NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE REALITY OF THE HOMELAND SECURITY ENTERPRISE INFORMATION SHARING ENVIRONMENT

by

Michael E. Brown

December 2017

Thesis Advisors: Erik Dahl
Robert Simeral

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE THE REALITY OF THE HOMELAND SECURITY ENTERPRISE INFORMATION SHARING ENVIRONMENT		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Michael E. Brown			
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 number 2016-0153-DD-N.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Responding to recommendations from the 9/11 Commission, Congress created the Information Sharing Environment (ISE) with the passage of the 2004 Intelligence Reform and Terrorism Prevention Act. Linked to the creation of the Office of the Director of National Intelligence and championed by that office's program manager for the ISE, the ISE has contributed to national intelligence reform by attempting to improve information sharing across the federal, state, local, territorial, and tribal domains. Given the rise in domestic terrorist attacks and the progress of intelligence reform over the last 16 years, this thesis explores an analysis of the ISE's effectiveness and an examination of alternative means of information sharing to address the remaining information-sharing challenges brought to light in attacks carried out between 2014 and 2017. Alternative information-sharing techniques have been used by our nation's special operations forces and by our largest police force, the New York Police Department. The best practices of organizations such as these may be leveraged by the ISE to further future intelligence-sharing reform.

14. SUBJECT TERMS Intelligence Reform and Terrorism Prevention Act, Information Sharing Environment, NYPD, Special Operations Forces, planning cells, counterterrorism operations, intelligence reform, collaboration, Office of the Director of National Intelligence, Posse Comitatus, Intelligence Community, field intelligence	**15. NUMBER OF PAGES** 91
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

THE REALITY OF THE HOMELAND SECURITY ENTERPRISE INFORMATION SHARING ENVIRONMENT

Michael E. Brown
Field Intelligence Officer, Transportation Security Administration
B.S., Excelsior University, New York, 2010

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 2017**

Approved by: Erik Dahl
Thesis Co-Advisor

Robert Simeral
Thesis Co-Advisor

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Responding to recommendations from the 9/11 Commission, Congress created the Information Sharing Environment (ISE) with the passage of the 2004 Intelligence Reform and Terrorism Prevention Act. Linked to the creation of the Office of the Director of National Intelligence and championed by that office's program manager for the ISE, the ISE has contributed to national intelligence reform by attempting to improve information sharing across the federal, state, local, territorial, and tribal domains. Given the rise in domestic terrorist attacks and the progress of intelligence reform over the last 16 years, this thesis explores an analysis of the ISE's effectiveness and an examination of alternative means of information sharing to address the remaining information-sharing challenges brought to light in attacks carried out between 2014 and 2017. Alternative information-sharing techniques have been used by our nation's special operations forces and by our largest police force, the New York Police Department. The best practices of organizations such as these may be leveraged by the ISE to further future intelligence-sharing reform.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AQI	Al Qaida in Iraq
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
CIA	Central Intelligence Agency
CIE	criminal intelligence enterprise
CJSOTF	Combined Special Operations Task Force
COA	course of action
CT	counterterrorism
CUI	controlled unclassified information
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOD	Department of Defense
EDC	enterprise data centers
EO	executive order
ESU	emergency services unit
EUROPOL	European Police Organization
FBI	Federal Bureau of Investigation
FIO	field intelligence officer
FSLTT	federal, state, local, territorial and tribal
GAO	Government Accountability Office
GWOT	global war on terrorism
HIDTA	high intensity drug trafficking area
HSC	Homeland Security Committee (House of Representatives)
HSDN	Homeland Security Defense Network
HSE	homeland security enterprise
HSIN	Homeland Security Information Network
HUMINT	human intelligence
IC	Intelligence community (U.S.)
ICD	intelligence community directive
IRB	Institutional Review Board
IRTPA	Intelligence Reform and Terrorism Prevention Act

