



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**INTELLIGENCE-DRIVEN BORDER SECURITY: A
PROMETHEAN VIEW OF U.S. BORDER PATROL
INTELLIGENCE OPERATIONS**

by

Gloria I. Chavez

December 2015

Thesis Co-Advisors:

Kathleen Kiernan
Erik Dahl

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<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.				
1. AGENCY USE ONLY <i>(Leave blank)</i>		2. REPORT DATE December 2015	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE INTELLIGENCE-DRIVEN BORDER SECURITY: A PROMETHEAN VIEW OF U.S. BORDER PATROL INTELLIGENCE OPERATIONS			5. FUNDING NUMBERS	
6. AUTHOR(S) Gloria I. Chavez				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) <p>Transnational criminal networks will continue to evolve. The United States Border Patrol's (USBP) intelligence-driven planning, resourcing, and operations need to be responsive to the constant evolution in adversary tactics, techniques, and procedures. To successfully standardize and institutionalize intelligence processes, a comprehensive evaluation was conducted on the current USBP intelligence architecture and intelligence processes.</p> <p>The research compared and contrasted the current Border Patrol intelligence mission with best practices, lessons learned, shared missions, and constraints within the Intelligence Community. The research focused on the synthesis of an intelligence-driven, law enforcement culture, one that will increase situational awareness and understanding of the homeland security ecosystem through efficient planning, collections, exploitation, processing, analysis, production, and dissemination of intelligence-related information to all components of the Department of Homeland Security (DHS). This study examines literature from the DHS strategic documents, Department of Defense intelligence doctrine, Government Accountability Office reports, internal USBP intelligence documents, and subject-matter expert perspectives.</p> <p>This research leads USBP to consider instituting an effective organizational architecture that supports the evolutionary development of its intelligence-driven, border security operations and intelligence-driven, decision-making process. The thesis concludes that the synergy between law enforcement culture and intelligence-driven operations is difficult to achieve, yet once established, it is very powerful, irreplaceable, highly effective, and self-sustainable. Evidence demonstrates that in order to institute a culture of an intelligence-driven border security agency, a more robust approach needs to be standardized to sustain the flexibility and adaptability the USBP requires to address future threats in the twenty-first century.</p>				
14. SUBJECT TERMS United States Border Patrol (USBP), intelligence enterprise, USBP agent, intelligence (BPA-I), information sharing, capability gap analysis process (CGAP), Tucson Sector Red Team			15. NUMBER OF PAGES 109	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**INTELLIGENCE-DRIVEN BORDER SECURITY: A PROMETHEAN VIEW OF
U.S. BORDER PATROL INTELLIGENCE OPERATIONS**

Gloria I. Chavez
Chief Patrol Agent–Spokane Sector, United States Border Patrol
B.A., Columbia Southern University, 2013

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
December 2015**

Approved by: Kathleen Kiernan
Thesis Co-Advisor

Erik Dahl
Thesis Co-Advisor and Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Transnational criminal networks will continue to evolve. The United States Border Patrol's (USBP) intelligence-driven planning, resourcing, and operations need to be responsive to the constant evolution in adversary tactics, techniques, and procedures. To successfully standardize and institutionalize intelligence processes, a comprehensive evaluation was conducted on the current USBP intelligence architecture and intelligence processes.

The research compared and contrasted the current Border Patrol intelligence mission with best practices, lessons learned, shared missions, and constraints within the Intelligence Community. The research focused on the synthesis of an intelligence-driven, law enforcement culture, one that will increase situational awareness and understanding of the homeland security ecosystem through efficient planning, collections, exploitation, processing, analysis, production, and dissemination of intelligence-related information to all components of the Department of Homeland Security (DHS). This study examines literature from the DHS strategic documents, Department of Defense intelligence doctrine, Government Accountability Office reports, internal USBP intelligence documents, and subject-matter expert perspectives.

This research leads USBP to consider instituting an effective organizational architecture that supports the evolutionary development of its intelligence-driven, border security operations and intelligence-driven, decision-making process. The thesis concludes that the synergy between law enforcement culture and intelligence-driven operations is difficult to achieve, yet once established, it is very powerful, irreplaceable, highly effective, and self-sustainable. Evidence demonstrates that in order to institute a culture of an intelligence-driven border security agency, a more robust approach needs to be standardized to sustain the flexibility and adaptability the USBP requires to address future threats in the twenty-first century.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
	A. BACKGROUND.....	3
	B. THE PROBLEM.....	7
	C. THE RESEARCH QUESTION.....	10
	D. METHODOLOGY.....	11
	E. CHALLENGES.....	13
II.	LITERATURE REVIEW.....	15
	A. USBP 2012–16 STRATEGIC PLAN AND CBP VISION 2020.....	15
	B. JOINT TASK FORCES AND FUSION CENTERS.....	17
	C. DEFINING INTELLIGENCE.....	20
	D. DEPARTMENT OF DEFENSE AND DOMESTIC LAW ENFORCEMENT INTELLIGENCE.....	21
III.	HOMELAND SECURITY INTELLIGENCE ENTERPRISE.....	25
	A. INTELLIGENCE AND BORDER SECURITY.....	25
	1. USBP Intelligence.....	27
	2. BPA-I.....	28
	3. BPA-I Requirements.....	31
	B. ON SITUATIONAL AWARENESS.....	33
	C. INTELLIGENCE AND POLICY.....	34
	D. NATURE OF THE THREAT.....	36
IV.	ANALYSIS.....	39
	A. CAPABILITY BASED ASSESSMENT—AN OPERATIONAL PERSPECTIVE OF INTELLIGENCE CAPABILITY GAPS.....	39
	B. CGAP INITIAL INTEL GAP ROLLUP.....	39
	C. LIMITATIONS.....	41
	D. GAPS REORGANIZED UNDER CBP INTELLIGENCE CYCLE.....	41
	E. INTELLIGENCE DRIVEN OPERATIONS AND OPERATIONS DRIVEN COLLECTIONS.....	43
	1. Survey Questions.....	44
	2. Key Findings.....	44
	F. STRATEGIC INDICATORS AND WARNING: A U.S. BORDER PATROL CASE STUDY—AJO STATION.....	46
	1. Timeline of Strategic Indicators and Warning.....	47

G.	LESSONS LEARNED	48
H.	ON ANTICIPATING SURPRISE.....	50
V.	SOLUTIONS AND RECOMMENDATIONS.....	59
A.	SUMMARY OF RECOMMENDATIONS.....	59
B.	DEFINING THE PROBLEM.....	59
C.	PLANNING	60
D.	COLLECTIONS	61
1.	The Collection Manager	63
2.	Collection at the Field Level.....	65
3.	Processing and Exploitation.....	65
4.	Analysis and Production.....	67
5.	Dissemination	68
6.	Red Team.....	69
E.	VISION FOR THE FUTURE	71
APPENDIX A.	PROFESSIONAL INTELLIGENCE ASSOCIATIONS— ADDITIONAL OPPORTUNITIES FOR BPA-IS	73
APPENDIX B.	IC BREAKDOWN	77
APPENDIX C.	TUCSON SECTOR INTELLIGENCE/INFORMATION SHARING STUDY: CRITICAL FINDINGS	79
LIST OF REFERENCES	85
INITIAL DISTRIBUTION LIST	89

LIST OF FIGURES

Figure 1.	Southwest Border Information Sharing Community	5
Figure 2.	CBP 2020 Vision and Strategy	16
Figure 3.	The Intelligence Community	26
Figure 4.	USBP Intelligence-driven Operations.....	28
Figure 5.	USBP Intelligence Synthesis	29
Figure 6.	U.S. Border Patrol Sector Intelligence Unit 1997 Standard Operating Procedure	30
Figure 7.	Commander’s Critical Information Requirements and Assessments	49
Figure 8.	General Intelligence Collection Requirements	62
Figure 9.	Collection Management Cross Section: Horizontal View	63
Figure 10.	Collection Management Cross Section: Vertical View	64
Figure 11.	DHS Data Framework.....	66
Figure 12.	Combating Terrorism Technical Support Office and CADENA Overview and Introduction to Joint Task Force-West.....	67
Figure 13.	Attributes of Excellent Intelligence	68

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Capability Gap Assessment40
Table 2. Consolidated Gaps43
Table 3. Timeline of Strategic Indicators and Warning.....47

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AMO	air marine operations
AOR	area of responsibility
AFCEA	Armed Forces Communications and Electronics Association
BPA-I	Border Patrol agent, intelligence
C2	command and control
CAG	Casa Grande Border Patrol Station
CBP	Customs and Border Protection
CGAP	Capability gap analysis process
CI	confidential informant
CIA	Central Intelligence Agency
CoC	chain of command
COI	community of interest
CRS	Congressional Research Service
DIT	data integrity team
DHS	Department of Homeland Security
DHS I&A	DHS Office of Intelligence and Analysis
DOD	Department of Defense
DOJ	Department of Justice
DTO	drug trafficking organization
ES2	every soldier is a sensor
FY	fiscal year
GEOINT	Geospatial intelligence
GTA	got-away
GAO	Government Accountability Office
HHS	Department of Health and Human Services
HSE	Homeland Security Enterprise
IALEIA	International Association of Law Enforcement Intelligence Analysts
IC	Intelligence Community
INSA	Intelligence and National Security Alliance
ISR	Intelligence, surveillance, reconnaissance

LTOV	latest time of value
MET	mission essential task
MRD	manpower requirements determination
ODNI	Office of the Director of National Intelligence
OFO	Office of Field Operations
OI	Office of Intelligence
OIIL	Office of Intelligence and Investigative Liaison
OIOC	Office of Intelligence and Operations Coordination
OIP	operational implementation plans
PIR	priority intelligence requirement
POE	port of entry
RSTA	reconnaissance, surveillance, target, acquisition
SBPA	supervisory Border Patrol agent
SIGNIT	signals intelligence
SIU	Sector Intelligence Unit
SOP	standard operating procedure
SPAD	Strategic Planning and Analysis Directorate
TACON	tactical control
TBS	turnbacks
TCA	Tucson sector
TTPs	Tactics, techniques, and procedures
SLATT	U.S. Department of Justice, Bureau of Justice Assistance, State and Local Anti-Terrorism
USBP	United States Border Patrol
USCG	United States Coast Guard

EXECUTIVE SUMMARY

United States Border Patrol (USBP) operations are dynamic. They encompass everything from static line-watch operations and narcotics seizures to serving high-risk warrants; yet, the most important mission of the USBP is preventing the entry of terrorist and terrorist weapons between U.S. ports of entry. This research provides an understanding of the USBP law enforcement culture, border security mission, and intelligence enterprise that will support the evolutionary development of its intelligence-driven, border security operations between U.S. ports of entry and abroad. This research focuses on the USBP and the challenges in synchronizing a law enforcement culture with intelligence and building intelligence based decision-making processes to drive all planning and execution of border security operations. The research question to answer is, how does the current USBP intelligence architecture provide the necessary intelligence support to more effectively plan, collect, identify, analyze, and disseminate intelligence-related information to all stakeholders while addressing emerging threats within its border security mission on the domestic and international fronts?

The flow of information between intelligence agents and operations is critical to situational awareness. Understanding the perceptions, perspectives, and requirements of intelligence agents and operations can reveal opportunities to enhance information sharing. The Department of Homeland Security Office of Intelligence and Analysis division and Customs and Border Protection Office of Intelligence could be considered the central nervous system of the homeland security friendly force ecosystem. If so, then the USBP and its Border Patrol Agent-Intelligence (BPA-I) personnel are the nerve endings and the sensory inputs into the friendly force information sharing network. With that said, it is recognized that there are a host of friendly force stakeholders that comprise the friendly force information-sharing network, but no single law enforcement agency has the intelligence collections human capital capabilities of the USBP.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my family for their unwavering love, patience, and understanding during this rigorous 18-month academic journey—all my love to you. To all my friends and colleagues whom I unintentionally disregarded while in this program, my most sincere apologies and heartfelt thanks for your understanding and support.

To my classmates from Cohorts 1403/1404—you are all an exceptional group of human beings, and I will forever cherish the experiences we lived through together at CHDS. To the professors and staff at the Naval Postgraduate School, especially Dr. Kathleen Kiernan and Dr. Erik Dahl, a world of gratitude to each of you for your patience, instruction, and wise counsel in strengthening my mind, capabilities, and foresight as a homeland security practitioner.

My sincere appreciation to all the men and women of CBP who work tirelessly every day in protecting the United States of America. A very special thanks goes to Dr. Renee Yengibaryan of the CBP Office of Intelligence—your tutelage was truly invaluable. A world of gratitude to Operations Officer Luis Tafoya of the U.S. Border Patrol Headquarters Intelligence Division and to Tucson Sector Douglas Station Supervisory Border Patrol Agent Ryan Riccucci for your motivation, guidance, and expertise in helping me link intelligence theory to practical reality.

But most of all, I'd like to extend my heartfelt gratitude to my brothers and sisters who wear the U.S. Border Patrol uniform. Thank you for your courage, determination, and resilience. No matter what the requirement, you humbly step up to the challenge each and every time and consistently deliver excellence. You have been my inspiration through this academic journey. I am honored to serve with you. For this reason, I dedicate this thesis to all of you.

Honor First!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

To prevent acts of terrorism on American soil, we must enlist all of our intelligence, law enforcement, and homeland security capabilities. We will continue to integrate and leverage state and major urban area fusion centers that have the capability to share classified information

National Security Strategy, 2010

The terrorist attacks of September 11, 2001 revealed to the world that the United States was not as stable and secure as previously assumed. The United States appeared shocked and surprised that the homeland was vulnerable to acts of terrorism.¹ From that infamous moment in time, it was obvious that the United States was in need of a robust Intelligence Community (IC) that could quickly and efficiently share information in order to inform decision makers with actionable intelligence to prevent acts of terrorism. On November 27, 2002, the president of the United States ordered the formation of a commission that would deliver a comprehensive account of the terror attacks and provide recommendations on how to avoid similar incidents from taking place against our nation in the future.

The report of the National Commission on Terrorist Attacks upon the United States (9/11 Commission), better known as the 9/11 Commission report, acknowledged there was a lack of unity among intelligence agencies that led to the attack by terrorists on United States on September 11, 2001. The report identifies four specific failures on the part of IC: “in imagination, policy, capabilities, and management”² Since its inception, the Department of Homeland Security (DHS) has made it a priority to support its mission of preventing terrorist attacks within the United States by infusing intelligence into its daily operations. Through information sharing with other federal, state, local, and private sector entities, DHS is able to further strengthen the overall stability of the United States. Information sharing is driven from the ground up by agents, assets, and

¹ National Commission on Terrorist Attacks upon the United States [9/11 Commission], *Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W. W. Norton, 2004). Hereafter, referred to *9/11 Commission Report*.

² *Ibid.*, 356.

stakeholders in the field; the challenge is how to aggregate, integrate, and analyze information to provide a fused picture of the homeland security environment.

This thesis examines the unique relationship between law enforcement personnel in the field and intelligence. As one of the largest uniformed federal law enforcement agencies in America, at an authorized strength of over 21,000 agents, the United States USBP (USBP) has a robust dispersion of agents along the southern, northern, and coastal borders. These agents provide pure horsepower for collections; they are the eyes and ears in the field for the homeland security intelligence enterprise. Since 9/11, the USBP has recognized the need for a specialized agent position, the USBP Border Patrol Agent-Intelligence (BPA-I), with the specific mission of driving field-level intelligence operations at the tactical level. The USBP has continually enhanced capability and capacity of its intelligence agents with a target of having approximately 1,000 BPA-I nationwide. This study compares and contrasts the current USBP intelligence mission with best practices, lessons learned, shared missions, and constraints with the IC. Furthermore, it introduces the concept of the tactical-level friendly force network, its construct, and the requirements and challenges associated with generating and sharing actionable information. The principal focus is the synthesis of an intelligence-driven, law enforcement culture in the USBP that will increase situational awareness and understanding of the homeland security ecosystem through efficient and effective collections and dissemination to all components of DHS. Through a holistic approach in evaluating the role of intelligence within the USBP, linkages between the strategic, operational, and tactical levels, this study provides a framework for risk-based, intelligence driven operations. The USBP will have to overcome the challenges of synchronizing its law enforcement culture with intelligence operations to more effectively identify, analyze, and prioritize enduring and emerging threats within the border security mission.

The thesis concludes that the synergy between law enforcement culture and intelligence operations is a difficult one to achieve yet once established, it is very powerful and irreplaceable because it can improve overall efficiency for an organization but most importantly save lives. This research leads USBP to consider instituting an

effective architecture that supports the evolutionary development of its intelligence driven border security operations and intelligence driven decision-making process at and between our U.S. ports of entry and abroad. This thesis examines the question: How does the current USBP intelligence architecture provide the necessary intelligence support to more effectively plan, collect, identify, analyze, and disseminate intelligence-related information to all stakeholders while addressing emerging threats within its border security mission on the domestic and international front?

Evidence demonstrates that over the last decade DHS, CBP, and the USBP have evolved and improved their intelligence focus and capabilities from reactive to proactively-led, intelligence-driven operations. To institute a culture of an intelligence-led border security agency, a more robust approach needs to be standardized to sustain the flexibility and adaptability the USBP requires to address future threats in the twenty-first century.

A. BACKGROUND

After the terrorist attacks of September 11, 2001, the stability of the United States was challenged by unconventional enemy tactics, techniques, and procedures (TTPs). As a result of the catastrophic event that shook our nation to its core, the U.S. Congress and the president on November 27, 2002, ordered the formation of a commission—one that would provide a full and complete account of the terrorist attacks and to provide recommendations on how to prevent similar attacks from taking place against our nation in the future.

As stated in the 9/11 Commission report, there was a lack of unity among intelligence agencies that led to the attack by terrorists on United States on September 11, 2001. The four specific failures on behalf of the IC of “imagination, policy, capabilities, and management”³ should be a reminder of what can happen when intelligence is not properly analyzed and disseminated.

³ Ibid.

The primary mission of the DHS is to “prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, and minimize the damage, and assist in the recovery from terrorist attacks that do occur in the United States.”⁴ Since 2003, DHS instituted an intelligence component known as the Directorate of Information Analysis and Infrastructure Protection that collects, analyzes, and integrates law enforcement and intelligence information. Through information sharing with other federal, state, local, and private sector entities, DHS is able to further strengthen the overall stability of the United States. DHS is part of a complex homeland security information sharing ecosystem. Figure 1 shows the southwest border information sharing community stakeholders.

⁴ P. L. 107-296, §101b(1), 116 STAT, 2142 (2002).

Figure 1. Southwest Border Information Sharing Community



Source: U.S. Department of Homeland Security, "Intelligence & Analysis Southwest Border Information Sharing Assessment," Version 1.0 (internal document, U.S. Department of Homeland Security, January 2010).

