> Jay Smith, “A Changing of the Guard: The U.S. National Guard and Homeland Defense,” Harvard University John F. Kennedy School of Government, ESDP-2003-1, May 2003, 10.

Though the community was small, it had a relatively small regional airport with an amateur aero club. The quick-witted sheriff made the decision to enlist the local aero club during one of its routine flights and requested that the pilot fly over or near the property of interest while an officer, as a passenger, observes and documents the ongoing activities below. Based on the observations, it was discovered that the property occupants were active in smuggling humans across the border using their property as a conduit. In turn, the discovery was turned over to state and federal authorities for further action.

Many would say that the acts of this sheriff were illegal and violate the property owner's civil rights as defined under the 4<sup>th</sup> Amendment.<sup>76</sup> In fact the sheriff did not violate any civil laws. Under such federal cases as *Florida v. Riley*, 488 U.S. 445 (1988) and *California v. Ciraolo*, 476 U.S. 207, 211 (1986), it was ruled that local law enforcement conducting surveillance by an aircraft (commercial, private, NG under SAD status) flying an approved Federal Aviation Administration (FAA) flight pattern, law enforcement officers, regardless of who is piloting the aircraft, do not violate constitutional rights.<sup>77</sup>

Unlike their larger metropolitan counterparts, smaller communities are often not afforded the budgets to create or accommodate an active aviation detachment. The lack of monitoring from the sky may allow illegal activities such as border crossings within a designated jurisdiction. With limited border patrol resources it may take days, if not weeks, for a federally funded air surveillance asset (e.g., unmanned aviation vehicle (UAV)) to be dispatched to fly over the area in question.

#### ***b. MASINT***

Thermal Imaging & Seismic Sensors: Considering the undocumented immigrants crossing the border using a privately owned farm as a conduit case. The use of technology such as thermal imaging and seismic sensors as collection mediums may

---

<sup>76</sup> The Fourth Amendment states: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

<sup>77</sup> Robert Gustafson, "Technological, electronic, or other surveillance," Gustafson law Office of Colorado Springs, <http://www.gustafsonlaw.com/crim-surveillance.htm> [last accessed 5 July 2007].

have contributed to the quicker discovery and apprehension of the smuggling ring. However, the legalities associated with using such technologies in surveillance activities have been questioned within the nation's courts often creating an environment where smaller communities local law enforcement become hesitant on utilizing such a capability. To counter the reluctant mindset, it has been ruled by the federal judicial system that surveillance through the use of MASINT technologies such as thermal imagery and seismic sensors does not violate statutes defining individual rights to privacy. In a federal case such as *United States v. Ishmael*, 48 F .3d 850 (5<sup>th</sup> Cir. 1995), it was held that thermal scan devices depends on the phenomenon of natural heat loss of which, in a sense, is analogous to "wasted heat" or items that are no longer of use to an individual (e.g., garbage).<sup>78</sup>

The legal factor of implementing MASINT is not the only issue that may dissuade an organization from using advanced ISR capabilities in its surveillance operations. The price tag associated with advanced technologies may also deter a small community from pursuing procurement. In the case of thermal imagery, the cost of a single thermal imagery sensor may range from \$4,000 - \$20,000.<sup>79</sup> In a law enforcement community with a small and restrictive annual budget (e.g., Batavia, NY - \$3.5M) the procurement of a single, if not multiple, thermal imaging device may be out of budget range.

With their annual budgets, state National Guard units may have procured modern surveillance devices in support of readiness posture or as Title 10 assets deployed over-seas. Under SAD status, the National Guard is a good candidate to provide surveillance support to local law enforcement assets as required. As a result of their training and gained experience, National Guard assets directly supporting local agencies (or acting as a information conduit while positioned in a state intelligence fusion center) have the intelligence collection, correlation, analysis, and dissemination skills required for an small community to effectively contribute to the overall HLS mission..

---

<sup>78</sup> Gustafson, "Technological, electronic, or other surveillance."

<sup>79</sup> MOROVISION Night Vision website, <http://www.morovision.com/thermalimages.htm> [last accessed 10 July 2007].

c. *HUMINT*

Community Outreach: There are various approaches to implementing a community outreach program to include establishing a community of practice, a community of interest, or virtual community. The following briefly defines each:

1) Community of Interest (CoI) – A group of individuals or separate organizations assembled to solve a common problem, develops skills, and share common practices. A community of interest may comprise of smaller subsets of individuals sharing information within their respective communities of practice (for example, information technology, logistics, administrative, law enforcement).