ISE	Information Sharing Environment
ISIL	Islamic State in Iraq and the Levant
ISP	Intelligence Support Program
IT	information technology
J-2	Joint Staff Intelligence Office
JSOU	Joint Special Operations University
JTF	joint task force
JTTF	joint terrorism task force
LMSI	Lower Manhattan Security Initiative
MIST	multimodal information sharing team
NCR	National Capital Region
NCTC	National Counterterrorism Center
NGA	National Geospatial Intelligence Agency
NIC	National Intelligence Council
NIP	National Intelligence Program
NIST	national intelligence support teams
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
NSI	Nationwide Suspicious Activity Report Initiative
NYPD	New York Police Department
O&I	operations and intelligence
ODNI	Office of the Director of National Intelligence
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
ORCON	originator control
OSINT	open-source intelligence
PC	personal computer
PM ISE	program manager Information Sharing Environment
RISSNET	Regional Information Sharing Systems Secure Cloud
SAD	state active duty
SBU	sensitive but unclassified

SCIF	sensitive compartmented information facility
SIGINT	signals intelligence
SOCOM	Special Operations Command (U.S.)
SOF	special operations forces
TCO	total cost of ownership
TIC	trusted Internet connection
TS/SCI	Top secret sensitive compartmented information
USDI	undersecretary for defense, intelligence
VDI	virtual desktop environment

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Terrorist attacks such as those between 2014 and early 2017 in Garland, San Bernardino, Orlando, Fort Lauderdale, Seaside, and Chelsea highlight the increased challenge of preventing terrorist and homegrown violent extremists in the homeland. At its core, the challenge for information sharing involves how federal, state, local, territorial, and tribal counterterrorism (CT) operations that collect, receive, and analyze act upon information and intelligence prior to an attack. The Information Sharing Environment (ISE) was intended to reform and improve how intelligence/information sharing for CT would be accomplished. Given the rising domestic terrorism threat almost 13 years after the ISE was signed into law, this thesis analyzes the remaining ISE challenges and explores two alternative approaches to information sharing that may pave a different path toward building trust across the CT communities.

The 9/11 Commission Report detailed a framework for future intelligence reform in section 13.2 titled Unity of Effort in the Intelligence community. While this directly led to the creation of the National Counter Terrorism Center, it was not until Congress passed the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA) that information sharing for counterterrorism became law. The 2004 IRTPA created the ISE and defined it as "an overarching approach to strengthening the sharing of intelligence, terrorism, homeland security, law enforcement, and other information among federal, state, local, tribal, international, and private sector partners."[1] However, despite the creation of the ISE and its program manager, challenges with information sharing exist. An inconsistent implementation dynamic has led to gaps in strategic CT capabilities. Local law enforcement lacks access to new, innovative national CT intelligence collection and analysis capabilities, which ultimately played a role in successful terrorist attacks from 2014 through 2017. Testimony from local leaders and other documentation

[1] Intelligence Reform and Terrorism Prevention Act, Pub. Law No. 108-458 (2004), https://www.nctc.gov/docs/pl108_458.pdf.

from national police organizations have linked the problem to a lack of local intelligence collection and sharing activities prior to the attacks.

This thesis attempts to outline and detail some of the challenges for the ISE and its implementation of information sharing strategies since 9/11. However, this thesis also proposes that the solutions to these ISE challenges may already exist within two existing yet disparate counterterrorism programs: U.S. special operations forces (SOF) and the New York Police Department Intelligence Program. When the best practices of each model are combined, SOF/Team-of-Teams and the NYPD intelligence unit, they form a framework that contributes to an environment that fosters "robust, real-time information sharing" to the lowest operator level possible. Along with other recommended revisions from Congress, these case studies can contribute to an improved information-sharing environment across the homeland security enterprise.

ACKNOWLEDGMENTS

To Sandra, you are an inspiration, and your presence as my lifelong partner always makes achievements like this possible. Your guidance, patience, and support made this seemingly impossible project come to light in the middle of some dark times. I know my career is a tough one in a tough field, but I would not be here today without you. Eu te amo.