CBP has a unique and multi-dimensional mission that is charged with the management and protection of our nation's borders within the air, land, and maritime domain environments. CBP's border security mission extends beyond the actual land

borders as personnel and resources are strategically placed in countries abroad to strengthen America's border security and counter-terrorism efforts.⁵

According to the CBP webpage, on any given day, agency personnel protect more than:

- 4,000 miles of border with Canada;
- 2,000 miles of border with Mexico, and;
- 2,600 miles of shoreline.⁶

CBP also processes approximately “340 million travelers and more than 29 million trade entries annually at our nation's ports of entry (POEs).”⁷ Due to the volume associated with CBP operations, CBP collects and analyzes information and intelligence, both domestically and internationally, to prevent terrorists and their weapons from entering and conducting terrorist acts against or within the United States. Additionally, through its intelligence systems and processes, CBP is able to identify, analyze, and target, transnational criminal organizations (TCOs) operating with a nexus to the border security environment. Working jointly with other law enforcement, intelligence, and investigative partner agencies, CBP leverages its resources to further disrupt, degrade, and dismantle TCOs therefore increasing the safety and security of the United States.

Operating under the DHS umbrella, CBP has prioritized intelligence requirements and established diverse intelligence capabilities into a single cohesive intelligence enterprise known as the Office of Intelligence (OI). The OI supports all three CBP operational components: the U.S. Border Patrol (USBP), Office of Field Operations (OFO), and Air Marine Operations (AMO). The USBP is a federal law enforcement agency with a workforce of over 21,000 uniformed USBP agents that conduct law

⁵ “About,” U.S. Customs and Border Protection, accessed September 11, 2015, <http://www.cbp.gov/about>.

⁶ “On a Typical Day in Fiscal Year 2014, CBP...” U.S. Customs and Border Protection, accessed September 11, 2015, <http://www.cbp.gov/newsroom/stats/typical-day-fy2014>.

⁷ “Joint Written Testimony of CBP's USBP Chief Michael Fisher, Office of Air and Marine Assistant Commissioner Michael Kostelnik, Office of Technology Innovation and Acquisition Assistant Commissioner Mark Borkowski, and Office of Field Operations Acting Assistant Commissioner Kevin McAleenan for a House Committee on Appropriations, Subcommittee on Homeland Security hearing on the President's Fiscal Year 2013 budget request for CBP,” February 29, 2012, U.S. Department of Homeland Security, <http://www.dhs.gov/news/2012/02/29/written-testimony-us-customs-and-border-protection-house-appropriations-subcommittee>.

enforcement operations in the United States and abroad. While USBP operations are dynamic, they encompass everything from static line-watch operations and narcotics seizures to serving high-risk warrants, yet the most important mission of the USBP is preventing the entry of terrorist and terrorist weapons between U.S. ports of entry (POE). This research provides an understanding of the USBP law enforcement culture, border security mission, and intelligence enterprise that will support the evolutionary development of its intelligence driven border security operations between U.S. ports of entry and abroad.

B. THE PROBLEM

There is nothing unifying DHS's resources, both intelligence and operational, to ensure information is available to those who need it, priorities are driven from the top down, and resources are expended efficiently.

2010 DHS Southwest Border Information Sharing Assessment

Since the creation of DHS in 2003, there has been a corporate investment by CBP to create and refine CBP intelligence to enhance intelligence collection, analysis, and dissemination of information among the CBP operational components to more effectively address unforeseen threats. Concurrently, the USBP has dedicated personnel, assets, and resources to enhance its intelligence capabilities. In conjunction with the CBP Office of Intelligence (OI) support, USBP intelligence is the major field-driven collection mechanism for homeland security. It is important to understand the history and nature of this relationship to identify areas where coordination could be enhanced.

During the past 12 years, the CBP Office of Intelligence (OI) has undergone continuous top-level senior leadership changes in the last two presidential administrations. For example, in 2007, the office until then known as the Office of Intelligence was renamed the Office of Intelligence and Operations Coordination (OIOC). The focus at that time was to create synergy and liaison between intelligence and operational components while integrating the mission between both to support the mission objectives of CBP.

Soon thereafter, after another change in leadership, the office was renamed the Office of Intelligence and Investigative Liaison (OIIL) and its mission focus was broader than collecting, analyzing, and disseminating data. In addition, OIIL's efforts were expanded to include investing in building professional relationships and partnerships with other federal, state, local, tribal and international investigative agencies with the goal of creating a more efficient and effective intelligence community that supported CBP's interests and mission objectives.

This past year, under new leadership, OIIL changed its component name back to Office of Intelligence (OI). In addition, it has reorganized with a more strategic focus to support the CBP *Vision and Strategy Plan 2020* that seeks to align CBP toward a common definition of success by articulating strategic objectives along with the accounting of performance measurements. Under this current leadership, OI is now aligning its efforts and identifying methods of approach to better support CBP mission objectives within the intelligence community, both domestically and abroad, with a focus on developing and implementing strategies that support a counter-network approach against terrorist and transnational criminal networks.

Although changes in senior leadership are often a necessary evolution of the organizational life cycle, these changes often cause disruption and inefficiency among mission stakeholders. In the current CBP environment, case studies reveal a perception that OI and the other components are detached from one another both functionally and operationally.⁸ The multiple rebranding or reorganization of OI creates challenges to the creation of harmony and synchronization with the other components. Furthermore, the constant change in leadership impedes the development of a mature strategy and degrades cohesion with the field. CBP possesses a professional cadre of intelligence experts at all levels that are underutilized in informing intelligence doctrine, strategy, and standardized training. The *Interagency Team to Counter Irregular Threats Handbook*, issued by Johns Hopkins University Applied Physics Laboratory, states, "The interagency wheel

⁸ U.S. Customs and Border Protection, *FY15 Capability Gap Analysis Process* (Washington, DC: U.S. Customs and Border Protection, 2015).

continually is being reinvented because of the dearth of formal doctrine and training.”⁹ This is apparent in the absence of doctrine, strategy, and standardized training within the CBP intelligence enterprise, potentially leading to policy failures due to the absence of standard operating procedures (SOPs) implemented and standardized among the CBP operational components. In some cases, a CBP operational component like the U.S. USBP, which relies on OI for intelligence, surveillance, reconnaissance (ISR), or high altitude imagery for planning and targeting at the operational and tactical level, experiences perceived delays or disconnect from the intelligence system. Some field agents and BPA-Is may simply not be aware or understand how OI supports the border security mission. This leads to another critical problem area: strengthening the skills of the intelligence workforce to educate, train, and develop personnel to understand basic intelligence functions and exploit the new intelligence methodologies or approaches implemented corporately by the organization.

Through this research, it became evident that within USBP headquarters for some, there is no clear understanding of the OI mission nor is there a clear USBP intelligence vision, mission, and goals linking to the USBP 2012–2016 strategic plan.¹⁰ There is a need to understand and gather the requirements for staffing the right amount of intelligence personnel, equipment, hardware, and software that a large law enforcement organization of over 21,000 uniformed personnel would require to function efficiently in today’s risk-based environment. The USBP is struggling to define the appropriate intelligence staffing model. To address this, the USBP has implemented a manpower requirements determination (MRD) process to conduct analysis on staffing and force requirements; the problem with MRD is that it lacked rigor and did not align with the reality of the field. Best practices in force restructuring consider task, standard, condition, ways, means, and effects to understand capabilities and the manpower required to execute

⁹ Johns Hopkins University Applied Physics Laboratory, *Interagency Teaming to Counter Irregular Threats Handbook* (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2009).

¹⁰ U.S. Customs and Border Protection, *2012–2016 USBP Strategic Plan* (Washington, DC: U.S. Customs and Border Protection, 2012), http://www.cbp.gov/sites/default/files/documents/bp_strategic_plan.pdf.

those capabilities.¹¹ MRD only seemed to audit tasks without consideration for the varying standards and conditions in every sector. More analysis is needed to understand the activities or mission essential intelligence tasks in every sector, as well as the standards and conditions that characterize success. Only then can the appropriate and required range of manpower be calculated to model an intelligence unit that can support the border security mission in each specific area.

In addition to adequate staffing, technology is needed to manage and analyze the massive amount of border security data generated daily; however, overreliance on either technology or human judgment alone can lead to shortfalls. Intelligence fusion balances the best attributes of humans and technology. Intelligence fusion, or the process of “sensemaking,” is a complex blend of both science and art. Technology can be used to manage big data pulled from multiple, often disparate sources, but ultimately it is humans who are responsible at every level to provide inputs and analyze outputs in order to achieve desired outcomes (i.e., actionable intelligence).¹² Without proper training and development, the USBP will not be able to take advantage of the amount of personnel it has at its disposal to execute the intelligence cycle.

C. THE RESEARCH QUESTION

This research is focused on the USBP and the challenges in synchronizing a law enforcement culture with intelligence and building intelligence based decision-making processes to drive all planning and execution of border security operations. The research question to answer is, how does the current USBP intelligence architecture provide the necessary intelligence support to more effectively plan, collect, identify, analyze, and disseminate intelligence related information to all stakeholders while addressing emerging threats within its border security mission on the domestic and international front?

¹¹ Joint Chiefs of Staff, *Capabilities-Based Assessment, User’s Guide Version 3, Force Structure, Resources, and Assessments Directorate* (JCS J-8) (Washington, DC: Joint Chiefs of Staff, 2009).

¹² Mark Lowenthal, *Intelligence: From Secrets to Policy*, 4th ed. (Washington, DC: CQ Press, 2009).

The following are a few ancillary questions for consideration in support of this research topic:

1. What is the USBP intelligence vision and mission in place to direct intelligence-driven, border security operations?
2. How does the USBP streamline collections and information sharing internally and externally within the homeland security ecosystem?
3. How has the workforce been adequately educated, trained, and equipped to facilitate intelligence driven operations?
4. What are the requirements for implementing information sharing technology to support intelligence collection, analysis, and dissemination for better efficiency, transparency, and accountability among its components and partner agencies?
5. How does the USBP use its Red Team capability in support of intelligence and operations to fully explore alternatives in plans, concepts, organizations, and capabilities in the context of the border security mission?
6. How can the USBP support its Intelligence Division to enhance its capability and capacity to execute the intelligence cycle in support of the *USBP 2012–2016 Strategic Plan*?

D. METHODOLOGY

This thesis stems from the past and present endeavors to build a robust, resilient, and high-functioning homeland security intelligence enterprise driven by open and timely information sharing among components. The foundation of the intelligence enterprise is the friendly force network, which is a framework of nodes (friendly force actors or stakeholders) and links (communication channels and relationships). The base unit of the friendly force network is people: the agents, officers, analysts, and professional staff that work for a federal, state, local, tribal, international, or private partners. In addition, communities of interest (COIs) are comprised of the private citizens who live and work in the border security environment. Together, it is the connections and relationships between people that provide the framework for information sharing at the lowest level. This thesis examines three case studies to analyze the USBP intelligence unit through a descriptive lens of complex realism, or analyzing the relationships between the USBP

intelligence enterprise and its individual units, to understand the phenomenology of information sharing from the ground up.¹³

Linking intelligence theory with practical application is a complex and traditionally challenging exercise common to many disciplines. The results of the fiscal year (FY) 15 USBP operational capability gap analysis process (CGAP) is the first case study in this thesis examining the intelligence gaps revealed nationwide. The CGAP methodology was developed by the USBP and the Johns Hopkins University Applied Physics Laboratory Asymmetrical Warfare Unit using the scientific method to apply rigorous modeling and analyses techniques to the border security environment.¹⁴ The CGAP was designed to provide the highest degree of expedience while preserving the core elements of scientific method, academic rigor, and analysis. The CGAP is a scalable, flexible, and versatile process that can escalate rigor and resource to be commensurate to the complexity of the problem or environment being analyzed based known time constraints. The USBP has been utilizing CGAP throughout the nation to identify operational gaps because it can be agent-executed, using basic metrics and analytical processes to assess the border security environment; or when applicable, it can utilize analytical support from outside contractors and scientists to apply rigorous modeling, analyses techniques, and evaluative measures. The fidelity of the information resulting from CGAP sessions is an accurate reflection of the rigor associated with completing the process.

The second case study this thesis adds granularity to the challenges associated with information sharing from the field to intelligence units, a USBP centric information sharing study was conducted in Tucson sector. The study focuses on assessing the level of ease and confidence through which USBP agents performing line-watch operations are able to share information they collected with intelligence personnel tasked with analysis. Additionally, the information sharing study looks to identify the gaps in effective

¹³ Liu Feng, and Zhang Ruizhuang, "The Typologies of Realism," *The Chinese Journal of International Politics* 1, no 1 (2006): 109–134.

¹⁴ Johns Hopkins University Applied Physics Laboratory, *Interagency Teaming to Counter Irregular Threats Handbook*.

communication and trust between the field collectors and the intelligence personnel. While there is a need to conduct additional research, the information sharing study indicates the need to standardize intelligence collections and dissemination processes to improve overall communications between the field and intelligence.

The third case study this thesis examines is the Red Team study conducted by a Tucson Sector Red Team in Ajo, Arizona, utilizing applied critical thinking skills, data analysis, threat assessments, and friendly force capabilities to assess whether there were any early warning factors that could have been identified and planned against to avoid a spike in illicit migration and narcotics smuggling through the named area of operations. The analysis yielded several strategic indicators that could have been utilized to develop and coordinate intelligence driven operations to mitigate the high rate of criminal activity traversing through the west desert.

This thesis will test the validity of two hypotheses:

- *Hypothesis 1:* The USBP has the capability and capacity to execute the intelligence cycle to provide situational awareness from the ground up; however, the USBP needs to understand its current capability baseline in order define capability gaps, mission needs, and requirement.
- *Hypothesis 2:* The USBP Intelligence Division does not have a published unified vision and mission that provides meaning, understanding, and guidance to the intelligence agent in the field of their role in the overall intelligence enterprise.

All portions of this study rely on the compiled literature on homeland security strategic documents, intelligence doctrine, and internal USBP intelligence documents.

E. CHALLENGES

According to the Central Intelligence Agency Center for the Study of Intelligence, analytical systematic biases can have an impact on the outcome of any intelligence analysis.¹⁵ This research must take into consideration three identified types of hindsight bias that could affect the analysis of the events concerning this thesis.

¹⁵ "Hindsight Biases in Evaluation of Intelligence Reporting," Center for the Study of Intelligence, Central Intelligence Agency, 1999, <http://www.au.af.mil/au/awc/awcgate/psych-intel/art16.html>.

- Overseers of intelligence production tend to overestimate the degree to which events might have been foreseen.
- Analysts tend to overestimate the accuracy of their own past judgments.
- Intelligence consumers tend to underestimate the true value of intelligence analysis.¹⁶

The Chapter II comprises a comprehensive synthesis of relevant doctrine, reports, and studies. Chapter III is an overview of the Homeland Security Intelligence Enterprise architecture, and Chapter IV provides in-depth analysis of USBP internal case studies on intelligence at the strategic, operational, and tactical level along with the assessment of a friendly force network to support intelligence efforts in the field environment. Chapter V outlines solutions and recommendations for the USBP to enhance intelligence capability and capacity.

¹⁶ Ibid.

II. LITERATURE REVIEW

Facts are stubborn things...Whatever may be our wishes, our inclinations, or the dictates of our passions; they cannot alter the state of facts and evidence.

John Adams

The following is a review of available literature that relates to the challenges and issues associated with synchronizing intelligence within a law enforcement culture and organization. This literature review also provides insight into the IC, Department of Defense (DOD), federal agencies, and domestic law enforcement intelligence to examine their strategic guidance, best practices, and lessons learned. In addition, the literature expands to border security and the role of intelligence within CBP and USBP to support intelligence driven border security operations and counter-network approaches that target transnational criminal organizations (TCOs). Other research to support this literature review includes reports from the Government Accountability Office (GAO), Congressional Research Service (CRS), public policy organizations, and academia.

A. USBP 2012–16 STRATEGIC PLAN AND CBP VISION 2020

The foundational doctrine in any organization communicates the vision and mission for the workforce so it can connect its daily activities to the overall strategic plan.¹⁷ “Strategic plans” are ordered and developed within each tier of the government to describe what these organizations are doing to successfully accomplish a “whole of government approach” to achieve the mission of national security.¹⁸ The CBP vision 2020 highlights the need for an enterprise information sharing system.

¹⁷ U.S. Department of Homeland Security, *Strategic Plan, Fiscal Years 2012–2016* (Washington, DC: U.S. Department of Homeland Security, 2012).

¹⁸ White House, *National Drug Control Strategy* (Washington, DC: White House, 2011), <https://www.whitehouse.gov/sites/default/files/ondcp/ndcs2011.pdf>.

Figure 2. CBP 2020 Vision and Strategy

CBP 2020 Vision and Strategy

To maintain a continuous understanding of the dynamic and asymmetric global threat environment, CBP must enhance its ability to collect, analyze, and appropriately share intelligence and information. This includes providing timely warnings of potential threats and proactive enforcement opportunities. No single agency has a complete picture of the entire threat environment. Thus, CBP must lead and aggressively champion strategic partnerships to enhance intelligence and information sharing with our Federal, state, local, tribal, territorial, and international stakeholders. In this regard, the CBP Law Enforcement Intelligence Enterprise serves as a powerful border security partnership connecting the law enforcement and intelligence communities.

Source: U.S. Customs and Border Protection, *2020 Strategic Overview: Vision and Strategy 2020* (Washington, DC: U.S. Customs and Border Protection, 2015), <http://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf>.

The literature review includes the analysis of an array of Government Accounting Office (GAO) reports, agency audits, and testimony relevant to national security. The GAO is tasked with the review of government agency strategic plans and provides progress reports to Congress on their success and failures. Reporting and accountability on valid performance measures is an important aspect to understanding the effectiveness of intelligence. Strategy and policy development also play a key role in outlining the role of intelligence in a border security agency like the USBP. In one report, the “GAO identified a set of desirable characteristics to aid government agencies in developing and implementing strategies and to enhance their usefulness in resource and policy decisions to better ensure accountability.”¹⁹ The characteristics the GAO identified are:

1. Purpose, scope, and methodology;
2. Problem definition and risk assessment;
3. Goals, subordinate objectives, and performance measures;
4. Resources, investments, and risk management;
5. Organizational roles, responsibilities, and coordination;
6. Integration and implementation.²⁰

¹⁹ U.S. Government Accountability Office, *Border Security: DHS Progress and Challenges in Securing the U.S. Southwest and Northern Borders* (GAO-11-508T) (Washington, DC: U.S. Government Accountability Office, 2011), 1.

²⁰ Ibid.

B. JOINT TASK FORCES AND FUSION CENTERS

The September 11, 2001 attacks were the impetus for new practices, partnerships, and innovations in information sharing among DOD, law enforcement, and private entities. As of 2015, there are over 78 fusion centers to facilitate the integration of federal, state, local, and territorial partners with the overarching goal to share information in order to prevent and combat potential terrorist activity.²¹ Strategic plans for government entities, such as the DOD, DHS, and the Department of Justice (DOJ), have tenets, objectives, or initiatives to support “whole of government” and “unity of effort” approaches to information sharing in order to leverage partnerships to enhance operational efficiency and effectiveness.²² Fusion centers are primarily intended to be a whole of government, integrated nexus of counterterrorism intelligence collection and analysis. Although fusion centers were originally intended to collect against terrorism and terrorist activities, fusion centers are utilized as all-purpose, all-source information centers that serve as a multiagency clearinghouses to address threats to the public domain relating to crime, hazards, and disaster response and recovery.