2) Community of Practice (CoP) – A community of practice is a group of individuals or organizations that share similar goals and interest. In an effort to achieve defined goals, the community of practice develops and implements common practices, common tools, and a common language.<sup>80</sup>

3) Virtual Community – A virtual community is created when either CoP or CoI is executed within an “online” computer based environment.

For the intent of this thesis, a CoP will be introduced in relation to the establishment of a HUMINT focused community. Volunteers, community outreach, and private commerce have a lot to offer when assisting smaller law enforcement agencies distributed across the country. However, before the model of employing small-town citizens to watch over their respective neighborhoods can be put into practice, the civil rights granted by the U.S. Constitution, roles and responsibilities, and standard operating procedures will need to be addressed.

To preserve civil rights and the trust of the general public, it is important that all community outreach participants understand that defined roles and responsibilities must be followed for a community-based program to work. Strict oversight regulations and procedures will need to be in place to reduce the fears of citizen watch groups

---

<sup>80</sup> Etienne Wenger, “Communities of Practice – Learning as a Social System,” *Systems Thinker*, June 1998, <http://www.co-i-l.com/coil/knowledge-garden/cop/lss.shtml> (last accessed July 2007).

encroaching on the privacy of law-abiding citizens and to ensure that federal, state, and local laws are not violated. Through a defined information-sharing path, the intelligence and information collected by the civilian elements may flow through the local law enforcement agency and may either be analyzed internally to the local organization or distributed into a regional or state level fusion center for processing. Further, to enhance the community network, law enforcement organizations should share successful community outreach best practices or lessons learned with other participating organization at federally or state funded information sharing forums.

### **3. Partnerships**

The formation of partnerships (e.g., public sector to private commerce, public sector to citizen, public organization to public organization) often brings the element of trust between organizations and is critical when establishing a robust network designed to detect, deter, and defeat the modern adversary. Without trust, organizations, regardless of size, are often hesitant to release sensitive information. The lack of organizational trust was experienced when I solicited the survey used in the research phase of this thesis (see Chapter III). As I independently contacted various law enforcement agencies spread out across the nation, it was quickly discovered that many agencies are reluctant to participate or release information pertaining to their organization (budget, standard operating procedures, shortfalls, strengths) because I was not incorporated in their trusted network. The experienced pushback escalated after I provided federal level Homeland Defense credentials and academic related intent. Of the twenty-five local law enforcement agencies polled, several agreed to participate in my research but only four returned completed surveys. However, because of the Naval Postgraduate School Center for Homeland Defense and Security (NPS-CHDS) program, a small network of trust had been formed between fellow cohort members representing local law enforcement agencies and myself. Of the completed surveys minimal resistance was experienced when I employed fellow cohort members to distribute my research survey through their respective trusted organizational networks and to collect valued research information. The philosophy of partnerships and the concept of trust have evolved between cohort

members through both the program's in-residence sessions and direct collaboration during the non-residence creating an information-sharing network. The NPS-CHDS program shows that through forums focused around information exchange and relationship building, the concept of trust will evolve through regular meetings and interaction.

It is difficult to disrupt the command, control and communications of the adversary if trusted relationships between local, state, federal, and at times international HLS participants are not well established.<sup>81</sup> The lack of trust and common understanding between HLS stakeholders creates gaps in the networked HLS infrastructure needed to keep the Homeland safe. The establishment of organizational relationships between HLS participants (federal, state, and local) will fill these gaps and should not end with exchanging business cards between the communities surrounding a respective jurisdiction. Well defined partnerships will create a concerted effort to reduce HLS related vulnerabilities, prepare our communities at all levels to effectively respond in the event of a terrorist attack, minimize damage associated with an attack, contribute to detecting malicious activities, and may deter terrorist attacks within the United States.

## **B. TRAINING**

The training of personnel is critical to the success of an organization's operations. As an organization evolves and standards (processes, technological, tactics) change, it is important for the patrol officer on the street to receive training. Reoccurring training is critical to intelligence assets because over time, officers run the risk of failing to retain the information taught in the previous training sessions thereby forgetting valuable intelligence collection techniques.<sup>82</sup> Each of the organizations surveyed in Chapter IV made mention that they have defined training cycles and expect their officers to remain

---

<sup>81</sup> US Government Accountability Office, "Combating Terrorism - Law Enforcement Agencies Lack Directives to Assist Foreign Nations to Identify, Disrupt, and Prosecute Terrorists," Report to the Ranking Member, Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, House of Representatives, 110th Congress, 1st Session, GAO-07-697, May 2007, <http://www.gao.gov/new.items/d07697.pdf> [last accessed 27 July 2007], 21.