To John Miller, you have been a mentor to me probably without even knowing it. Thank you for agreeing to be interviewed for this project. It served as a steady guiding hand throughout the process. I look forward to continuing our relationship in the future.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION: THE ISE, ITS IMPLEMENTATION, AND ALTERNATIVE INFORMATION SHARING STRATEGIES

Terrorist attacks such as those between 2014 and 2017 in Garland, Texas; San Bernardino, California; Orlando and Fort Lauderdale, Florida; Seaside Park, New Jersey; and Chelsea, New York highlight the increased challenge of preventing terrorist and homegrown violent extremists (HVEs) in the homeland. At its core, the challenge for information sharing involves how federal, state, local, territorial and tribal (FSLTT) counterterrorism operations collect, receive, analyze, and act upon information /intelligence prior to an attack. Over the last decade and a half, the U.S. government has attempted to address intelligence sharing in support of counterterrorism operations in several ways. The *9/11 Commission Report* details a framework for future intelligence reform in § 13.2, entitled "Unity of Effort in the Intelligence community." While this "Unity of Effort" led to the creation of the National Counterterrorism Center (NCTC), it was not until Congress passed the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA) that information sharing for counterterrorism became law.[1]

The 2004 IRTPA created the information-sharing environment (ISE), which was intended to reform and improve how intelligence/information sharing for CT would be accomplished. [2] The ISE is best defined as "an overarching approach to strengthening the sharing of intelligence, terrorism, homeland security, law enforcement, and other information among federal, state, local, tribal, international, and private sector partners."[3] Given the rising domestic terrorism threat almost 13 years after the ISE was signed into law, this thesis analyzes the remaining ISE challenges and explores two alternative

[1] Jerome P. Bjelopera, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress* (CRS Report No. 7-5700) (Washington, DC: Congressional Research Service, 2011), https://fas.org/sgp/crs/intel/R40901.pdf, 1.

[2] According to the IRTPA, "The terms "information sharing environment'' and ''ISE'' mean an approach that facilitates the sharing of terrorism information…" Intelligence Reform and Terrorism Prevention Act, Pub. Law No. 108-458 (2004), 28–29.

[3] U.S. Government Accountability Office [GAO], *High-Risk Series an Update, Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland* (GAO 15-290) (Washington, DC: U.S. Government Accountability Office, 2015), http://www.gao.gov/assets/670/668415.pdf, 227–240.

approaches to information sharing that may pave a different path toward building trust across the counterterrorism communities. It proposes that alternative approaches to counterterrorism are worth incorporating into future ISE reform.

A. DEFINING THE PROBLEM

As previously outlined, Congress created the ISE with the passage of the 2004 IRTPA. Linked to the creation of the Office of the Director of National Intelligence (ODNI) and championed by its program manager (PM) for the Information Sharing Environment, the ISE has contributed to national intelligence reform by attempting to improve information-sharing policies and guidance across FSLTT domains.[4] Given the rise in domestic terrorist attacks and the progress of intelligence reform over the last 16 years, an analysis of the ISE's effectiveness and an examination of alternative means of information sharing is necessary to address the remaining challenges brought to light in attacks carried out between 2014 and 2017. Over the last 16 years, the counterterrorism community has provided excellent examples of information-sharing strategies. Our nation's special operations forces (SOF) and largest police force, the New York Police Department (NYPD), are possibly two of the best examples of integrated intelligence support for counterterrorism operations. It is time to consider how the best practices of these organizations might be leveraged by the ISE program office to further future national intelligence reform and information sharing.

B. RESEARCH QUESTIONS

The principal questions this thesis examines concern information sharing policy, accountability for implementation, and outcomes. The 2004 IRTPA defines the ISE as "an approach that facilitates the sharing of terrorism information, which approach may

[4] As of mid-2017, the PM-ISE office has been designated as the new Partner Engagement Information Sharing Environment office or PE ISE. This office still retains the same responsibilities as and operations under the same authorities as the original PM ISE office under the Office of the Director of National Intelligence. Therefore, the same topics outlined within this thesis concerning the PM-ISE apply to the new PE ISE office. Throughout the thesis, I will refer to the PM ISE, this should be considered as synonymous with the new PE ISE designation. For more information on the new PE ISE office please reference the following online source: Office of the Director of National Intelligence, "Partnerships—ISE," accessed October 15, 2017, https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-partnerships.

include any methods determined necessary and appropriate."[5] While the passing of the IRTPA led to the creation of state and major urban area fusion centers and involved other ISE-centric programs, such as the program manager for ISE and the National Counterterrorism Center, this thesis asks the follow questions:

- Has the ISE actually improved the capacity for agencies at all levels of government to conduct counterterrorism operations?
- Moreover, given the continued challenges, how can the ISE leverage successful alternative information-sharing approaches, like those employed by the NYPD and SOF, to improve capacity and efficiency?