There are questions and concerns as to whether and to what degree fusion centers are effective at preventing and anticipating terrorism, the nature of fusion center law enforcement support, and the irresponsible or illegal collection, analysis, and dissemination of information on U.S. citizens. Administrative issues persist regarding efficient command and control (C2) common to multiagency cooperation. The purpose of this section is to examine the research on fusion centers to discern the fundamental gaps in knowledge and determine where more research is needed to elucidate the true efficacy and/or deficiencies of fusion centers.

The Government Accountability Office (GAO) reports reveal that the majority of fusion centers were established to address information sharing gaps and generally have broad mission parameters encompassing intelligence collection related to counterterrorist

²¹ U.S. Department of Homeland Security, “State and Major Urban Area Fusion Centers,” last modified September 14, 2015, <http://www.dhs.gov/state-and-major-urban-area-fusion-centers>.

²² Torin Monahan, and Neal A. Palmer, “The Emerging Politics of DHS Fusion Centers,” *Security Dialogue* 40, no. 6: (2009): 617–636.

activity and as well as other pertinent law enforcement information.²³ These guidelines allow for the expanded scope of practice from counterterrorism collection to “all crimes with national security implication” and “all hazards” information that are deemed fundamentally important to the information sharing environment and implement the national strategy.

Bustria, Shenouda, and McDaniel note that the challenge of establishing a fusion center is identifying a “systematic process that translates national strategy and guidelines into state and local policies that will drive the operations of the fusion center.”²⁴ Paté-Cornell presents a quantitative research study examining the probability and risk analysis of information collected and analyzed by fusion centers. Additionally, Paté-Cornell’s main holding simplifies the fusion center to two essential functions: internal communications and the merging of intelligence collected.²⁵ Thus, the primary goal of fusion centers is to collect information to prevent terrorism, but the functional role of fusion centers is to leverage partnerships to enhance effectiveness against common “all crime” or “all hazard” targets.²⁶

There have been few reportable terrorism related incidents that have been prevented; hence, the paradox of knowing the unknowable.²⁷ Experts have maintained that a catastrophic event like 9/11 has such a low probability that there is little likelihood that a terrorism plot could be uncovered by fusion centers.²⁸ The research shows that

²³ U.S. General Accountability Office, *Northern Border Security: DHS’s Report Could Better Inform Congress by Identifying Actions, Resources, and Time Frames Needed to Address Vulnerabilities* (GAO-09-93), (Washington, DC: U.S. General Accountability Office, 2008).

²⁴ John Bustria, Emad Shenouda, and Michael McDaniel, “The Functional Desks as Collaborative Mechanisms in the Michigan Intelligence Operations Center,” *Homeland Security Affairs*, Supplement no. 2 (2008) <http://www.hsaj.org/?article=supplement.2.4>.

²⁵ Elisabeth Paté-Cornell, “Fusion of Intelligence Information: A Bayesian Approach,” *Risk Analysis* 22, no. 3 (2002): 445–454.

²⁶ Bart Johnson, “A Look at Fusion Centers: Working Together to Protect America,” *FBI Law Enforcement Bulletin* 76, no. 12 (2007): 28–32.

²⁷ James N. Mattis, *USJFCOM Commander’s Guidance for Effects-based Operations* (Carlisle Barracks, PA: Army War College, 2008); Jude McCulloch, and Sharon Pickering, “Pre-crime and Counter-terrorism Imagining Future Crime in the ‘War on Terror,’” *British Journal of Criminology* 49 no. 5 (2009): 628–645.

²⁸ Torin Monahan, “The Future of Security? Surveillance Operations at Homeland Security Fusion Centers,” *Social Justice* 37, no. 2–3 (2010): 84–98.

outside of “pro law enforcement” studies, fusion centers are undervalued or criticized for their contribution to everyday law enforcement efforts. It is evident from various doctrines that although counterterrorism is the primary goal of fusion centers, secondary functions include supporting law enforcement efforts. In addition, fusion centers are commonly known to provide valuable services outside the usual counterterrorism mission, such as assistance with routine criminal investigations, public safety, or disaster response, and recovery efforts.

The U.S. Senate Committee on Homeland Security and Governmental Affairs conducted an investigation into fusion centers to determine if there has been an acceptable return on investment. Upon completion, the investigation revealed that the collaboration between DHS and local fusion centers was not productive and had not yielded any valuable support towards federal counterterrorism efforts.²⁹ The Senate report was contemptuous in tone as it contradicts public statements made by DHS officials, who described fusion centers as “one of the center pieces of our counter terrorism strategy and a major force multiplier in the counterterrorism enterprise.”³⁰ The Senate committee investigation also recognized that fusion centers “often produced irrelevant, useless or inappropriate intelligence reporting to DHS, and many produced no intelligence reporting whatsoever.”³¹ The most poignant criticism of fusion centers is that no fusion center reporting has uncovered a terrorist or contributed to any disruption of an active terrorist plot. The Senate report specifically states that it was evaluating fusion centers on the sole criteria of the “counterterrorism objectives established by law, Executive Strategy, and DHS policy statements and assessments.”³² This assessment methodology drastically undervalues the operational effectiveness of fusion centers as they contribute to other objectives that support national strategic plans. One valid

²⁹ U.S. Senate Permanent Subcommittee on Investigations Committee on Homeland Security and Governmental Affairs, *Federal Support for and Involvement in State and Local Fusion Centers Majority and Minority Staff Report Permanent Subcommittee on Investigations*, 2012, <https://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers>.

³⁰ Ibid.

³¹ Ibid.

³² Ibid.

conclusion of the Senate committee report was the need for “oversight to strengthen the protection of civil liberties in fusion center intelligence reporting.”³³ The largest deficiency of the report was that it did not evaluate any other metrics related to the benefits of fusion centers outside of counterterrorism efforts. If all agencies with a counterterrorism mandate were evaluated by similar standards, similar disparaging results would occur.

Joint intelligence-sharing fusion centers are a theoretically sound and logical framework to share, collate, and analyze information among federal, state, local, and tribal law enforcement partners. Fusions centers provide a focal point for raw data to be merged, analyzed, and processed into viable intelligence. It is evident that there is a perception that fusion centers potentially abuse the mandate of conducting counterterrorism collections by surreptitiously collecting information about U.S. citizens.³⁴

More research on fusion centers is needed to illuminate present issues. Policy needs to be scrutinized to ensure adequate measures to protect U.S. citizen’s right to privacy are being implemented and adhered to on a regular and enforceable basis. Best practices on how to process the massive amounts of information and separate the wheat from the chaff is another persistent concern. There are evident problems with establishing a joint chain of command and how to develop and sustain the culture of a “need to share” environment from the traditional “need to know” custom. Research is needed to examine the enablers of a strong unity of effort within law enforcement culture to dispel the tribalism among individual groups and agencies. In the current government economic situation with large depth and looming budget cuts, programs must be resource neutral in the current and future resource constrained environment.

C. DEFINING INTELLIGENCE

A review of available literature demonstrates that there is not a standard definition of intelligence used by all. On the contrary, defining intelligence is more unique and

³³ Ibid.

³⁴ Monahan, and Palmer, “The Emerging Politics of DHS Fusion Centers.”

complex. The Federal Bureau of Investigation website defines intelligence. It states, “intelligence is information that has been analyzed and refined so that it is useful to policymakers in making decisions—specifically, decisions about potential threats to our national security.”³⁵

In his book titled, *Intelligence: From Secrets to Policy*, Mark Lowenthal defines intelligence as “information that meets the stated or understood needs of policymakers and has been collected, processed, and narrowed to meet those needs.”³⁶ In a way, intelligence is information that provides greater situational awareness to the policymaker on a particular topic to influence decision making. However, as Lowenthal clearly outlines, “All intelligence is information; not all information is intelligence.”³⁷ The USBP has not clearly messaged to the field a clear and concise intelligence definition therefore delaying the internal intelligence maturation process.

D. DEPARTMENT OF DEFENSE AND DOMESTIC LAW ENFORCEMENT INTELLIGENCE

The homeland security joint publication published by the Joint Chiefs of Staff:

directs commanders of combatant commands, sub-unified commands, joint task forces, subordinate components of these commands, and the Services to conduct planning and operations to prepare to detect, deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests, and to mitigate the impact of adversary actions.³⁸

Intelligence related information plays a critical role within the DOD, especially in the homeland defense and civil support arena when engaging in emergency preparedness.

Domestic law enforcement intelligence related information is also crucial to the stability of the United States, its borders, and its communities. The U.S. Department of Justice (DOJ) has invested a significant amount of effort in strengthening and streamlining the information sharing capabilities among domestic law enforcement

³⁵ Federal Bureau of Investigation, “Intelligence Defined,” accessed November 22, 2014, <http://www.fbi.gov/about-us/intelligence/defined>.

³⁶ Lowenthal, *Intelligence: From Secrets to Policy*.

³⁷ Ibid.

³⁸ Joint Chiefs of Staff, *Counterterrorism* (JP 3-26), (Washington, DC: Joint Chiefs of Staff, 2005).

agencies. Through its various information sharing programs, DOJ has increased the capabilities of local law enforcement by providing it actionable information increasing the situational awareness of officers at all levels of government.

According to the Homeland Security Act of 2002:

The primary mission of the Department of Homeland Security (DHS) is to 'prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, and minimize the damage, and assist in the recovery from terrorist attacks that do occur in the United States.'³⁹

Since 2003, DHS instituted an intelligence component known as the Directorate of Information Analysis and Infrastructure Protection that collects, analyzes, and integrates law enforcement and intelligence information.

The 9/11 Commission report from 2004 identified the ability to share information as one of the key factors associated with the failure in preventing the attacks of September 11, 2001.⁴⁰ Similarly, Mark Randol in a 2010 Congressional Research Service (CRS) report points out:

Congress also made information sharing a top priority of the new DHS intelligence organization, requiring it to disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal government with responsibilities related to homeland security, and to agencies of State and local government and private sector entities, with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.⁴¹

Also in a CRS report, Randol describes the larger DHS intelligence enterprise and provides an understanding of the DHS stakeholder agencies with intelligence responsibilities.⁴² This report provides a clear delineation on the role and duties of each agency and their contribution to the overall DHS intelligence and counter-terrorism

³⁹ P. L. 107-296, §101b(1), 116 STAT. 2142 (2002).

⁴⁰ 9/11 Commission, *9/11 Commission Report*, 353–356 and 416–418.

⁴¹ P. L. 107-296, §201d(1), 116 STAT. 2146 (2002); Mark A. Randol, *The Department of Homeland Security Enterprise: Operational Overview and Oversight Challenges for Congress* (Washington DC: Congressional Research Service, 2009).

⁴² Randol, *The Department of Homeland Security Enterprise*.

effort. Randal writes that some argue the DHS intelligence enterprise is too broad and counterproductive, as a result of the vast amount of information

Richard Best, in a CRS report titled, *Securing America's Borders: The Role of the Intelligence Community*,⁴³ explains the role that the various federal agencies and local law enforcement play within the intelligence community. He further explains that one of the challenges of information sharing between federal and local law enforcement is that at times both are gathering intelligence from the same sources and therefore, creating duplication of effort or redundancies.

This literature review demonstrates that intelligence is vital to DHS, CBP, and the USBP as it provides critical information for increased situational awareness on known threats against the homeland. This type of information allows decision makers and policymakers within the USBP organization to execute tactical, operational, and strategic decisions within the homeland security environment that impacts the safety and security of its personnel, citizens, borders, and critical infrastructure.

⁴³ Richard Best, *Securing America's Borders: The Role of the Intelligence Community* (Washington DC: Congressional Research Service, 2010).

THIS PAGE INTENTIONALLY LEFT BLANK

III. HOMELAND SECURITY INTELLIGENCE ENTERPRISE

The Department of Homeland Security was created not to increase the size of the government, but to focus and integrate our collective efforts.

DHS 2004, *Securing our Homeland*.

A. INTELLIGENCE AND BORDER SECURITY

Although the terrorist attacks against the United States took place over 14 years ago, our country continues to confront a complex and rapidly changing security environment. The Homeland Security Enterprise (HSE) is inclusive of all stakeholders within DHS, including its component organizations and its intelligence offices, the members of the Intelligence Community (IC), the private sector, and state, local, tribal, and territorial governments.⁴⁴ The DHS Office of Intelligence and Analysis (I&A) is the lead provider of intelligence and analysis for the HSE. The DHS I&A's mission encompasses four core functions to: analyze, collect, share, and manage.⁴⁵ DHS I&A and the U.S. Coast Guard are the only two DHS agencies identified as members of the Intelligence Community.

The Intelligence Community is defined by the Office of the Director of National Intelligence (ODNI) as “a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.”⁴⁶ Some of these activities include:

- Collection of information needed by the president, the National Security Council, the secretaries of state and defense, and other executive branch officials for the performance of their duties and responsibilities.
- Production and dissemination of intelligence.

⁴⁴ U.S. Department of Homeland Security, *Intelligence and Analysis Strategic Plan 2011–2018* (Washington, DC: U.S. Department of Homeland Security, 2011).

⁴⁵ *Ibid.*

⁴⁶ Office of the Director of National Intelligence, “ODNI FAQ,” accessed April 4, 2015, <http://www.dni.gov/index.php/about/faq?start=2>.

1. USBP Intelligence

Since 2012, the USBP has incrementally increased its intelligence capabilities and capacity with a target hiring of 1000 USBP BPA-Is. BPA-Is are supported by non-uniformed intelligence analysts, typically at an approximate ratio of less than one analyst per 10 BPA-I. In addition, stations and sectors may choose to authorize collateral intelligence duties for regular agents. Stations also support the USBP intelligence enterprise with agents tasked with tactical collections and plain clothes or low profile operations to disrupt smuggling. The USBP currently has 1026 intelligence agents or BPA-Is. As intelligence practitioners, the BPA-I acts as intelligence collectors and analysts at the field level. The BPA-I mission is to perceive, understand, and communicate the approximate reality of the border environment to policymakers, or in the USBP's case the chain of command (CoC) of first and second line supervisors through the patrol agent in charge at the station level, chief patrol agent of a sector, and headquarters staff up to the chief of the USBP. Although Lowenthal states that intelligence is not about the truth,⁴⁸ the BPA-I must endeavor to stay true to the intelligence mission to inform operations. BPA-I must try to remain objective, minimize bias, and to operate independently of policy considerations; objectivity is the intelligence agent's first commandment.⁴⁹

⁴⁸ Lowenthal, *Intelligence: From Secrets to Policy*.

⁴⁹ Robert Clark, *Intelligence Analysis*, 4th ed. (Washington, DC: CQ Press, 2013), 336.

Figure 4. USBP Intelligence-driven Operations

USBP 2012–2016 STRATEGIC PLAN

Intelligence-Driven Operations

Identifying and developing a comprehensive understanding of terrorist and transnational criminal threats to the Nation's borders is paramount in accomplishing the Border Patrol's mission. We must operate by strategically using intelligence to ensure that Border Patrol operations are focused and targeted against areas of high risk, such as potential terrorist threats and Transnational Criminal Organizations (TCO).

To accomplish the Border Patrol's mission, we must continue to integrate intelligence and enforcement capabilities into the planning and execution of CBP

Source: U.S. Customs and Border Protection, *2012–2016 USBP Strategic Plan*.

2. BPA-I

The BPA-I position was implemented in 2012 and is currently staffed at approximately 1026 agents throughout the nation. What this means for the USBP as an organization is the standardization and implementation of a nationally recognized position through the Office of Personnel Management. The USBP has now distinguished one set of USBP agents from the other based on a job description that is specific to a certain discipline. While being a BPA is still a current precursor requirement for the BPA-I, it will soon create a wider knowledge gap between a BPA and a BPA-I with the standardization and institutionalization of training and job requirements. BPA-Is will have a separate set of tasks from the recurring USBP mission essential tasks of detecting, identifying, classifying, responding, and resolving. The BPA-I is the only position within federal law enforcement with a specific intelligence nexus that does not require an agent having an intelligence background or experience. While most BPA-Is tend to have some sort of intelligence background, the USBP has not standardized, institutionalized, or memorialized the requirements for the BPA-I other than minimal information used in vacancy announcements.

Figure 5. USBP Intelligence Synthesis



Source: U.S. Customs and Border Protection, *2012-2016 USBP Strategic Plan*.

The current lack of BPA-I training and lack of established doctrine resembles a common theme throughout the USBP. Even with the lack of doctrine within the USBP and more specifically USBP intelligence that does not mean the organization has operated without any established process throughout the years. There are several different standard operating USBP 2012-2016 STRATEGIC PLAN procedure (SOP) documents that detailed the SIU roles and responsibilities. One example is a 1997 document titled *U.S. Border Patrol Sector Intelligence Unit: Standard Operating Procedure*, which references the *Border Patrol Handbook* (Rev. 04/85), *Immigration and Naturalization Services (I&NS) Administrative Manual (AM)*, *I&NS Intelligence Officer Handbook* (Rev. 10/88), and *Guidelines for Intelligence Analysis* (Rev. 09/93). This is proof that the USBP has made several efforts throughout its history to standardize, institutionalize, and memorialize an operationally functional intelligence construct. Previously drafted intelligence related documents that guide the USBP through and towards a productive

and comprehensive implementation of the intelligence cycle have been generated consistently for over 25 years. Without continuity within the USBP intelligence units at all levels, there is no succession management and hefty corporate knowledge losses due to attrition and career progression.

The USBP has routinely adapted military planning and coordination as an internal planning process. The researched USBP intelligence SOPs follow the SMEAC format (situation, mission, execution, administration/logistics, command/signal), which provides the reader with simple yet detailed information needed to accomplish the mission. The mission excerpt in Figure 6 was taken from an intelligence SOP from 1997 to illustrate the similarity of expected outcomes from times past to current operational needs.

Figure 6. U.S. Border Patrol Sector Intelligence Unit 1997 Standard Operating Procedure

Mission: The mission of the Sector Intelligence Unit (SIU) is to provide the Chief Patrol Agent, his staff, Patrol Agents in Charge and field agents with current intelligence. The SIU will continually analyze information gathered from all sources in order to predict future changes in the operational environment relating to the enforcement of Title 8 U.S.C. (alien smuggling) and Title 21 U.S.C. (narcotics smuggling) in support of the Chief Patrol Agent's operational strategy and the mission of the United States Border Patrol. The SIU is also responsible for coordinating the flow of intelligence information throughout the sector and the collection and dissemination of information to and from higher headquarters, adjacent sectors and other law enforcement agencies." (U.S. Border Patrol Sector Intelligence Unit—Standard Operating Procedure 1/1/1997).

Source: U.S. Border Patrol Sector Intelligence Unit, *Standard Operating Procedure* (Washington, DC: U.S. Border Patrol Sector Intelligence Unit, 1997).