<sup>82</sup> Steve Finney, "Training through repetition," *Police Link*, 11 June 2007, <http://policelink.com/training/articles/2262-training-through-repetition> [last accessed 10 July 2007].

proficient in defined skill sets. These cycles can span anywhere between three to five years from start to end and may include several training topics. In these training sessions, decision makers, patrol officers, and support elements (e.g., intelligence, administration, maintenance, logistics) learn updated procedures and techniques while refreshing themselves on the basics TTPs respective to duties and responsibilities. Two elements pertaining to local law enforcement organizations were addressed in the survey: language and culture (includes special interest groups) and information technology.

## **1. Language and Culture Differences**

With immigration comes a variance of religion, language, and social habits. Historically, immigration trends stopped at the city limits of our larger metropolitans. However, with the vast employment opportunities offered across the nation, immigrants (documented and undocumented) are also settling in the smaller communities distributed across the nation. With this said, cultural awareness training has become increasingly important in our ever-evolving ethnically diverse nation. Cultural awareness provides each officer an environment to examine personal biases and to learn the various ways to work effectively with diverse populations. With an understanding of the various cultures of immigrants settling within their jurisdictions law enforcement patrol officers have the ability to differentiate the differences between potentially malicious activity and cultural norms.

Historically, the law enforcement agencies of our larger metropolitan areas have either invested in or addressed the issue of training its officers on the various languages and cultures associated with immigration trends within their jurisdictions.<sup>83,84</sup> However, more times than none, smaller municipalities and rural communities are not afforded the luxury of the staffing and funds required to support such a training effort. Of the surveyed organizations, it was discovered that training respective to providing patrol

---

<sup>83</sup> New York City Police Department, "Police Practices and Civil Rights in New York City," *NYPD Recruit Training Manual*, Chapter 2. [http://www.usccr.gov/pubs/nypolice/ch2.htm#\\_ftn198](http://www.usccr.gov/pubs/nypolice/ch2.htm#_ftn198) [last accessed 27 June 2007].

<sup>84</sup> US Commission on Civil Rights, "Racial and Ethnic Tensions in American Communities: Poverty, Inequality, and Discrimination," *US Commission on Civil Rights*, Volume V- The Los Angeles Report. <http://www.usccr.gov/pubs/larpt/chapter7.htm#C1> [last accessed 26 June 2007].

officers and supporting employees a better understanding of differences between settling immigrants have been limited. Those that responded to the distributed survey declared that very little time is spent training its officers on the elements of language and culture. Further, it was also discovered that the intensity and re-occurrence of cultural awareness training is dependent on local budgets; as the size of training budgets decrease, the intensity of the training decreases, while the time between training sessions increases. Many local law enforcement budgets may not accommodate detailed training for their officers.

## **2. Information Technology**

Prior to 11 September 2001, the nation as a whole did not give much thought to coordinating operations with local and state law enforcement agencies. It has become public knowledge that many federal level intelligence agencies expended resources in the collection and analysis of terrorist oriented intelligence; however the processed information was not disseminated to organizations residing on the outer-circles of the immediate information-sharing environment.<sup>85</sup> A criterion of taking a defensive posture in securing the Homeland is efficient information and intelligence sharing between all layers of government to include local law enforcement resources.<sup>86</sup> Though the sharing of information and intelligence associated with taking a preventive HLS posture is critical, current restrictions associated with information assurance dampens sharing efforts, thereby discouraging agencies from readily releasing information and intelligence to local law enforcement in support of the HLS mission. Based on the research survey findings (please see Chapter IV, pages 56-69), many of the smaller organizations are left to fend for themselves when it comes to funding IT based collection and dissemination systems.

---

<sup>85</sup> Richard Shelby, "September 11 and the Imperative of Reform In the US Intelligence Community," Office of Senator Richard Shelby, 10 December 2002, <http://intelligence.senate.gov/shelby.pdf> (last accessed 15 June 2007).

<sup>86</sup> Mark Willoughby, "Information Sharing Seen as Key to Homeland Defense," *Computerworld Security*, 17 June 2004, <http://www.computerworld.com/securitytopics/security/story/0,10801,93898,00.html?f=x73> (last accessed 17 June 2007)



## **C. SUMMARY**

To summarize, the law enforcement resources of our smaller municipalities and rural communities have become increasingly important in fight against domestic terrorism. Though these HLS assets have been recognized by the federal government and the decisions makers in their respective states, such organizations still experience shortfalls respective to available resources and training when it comes to day-to-day operations, especially with respect to domestic intelligence collection, processing, and dissemination.