C. LITERATURE REVIEW

The literature review focuses on primary and secondary sources that offer a review of the ISE since the 2004 IRTPA and two case studies (SOF and NYPD) that offer viable alternatives for ISE operations. What follows is a description of the literature across these two topically relevant areas for the ISE as well as an overview of the source material used in the two cases studies.

1. National Level Challenges

The national intelligence-sharing policy has changed significantly, not only since 9/11 but also since the passage of the 2004 IRTPA. This research included a review of primary and secondary sources from government entities or analysis of associated government programs in an effort to analyze the current state of the ISE. For example, government documents like the *National Intelligence Strategy* (NIS), first developed in 2005, were some of the first sources to articulate a new "national intelligence" policy and what was codified by the intent of the IRTPA.[6] In addition, a review of the 2014 NIS reveals the historically unstable strategic environment in which it was written and the "perfect storm" of other events that have reduced and degraded the capabilities of the

[5] Intelligence Reform and Terrorism Prevention Act.

[6] Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America Transformation through Integration and Innovation* (Washington, DC: Office of the Director of National Intelligence, 2005), https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/NISOctober2005.pdf, 3.

intelligence community.[7] However, there are few additional details on either of these two major effects within the body of the 2014 NIS itself. The 2014 NIS does do an excellent job of outlining the intelligence community's core objectives without revealing sources and methods of achieving them, which is critical to the protection of intelligence community capabilities. The 2014 NIS is a valuable source for outlining new initiatives like "anticipatory intelligence" and in mentioning intelligence community functional areas that need additional improvement and focus.[8]

The 2014 NIS and previous editions do not provide the specific details that facilitate implementation. Additionally, it lacks prioritization of the mission and enterprise objectives sections. However, it does reference another document, the *National Intelligence Priorities Framework*, which sets prioritization for the intelligence community. The 2014 NIS provides a specific emphasis on the need for "unity of effort" across the intelligence community and states that products should be "classified at the lowest possible level."[9] However, the NIS does not elaborate whether that phrasing means a reduction in the amount of dissemination controls on intelligence products or how "unity of effort" translates to increased interagency all-source analysis and production.

These types of non-specific operational guidance products could offer detailed implementation strategies for improving intelligence sharing but currently do not, leading to the strategic challenges that endure within the ISE. Other primary sources that reveal strategic issues related to the ISE include the GAO report *Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland*. This report reviews GAO efforts at monitoring federal implementation of the

[7] Zach Bowling, "DNI: Fiscal Challenges and Snowden Leaks Created 'Perfect Storm,'" *Homeland Security Today*, September 30, 2014, http://www.hstoday.us/single-article/dni-fiscal-challenges-and-snowden-leaks-created-perfect-storm/de6feaa607915b03c637cbcafb32cb1e.html.

[8] Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America* (Washington, DC: Office of the Director of National Intelligence, 2014), http://www.dni.gov/files/documents/2014_NIS_Publication.pdf, 5–6.

[9] Ibid., 16.

ISE.[10] The GAO is a critical source when addressing the progress of the federal government's intelligence sharing efforts since the 2004 Intelligence Reform and Terrorism Prevention Act.[11] This GAO report also reviews the implementation plans that provide "detailed guidance" for priority objectives and milestones.[12] Posner, in his 2005 work *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11*, offers a valuable and independent analysis of the early implications and issues surrounding the 2004 IRTPA and intelligence reform in general.[13] The DOD Joint Staff's *Joint Intelligence* (JP 2-0) reviews "the current guidance for conducting joint and multinational intelligence activities across the range of military operations."[14] While this source is specific to the DOD, there are plenty of applicable components within the JP 2-0 for domestic intelligence operations, such as the "principles of joint intelligence."[15]

The DHS's *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* in 2010 and the DOD *Quadrennial Defense Review* of 2014 set their respective organizations' enterprise missions, objectives, and strategies for the next four years.[16] However, these sources do not accurately characterize national ISE efforts to date. Also, they do not provide enough operational or implementation guidance and funding to achieve improvements within the information/intelligence sharing environment. Other sources for evaluating the strategic problems for the national ISE, such as the National Intelligence Program (NIP)'s fiscal year (FY) 2016 factsheet and the House Homeland Security Committee (HSC)'s *Terror Threat Snapshot*, are useful for providing supporting details on the homeland's domestic intelligence

---

[10] GAO, *Establishing Effective Mechanisms*, 227.