It is difficult to make a comparison between a BPA-I and other intelligence related positions within the federal government. The fact is that intelligence agencies have very specific job responsibilities for those that are intelligence professionals. The reason for the level of specificity amongst intelligence practitioners is the level proficiency not only needed to develop but to implement their specific skill set to a national security issue. Moreover, the intelligence professional needs to have access to

top secret compartmented information in order to adequately conduct the proper analysis. BPA's are not currently required to have any clearance when first employed with the USBP. The lack of across the board standardized security clearances for USBP agents may adversely delay the organizational ability to adapt to emerging threats due to a lack of established processes.

For the purposes of context in comparing and contrasting BPA-I with other intelligence professionals, below are the requirements and specific experiences needed for a general scale 12, intelligence specialist position with the Department of Defense:

- Working knowledge of the DOD IC, including analytical production and intelligence requirements validation.
- Working with a management team to develop and implement an assessment methodology that can be duplicated on a consistent basis.
- Applying techniques and methodologies to problems with different aspects.
- Preparing a variety of written reports to establish tactical and strategic planning with regards to future utilization of a signals intelligence (SIGINT) collection asset.

Specifically, the specialist will be evaluated on the following competencies:

1. Knowledge of the Intelligence Community and the intelligence requirement process.
2. Knowledge of SIGINT and geospatial intelligence (GEOINT).
3. Ability to work independently with minimal guidance and direction.
4. Knowledge of foreign intelligence services, organizations, objectives and modus operandi.⁵⁰

3. BPA-I Requirements

The basic qualification requirements for a BPA-I position includes “experience in law enforcement or other responsible work that demonstrates the ability to make arrests and exercise sound judgment in the use of firearms; to deal effectively with individuals or

⁵⁰ “Intelligence Operations Specialist—SV-0132-J,” Office of Personnel Management, accessed November 5, 2015, <https://www.usajobs.gov/GetJob/ViewDetails/422301600>.

persons in a courteous, tactful manner; and to analyze information rapidly and make prompt decisions.”⁵¹

The above comparison is extremely skewed towards intelligence professionals conducting intelligence operations. A BPA-I needs only to be a BPA in good standing with the required time in service that accurately reflects the “required” experience. There is no mention or elicitation of specific intelligence requirements, whether they be academic or on learned on the job through experience. As the USBP continues to evolve, intelligence operations need to keep up with established IC guidelines to ensure data integrity and analysis fidelity. This can be instituted through a standardized training curriculum that will institutionalize the requirements for a dynamic BPA-I workforce. Additionally, it should not go unmentioned that the USBP has the capability of being one of the most proficient federal law enforcement collection agencies in the country due to the sheer number of uniformed personnel. This could be accomplished by emulating and instituting the “every soldier is a sensor (ES2)” concept developed by the Army.

According to an Army field manual, soldiers that have been immersed within an ES2 construct will be:

trained to actively observe for critical indicators related to CCIRs; will be competent in reporting their experience, perception, and judgments in a concise, accurate manner; Leaders will understand how to optimize the collection, processing, and dissemination of information in their organization to enable the generation of timely intelligence; and, technology enablers will anticipate and requisition to connect the Soldier to the intelligence process through digital reporting in real time.⁵²

According to the 2008 Army posture statement:

The routine observation and reporting of patterns and changes in the operating environment through interaction with the local populace are ES2 tasks now incorporated in Army doctrine, all initial entry training, and collective training at Army combat training centers.⁵³

⁵¹ Ibid.

⁵² Headquarters, Department of the Army, *Soldier Surveillance and Reconnaissance: Fundamentals Of Tactical Information Collection* (FM 2-91.6) (Washington, DC: Headquarters, Department of the Army, 2007).

⁵³ “2008 Army Posture Statement,” U.S. Army, February 6, 2008, <http://www.army.mil/aps/08/>.

Strategic messaging and training will be necessary to implement an ES2 type capability in the USBP. This strategic message should align to the strategic goals and objectives of a higher-level intelligence plan, but communicate directly to every agent, asset, and stakeholder in the field that *they* are a collector. To keep it simple, a USBP ES2 concept requires three elements. First, agents should be provided a simple indicator list, a list of observable phenomenon for agents to look for, by their local intelligence unit. Second, agents should be provided a method of communication that is simple, fast, and easy to execute to send information. Third, agents should be provided feedback on the information they collect for validation and training purposes. These concepts are further explored in the analysis and solutions sections of this paper.

B. ON SITUATIONAL AWARENESS

It is assumed that good situational awareness leads to good decision-making, which is expected to result in a good outcome.

Melinda Stanners and Han Tin French, 2005.

The 2004 DHS strategic plan was the first effort to describe an enterprise approach to homeland security after the 9/11 attacks. The first goal outlined in the 2004 DHS strategic plan was “**Awareness:** Identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.” Awareness, or more precisely situational awareness (SA), is not only an end state but also a constant action to be cognizant of the state of affairs at any given moment. The USBP defines SA as:

Knowledge and understanding of information that promotes timely, relevant, and accurate assessment of friendly, enemy, and other activities within the operational environment to facilitate decision making. An operational/informational perspective to determine quickly the context and relevance of events as they happen.⁵⁴

⁵⁴ Mica R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems,” *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37, no. 1 (1995): 32–64; Peter P. Perla, Michael C. Markowitz, and Christopher, A. Weuve, *Transforming Naval Wargaming: A Framework for Operational-Level Wargaming* (Alexandria, VA: Center for Naval Analysis, 2004), <https://www.usnwc.edu/getattachment/Research---Gaming/War-Gaming/Documents/Publications/Articles/Transforming-Naval-Wargaming-A-Framework-for-Operational-Level-Wargaming.pdf.aspx>.

Endsley conceptualizes SA as a function of time and space, perception of the past, compression of the present, and projection of the future. Rephrased, this is a cycle of being cognizant of “what has happened” in order to create meaning that informs the impacts on current events. Projection, perhaps the most important yet most difficult aspect of SA, is to anticipate the future and preemptively adjust actions to shape the future by influencing a desired outcome and mitigating undesirable outcomes. This is the essence of the role of intelligence on operations: to understand the truth of a situation. It is useful to analyze the nature of truth and its relationship to intelligence.⁵⁵

The original entrance to Central Intelligence Agency (CIA) headquarters at Langley has a Bible verse etched in the wall, “And ye shall know the truth, and the truth shall make you free.” Clark quotes Pontius Pilate, who asked “What is truth?”⁵⁶ The concept of and meaning of truth has been debated and discussed throughout the ages in many cultures and religions.⁵⁷ These are the questions we are examining now through the filter of intelligence. DHS, CBP, and ultimately the USBP seek “truth” in establishing situational awareness to inform understanding, measuring, and defining border security. The USBP will need to continue to refine its intelligence mission to deliver timely, accurate, and relevant information to add context to the state of the border.

C. INTELLIGENCE AND POLICY

The nature of intelligence is not only to provide situational awareness to the agents in the field but to inform strategy and policy throughout the USBP CoC. Members of the CoC has a constant need for intelligence to inform their decisions.⁵⁸ BPA-Is then must not be influenced by the CoC and seek information solely to confirm their decisions with disregard to other relevant information. BPA-I must be policy neutral or risk the politicizing the intelligence. Lowenthal suggests that the politicization of intelligence is

⁵⁵ Mica R. Endsley, “Measurement of Situational Awareness in Dynamic Systems,” *Human Factors*, 37 (1995): 32–64.

⁵⁶ Clark, *Intelligence Analysis*, 127.

⁵⁷ John Koethe, “Poetry and Truth,” *Midwest Studies in Philosophy* 33, no. 1 (2009): 53–60; David Simson “Truth, Truthfulness and Philosophy in Plato and Nietzsche,” *British Journal for the History of Philosophy* 15, no. 2 (2007): 339–360.

⁵⁸ Lowenthal, *Intelligence: From Secrets to Policy*, 3.

“one of the strongest expressions of opprobrium that can be leveled in the U.S. intelligence community.”⁵⁹ Bruce and George advocate for focus on maintaining policy relevance while avoiding policy advocacy.⁶⁰ The nature of the BPA-I mission, the command structure of the CoC, and the culture of law enforcement should mitigate the potential for political bias toward any specific agenda.

The BPA-I and the CoC should have a symbiotic relationship. The CoC provides guidance, intent, and direction, while the BPA-I provides the CoC with estimates, facts, and informed assumptions to provide greater understanding of the border security environment. Nonetheless, it should be noted that both parties are subject to bias. The best-case scenario would be where the BPA-I and the CoC seek to know the “truth” of a situation and desire to understand and frame the truth in a useful context. The worst-case scenario would be the politicization of intelligence based on poor analysis influenced by bias. Reality is somewhere in between. It is the duty of the BPA-I and the CoC to commit to objectivity to accomplish the mission: the protection of the American people, the preservation of freedom, and the continual improvement of the analytical process.

Often, too much bureaucratic oversight influences analysts to find the “book answer or politically correct answer”⁶¹ Analysts need the freedom to explore alternative perspectives and be unburdened from fear of erring. Luikart suggests that the “farther away” an intelligence analysis is removed from a decision maker, the more likely the information may not be taken seriously. In nearly every intelligence failure, the dissemination process did not communicate the right information to the right people who could act upon it.⁶² Effective warning and response are vulnerable to the potential gap between the CoC and BPA-I. Luikart explains that to bridge the gap between warning and response, the CoC and BPA-I will have to “search for common ground in understanding the strengths and weaknesses of the analytical process so that warnings of

⁵⁹ Ibid.

⁶⁰ James B. Bruce, and Roger Z. Greg, *Intelligence Analysis-The Emergence of a Discipline* (Washington D.C.: Georgetown University Press, 2008), 9.

⁶¹ Kenneth Luikart, “Homeland Security: Intelligence Indications and Warning,” *Strategic Insights*, 1 no. 10 (2002): 3.

⁶² Ibid.

the most fantastic types of terrorist activity can be used to shape policy in constructive ways.”⁶³

D. NATURE OF THE THREAT

Transnational criminal organizations (TCOs) fit the definition of asymmetrical, non-state actors by the nature of both their network and operations. The non-state, asymmetrical nature of the certain adversaries creates challenges associated with planning, collecting, and analyzing warning intelligence. Butterfield, Meissner, and Kulisch define asymmetrical as an adversary with “no correlation of forces” that utilizes unconventional attacks to compensate for a perceived disadvantage.⁶⁴ The nature of TCOs techniques, tactics, and procedures have the characteristics of an asymmetric adversary. The USBP needs an agile, adaptive, and situationally aware intelligence presence in the field to inform operations and policy that counter TCO activities.

Combating asymmetrical actors like TCOs requires forward-looking, critical, and creative thinking. Traditional views on intelligence failure and surprise attack are anchored in the past. New knowledge and understanding of strategic warning dictates that the USBP must be asymmetrical in its methodology. The USBP SIU must not only be flexible in analyzing atypical indicators as opposed to traditional patterns, but it must also analyze traditional strategies and then abandon them if they do not yield high value information. Additionally, the USBP must continue to challenge assumptions and seek alternative perspectives on asymmetrical threats to improve strategic warning and reduce the likelihood of surprise. The USBP is growing its capability to leverage and exploit technology in the form of advanced analytics and technical collections. Dahl outlines the traditional view of intelligence as being inherently difficult and susceptible to error. He further delineates the “new school” of intelligence, or *information age optimists*, who

⁶³ Ibid.

⁶⁴ Alexander Butterfield, Terry Meissner, and Gail Kulisch, *Against Al Qaida: Improving Warning in the Asymmetric Environment* (Cambridge, MA: Harvard University Press 2008), 8.

take into account leveraging technology to exploit information and communications while noting that human intelligence is key to addressing terrorism.⁶⁵

Traditional views of intelligence generally focus on collecting information on traditional activities. In the new age of information, the Rand Corporation proposes a concept based on collecting information on atypical signals to indicate suspicious behavior.⁶⁶ Additionally, the Rand Corporation notes that today's security environment is characterized by a large volume and scope of information flow that exceeds the conventional capabilities to process it all. The USBP generates large amounts of data daily in locations all over the country and in Puerto Rico. The USBP requires the capability to integrate, fuse, and exploit all the generated border data into intelligence that correlates links, trends, and patterns of the adversary threat network.

Traditional views on intelligence failure and surprise attack often examine traditional actions associated with war: troop movements, political rhetoric, and engagement. Williams suggest that law enforcement and, by proxy, the IC should be monitoring the financial indicators and their significance as related to a potential attack on the U.S.⁶⁷ In addition, Williams outlines the U.S.'s strategy of "freeze and seize" terrorist funds but notes that this traditional strategy deprives the IC of a valuable tool to monitor, track, and exploit information gained from financial transactions.⁶⁸ In addition, the freeze and seize strategy is not of a particularly high-payoff because of three factors: the limitations of international methodology monitor global financial operations, the relative low cost of terrorist operations compared to military actions, and the use of black market or illegal funding streams. In conclusion, Williams recommends abandoning the traditional strategies associated with attacking the finances of an asymmetrical adversary and instead develop methodologies to exploit their financial operations as a means to

⁶⁵ Eric Dahl, *Warning of Terror: Explaining the Failure of Intelligence against Terrorism* (Medford, MA: Tufts University, 2004), 2.

⁶⁶ John S. Hollywood et al., *Connecting the Dots in Intelligence: Detecting Terrorist Threats in the Out-of-the-Ordinary* (Santa Monica, CA: Rand Corporation, 2005).

⁶⁷ Phil Williams, "Warning Indications, Terrorist Finances, and Terrorist Adaption," *Strategic Insights* 4, no 1 (2005).

⁶⁸ *Ibid.*, 2.

enhance detection of strategic indicators and warnings.⁶⁹ The USBP can leverage the task force officers to query financial databases to detect indicators and warnings of illicit activity.

One bias common of U.S. intelligence agencies is a rationality or coherence bias, also known as mirror imaging, which is along the same family tree as ethnocentrism.⁷⁰ The 1962 Cuban missile crisis and the 1973 Egyptian/Middle East conflict are examples of this. CIA analysts rationalized information to fill in gaps about foreign leader's perspectives based on what made sense to the analyst. These biases are not new, and they have persistently endured because of the human condition. The USBP intelligence unit must be careful not to construe the adversary as acting the way we (Americans) would act. This means that a BPA-I must try to understand the belief system, worldview, culture, socio-economics, history, etc., from the adversary's perspective. Then, it may be possible for BPA-I to forecast potential outcomes based on adversary behavior while mitigating mirror image bias.

⁶⁹ Ibid.

⁷⁰ Lowenthal, *Intelligence: From Secrets to Policy*; Jack Davis, "Why Bad Things Happen to Good Analysts," in *Intelligence Analysis-The Emergence of a Discipline*, ed. Roger Z. George and James B. Bruce (157–170) (Washington DC: Georgetown University Press, 2008).

IV. ANALYSIS

This analysis is based on three case studies conducted internally to the USBP at the strategic, operational, and tactical levels.

A. CAPABILITY BASED ASSESSMENT—AN OPERATIONAL PERSPECTIVE OF INTELLIGENCE CAPABILITY GAPS

Throughout fiscal year 2015 (FY15), teams of USBP agents from the Strategic Planning and Analysis Directorate (SPA), Operational Requirements Management Division (ORMD) deployed to every sector nationwide to conduct training (train-the-trainer) and execute the capability gap analysis process (CGAP). The CGAP is a scenario-driven, capability based assessment process designed to compare adversary and friendly force capabilities to determine whether or to what degree an imbalance in those capabilities exists (i.e., identify friendly force capability gaps). The CGAP resulted in the production of data, analytical tools, and actionable knowledge that informed resourcing and acquisitions at the station, sector, and headquarters level through repeatable, traceable, and defensible systems analysis approach.

Although the perspective of the FY15 CGAP was operational in nature, it revealed 21 high-level gaps from agents in the field. Each gap was correlated to a mission essential task (MET) or stage in the CBP intelligence cycle: planning and direction, collection, processing and exploitation, analysis and production, and dissemination.⁷¹

B. CGAP INITIAL INTEL GAP ROLLUP

Table 1 is a capability gap assessment process that captures a description of current intelligence gaps as described by the agents in the field.

⁷¹ Capability Gap Analysis Process conducted throughout the nation at all USBP sectors during fiscal year 2014 at the direction of USBP Chief Michael J. Fisher. U.S. Border Patrol, Office of the Chief, *Memorandum for All Chief Patrol Agents: Fiscal Year 2015 Capability Gap Analysis Process* (Washington, DC: U.S. Border Patrol, Office of the Chief, 2014).

Table 1. Capability Gap Assessment

GAP #	GAP Description
15-USBPINTEL-01	USBP has limited ability to collect signals intelligence (SIGINT)
15-USBPINTEL-02	USBP has a limited to no ability to disrupt or disable adversary communications (particularly scouts and guides)
15-USBPINTEL-03	Due to shift times and Union issues, BPAs are generally unable to conduct long-term reconnaissance operations with agents in covert LP/OPs
15-USBPINTEL-04	BPAs are unable to quickly capture, submit, and receive intelligence in the field.
15-USBPINTEL-05	BPAs have a limited ability to extract and exploit data from seized electronic devices
15-USBPINTEL-06	BPAs are unable to quickly and competitively pay human intelligence (HUMINT) sources
15-USBPINTEL-07	Agents receive a limited amount of timely, relevant, and standardized information from Station and Sector Intelligence shops
15-USBPINTEL-08	USBP has a limited ability to analyze information/trends in order to predict future events and activity
15-USBPINTEL-09	BPAs have a limited ability to conduct investigations
15-USBPINTEL-10	USBP has a limited ability to receive and share information/intelligence with stakeholders (foreign and domestic)
15-USBPINTEL-11	Many BPAs have a limited ability to execute intelligence functions due to a lack of Intelligence training (Intel Cycle, LETC, DD/ER, targeting, collections PIRs etc.)
15-USBPINTEL-12	USBP has a limited ability to collect multiple-source intelligence on a consistent and timely/actionable basis.
15-USBPINTEL-13	USBP has a limited ability to process and exploit multiple-source intelligence on a consistent and timely/actionable basis.
15-USBPINTEL-14	USBP has a limited ability to analyze and produce intelligence products on a consistent and timely/actionable basis.
15-USBPINTEL-15	BPAs have a limited ability to fuse information due to system incompatibilities
15-USBPINTEL-16	Some locations have a limited ability to conduct effective Intelligence functions do to manpower restrictions
15-USBPINTEL-17	BPAs have a limited ability to interview and collect intelligence from subjects who speak unfamiliar languages
15-USBPINTEL-18	BPA have a limited ability to access classified information (clearances and/or facilities)
15-USBPINTEL-19	USBP has a very limited ability to exploit crime scene evidence (fingerprints, fiber analysis, DNA, etc.)
15-USBPINTEL-20	BPAs have a limited ability to determine if reports made to a Station are a ruse that is intended to deceive or distract agents
15-USBPINTEL-21	BPAs have a limited ability to receive timely feedback after Field Information reports are submitted

Adapted from: Internal USBP CGAP work performed in FY15 across the nation.