THIS PAGE INTENTIONALLY LEFT BLANK

## VI. RECOMMENDATIONS AND FINAL THOUGHT

The major concerns of the agencies interviewed for this thesis related to the lack of ISR, manning, training, and information sharing. Overhauling the existing intelligence community with vested local community resources and interagency information sharing will create an atmosphere where the national intelligence domain is enhanced, thereby escalating the overall effectiveness of existing HLS operations. Effective change may be achieved through modifying the existing policies, plans, and processes resident to each law enforcement organization. This chapter will suggest recommendations for local law enforcement agencies to enhance their presence in the national intelligence process.

### A. AVAILABLE ISR RESOURCES

**Recommendation 1: Using non-government assets for ISR (HUMINT)** — It is recommended that small town decision makers define or enhance their community outreach initiatives and train elements of the community to be more observant of their immediate surroundings. Such an initiative will allow for law enforcement to leverage community resources as basic HUMINT assets to identify suspicious activities related to crime and potential terrorist activities. Under the premise of a program called Citizen Corp, an effort headed by the U.S. Department of Justice, larger metropolitans such as Boston have taken steps to encompass the community in their efforts to locate potential terrorist activities.<sup>87</sup>

**Recommendation 2: Using non-government assets for ISR (MASINT)** — To enhance their surveillance capabilities, it is also recommended the smaller municipalities and rural communities create or improve their relationships with local National Guard units and through respective state level request for forces processes, employ National Guard assets in supporting law enforcement roles as required and as respective state laws

---

<sup>87</sup> Suzanne Smalley, "Boston homeland security plan relies on watch groups," *Boston Globe*, 30 May 2005, [http://www.boston.com/news/local/articles/2005/05/30/boston\\_homeland\\_security\\_plan\\_relies\\_on\\_watch\\_groups/](http://www.boston.com/news/local/articles/2005/05/30/boston_homeland_security_plan_relies_on_watch_groups/) (last accessed 5 July 2007).

allow. With such relationships there should be a focus on integrating available MASINT capabilities such as thermal imagery and seismic sensors into local law enforcement and HLS efforts as required. As applicable, the MASINT resources will be in a supporting role to the local authorities and may not retain possession of the collected materials upon the completion of the operations.

There is a possibility that such a relationship will increase local dependencies on state resources. To reduce this risk, it is also recommend that local law enforcement agencies partner with neighboring jurisdictions in an effort to consolidate funding lines to procure shared MASINT and other technology based collection systems. The procurement of locally owned ISR equipment will reduce the chance of the local governments to form a sense of dependency on external sources such as the National Guard. Further, a consolidated procurement approach will ensure that “stove-piped” systems centric organizations are not developed or implemented.

## **B. MANNING**

**Recommendation 3: Leveraging the National Guard** — It is recommended that smaller municipalities and rural communities create a point of presence or enhance direct working relationships with their respective state’s National Guard Office (NGO) as a possible solution to increase their workforce. The focus of the relationships should be on integrating NGO capabilities into local intelligence efforts to the extent possible, as defined by local and state law, and identifying support requirements that might be required to construct an ad hoc intelligence collection or processing environment (if required). Under this construct, the NGO will be in a supporting role to the local authorities and will not obtain control over intelligence activities within the respective jurisdiction. As a supporting element, the National Guard may provide resources ranging from administrative staff to intelligence (analysts, collection specialists) personnel.

## C. TRAINING

**Recommendation 4: Enhancing language and culture training** — It is recommended that the nation's smaller communities continuously push the governments of their respective state legislatures and the federal government to provide a training program specifically focused on language and culture awareness of the ethnic groups settling in their respective jurisdictions.

**Recommendation 5: Information technology** — It is recommended that smaller communities continue to petition the governments of their respective states and the USG, to further invest in intelligence dissemination technologies to bridge the information sharing gaps that separate the various levels of HLS participation.

It is also recommended that smaller municipalities and rural communities petition their respective counties and states to receive training on existing federally provided HLS related IT based systems.

## D. INFORMATION SHARING

**Recommendation 6: Creating partnerships** — It is recommended that smaller communities allocate a portion of their annual budgets or petition for HLS related grants for national level travel, conference participation, joint training exercises, and creation or enhancement of virtual communities of practice. With such activities, the representatives of the smaller communities will have the opportunity to form the needed relationships with others with similar mission sets and gain knowledge of alternate methods of executing HLS related tasks. These organizations may reside in regions outside their immediate or surrounding areas of responsibilities.

**Recommendation 7: Participation in the National Information Sharing Environment** — It is recommended that each organization should engage themselves in the national Information Sharing Environment (ISE) efforts.<sup>88</sup> With such participation, the organization will join a forum where they can create, coordinate, establish, and

---

<sup>88</sup>Office of the Program Manager, Information Sharing Environment (PM-ISE) web site, <http://www.ise.gov/> [last accessed 5 July 2007].

publicize respective organizational processes defining information management, collaboration, and communication resources with agencies near and distant with respect to their jurisdiction. The failure to identify or adhere to a uniform information management plan can delay and degrade overall HLS related command and control efforts and common situational awareness. Such a failure can be detrimental to ensuring that the Homeland remains secure.