C. LIMITATIONS

The intelligence gaps revealed outputs of the operational CGAP have certain limitations that must be addressed:

1. The CGAP process calls for a range of participants to attend the field Collaborative Analysis Exercise (workgroup); sectors assigned personnel based on availability and impact to the mission. Although recommended, there was no standard requirement for BPA-I participation.
2. The gaps are based on an operator's *perspective*. The gaps may not necessarily be "true" per se but reflect the respondents' worldview based on their specific experiences and access to knowledge. A gap may reflect a messaging or communications issue.
3. The gaps are aggregated based on the nationwide CGAP and are not necessarily true for all areas. More research is needed at the field level to understand the gaps in specific areas.

D. GAPS REORGANIZED UNDER CBP INTELLIGENCE CYCLE

The identified gaps in the study were reorganized to align with the CBP intelligence cycle are broad, generalized statements regarding USBP intelligence gaps.⁷² Although useful, more research is needed to understand the baseline of both current capabilities and capability gaps. The gaps are informative from a perspective of what the general mission needs. In addition, the gaps can be used to inform doctrine and strategic guidance. For instance, the USBP Intelligence Division can analyze the perceived gaps and mission needs and translate that information into strategy. This strategy should articulate the executive vision and mission of the Intelligence Division while also highlighting the goals and objectives of intelligence that support the USBP *2012–2016 Strategic Plan*. Furthermore, an Intelligence Division strategy should provide the guidance for a sector level intelligence supplement to operational implementation plans (OIPs), and the sector's campaign plan should outline how it will contribute to the mission, goals, and objects of the USBP *2012–2016 Strategic Plan*. At the lowest level, gaps, needs, and requirements can be captured and documented in each area. Senior executives must then prioritize each sectors' intelligence requirements based on risk.

⁷² U.S. Border Patrol, "Tucson Sector CGAP" (internal document, U.S. Border Patrol, Tucson Sector Intelligence Unit, Tucson, AZ, 2014).

Table 2 is a chart depicting the results of a case study conducted by the USBP Tucson Sector Intelligence Unit in 2014. In addition, the chart outlines the CBP intelligence cycle. Each section contains the identified gaps at the field level in each category of the cycle. For example, in the area of planning and direction, there is a need to provide intelligence training to USBP agents (BPAs) so they are able to better execute intelligence functions in the field environment. In the area of collection, BPAs need to be able to recognize and exploit information and evidence that could provide intelligence value for the organization.

In the area of processing and exploitation, the agency needs to increase data modernization systems so as to be able to fuse information more efficiently. In addition, the analysis section requires subject matter experts, such as intelligence analysts, to build consistency in providing intelligence products in a timely basis. Furthermore, in the area of dissemination, sector intelligence units need to do more to provide feedback to uniformed USBP agents on the information they provide on a daily basis.

As a result of this study, a major gap in the intelligence training area is identified as a priority as it provides the awareness and lays the foundation to build a sound intelligence architecture with USBP.

Table 2. Consolidated Gaps

Planning & Direction	Many BPAs have a limited ability to execute intelligence functions due to a lack of Intelligence training (Intel Cycle, LETC, DD/ER, targeting, collections PIRs etc.)
	BPAs have a limited ability to determine if reports made to a Station are a ruse that is intended to deceive or distract agents
Collection	USBP has limited ability to collect signals intelligence (SIGINT)
	Due to shift times and Union issues, BPAs are generally unable to conduct long-term reconnaissance operations with agents in covert LP/OPs
	BPAs have a limited ability to extract and exploit data from seized electronic devices
	BPAs are unable to quickly and competitively pay human intelligence (HUMINT) sources
	BPAs have a limited ability to conduct investigations
	USBP has a limited ability to receive and share information/intelligence with stakeholders (foreign and domestic)
	USBP has a limited ability to collect multiple-source intelligence on a consistent and timely/actionable basis.
	BPAs have a limited ability to interview and collect intelligence from subjects who speak unfamiliar languages
	USBP has a very limited ability to exploit crime scene evidence (fingerprints, fiber analysis, DNA, etc.)
Processing & Exploitation	USBP has a limited ability to analyze information/trends in order to predict future events and activity
	USBP has a limited ability to process and exploit multiple-source intelligence on a consistent and timely/actionable basis.
	BPAs have a limited ability to fuse information due to system incompatibilities
Analysis & Production	USBP has a limited ability to analyze and produce intelligence products on a consistent and timely/actionable basis.
Dissemination	Agents receive a limited amount of timely, relevant, and standardized information from Station and Sector Intelligence shops
	BPAs have a limited ability to receive timely feedback after Field Information reports are submitted
All Phases of Intel Cycle	BPAs are unable to quickly capture, submit, and receive intelligence in the field.
	Some locations have a limited ability to conduct effective Intelligence functions do to manpower restrictions
	BPA have a limited ability to access classified information (clearances and/or facilities)

Adapted from: U.S. Border Patrol, "Tucson Sector CGAP."

E. INTELLIGENCE DRIVEN OPERATIONS AND OPERATIONS DRIVEN COLLECTIONS

The flow of information between intelligence agents and operations is critical to situational awareness. Understanding the perceptions, perspectives, and requirements of

intelligence agent and operations can reveal opportunities to enhance information sharing.

In May 2014, the USBP Tucson Sector Intelligence Unit conducted a study involving intelligence agents to BPAs, supervisory USBP agents (SBPAs), and command staff.⁷³ at three stations in Tucson Sector (Douglas, Brain A. Terry, and Willcox border patrol stations) to assess the level and effectiveness of communication between station intelligence units and the field.⁷⁴ Station personnel were asked a series of weighted questions about their perceptions of communication between intelligence units and the field. In total, 310 agents were surveyed; 239 USBP agents, 50 supervisory USBP agents, and 21 command staff including, second line supervisors to patrol agents in charge. The survey results revealed key areas where intelligence units can enhance communications.

1. Survey Questions

1. Do you know who all the BPA-I's are at your station?
2. How likely are you to contact a BPA-I if you had info?
3. How likely are you to get feedback from a BPA-I if you gave them info?
4. How would you provide a BPA-I with info?
5. How you rate communication between Intel and the field?

2. Key Findings

1. Do you know who all the BPA-I's are at your station?
About 55 percent of agents know more than half or most of the BPA-Is at the station.

About 20 percent of agents know less than half of the BPA-Is at the station
2. How likely are you to contact a BPA-I if you had info?
Approximately 75 percent of agents would probably provide info to BPA-Is.

Approximately eight percent of agents would not likely provide info to BPA-Is.

⁷³ Ibid.

⁷⁴ Ibid.

3. How likely are you to get feedback from a BPA-I if you gave them info?
Approximately 55 percent of agents think they would get feedback from BPA-Is.
Approximately 25 percent of agents think they would NOT get feedback from BPA-Is.
4. How would you provide a BPA-I with info?
35 percent of agents prefer face-to-face; 34 percent preferred a phone call.
5. How you rate communication between Intel and the field?
Nearly 60 percent of agents think communication is good or outstanding.
Nearly 40 percent of agents think communication is fair or worse.⁷⁵

The survey also captured qualitative elicitations via an open comment section on what BPA-I can do to improve communications with the field. Comments were analyzed, classified, and aggregated by theme. The top five results are as follows, in order of frequency:

1. More muster presentations.
2. Educate and inform agents about BPA-I duties, functions, and capabilities.
3. Dispel the “secret squirrel” perception and clarify what information is “need to know.” *Note:* “secret squirrel” is derogatory slang for someone working in covert operations.
4. Continue doing what you are doing.
5. Provide feedback to agents that provided information to BPA-I.⁷⁶

The results of this study demonstrate that there is a constituency of agents who are generally aware of the intelligence mission and have the means and incentive to share information. The qualitative comments demonstrate a desire by agents for more information and to understand more about BPA-I tasks. The desire to dispel the “secret squirrel” perception of BPA-I also supports the need for more messaging and information about BPA-I duties. While disseminating information is part of the CBP intelligence cycle, the USBP needs to provide agents at all levels with a clear and concise message on how intelligence operations are conducted.

⁷⁵ Ibid.

⁷⁶ Ibid.

F. STRATEGIC INDICATORS AND WARNING: A U.S. BORDER PATROL CASE STUDY—AJO STATION

The best we can do is a compromise: learn to recognize situations in which mistakes are likely and try harder to avoid significant mistakes when the stakes are high.

Daniel Kahneman, *Thinking, Fast and Slow*

In February 2014, the chief patrol agent of Tucson sector sent a Red Team to Ajo to understand why the interdiction effectiveness rate had decreased dramatically (and unexpectedly). The Red Team found that from June 2013 through February 2014, the Ajo Border Patrol Station experienced a sudden increase in got-aways (GTAs)—detected illegal entries that avoid or evade apprehension.⁷⁷ This analysis reveals that potential indicators and strategic warning signs were first detected in June 2013, but there was no significant action to address this situation until approximately eight months later when Ajo reported approximately 6700 GTAs for the first quarter of FY14. The list below summarizes the results of the Red Team analysis:

- Throughout the 2013 fiscal year, TCA executed Operation United Front II, a focused operation designed to significantly displace and deflect illicit activity in the Casa Grande Border Patrol Station (CAG) area of responsibility (AOR), the AOR directly adjacent to the Ajo AOR.
- In the early spring of 2013, intelligence indicated that drug trafficking organizations were disallowing any alien trafficking from occurring in the Ajo AOR and threatening violent reprisal if anyone violated this order.
- In March 2013, four Mexican nationals, who had allegedly been attempting to smuggle illegal aliens near the CAG and Ajo seam, were attacked by the DTO. All four smugglers were tied up and had their throats slashed; two perished and two managed to survive.⁷⁸
- In June 2013, Ajo significantly increased its situational awareness through increased reconnaissance, surveillance, target, acquisition (RSTA) technology deployments and the establishment of a data integrity team (DIT). A DIT is a specialty unit whose mission is to detect and reconcile illicit entries with apprehensions, turnbacks (TBS), and GTAs.

⁷⁷ Tucson Sector Chief Manuel Padilla Jr. requested the Red Team conduct an assessment on operations at the Ajo USBP station 2013–2014. U.S. Border Patrol, Tucson Sector Operations Division, “Red Team Operational Exercise: Ajo Analysis” (internal document, U.S. Border Patrol, Tucson Sector Operations Division, Tucson, AZ, March 2014).

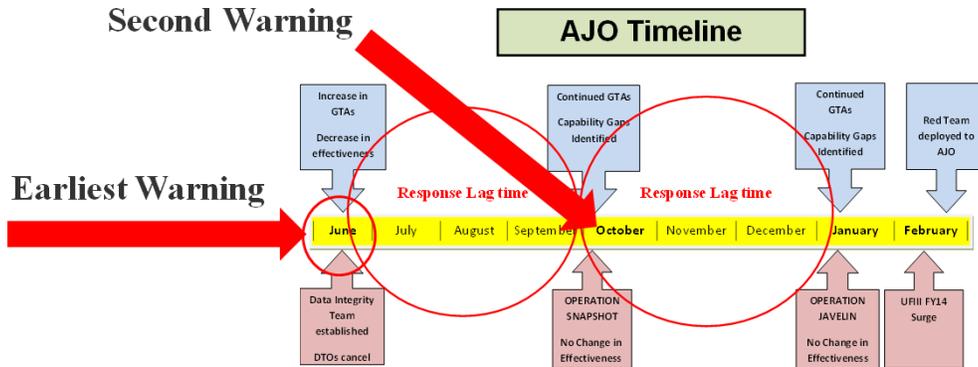
⁷⁸ Ibid.

- In June 2013, the Ajo station began reporting a significant increase in detected illegal entries and a commensurate number of GTAs.
- In October 2013, TCA implemented Operation Snapshot, an operation to provide a proof of concept based on the Comprehensive Immigration Reform definition of “effective control” or the “ability to achieve and maintain persistent surveillance and an effectiveness rate of 90 percent or higher.”⁷⁹ Effectiveness is “calculated by the number of apprehensions and turnbacks by the total number of illegal entries (note this formula does not take into account GTAs).”⁸⁰ Operation Snapshot deployed additional RSTA assets and manpower to provide adequate response and resolve capability to address the surge in illicit activity.
- The after action review of Operation Snapshot revealed that this operation did not achieve its objective of persistent surveillance or 90 percent operational effectiveness. Post-operational assessment revealed that the additional surge technology deployments did not provide the desired results within the identified target areas. The operation achieved an overall effectiveness rate of 57percent in the target area. This effectiveness rate is a drop from Ajo’s overall effectiveness rate of 62 percent for August and 70 percent in September prior to the execution of Operation Snapshot.

1. Timeline of Strategic Indicators and Warning

Table 3 contains the Ajo timeline of strategic indicators and warnings.

Table 3. Timeline of Strategic Indicators and Warning



Source: U.S. Border Patrol, Tucson Sector Operations Division, “Red Team Operational Exercise: Ajo Analysis”

⁷⁹ Border Security, Economic Opportunity, and Immigration Modernization Act (2013).

⁸⁰ Ibid.

This outcome caused the Ajo station to be considered high risk to border security based on the USBP's current definition of risk.⁸¹ The Ajo AOR is rural, remote, and expansive, which makes it difficult for agents to detect, identify, classify, and rapidly respond to threats.

G. LESSONS LEARNED

Author Joshua Cooper Ramo, in his book *The Age of the Unthinkable*, addresses the need for deep security as a system to be flexible and adaptive to new threat.⁸² Deep security dictates aggressively communicating indicators and warning for timely intelligence. This means that the BPA-I must be bold, direct, and succinct in communication of indicators and warning to the CoC. Likewise, leaders throughout the CoC must apply these principles to concise yet aggressive messaging to brief all the high points clearly and directly, supporting the superior commander with information needed for timely action.

One of the greatest hurdles affecting timely action necessary to counter threats is the excessive amount of information given to policymakers. To counter this, agents should use commander's critical information requirements (CCIRs) and their derivatives to focus intelligence collections.⁸³ CCIRs are developed with commanders and policymakers in mind and with their input, but they also include input from the field. CCIRs are the key questions, the critical pieces of information that reduce uncertainty and support decision making.⁸⁴ Moreover, CCIRs help reduce inundation of information by focusing on the truly important. This can reduce the information overload factor by allowing the commander to dictate what information she or he requires (see Figure 7).

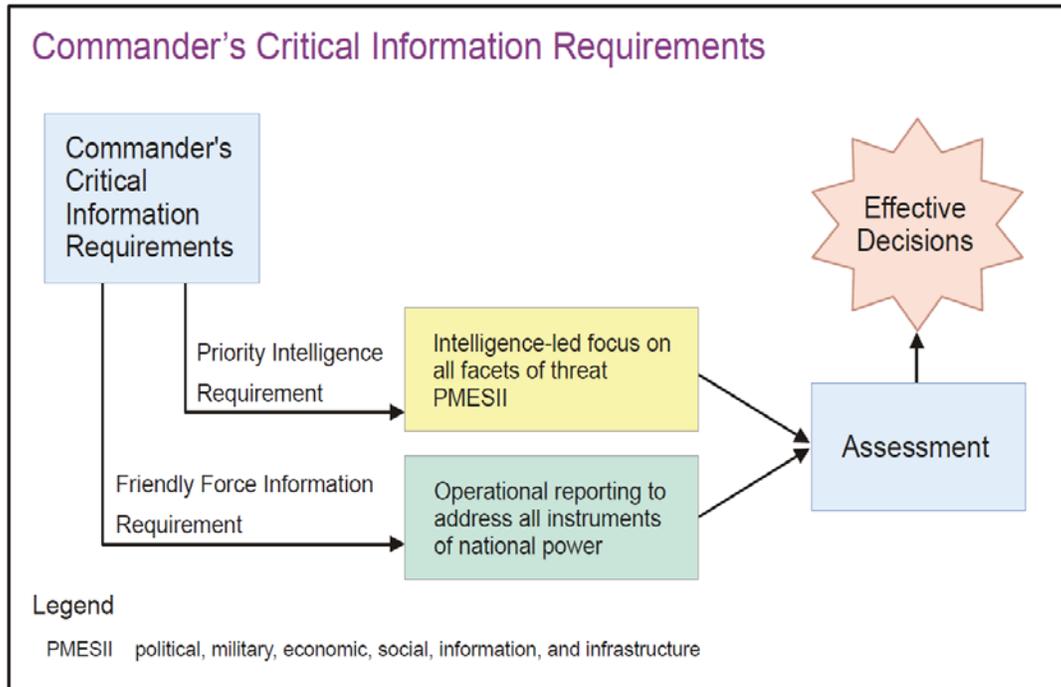
⁸¹ Robert D. Schroeder, "Institutionalizing a Risk-Based Approach in the USBP," *Small Wars Journal* (January 2014), <http://smallwarsjournal.com/jrnl/art/institutionalizing-a-risk-based-approach-in-the-us-border-patrol>.

⁸² Joshua Cooper Ramo, *The Age of the Unthinkable, Why the New World Disorder Constantly Surprises Us and What We Can Do about It* (New York: Hachett Book Group, 2009).

⁸³ Joint Chiefs of Staff, *Joint Intelligence* (JP-2-0) (Washington, DC: Joint Chiefs of Staff, 2007).

⁸⁴ *Ibid.*

Figure 7. Commander's Critical Information Requirements and Assessments



Source: Joint Chiefs of Staff, *Joint Intelligence*.

McLaughlin relates that in his experience, he has encountered two types of intelligence consumers: those who know how to correctly interpret intelligence and those who did not nor would not.⁸⁵ In that aspect, the BPA-Is must focus their intelligence briefs to the “lowest common denominator” in order to ensure proper messaging to a broad audience. The Red Team briefing 101 states, “Knowing the audience is the key to success.”⁸⁶ Who is the audience, what do they need to know, and ends with a clearly stated “path forward.”⁸⁷ Well rounded BPA-Is must be proficient in communication as they operate in research and analysis. The USBP should be able to tailor or message to the audience in such a manner that makes sense to that specific group of information recipients to ensure common understanding and transparency.

⁸⁵ John McLaughlin, “Serving the National Policymaker,” in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, ed. Roger Z. George and James B. Bruce (Washington DC: Georgetown University Press 2008), page 72.

⁸⁶ *Red Team Handbook*, version 6.0 (Fort Leavenworth, KA: University of Foreign Military and Cultural Studies, 2012).

⁸⁷ *Ibid.*

If a high-risk border security event was imminent in the United States, such as the recent unaccompanied juvenile crisis,⁸⁸ and the SIU produced reliable indications and warnings, our field personnel would be prepared to address and mitigate any potential risk to national security. Lowenthal summarizes the three hurdles that affect timely action necessary to counter a threat. For example, he suggests that warning, analytical process, and information sharing are the analytical standards that support timely action to counter threats.⁸⁹ In addition, Lowenthal highlights 9/11 as an example of warning in that the intelligence community failed to fully communicate about the impending nature of the threat.⁹⁰ Policymakers were left with an imprecise sense of the threat.⁹¹ The analytical process “connects the dots” illustrating patterns and linkages to provide a comprehensive picture of the threat.⁹² In the case of the Ajo Border Patrol Station, the deficiency was not necessarily the inability to connect the dots but to “align the arrows.” The Tucson Sector CoC needed to understand the forecasted trends and patterns of a surge in illicit traffic that would exceed the organic capabilities to respond and resolve the surge effectively. With these warning signs and knowledge of the constant difficulty associated with maintaining a fully staffed station due to the remoteness of the area, the CoC could have implemented changes to mitigate the increased illicit activity.

H. ON ANTICIPATING SURPRISE

As part of the discussion on timely warnings, it is useful to examine human nature and the difficulty of anticipating surprise. Historically, there is a common theme as to why people have trouble believing indications and warnings prior to an event and why countries are caught unaware by surprise. Determining the warning signals from the background noise is difficult.⁹³ The warning process must yield information that is

⁸⁸ U.S. Department of Homeland Security, “DHS Humanitarian Crisis 2015” (internal document, U.S. Department of Homeland Security, Washington, DC, 2015).

⁸⁹ Lowenthal, *Intelligence: From Secrets to Policy*, 143.

⁹⁰ *Ibid.*

⁹¹ *Ibid.*

⁹² *Ibid.*

⁹³ James Wirtz, and Douglas Porch, “Surprise and Intelligence Failure,” *Strategic Insight* 1, no. 7 (2002).

timely, relevant, actionable, and believable. Perception, bias, and uncertainty make people and countries fall victim to surprise. Wirtz and Porch highlight three common reasons that often factor into intelligence failures: the challenge of harvesting actionable information in the “noise” created by mass data collection, underestimating the enemy’s capabilities to take action, and mirror imaging (the assumption that enemy actions are unlikely because it was “illogical).”⁹⁴ As previously mentioned, mirror imaging is a common bias that results in surprise because friendly forces evaluate enemy actions based on a common “rationality” or a common worldview where all rational actors would make similar decisions. People and countries assume that the enemy thinks like them. This bias can be mitigated by analyzing the enemy in depth from its own perspective. Davis recommends bringing in Red Teams on major analytic problems to work with analysts.⁹⁵ One function of the Red Team is to assess, analyze, and understand the factors that shape the enemy’s environment. Analysts need to consider culture, socioeconomics, politics, religion, and other critical variables when trying to understand the enemy worldview and value system. If used effectively, a Red Team can help mitigate bias by challenging assumptions and informing decisions.⁹⁶ It should be noted that Tucson Sector brought in a Red Team after the fact to understand the problem in Ajo. In hindsight, it might have been valuable to insert the Red Team’s analysis early in the intelligence process to help mitigate surprise.

Perception is another component that compromises the ability of people to understand warning and thus enables surprise. Grabo notes that actors typically assume their adversary will act in a manner consistent with their historical actions.⁹⁷ Grabo holds that this is often true but warns that historical precedence must be discounted in light of current information that indicates the contrary; an adversary may act differently than its traditional behavior.⁹⁸ Grabo calls this “a fundamental cause of warning failures—that

⁹⁴ Ibid.

⁹⁵ Davis, “Why Bad Things Happen to Good Analysts.”

⁹⁶ Defense Science Board, *Summer Study on Capability Surprise*, Vol. I (Washington, DC: Office of the Under Secretary of Defense for Acquisition Technology and Logistics, 2009).

⁹⁷ Cynthia Grabo, *Anticipating Surprise, Analysis for Strategic Warning* (Lanham, MD: UPA, 2004).

⁹⁸ Ibid.

the behavior of the aggressor appears inconsistent that what we expect them to do.”⁹⁹ The perception of historical actions by the adversary to predict future behavior is a useful heuristic, but it is not an anchor. Grabo advises that analysts must consider the perception of the enemy to understand what they *might* do.¹⁰⁰ Objective analysis of current information must be analyzed at face value to assess current indicators and the reality of potential threats. Therefore, it is critically important to have a basic understanding of intelligence and the importance of analytical information to recognize the tactics, techniques, and procedures used by an adversary.

People and countries fall victim of surprise due to their perception of the environment or their perceived situational awareness. This is true for intelligence analysts as well. Often, analysts focus only on what they know. Yet, it is the uncertainty and the unknown that present the greatest risk of surprise. Davis notes that Rumsfeld Commission tasked analysts with taking greater consideration of what they do not know.¹⁰¹ Red Team methodology encourages taking that concept of “what we don’t know” one step further: to consider the things *we do not know* we do not know. The highly speculative and deeply philosophical nature of this concept makes it challenging to apply, but it can be a valuable tool. Exploring the potential information we do not know that we do not know can yield new questions to reduce uncertainty, understand warning, and mitigate surprise.

According to Grabo, “warning intelligence...is not produced in a vacuum, divorced from the rest of the intelligence process or from any number of other influences.”¹⁰² These influences can be blinding to analysts and policymakers as they evaluate and come to conclusions regarding the validity of indications and warning. Grabo further explains that the greatest factor of influence is the inability to conceive of the possibility.¹⁰³ Considering that no major attack had been perpetrated on American

⁹⁹ Ibid. 86.

¹⁰⁰ Ibid.

¹⁰¹ Davis, “Why Bad Things Happen to Good Analysts,” 7.

¹⁰² Grabo, *Anticipating Surprise, Analysis for Strategic Warning*, 157.

¹⁰³ Ibid.

soil by a foreign aggressor in six decades, the indications and warnings leading up to the 9/11 attacks were largely ignored because the information seemed to suggest the impossible. Porch and Wirtz explain that it is not unusual for indications and warnings to be set aside if they seem unbelievable.¹⁰⁴ This was especially true of intelligence leading up to the 9/11 attacks.

Relevant information may be filtered out as it is sent up the bureaucratic chain because it seems unimportant, trivial or irrelevant to more important concerns—such as local FBI agents reporting that Arab students in flight schools only wished to learn how to take off, not to land,¹⁰⁵

In hindsight, this was incredibly obvious that these individuals were not seeking to land.

Although information can be deemed irrelevant for analysis, it can also be pushed aside as impossible due to “...’mirror-imaging’—the belief that the perpetrators will not carry out a particular act because the defender, in their place, would not do it.”¹⁰⁶ In the case of the Pearl Harbor and 9/11 attacks,

The notion of ‘suicide bombing’ [was] so alien to the American—indeed the Western—outlook, that we find it difficult to fathom the mindset of enemies prepared to conceive of an operation of such horrific proportions, one in which they are prepared to immolate themselves in acts of fiery desperation.¹⁰⁷

This is what leads countries, including the United States, to be caught unaware by surprise. The inability to believe that an attack is possible, that the perpetrator would utilize a certain method of attack, such as suicide bombing, and an overabundance of unanalyzed intelligence all lead to surprise and what appears to be a complete lack of warning. Making improvements to the intelligence system of collection, analysis, and dissemination is important in light of failures; however, it is also important to remember:

¹⁰⁴ Wirtz, and Porch, “Surprise and Intelligence Failure.”

¹⁰⁵ *Ibid.*, 3.

¹⁰⁶ *Ibid.*

¹⁰⁷ *Ibid.*

There is no way, short of being able to read the adversary's mind, that we can be confident that our warning judgments, or even many of our 'facts,' are going to be correct... As we have been surprised in the past, we shall be surprised again in the future.¹⁰⁸

As previously experienced with the 9/11 attacks, intelligence products need to be socialized and further processed amongst the IC to identify and develop alternative possibilities on the data collected. For example, if a high-risk border security event were imminent in the United States and sector intelligence units produced reliable indications and warnings, another barrier would be the "black swan" effect. In 2007, Nassim Nicholas Taleb published *The Black Swan: The Impact of the Highly Improbable*, in which he argues that we should never ignore the possibility or importance of rare, unpredictable events. Taleb defines a black swan event as one that has a low probability of occurring but that would have a massive impact.¹⁰⁹ This is a problem of predictive analysis; analysts often focus on the most likely enemy course of action without fully considering how to mitigate the effects of the enemy's most dangerous course of action. Policymakers are typically the primary consumers of intelligence products. According to McLaughlin, there are two types of intelligence consumers: those who know how to interpret intelligence correctly and those who did not or would not.¹¹⁰ Before 9/11, most people would have thought it preposterous that terrorists could fly a plane into the World Trade Center. This paradigm changed dramatically and forever after on the day after 9/11. Recently, the USBP experienced a crisis of mass migration of unaccompanied children from Central America, overwhelming the capability to house, feed, and meet the special needs of the detained children. Prior to the crisis, the USBP assumed the Department of Health and Human Services (HHS) would manage unaccompanied children, as meeting these needs were within HHS mission parameters. However, HHS was quickly overwhelmed and the USBP had to quickly adapt and transform its capability so it could safely and humanly manage hundreds of thousands of

¹⁰⁸ Grabo, *Anticipating Surprise, Analysis for Strategic Warning*, 162.

¹⁰⁹ Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007).

¹¹⁰ McLaughlin, "Serving the National Policymaker," 72.

unaccompanied children. There is some evidence that the available intelligence warning and the USBP response was predicated on other factors that were not validated, adding to the unanticipated surprise.

The Ajo study highlights a common challenge that impacts timely action to counter an imminent event.¹¹¹ The effect of “crying wolf” is a common theme in many intelligence textbooks. Lowenthal cites this as a “numbing effect” on policymakers that occurs with the ongoing production and delivery of intelligence products.¹¹² Repeatedly messaged threats lose impact and urgency. In addition, it is difficult to prove when intelligence successfully counters a threat. For example, suppose that an intel unit receives timely and credible intelligence about a potential attack on a military base. The intel unit informs the base commander, who implements security measures to prevent the attack. Due to an increased security posture, the attack never occurs. How can the commander be sure that the attack would have happened without the additional security measures? It is extremely difficult to prove a negative, to prove that an event never happened due to timely exploitation of actionable intelligence. A parallel can be drawn from this to Border Patrol operations. If the amount of illegal aliens and or seizures made in a high activity area begin to decrease, can this be attributed to a shift in line operations? Or, when there is a sudden increase in GTA at a station, what was the actual change, did the adversary’s effectiveness increase? Did the friendly force capability or effectiveness decrease? Or potentially an unknown factor has influenced operations? In the case of Ajo, it was apparent that a breakdown in communications occurred at every level.

Lowenthal cites another challenge to timely action, the struggle between current and long-term intelligence.¹¹³ The nature and expediency of analyzing and producing current intelligence is a constraint to timely action. The analysts will be pressed for time

¹¹¹ U.S. Border Patrol, Tucson Sector Operations Division, “Red Team Operational Exercise: Ajo Analysis.”

¹¹² Lowenthal, *Intelligence: From Secrets to Policy*, 111.

¹¹³ *Ibid.*, 113.

to add the depth and context to that they deem valuable.¹¹⁴ Moreover, Clark notes that the intelligence process is very fast at the tactical level.¹¹⁵ Indeed, this is often true for the USBP. For example, a USBP priority intelligence requirement (PIR) may be “when and where do smugglers attempt to illegally cross the border?” Presume BPA-I has a confidential informant (CI) that has credible information about an illegal crossing that will occur that evening sometime after midnight. This would be the latest time of value (LTOV), the latest time this information will be actionable. When the CI calls in the LTOV information that the event is about to occur, a sequence of events must be executed expeditiously. The BPA-I must alert the commander of the AOR. The commander must consider the appropriate deployment of resources and synchronize the ground troops with intelligence surveillance reconnaissance/reconnaissance surveillance target acquisition (ISR/RSTA) assets. All the interdiction resources must then respond to the area and execute the interdiction. Furthermore, all this must occur within the window of opportunity before the smugglers can blend in with the local populace.

There are many barriers to executing action to counter an impending threat. It is imperative for the analyst to communicate as complete of a threat picture as possible and provide as much relevant information in a succinct package for policymakers.

While tactical warning often focuses on measurable indicators, such as the deployment of enemy forces in an area, strategic warning is often ambiguous and open to interpretation. Leaders often disbelieve ambiguous strategic warning or warning without sufficient evidence to support it. Prior to the start of the Berlin blockade, General Lucius Clay sent a message to Washington that said,

Within the last few weeks, I have felt a subtle change in Soviet attitude, which I cannot define but which now gives me a feeling that it [war] may come with dramatic suddenness. I cannot support this change in my own thinking with any data or outward evidence in relationships other than to describe it as a feeling of a new tenseness in every Soviet individual with whom we have official relations.¹¹⁶

¹¹⁴ Ibid., 114.

¹¹⁵ Clark, *Intelligence Analysis*, 53.

¹¹⁶ Grabo, *Anticipating Surprise, Analysis for Strategic Warning*, 77–78

Such absence of definitive detail is fairly common in strategic warning, and decision makers are unable to respond to all non-specific warnings due to a lack of time and resources. They must decide which warnings to heed and ignore. Since intelligence analysts and policymakers must utilize incomplete information or information from uncertain sources to provide warning or implement countermeasures, there is a wide margin for error. Any warning from intelligence analysts must be convincing enough and have enough evidence to spur decision makers, who have an “aversion to undertaking costly, unpopular, and otherwise inconvenient countermeasures,” into action.¹¹⁷ Because of the massive volume of information that analysts and decision makers receive, underestimation of adversaries and biases, such as mirror imaging warnings,¹¹⁸ such as the 9/11 attacks, get missed. Thus, countries such as the U.S. are caught flat-footed.

Cynthia Grabo wrote of vague warnings, “More rather than fewer facts, specific rather than generalized assessments, clear and realistic descriptions of the various alternatives rather than vague possibilities, and firm and unequivocal statements of the adversary’s capabilities and possible or probable intentions are required.”¹¹⁹ It is an unfortunate reality that sometimes the intelligence to fully identify a threat just does not exist. When that happens, although a policymaker realizes she or he has been warned, he or she does not know exactly *what* the warning is about. A vague warning provides little to act upon, and so very often, nothing is done about it.

The “tyranny of current intelligence” is the cognitive trap that causes analysts to overemphasize the “now.” Current intelligence is important to the tactical level, or combat support operations, which require real-time information to respond to threats.¹²⁰ Fusion centers are designed “to facilitate the fast synthesis of data to support ongoing tactical operations and to allow additional collection to be done intelligently in a short period of time.”¹²¹ In addition, fusion centers are a relatively new development in the IC.

¹¹⁷ Davis, “Why Bad Things Happen to Good Analysts,” 2–4.

¹¹⁸ Wirtz, and Porch, “Surprise and Intelligence Failure,” 2–3.

¹¹⁹ Grabo, *Anticipating Surprise, Analysis for Strategic Warning*.

¹²⁰ Clark, *Intelligence Analysis*, 50.

¹²¹ *Ibid.*, 55.

Originally, fusion centers came about after 9/11 as a means to address the stovepipe effect and lack of information sharing that contributed to the inability to prevent 9/11. Over the last 10 years, there was a natural progression for fusion centers in which they have generally shifted focus to criminal activity in order to be productive. Ideally, fusion centers function as a clearinghouse for data from all levels of law enforcement from the local, state, federal, tribal, and sometimes international law enforcement partners.¹²² Clark highlights two of the major criticisms of fusion centers: that they do little true fusion of intelligence and the risk of violations of U.S. citizen privacy and civil liberties.¹²³ A true fusion of intelligence will eventually occur. The first steps of bringing IC partners to a centralized point and establishing processes to exchange information have occurred. Next, transparency and accountability must be assessed for fidelity to identify deficiencies. Fusion centers should continue to implement and improve self-inspection programs to ensure policy compliance with constitutional law. Furthermore, fusion centers need refinement to enhance efficiency and effectiveness; they are the future of a whole-of-government approach to intelligence analysis.

¹²² Ibid.

¹²³ Ibid.

V. SOLUTIONS AND RECOMMENDATIONS

A. SUMMARY OF RECOMMENDATIONS

1. Conduct a thorough, field-level analysis to establish a baseline of current intelligence capabilities, capability gaps, and mission needs.
2. Provide intelligence-centric strategic guidance to unify, synchronize, and coordinate efforts to continue to expand and enhance the friendly force information-sharing network.
3. Establish clear guidelines and standard operating procedure (SOP) for collections at the field level, facilitated by a collection manager, to ensure useful, timely, and relevant intelligence collections.
4. Understand the mission needs and requirements for information-sharing technology for future acquisitions.
5. Gain an understanding of all Red Team efforts in the field and better utilize the cadre of trained Red Team personnel as an additional level of analytical rigor for high-level projects.
6. Begin intelligence indoctrination at the academy to reinforce that every agent is a collection asset.

B. DEFINING THE PROBLEM

If I had an hour to solve a problem and my life depended on the solution, I would spend the first 55 minutes determining the proper question to ask, for once I know the proper question, I could solve the problem in less than five minutes.

Albert Einstein

Before addressing solutions and recommendations, it must be acknowledged that correctly *framing the problem* is always the first step toward improving a system. That does not preclude this study from making high-level recommendations, but it highlights the need for deep dive analysis at the field level to understand the mission needs and requirements from the ground up. The USBP Intelligence Division is currently planning capability gap analysis process (CGAP) of intelligence functions and operations. The results of the CGAP should provide a baseline measurement of the USBP's capability to execute the intelligence cycle properly. A thorough understanding of USBP intelligence capabilities and capability gaps, viewed through the lens of strategic goals and objectives,

will outline the priorities for a path forward to developing the requirements to transition the USBP sector intelligence units into the premier border security intelligence enterprise system.

C. PLANNING

Plans are nothing, planning is everything.

Dwight. D. Eisenhower

A wealth of guidance, vision, and strategic level direction has been published by DHS, CBP, and the USBP. The DHS *National Response Framework* states, “Planning across the full range of homeland security operations in an inherent responsibility of every level of government.”¹²⁴ Historically, the centralized planning and decentralized execution of strategy has allowed field commanders to accomplish the mission based on their wisdom, judgment, and experience. The USBP has made great strides in publishing a strategic plan with associated measure and metrics to inform on the progress of accomplishing the mission; however, the USBP could provide more specific guidance to unify, synchronize, and coordinate efforts to continue to expand and enhance the friendly force information-sharing network at the field level. For example, an intelligence planning supplement to the USBP *2012–2016 Strategic Plan* or future plan would be useful to describe the high level vision, mission specific guidance to the USBP intelligence division, the goals and objectives of the intelligence mission in supporting operations. An intelligence plan should also have measures and milestones to inform about progress to meeting the chief’s priorities.

¹²⁴ U.S. Department of Homeland Security, *National Response Framework* (Washington, DC: Department of Homeland Security, 2013).

There are opportunities to provide additional clarification at the sector level. Every sector must produce an operational implementation plan (OIP). The OIP is the articulation of that sector chief's priorities, strategy, and objectives in furtherance of the national strategy. An intelligence plan supplement to the OIP would capture the sector intelligence unit's specific goals and objects in support of sector operations. Again, the value in these documents are the measures and milestones that inform toward progress and performance. These intelligence annexes would also serve as a guide to field commanders when synchronizing tactical level operations with operational and strategic level intelligence requirements.