It is also recommended that the national intelligence community, to include intelligence assets from United States Northern Command (USNORTHCOM), continue their efforts to build multi-agency relationships and extend their intelligence support to the state and local law enforcement communities. Extended support may include, but is not limited to, the distribution of common analytic products at uniform classification levels; when applicable (e.g., complying with intelligence oversight policies), leveraging intelligence collection resources; and modifying respective TTPs to accommodate a common collection strategy.

## **E. FINAL THOUGHT**

While several recommendations have been suggested to mitigate the shortfalls discussed in this thesis, many hurdles still need to be overcome before United States Decision makers can say that the Nation has the ability to detect adversarial activities ten times out of ten or formally declare they have successfully deterred terrorist groups such as Al Qaeda from taking action against the United States. Many changes have been implemented to make the Homelands safer since the 11 September 2001, but for every one change implemented, dozens more have either not made it past the proposal phase of a project or have been approved but postponed for future implementation due to limited budgets. On the levels of federal and state governments, many of these deferred projects involve the smaller communities of our nation. While these overdue projects remain in the queue, smaller communities of our nation remain impacted and feel that their contribution to the overall HLS mission is minimal. If the modern adversary is to be

defeated, the decision makers of our state and federal governments will need to truly consider small community law enforcement as viable participants in the overall HLS effort.

THIS PAGE INTENTIONALLY LEFT BLANK



## BIBLIOGRAPHY

- Axtman, Kris. "Changing Landscape of an Underground Trade." *Christian Science Monitor*, 17 July 2003. <http://csmonitor.com/2003/0717/p03s01-usgn.htm> [last accessed 20 February 2007].
- Bauer, Lynn. "Local Law Enforcement Block Grant Program, 1996-2004." US Department of Justice - Bureau of Justice Statistics Technical Report NCJ 203096, September 2004.
- Bergman, Lowel. "The Enemy Within." Transcripts from the Public Broadcasting System (PBS) Frontline, 10 October 2006. <http://www.pbs.gov/wgbh/pages/frontline/enemywithin/etc/script.html> [last accessed 26 January 2007].
- British Broadcasting Company (BBC). "Hijack 'Suspects' Alive and Well." British Broadcasting Company, 23 September 2001. [http://news.bbc.co.uk/2/hi/middle\\_east/1559151.stm](http://news.bbc.co.uk/2/hi/middle_east/1559151.stm) [last accessed 2 January 2007].
- Camarot, Steven. "Census Bureau: Over 100,000 Illegal Aliens from the Middle East." Center for Immigration Studies, 22 January 2002. <http://www.cis.org/articles/2001/censusillegalsme.html> [last accessed 11 July 2007].
- Cherry, Steven. "Terror Goes Online." *IEEE Spectrum*. <http://www.spectrum.ieee.org/pring/2472> [last accessed 29 December 2006].
- Committee on Intelligence. *IC2: The Intelligence Community in the 21<sup>st</sup> Century*. US House of Representatives. 104<sup>th</sup> Congress, November 2004. [http://www.fas.org/irp/congress/1996\\_rpt/ic21/ic21007.htm](http://www.fas.org/irp/congress/1996_rpt/ic21/ic21007.htm) [last accessed 23 March 2007].
- Copeland, Larry. "Domestic Terrorism: New Trouble at Home." *USA Today*, 14 November 2004. [http://www.usatoday.com/news/nation/2004-11-14-domestic-terrorism\\_x.htm](http://www.usatoday.com/news/nation/2004-11-14-domestic-terrorism_x.htm) [last accessed 26 January 2007].
- Corera, Gordon. "Al-Qaeda undimmed by sanctions." British Broadcasting Company, 27 August, 2004. <http://news.bbc.co.uk/1/hi/world/americas/3606384.stm> [last accessed 28 April 2007].
- Court TV. "The Unabomber." Court TV Online. <http://www.courtstv.com/trials/unabomber/bombings.html> [last accessed 21 January 2007].