Planning and Direction is the first phase of the intelligence cycle, yet anecdotal and empirical evidence suggests no intelligence-centric planning training exists. Because the USBP is still working on developing and subsequently publishing intelligence doctrine, there is no common understanding on what is needed to accomplish certain tasks.

D. COLLECTIONS

Everyone is an intelligence officer—that's sort of our theme. If you're talking about a paradigm shift, this is it: You have to see everyone you come in contact with as having intelligence value.

MAJ Michael S. Patton, Operations Officer, 4–27 Field Artillery Battalion, Baghdad
The Washington Post, 5 November 2003

Figure 8 describes the General Intelligence Collection Requirements.

Figure 8. General Intelligence Collection Requirements

- 
- General Intelligence Collection Requirements**
1. Terrorism
 2. Threats to National Security
 3. Alien Smuggling
 4. Drug Trafficking
 5. Illegal Entry into the United States
 6. Threats Against OBP Operations
 7. Mass Illegal Immigration
 8. Sensitive Events
 9. Foreign Conditions Affecting Immigration
 10. Domestic Conditions Affecting Immigration
 11. Crimes by Aliens
 12. Fraudulent Identities, Entries, and Applications
 13. Counterfeiting Immigration-related Documents
 14. Asset Concealment
 15. Removable Aliens
 16. Employment of Unauthorized Aliens.

Source: “USBP Intelligence Unit” (internal document, U.S. Customs and Border Patrol, Washington, DC, 2014).

Collections is a major activity that drives the intelligence cycle, yet anecdotal evidence indicates collections may be undervalued at the field level. The establishment of clear guidelines and standard operating procedure for collections at the field level is paramount for thorough and consistent intelligence collections. Identification of collection requirements with stakeholders, doctrinal procedure, methods for data management, and accountability and tasking of collection assets are the core of the collections process. The development of USBP intelligence doctrine, and subsequent

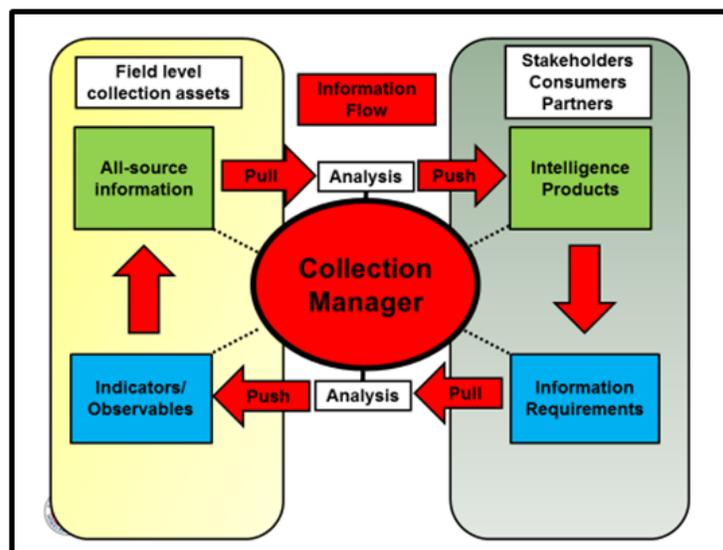
field manuals would help agents understand what guiding principles to adhere to when conducting information collection duties.

1. The Collection Manager

It is readily apparent that there is not an “official” collection manager position. Collection management varies station to station, sector to sector based on local requirements (see Figure 9). The Army’s 2013 Field Manual 3–55, *Information Collection* states:

Respective collection managers employ organic means to cover the seams and gaps between units. These organic means provide the deploying tactical force with the most complete portrayal possible of the enemy and potential adversaries, the populace, and the environmental situation upon entry.¹²⁵

Figure 9. Collection Management Cross Section: Horizontal View



Source: Headquarters, Department of the Army, *Information Collection*.

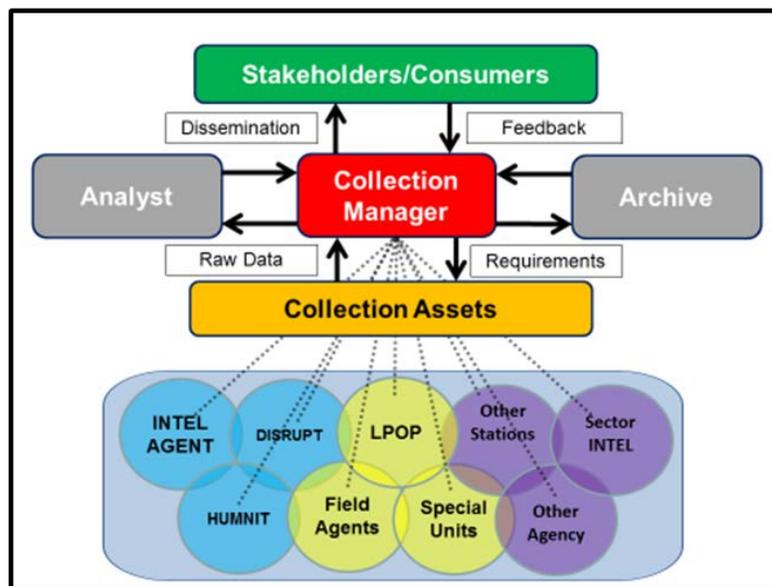
At the field level, the collection manager is a relationship based, task facilitator. Additionally, the collection manager must be familiar with all the collection capabilities

¹²⁵ Headquarters, Department of the Army, *Information Collection* (FM 3-55) (Washington, DC: Headquarters, Department of the Army, 2013), http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_55.pdf.

at their disposal, and the people who have tactical control (TACON) of those capabilities. Understanding that collection assets are finite, the collection manager has the task of coordinating the most effective means of collection based on prioritization and risk. Collection managers' duties include those listed in Figure 10.

- Facilitating the development of integrated collection strategies against priority collection targets
- Optimizing the employment of collection assets
- Requesting collection resources (e.g., SIU, OI, DHA IA)
- Pushing and/or pulling information and requirements from collection assets to stakeholders and command staff
- Ensuring prioritized intelligence collections
- Identifying intelligence collection capability shortfalls
- Gathering information is prioritized, prepped, and transferred to intel agent for analysis
- Understanding analysis driven collection feeds intelligence driven operations

Figure 10. Collection Management Cross Section: Vertical View



Source: Headquarters, Department of the Army, *Information Collection*.

2. Collection at the Field Level

Every agent, asset, and stakeholder in the field is a potential collection asset. The USBP needs to provide a *field-level* list of indicators (observable phenomenon) in a simple, easily understood manner. This list should map to the station's respective priority intelligence requirements.

An indicator list, simply defined, is a compilation of projected, anticipated or hypothetical actions which any nation might take in preparation for hostilities or other inimical actions. Such lists, often compiled without regard to whether it was likely or even possible to collect the desired information, proved of assistance to both collectors and analysts, provided they were not regarded as a bible of what to expect.¹²⁶

As demonstrated in the Tucson *Intelligence/Operations Communications Study*, there is an appetite for agents to know what they should “look out” for in the field, and it is the responsibility of the BPA-Is and collection managers to communicate those indicators and provide feedback on information collected.¹²⁷

3. Processing and Exploitation

We face a dispersed, complex, and “asymmetric” threat environment in which information technology makes everything move faster; in which strategic and tactical requirements are becoming more blurred; and in which diverse and shifting priorities increase the demands from consumers for expert analysis in real time and from collectors who, more than ever, need sustained guidance on priorities and greater assistance with exploitation.

Dr. William J. Lahneman, *The Future of Intelligence Analysis*, 2006

Processing and exploitation is critical to managing collections, as it is the cleansing and organizing stage of the intelligence cycle and a necessary precursor to “sensemaking,” or analysis and production. Integral to processing and exploitation, an information sharing architecture, is needed to link the 900 disparate systems in DHS,

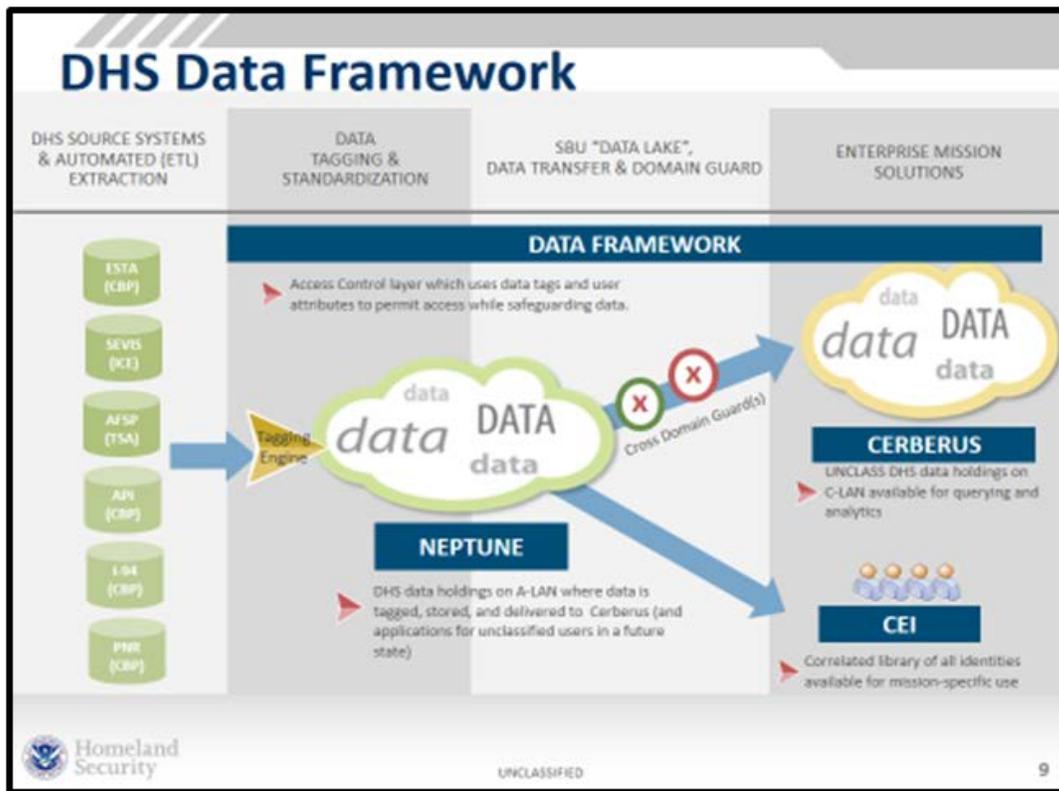
¹²⁶ Grabo, *Anticipating Surprise, Analysis for Strategic Warning*, 63.

¹²⁷ U.S. Border Patrol, Tucson Sector Operations Division, “Red Team Operational Exercise: Ajo Analysis.”

located primarily on unclassified networks with a variety of user populations.¹²⁸ At least 250 data sets have multiple data formats and standards, non-Title 50 data, U.S. persons, and special protected class information.

In the 2004 GAO report, *Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*, the GAO stated, “The Department of Homeland Security (DHS) is attempting to integrate 22 federal agencies, each specializing in one or more interrelated aspects of homeland security.” An enterprise architecture is a key tool to achieve this effectively and efficiently. In September 2003, DHS issued an initial version of its architecture (see Figure 11).

Figure 11. DHS Data Framework



Source: U.S. Department of Homeland Security, "Data Framework."

¹²⁸ U.S. Department of Homeland Security, "Data Framework" (internal document, DHS Joint Requirements Council, Washington, DC, 2015).

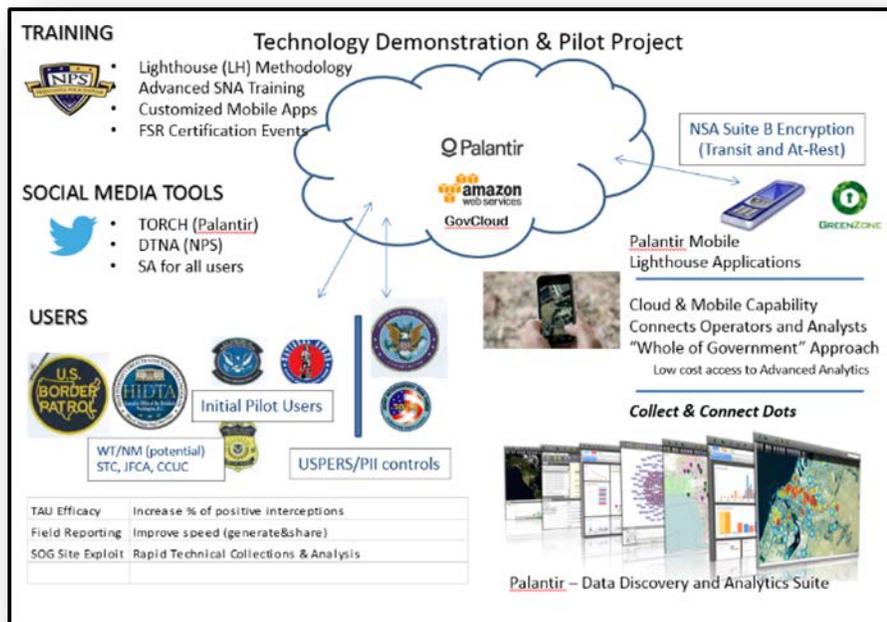
DHS has been struggling since 2003 to implement a functional, accessible, information sharing architecture and efforts are still ongoing.” It is a testament to the challenge of information sharing that 12 years after the 2004 GAO report, DHS continues to research and develop an information sharing architecture. In FY15 the USBP demonstrated a technology pilot for information sharing and advanced analytics. Currently, efforts are underway to develop joint requirements for the acquisition of an information sharing technology for CBP.

4. Analysis and Production

And then there is that other thinking: Thinking about the conundrums that we face, the alternatives and choices we have to make on larger issues, the dilemmas we wish to resolve.

Mark Lowenthal

Figure 12. Combating Terrorism Technical Support Office and CADENA Overview and Introduction to Joint Task Force-West



Source: U.S. Department of Homeland Security, "Data Framework."

Analysis and production (sometimes referred to as visualization) is often overvalued as the most critical phase of the intelligence cycle, as it is the culmination and representation of actionable intelligence. BPA-Is need a suite of tools to produce and visualize intelligence to stakeholders, consumers, and decision makers (see Figure 13).

Figure 13. Attributes of Excellent Intelligence



Figure II-2. Attributes of Intelligence Excellence

Source: Joint Chiefs of Staff, *Joint Intelligence*.

Often, production becomes a reporting requirement that becomes perfunctory as a “report card” or artifact. BPA-Is should measure the value of analysis and production through the filter of the eight attributes of intelligence excellence. In addition, BPA-Is should assess and challenge commanders for feedback on their products and constantly strive to improve and enhance the value and usability of products.

5. Dissemination

The goal of a knowledge sharing process is to create, facilitate, and manage a horizontally based, vertically integrated knowledge transfer system designed to harness emerging enemy and friendly information to create a competitive advantage against a networked threat through technological innovation and cultural engagement.

Commander’s Handbook for Attack the Network

In the U.S. Border Patrol, there is no lack of dissemination. The problem is too much or duplicative dissemination. The transition from a need to know to a need to share has created a culture where email is the primary channel of communication while also

used as a system of record. Anecdotally, from supervisors on up, agents are inundated with many (tens to hundreds) of emails per day. There is no logical, practical method of labeling or tagging information in emails to categorize urgent information by importance and value. Often, it is up to the users to determine the value of the information in email *to them*. The USBP needs to understand the users' needs and develop a plan for a complete dissemination overhaul leveraging modern technology to ensure the right people get the information they need in time to use it. Conversely, all others should have access to the information in a searchable, user-friendly database to access data that would otherwise flood their inbox on an hourly basis.

6. Red Team

What is Red Teaming?

Red teaming is “diagnostic, preventative, and corrective; yet it is neither predictive or a solution. Our goal is to be better prepared and less surprised in dealing with complexity. Red Teaming is a function executed by trained, educated, and practiced team members that provides commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations, and capabilities in the context of the operational environment and from the perspectives of our partners, adversaries, and others.”¹²⁹

Red Team Handbook 7.0, 2015

In 2004, the Army Chief of Staff, General Peter Schoomaker, recognized a need for advanced analytical support for planning, intelligence, and decision making.¹³⁰ The intent of Red Teaming is to foster critical thinking, develop cultural empathy, promote consideration of alternative perspectives on problems, engage everyone in the network, and encourage introspection and self-awareness.¹³¹ Since 2009, the USBP has been working with the U.S. Army's University of Foreign Military and Cultural Studies to develop a Red Team capability organic to the U.S. Border Patrol. Approximately, 120 agents have graduated from the Red Team program, but the return on investment is

¹²⁹ *Red Team Handbook*, version 6.0.

¹³⁰ *Ibid.*

¹³¹ *Ibid.*

unknown at this point. Although a thorough audit nationwide has not been done, an informal review yielded the following examples of U.S. Border Patrol Red Team projects:

USBP

- May 2013: U.S. Border Patrol *Strategic Plan/Balanced Scorecard Analysis*

Tucson Sector

- March 2013 *Ajo Gotaway Red Team Study*
- April 2013: *Mariposa Port of Entry Cargo Operations Study*

El Centro Sector

- September 2015: *Eastbound I-8 Checkpoint Analysis*¹³²

Both the Army and the USBP have had challenges in leveraging the Red Team capability for two major reasons. The first major constraint was that the “best and brightest,” the ideal Red Team candidates, cannot often be spared the time for Red Team training or Red Team projects. This has often led to staffing Red Team trainings with those most available but not necessarily the best candidates, undermining the effectiveness of the concept. Second, there is no clear place to put the function as Red Teaming can support intelligence by providing alternative adversary analysis, support operations with alternative analysis, and support decision making with a host of Red Team tools to reveal unintended consequences. The Army has appeared to find a compromise where division and headquarters are staffed with officers who are Red Team trained. When the commander or chief of staff needs a Red Team effort, he or she can pull together a focused Red Team from across the staff that is trained in Red Team tools and methods.¹³³

Planning, intelligence, and Red Teaming are independent functions, yet they need to be cross-functional in execution to attain strategic, operational, and tactical goals. The USBP has an organic Red Team capability that can work with the Intelligence and Operations Division to add the value and rigor of critical and creative thinking toward the

¹³² Ibid.

¹³³ Ibid.

complex problem of adaptive adversary operations in the homeland security ecosystem. It is highly recommend that the USBP gain an understanding of all Red Team efforts and outcomes in the field. In addition, the USBP could better utilize its cadre of trained Red Team personnel as an additional level of analytical rigor, validation, and verification of assumptions for critical topics such use of force, body-worn cameras, and human rights.

E. VISION FOR THE FUTURE

Intelligence is a specialized form of knowledge, an activity, and an organization. As knowledge, intelligence informs leaders, uniquely aiding their judgment and decision-making. As an activity, it is the means by which data and information are collected, their relevance to an issue established, interpreted to determine likely outcomes, and disseminated to individuals and organizations who can make use of it, otherwise known as “consumers of intelligence.”

An intelligence organization directs and manages these activities to create such knowledge as effectively as possible.