- Davick Services. "Increasing Coordination Between Mexican Drug Cartels, Human Smuggling Networks, and U.S. Based Gangs." *News For Public Officials Newsletter Online*. [http://www.davickservices.com/line/in\\_sand3.htm](http://www.davickservices.com/line/in_sand3.htm) [last accessed 20 February 2007].
- Davidson, Thomas II. "Terrorism and Human Smuggling Rings in South and Central America." *Terrorism Monitor* III, Issue 22, 17 November 2005.
- Dempsey, James X. "Civil Liberties in a Time of Crisis." *Human Rights Magazine Online*, Winter 2002.  
<http://www.abanet.org/irr/hr/winter02/dempsey.html> [last accessed 2 January 2007].
- Department of Homeland Security Public Affairs. "Homeland Security Agencies Thwart Unusual Human Smuggling Scheme Involving Luxury Sailing Yacht." Department of Homeland Security, 1 September 2004,  
<http://www.uscg.mil/pacarea/news/newsreleases/2004/sept/sept21a.htm> [last accessed 20 February 2007].
- Dixson, John and Chris Rofrano. "Intelligence Operations Briefing."  
[http://www.ngb.army.mil/jointstaff/pslja/conference/2007/intelligence\\_oversight.ppt](http://www.ngb.army.mil/jointstaff/pslja/conference/2007/intelligence_oversight.ppt) [last accessed 28 June 2007].
- Donnell, Harrison. "Preparedness Leader: Strengthening Homeland Security through Geospatial Information." *Military Geospatial Technology Online*, [http://www.military-geospatial-technology.com/print\\_article.cfm?DocID=198](http://www.military-geospatial-technology.com/print_article.cfm?DocID=198) [last accessed 27 April 2007].
- Dwyer, John. "General Hayden: Man on a Mission." *American Thinker Online*, 29 January 2007,  
[http://www.americanthinker.com/blog/2006/05/general\\_hayden\\_man\\_on\\_a\\_mission.html](http://www.americanthinker.com/blog/2006/05/general_hayden_man_on_a_mission.html) [last accessed 29 January 2007].
- Elliott, Michael. "The Shoe Bomber's World." *Time Magazine*. 16 February 2002.  
<http://www.time.com/time/world/article/0,8599,203478,00.html> [last accessed 26 February 2007].
- Finney, Steve. "Training through repetition." *Police Link*, 11 June 2007.  
<http://policelink.com/training/articles/2262-training-through-repetition> [last accessed 10 July 2007].
- Fisk, Daniel W. "Top Priorities For Improving Intelligence and Law Enforcement Capabilities." A Report of the Working Group on Intelligence and Law Enforcement Capabilities. Washington, D.C.: The Heritage Foundation, 2002.

- Florida Domestic Security Oversight Council. "Domestic Security in Florida: Making Florida Safer." 2005 Domestic Security Annual Report, December 2005.
- Folmar, Kate. "California Bill Proposed to Limit Activity of National Guard." *San Jose Mercury News*, 26 April 2006.  
[http://www.constitutioncenter.org/education/TeachingwithCurrentEvents/ConstitutionNewswire/16083\\_print.shtml](http://www.constitutioncenter.org/education/TeachingwithCurrentEvents/ConstitutionNewswire/16083_print.shtml) [last accessed 29 June 2007].
- Gaudin, Sharon. "The Terrorist Network." *Network World*, 26 November 2001.  
<http://www.networkworld.com> [last accessed 16 February 2007].
- George, Rodger and Robert Kline. *Intelligence and the National Security Strategist*. United States: Rowman and Littlefield Publishers, 2006.
- Global Security. "Wail al-Shehri." Global Security Online.  
[http://www.globalsecurity.org/security/profiles/wail\\_al-shehri.htm](http://www.globalsecurity.org/security/profiles/wail_al-shehri.htm) [last accessed 26 January 2007].
- Griffith, S. B. *Sun Tzu Art of War*. London: Oxford University Press, 1971.  
Johnson and Wirtz, *Strategic Intelligence – Windows into a Secret World*. Los Angeles, CA: Roxbury Publishing, 2004.
- Gustafson, Robert. "Technological, electronic, or other surveillance." Gustafson Law Office of Colorado Springs. <http://www.gustafsonlaw.com/crim-surveillance.htm> [last accessed 5 July 2007].
- Harris, Shane. "Expansion of local intelligence-sharing centers sparks controversy." *Government Executive*, 13 February 2007.  
[http://www.govexec.com/story\\_page.cfm?articleid=36121](http://www.govexec.com/story_page.cfm?articleid=36121) [last accessed 27 April 2007].
- Homeland Security Advisory Council. "Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion." US Department of Homeland Security, 28 April 2005.
- Homeland Security Act of 2002, Pub. L. No 107-396, Title VIII Section 201.
- Houser, Mark. "Illegal Immigration face crackdown in Pennsylvania." *Pittsburgh Tribune – Review*, 23 July 2006.
- Jean, Grace. "Guard Balancing Emerging Roles in Homeland Defense." *National Defense Magazine*, September 2005.  
[http://www.nationaldefensemagazine.org/issues/2005/sep/guard\\_balancing.htm](http://www.nationaldefensemagazine.org/issues/2005/sep/guard_balancing.htm) [last accessed 26 July 2007].