David Moore, *Critical Thinking and Intelligence Analysis*

The DHS Office of Intelligence & Analysis and CBP Office of Intelligence could be considered the central nervous system of the homeland security friendly force ecosystem. If so, then the USBP and its BPA-Is are the eyes and ears (i.e., the nerve endings and the sensory inputs into the friendly force information sharing network). Of course, there are a host of friendly force stakeholders that comprise the friendly force information-sharing network, but no single agency has the intelligence collections manpower of the USBP. The USBP can continue to develop and enhance the BPA-Is’ capability and capacity to execute every stage of the intelligence cycle with excellence.

The USBP is at the precipice of a new age in information sharing. Massive efforts have been underway to provide an enterprise architecture to provide the connectivity and access to the full breadth and depth of the homeland security information and data management systems. The USCG and DHS IA may be actual members of the IC, but the U.S. Border Patrol has a significant advantage: its 21,000 agents embedded in the border security environment. The USBP should start indoctrinating all agents at the academy about their role in collections and the function of the intelligence cycle. Furthermore, the

U.S Border Patrol must evolve its paradigm of the agent's role in border security to emphasize collection and information sharing holistically and comprehensively. The time is now for the U.S. Border Patrol to harness and exploit the full power and capability of its intelligence enterprise by understanding current capabilities and charting a path forward to establishing a professional intelligence enterprise driven from the ground up.

APPENDIX A. PROFESSIONAL INTELLIGENCE ASSOCIATIONS—ADDITIONAL OPPORTUNITIES FOR BPA-IS

Consummate Border Patrol intelligence professionals should seek to enrich their knowledge and personnel development by engaging others in the law enforcement intelligence field. There are a wealth of low-cost or no-cost opportunities available. The USBP Intelligence Division should conduct a market survey and develop a list of resources, available to BPA-IS.

A preliminary market survey revealed the intelligence associations outlined below.

International Association of Law Enforcement Intelligence Analysts (IALEIA)

IALEIA is the largest professional organization in the world representing law enforcement analysts. It is based in the United States, and is a non-profit 501(c)3 corporation.¹³⁴



Source: “International Association of Law Enforcement Intelligence Analysts (IALEIA),” International Association of Law Enforcement Intelligence Analysts.

Armed Forces Communications and Electronics Association (AFCEA)

According to the AFCEA website,

AFCEA is an international organization that serves its members by providing a forum for the ethical exchange of information. AFCEA is

¹³⁴ “International Association of Law Enforcement Intelligence Analysts (IALEIA),” International Association of Law Enforcement Intelligence Analysts, accessed August 2015, <http://www.ialeia.org/>.

dedicated to increasing knowledge through the exploration of issues relevant to its members in information technology, communications, and electronics for the defense, homeland security and intelligence communities.¹³⁵



Source: “Armed Forces Communications and Electronics Association (AFCEA),” Armed Forces Communications and Electronics Association.

Intelligence and National Security Alliance(INSA)

INSA is the premier intelligence and national security organization that provides a unique venue for collaboration, networking, and examination of policy issues and solutions. Representing an unprecedented alliance among senior leaders from the public, private, and academic sectors, INSA members form an unparalleled community of experts who collaborate to develop creative, innovative, and timely solutions to the intelligence and national security issues facing the United States.¹³⁶



Source: “Intelligence and National Security Alliance (INSA),” Intelligence and National Security Alliance.

¹³⁵ “Armed Forces Communications and Electronics Association (AFCEA),” Armed Forces Communications and Electronics Association, accessed August 5, 2015, <http://www.afcea.org/>.

¹³⁶ “Intelligence and National Security Alliance (INSA),” Intelligence and National Security Alliance, accessed August 20, 2015, <http://www.insonline.org/>.

U.S. Department of Justice, Bureau of Justice Assistance, State and Local Anti-Terrorism (SLATT)

The State and Local Anti-Terrorism Training (SLATT) Program is funded by the United States Department of Justice, Bureau of Justice Assistance. The Program is dedicated to providing critical training and resources to our nation's law enforcement, who face the challenges presented by the terrorist/violent criminal extremist threat. To help confront this threat, the SLATT Program provides specialized multiagency anti-terrorism detection, investigation, and interdiction training and related services to state, local, and tribal law enforcement and prosecution authorities.¹³⁷



Source: U.S. Department of Justice, Bureau of Justice Assistance, "State and Local Anti-Terrorism (SLATT)."

¹³⁷ U.S. Department of Justice, Bureau of Justice Assistance, "State and Local Anti-Terrorism (SLATT)," accessed August 20, 2015, <https://www.slatt.org/>.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. IC BREAKDOWN



Source: Center for Intelligence and Security Studies, "CISS Names as a Center of Academic Excellence," 2015, <http://ciss.olemiss.edu/the-center/center-of-academic-excellence/>

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. TUCSON SECTOR INTELLIGENCE/ INFORMATION SHARING STUDY: CRITICAL FINDINGS

1. Do you know who all the BPA-I's are at your station?	None	Less than half	About half	More than half	Most/all of them
Percentage	2%	19%	22%	23%	34%

Analysis

Approximately 1/5 of the stations, the majority are BPAs, know less than half of the station BPA-Is. If field agents are unaware of who is a BPA-I, they will be unable to share any pertinent information to the appropriate personnel for analysis.

Recommendations

FA3 Intel Units will ensure that a contact list of BPA-I with phone numbers and email is included in Muster Modules, briefs, etc. The Intel contact list will be posted in all common areas for increased visibility.

Target Goals

1. Do you know who all the BPA-I's are at your station?	None	Less than half	About half	More than half	Most/all of them
Percentage	0%	5%	10%	35%	50%
Percentage Change	-100%	-73%	-54%	+52%	+47%

2. How likely are you to contact a BPA-I if you had info?	Not likely	Maybe	Probably	Most likely	Definitely
Percentage	2%	6%	16%	39%	37%

Analysis

76% of FA3 would “Most likely” or “Definitely” contact a BPA-I with info.

Recommendations

Develop a “go by” for all station personnel that will standardize the information sharing process.

Target Goals

2. How likely are you to contact a BPA-I if you had info?	Not likely	Maybe	Probably	Most likely	Definitely
Percentage	0%	5%	10%	35%	55%

Percentage Change	-100%	-17%	-38%	-10%	+49%
--------------------------	--------------	-------------	-------------	-------------	-------------

3. How likely are you to get feedback from a BPA-I if you gave them info?	Not likely	Maybe	Probably	Most likely	Definitely
Percentage	11%	13%	20%	38%	17%

Analysis

Approximately 24% of FA3 feels that it is “Not likely” or “Maybe” they will get feedback from a BPA-I on information provided. If field agents are not receiving feedback they will be less likely to share information.

Recommendations

Implement an initiative to track and respond to any agent submitting information to Intel.

Target Goals

3. How likely are you to get feedback from a BPA-I if you gave them info?	Not likely	Maybe	Probably	Most likely	Definitely
Percentage	5%	5%	10%	50%	30%
Percentage Change	-54%	-62%	-50%	+32%	+76%

4. How would you provide a BPA-I with info?	Don't Know	Face-to-face	Note	Phone call	Email
Percentage	0%	35%	14%	17%	34%

Analysis

The majority of the station prefers face-to-face or email to communicate info. Face to face interaction is invaluable, yet there should be a standardized process to collect and memorial.

Recommendations

Establish a “go by” to standardize the intelligence sharing process from the field to Intel.

Target Goals

4. How would you provide a BPA-I with info?	Don't Know	Face-to-face	Note	Phone call	Email
Percentage	0%	35%	14%	17%	34%
Percentage Change	0%	0%	0%	0%	0%

5. How would you rate communication between Intel and the field	None	Poor	Fair	Good	Outstanding
--	-------------	-------------	-------------	-------------	--------------------

Percentage	3%	17%	32%	43%	5%
-------------------	-----------	------------	------------	------------	-----------

Analysis

Approximately 50% of the station perceives that communication is Fair or worse.

Recommendation

Standardize, institutionalize, and memorialize of identified best practices for sharing information to increase communication and situational awareness between field and Intel agents.

Target Goals

5. How would you rate communication between Intel and the field	None	Poor	Fair	Good	Outstanding
Percentage	0%	10%	20%	65%	10%
Percentage Change	-100%	-41%	-38%	+51%	+100%

6. What can Intel do to improve communications with the field? (Top five suggestions)
1) Increase Intelligence Muster Presentations
2) Educate/Inform Agents about Intel duties, functions, and capabilities
3) Dispel the “secret squirrel” perception and clarify what information is need to know
4) Provide feedback to agents who have submitted information to Intel
5) Make sure all shifts are getting the same Intel briefs at muster on any given day

Analysis

This question yielded 168 relevant, appropriate, and actionable responses.

Recommendations

- 1) Increase Intelligence Muster Presentations
 - Continue to attend station musters with a goal of 100% attendance
 - Disseminate information and intelligence on current trends, patterns, and predictive analysis of potential futures
 - Seek out agents directly after muster to develop coalescent knowledge of current trends and patterns
- 2) Educate/Inform Agents about Intel duties, functions, and capabilities
- 3) Dispel the “secret squirrel” perception and clarify what information is “need to know”
 - Create Intel 101 Presentation to be disseminated via email to all agents

- Update presentation for presentation at musters at the beginning of each Fiscal year
 - Utilize face-to-face interactions as “teachable moments” to explain the intelligence process
- 4) Provide feedback to agents who have submitted information to Intel
- Provide timely feedback to agents on any information that is provided to Intel
 - Exploit opportunities to provide feedback and follow-up on significant events, issues, and occurrences to providing informal training to the field
 - Continue to provide specific indicators to agents at muster and solicit feedback from agents on refining indicators based on observations
- 5) Make sure all shifts are getting the same Intel briefs at muster on any given day
- Standardize communication between Intel agents on each shift to provide visibility of what was briefed and ensure the same information is briefed at each muster

A six-question survey was created to gauge agent, supervisor, and command staff perception about elements of communication between intelligence and field units. Surveys were administered one-on-one to the target demographic. The survey administrator read the question and responses to the agent surveyed to ensure comprehension. For question 6, survey administrator encouraged the agent surveyed to provide candid but constructive feedback.

Survey Format:

Name (optional):	Time in Service:				
1. Do you know who all the BPA-Is are at your station?	None	Less than half	About half	More than half	Most/all of them
2. How likely are you to contact a BPA-I if you had info?	Not likely	Maybe	Probably	Most likely	Definitely
3. How likely are you to get feedback from a BPA-I if you gave them info?	Not likely	Maybe	Probably	Most likely	Definitely
4. How would you provide a BPA-I with info?	Don't Know	Face-to-face	Note	Phone call	Email
5. How would you rate communication between Intel and the field	None	Poor	Fair	Good	Outstanding
6. What can intel do to improve	Anecdotal answer; write down agent response				

communications with the field?	
--------------------------------	--

Survey responses were compiled, tabulated, and normalized for comparison and analysis. Agent responses to survey question 6 were analyzed and reorganized into general categories and ranked in descending order based on frequency of occurrence. Results were analyzed to reveal agents perceptions in communication gaps and deficiencies between intel and the field. Reccomendations were generated to enhance specific gaps and deficiencies, and target goals were identified for future evaluation.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Bruce, James B., and Roger Z. Greg. *Intelligence Analysis-The Emergence of a Discipline*. Washington, DC: Georgetown University Press, 2008.
- Butterfield, Alexander, Terry Meissner, and Gail Kulisch. *Against Al Qaida: Improving Warning in the Asymmetric Environment*. Cambridge, MA: Harvard University Press 2008.
- Bustria, John, Emad Shenouda, and Michael McDaniel. "The Functional Desks as Collaborative Mechanisms in the Michigan Intelligence Operations Center." *Homeland Security Affairs*, Supplement no. 2 (2008). <http://www.hsaj.org/?article=supplement.2.4>.
- Clark, Robert. *Intelligence Analysis*. 4th ed. Washington, DC: CQ Press, 2013.
- Dahl, Eric. *Warning of Terror: Explaining the Failure of Intelligence against Terrorism*. Medford, MA: Tufts University, 2004.
- Davis, Jack. "Why Bad Things Happen to Good Analysts." In *Intelligence Analysis-The Emergence of a Discipline*, edited by Roger Z. George and James B. Bruce (157–170). Washington, DC: Georgetown University Press, 2008.
- Defense Science Board. *Summer Study on Capability Surprise*. Vol. I. Washington, DC: Office of the Under Secretary of Defense for Acquisition Technology and Logistics, 2009.
- Endsley, Mica R. "Measurement of Situational Awareness in Dynamic Systems." *Human Factors*, 37 (1995): 32–64.
- Endsley, Mica R. "Toward a Theory of Situation Awareness in Dynamic Systems." *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37, no. 1 (1995): 32–64.
- Feng, Liu, and Zhang Ruizhuang. "The Typologies of Realism." *The Chinese Journal of International Politics* 1, no 1 (2006): 109–134.
- Grabo, Cynthia. *Anticipating Surprise, Analysis for Strategic Warning*. Lanham, MD: UPA, 2004.
- Headquarters, Department of the Army. *Information Collection (FM 3–55)*. Washington, DC: Headquarters, Department of the Army, 2013. http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_55.pdf.

- . *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection* (FM 2–91.6). Washington, DC: Headquarters, Department of the Army, 2007.
- Hollywood, John S., Diane Snyder, Kenneth N. McKay, and John E. Boon, Jr., *Connecting the Dots in Intelligence: Detecting Terrorist Threats in the Out-of-the-Ordinary*. Santa Monica, CA: Rand Corporation, 2005.
- Johns Hopkins University Applied Physics Laboratory. *Interagency Teaming to Counter Irregular Threats Handbook*. Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2009.
- Johnson, Bart. “A Look at Fusion Centers: Working Together to Protect America.” *FBI Law Enforcement Bulletin* 76, no. 12 (2007): 28–32.
- Joint Chiefs of Staff. *Capabilities-Based Assessment, User’s Guide Version 3, Force Structure, Resources, and Assessments Directorate* (JCS J-8). Washington, DC: Joint Chiefs of Staff, 2009.
- . *Counterterrorism* (JP 3–26). Washington, DC: Joint Chiefs of Staff, 2005.
- . *Joint Intelligence* (JP-2-0). Washington, DC: Joint Chiefs of Staff, 2007.
- Koethe, John. “Poetry and Truth.” *Midwest Studies in Philosophy* 33, no. 1 (2009): 53–60.
- Lowenthal, Mark. *Intelligence: From Secrets to Policy*, 4th ed. Washington, DC: CQ Press, 2009.
- Luikart, Kenneth. “Homeland Security: Intelligence Indications and Warning.” *Strategic Insights*, 1 no. 10 (2002): 3.
- Mattis, James N. *USJFCOM Commander’s Guidance for Effects-based Operations*. Carlisle Barracks, PA: Army War College, 2008.
- McCulloch, Jude, and Sharon Pickering. “Pre-crime and Counter-terrorism Imagining Future Crime in the ‘War on Terror.’” *British Journal of Criminology* 49 no. 5 (2009): 628–645.
- McLaughlin, John. “Serving the National Policymaker.” In *Analyzing Intelligence: Origins, Obstacles, and Innovations*, edited by Roger Z. George and James B. Bruce (72–81). Washington, DC: Georgetown University Press 2008.
- Monahan, Torin. “The Future of Security? Surveillance Operations at Homeland Security Fusion Centers.” *Social Justice* 37, no. 2–3 (2010): 84–98.

- Monahan, Torin, and Neal A. Palmer. "The Emerging Politics of DHS Fusion Centers." *Security Dialogue* 40, no. 6: (2009): 617–636.
- National Commission on Terrorist Attacks upon the United States. *Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W. W. Norton, 2004.
- Paté-Cornell, Elisabeth. "Fusion of Intelligence Information: A Bayesian Approach." *Risk Analysis* 22, no. 3 (2002): 445–454.
- Perla, Peter P., Michael C. Markowitz, and Christopher, A. Weuve. *Transforming Naval Wargaming: A Framework for Operational-Level Wargaming*. Alexandria, VA: Center for Naval Analysis, 2004. <https://www.usnwc.edu/getattachment/Research---Gaming/War-Gaming/Documents/Publications/Articles/Transforming-Naval-Wargaming-A-Framework-for-Operational-Level-Wargaming.pdf.aspx>.
- Ramo, Joshua Cooper. *The Age of the Unthinkable, Why the New World Disorder Constantly Surprises Us and What We Can Do about It*. New York: Hachett Book Group, 2009.
- Randol, Mark A. *The Department of Homeland Security Enterprise: Operational Overview and Oversight Challenges for Congress*. Washington, DC: Congressional Research Service, 2009.
- Red Team Handbook*. Version 6.0. Fort Leavenworth, KA: University of Foreign Military and Cultural Studies, 2012.
- Schroeder, Robert D. "Institutionalizing a Risk-Based Approach in the USBP." *Small Wars Journal* (January 2014). <http://smallwarsjournal.com/jrnl/art/institutionalizing-a-risk-based-approach-in-the-us-border-patrol>.
- Simson, David. "Truth, Truthfulness and Philosophy in Plato and Nietzsche." *British Journal for the History of Philosophy* 15, no. 2 (2007): 339–360.
- Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2007.
- U.S. Government Accountability Office. *Border Security: DHS Progress and Challenges in Securing the U.S. Southwest and Northern Borders* (GAO-11-508T). Washington, DC: U.S. Government Accountability Office, 2011.
- . *Northern Border Security: DHS's Report Could Better Inform Congress by Identifying Actions, Resources, and Time Frames Needed to Address Vulnerabilities* (GAO-09-93). Washington, DC: U.S. General Accountability Office, 2008.

- U.S. Border Patrol, Office of the Chief. *Memorandum for All Chief Patrol Agents: Fiscal Year 2015 Capability Gap Analysis Process*. Washington, DC: U.S. Border Patrol, Office of the Chief, 2014.
- U.S. Customs and Border Protection. *2012–2016 USBP Strategic Plan*. Washington, DC: U.S. Customs and Border Protection, 2012. http://www.cbp.gov/sites/default/files/documents/bp_strategic_plan.pdf.
- . *FY15 Capability Gap Analysis Process*. Washington, DC: U.S. Customs and Border Protection, 2015.
- U.S. Department of Homeland Security. *Intelligence and Analysis Strategic Plan 2011–2018*. Washington, DC: U.S. Department of Homeland Security, 2011.
- . *National Response Framework*. Washington, DC: Department of Homeland Security, 2013.
- . *Strategic Plan, Fiscal Years 2012–2016*. Washington, DC: U.S. Department of Homeland Security, 2012.
- White House. *National Drug Control Strategy*. Washington, DC: White House, 2011. <https://www.whitehouse.gov/sites/default/files/ondcp/ndcs2011.pdf>.
- Williams, Phil. “Warning Indications, Terrorist Finances, and Terrorist Adaption.” *Strategic Insights* 4, no 1 (2005).
- Wirtz, James, and Douglas Porch. “Surprise and Intelligence Failure.” *Strategic Insight* 1, no. 7 (2002).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California