- Keefe, Patrick. *Chatter*. New York, NY: Random House, 2005.
- Krikorian, Mark. "The Security Costs of Immigration." *American Outlook*, February 2003, <http://www.cis.org/articles/2003/msksecurityoped203.html> [last accessed 21 January 2007].
- Lowenthal, Mark. *Intelligence – From Secrets to Policy*. Washington DC: CQ Press, 2006.
- Lytle, Peter C. "Postal Terrorism White Paper." The Business Development Group. 15 October 2001. <http://www.bdgpartners.com/postalterrorism.htm> [last accessed 25 February 2007].
- Marks, Alexandra. "Are terrorist cells still in the US?" *Christian Science Monitor*, 10 August 2005. <http://www.csmonitor.com/2005/0810/p02s01-ussc.html> [last accessed 10 July 2007].
- Marsh, Derek J. "Issues Impacting Human Trafficking Collaborations: A Local Law Enforcement Perspective." Orange County Human Trafficking Task Force. Westminster Police Department, March 20, 2007. <http://homeland.house.gov/SiteDocuments/20070321101447-62337.pdf> [last accessed 26 July 2007].
- Middle American News. "Al Qaeda Seeks Ties to Latin Gangs." *Middle American NewsOnline*, <http://www.manews.org/1104alqaeda.html> [21February 2007].
- MOROVISION Night Vision web site. <http://www.morovision.com/thermalimages.htm> [last accessed 10 July 2007].
- Murray, Charles. "Wanted: Next-gen tech for weapons detection." *EE Times*, September 2001. <http://www.cia.gov/cia/publications/factbook/geos/uk.html#Comm> [last accessed 29 December 2006].
- New York City Police Department. "Police Practices and Civil Rights in New York City." *NYPD Recruit Training Manual*, Chapter 2. [http://www.usccr.gov/pubs/nypolice/ch2.htm#\\_ftn198](http://www.usccr.gov/pubs/nypolice/ch2.htm#_ftn198) [last accessed 27 June 2007].
- Office of the Chief of Naval Operations. "Naval Intelligence – Naval Doctrine Publication (NDP) 2." Department of the Navy, <http://www.fas.org/irp/doddir/navy/ndp2.htm> [last accessed 19 March 2007].

- Office of the Director of National Intelligence. *National Intelligence Strategy of the United States of the America: Transformation through Integration and Innovation*. Washington, D.C.: Government Printing Office, 2005.
- . *U.S. Intelligence Community's Five Year: Strategic Human Capital Plan*. Washington, D.C.: Government Printing Office, 2006.
- Office of the Inspector General. "The Federal Bureau of Investigations Efforts to Improve the Sharing of Intelligence and Other information." US Department of Justice, Report No. 04-10, December 2003.  
<http://www.usdoj.gov/oig/reports/FBI/a0410/findings.htm> [last accessed 26 July 2007].
- Office of the Program Manager. Information Sharing Environment (PM-ISE).  
<http://www.ise.gov/> [last accessed 5 July 2007].
- Posner, Richard. *Not a Suicide Pact: The Constitution in a Time of National Emergency*. New York, NY: Oxford University Press, 2006.
- Park, Steven, Charles Webster and Tony Wilson. "Effective Decision-making Processes for the Joint Force Commanders." *Air Land Sea Bulletin at the Air Land Sea Application Center*. [http://www.au.af.mil/au/awc/awcgate/dod/effective\\_decision.htm](http://www.au.af.mil/au/awc/awcgate/dod/effective_decision.htm) [last accessed 26 July 2007].
- RAND Corporation. *When Terrorism Hits Home – How Prepared Are State and Local Law Enforcement?* Santa Monica, CA: RAND Corporation, 2004.
- Rosenau, William and Peter Chalk. "Can We Learn From Others?" RAND Corporation article published in the *Wall Street Journal*, 15 April 2004.  
<http://www.rand.org/commentary/041504WSJ.html> [last accessed 26 April 2007].
- Ross, Brian and Richard Eposito. "Surge in Sale of Disposable Cell Phones May Have Terror Link." *ABC News*, 12 Jan 2006.  
<http://abcnews.go.com/WNT/Investigation/story?id=1499905> [last accessed 24 February 2007].
- Schroen, Gary C. *First In: An Insiders Account of How the CIA Spearheaded the War on Terror in Afghanistan*. New York, NY: Ballentine Books, 2005.
- Seymour, Mary. "Fed court limits power to monitor cell phones." *Bloomberg*, 29 November 2005. <http://www.rationalreview.com/content/4416> [last accessed 17 February 2007].

- Shelby, Richard. "September 11 and the Imperative of Reform in the US Intelligence Community." Office of Senator Richard Shelby, 10 December 2002.  
<http://intelligence.senate.gov/Shelby.pdf> [last accessed 15 June 2007].
- Smalley, Suzanne. "Boston homeland security plan relies on watch groups." *Boston Globe*, 30 May 2005.  
[http://www.boston.com/news/local/articles/2005/05/30/boston\\_homeland\\_security\\_plan\\_relies\\_on\\_watch\\_groups/](http://www.boston.com/news/local/articles/2005/05/30/boston_homeland_security_plan_relies_on_watch_groups/) [last accessed 5 July 2007].
- Smith, Jay. "A Changing of the Guard: The U.S. National Guard and Homeland Defense." Harvard University John F. Kennedy School of Government, ESDP-2003-1, May 2003.
- Statement by Director of Central Intelligence George J. Tenet Before the House Permanent Select Committee on Intelligence, 106<sup>th</sup> Congress, 2<sup>nd</sup> Session 12 April 2000, Routine proceedings S2553-S2646.  
[http://www.odci.gov/cia/public\\_affairs/speeches/dci\\_speech\\_041200.html](http://www.odci.gov/cia/public_affairs/speeches/dci_speech_041200.html) [last accessed 29 January 2007].
- Suskind, Ron. "The Untold Story of Al-Qaeda's plot to Attack the Subways." *Time Magazine*, 26 June 2006.  
<http://www.time.com/time/magazine/article/0,9171,1205478,00.html> [last accessed 26 February 2007].
- The 9/11 Commission. *9-11 Commission Report*. Washington, D.C.: Government Printing Office, 2004.
- The Associated Press. "Kaczynski Pleads not guilty to Unabomber Charges," *USA Today*, 10 December 2006. <http://www.usatoday.com/news/index/una77.htm>. [last accessed 24 February 2007].
- Thomas, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'" *Parameters – US Army War College Quarterly*, Spring 2003.  
<http://www.carlisle.army.mil.usawc/Parameters/03spring/thomas.htm> [last accessed 29 December 2006].
- United States Air Force. "Air Force Pamphlet 14-210: USAF Intelligence Targeting Guide." Headquarters Department of the Air Force, 1 February 1998.
- United States Army. "Field Manual 2-0 (FM-2-0): Intelligence," Headquarters Department of the Army, May 2004.

- United States Commission on Civil Rights. "Racial and Ethnic Tensions in American Communities: Poverty, Inequality, and Discrimination." *US Commission on Civil Rights, Volume V- The Los Angeles Report*.  
<http://www.usccr.gov/pubs/larpt/chapter7.htm#C1> [last accessed 26 June 2007].
- United States Congress. "The Statement for the Record By Lieutenant General Michael V. Hayden Before the Joint Inquiry of The Senate Select Committee on Intelligence and the House permanent Select Committee on Intelligence." 107th Congress, 2nd Session. 17 October 2002.
- United States Department of State. "Funding Terror Becoming Costlier, Riskier, U.S. Official Says." United States Department of State.  
<http://usinfo.state.gov/ei/Archive/2004/Sep/30-755521.html> [last accessed 28 April 2007].
- US Government Accountability Office. "Combating Terrorism - Law Enforcement Agencies Lack Directives to Assist Foreign Nations to Identify, Disrupt, and Prosecute Terrorists." Report to the Ranking Member, Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, House of Representatives, 110th Congress, 1st Session, GAO-07-697. May 2007.  
<http://www.gao.gov/new.items/d07697.pdf> [last accessed 27 July 2007].
- United States Intelligence Community. "Intelligence Cycle,"  
[http://www.intelligence.gov/2-business\\_cycle1.shtml](http://www.intelligence.gov/2-business_cycle1.shtml) [last accessed 26 March 2007].
- Verton, Dan. *Black Ice: The Invisible Threat of Cyber – Terrorism*. New York: McGraw-Hill, 2003.
- Wenger, Etienne. "Communities of Practice – Learning as a Social System." *Systems Thinker*, June 1998. <http://www.co-i-l.com/coil/knowledge-garden/cop/lss.shtml> [last accessed July 2007].
- Willoughby, Mark. "Information Sharing Seen as Key to Homeland Defense." *Computerworld Security*, 17 June 2004.  
<http://www.computerworld.com/securitytopics/security/story/0,10801,93898,00.html?fx73> [last accessed 17 June 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