[11] Intelligence Reform and Terrorism Prevention Act.

[12] Ibid., 228.

[13] Richard A. Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11* (Lantham, MD: Rowman & Littlefield Publishing Inc., 2005).

[14] Joint Chiefs of Staff [JCS], *Joint Intelligence* (Joint Publication 2-0) (Washington, DC: Joint Chiefs of Joint Staff, 2013), http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf, 2.

[15] Ibid., 49.

[16] U.S. Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review Report* (Washington, DC: U.S. Department of Homeland Security, 2014), https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

capabilities.[17] However, these sources are limited in how they relate to one another and in discussion of how the ODNI and HSC collaborate as part of the ISE.

2. Local Challenges

This literature review includes a summary of the field limitations for local programs, which hinder improved intelligence sharing among counterterrorism law enforcement, intelligence, and security partners. One of the best sources in this regard is Erik Dahl's article "Local Approaches to Counterterrorism: The New York Police Department Model." Dahl observes that the current approach to counterterrorism is mostly at the federal and national-level approach, and he proposes an alternative solution. Considering that most responses to terrorism are local, he goes on to state that the current, federal approach is flawed: "Although it is often recognized that 'all terrorism is local,' most counterterrorism is federal or above."[18] In addition, Dahl explores how the homeland's largest police department, the NYPD, has also recognized this flawed approach to counterterrorism and how it has implemented a unique alternative approach to solving some of the issues surrounding intelligence sharing. For instance, it integrates interagency and intergovernmental representatives in a "joint style" operational intelligence environment as one of those steps. While there are issues that remain regarding the effectiveness of implementing such a strategy on a national scale or by other localities, such a program serves as a potential solution to tactical intelligence sharing problems. Other authors like Lowenthal, Gerber and Sims, and Zegart also cover aspects of ISE challenges but do so with a focus on national-level policy.[19] A comparison among the sources that focus on national-level and local-level information sharing

[17] Office of the Director of National Intelligence, "FY 2016 National Intelligence Program Fact Sheet," accessed October 15, 2017, https://www.dni.gov/files/documents/Newsroom/Press%20Releases/FY2017NIPRequestedfactsheet.pdf; House Committee on Homeland Security, "The Islamist Terror Threat," *Terror Threat Snapshot* (November 2015), https://homeland.house.gov/wp-content/uploads/2015/11/November-Terror-Threat-Snapshot.pdf.

[18] Erik J. Dahl, "Local Approaches to Counterterrorism: The New York Police Department Model," *Journal of Policing, Intelligence and Counter Terrorism* 9, no. 2 (2014): 81.

[19] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington DC: CQ Press, 2011), Kindle ed; Burton Gerber and Jennifer E. Sims, *Transforming U.S. Intelligence* (Washington DC: Georgetown University Press, 2005), Kindle ed; Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton: Princeton University Press, 2009), Kindle ed.

challenges is missing from the sources reviewed for this thesis. Additionally, the overwhelming majority of sources reviewed focused solely on national-level ISE policy and operations rather than the local aspects of intelligence sharing.

Other dimensions of the local problem for intelligence sharing are how and what intelligence is gathered and its importance to different jurisdictions. Heuer's *Psychology of Intelligence Analysis* offers a unique perspective from seasoned intelligence analysts who present explanations on topics such as biases, lack of analytical science knowledge and application, as well as the quality and evolution of analysis within Central Intelligence Agency over time.[20] This source offers a great deal of insight into the challenges still impacting local agencies, such as NYPD's Intelligence Division and DHS field intelligence officers. The bias that remote headquarters' intelligence cells have the best analysis regarding threats experienced in local neighborhoods is not addressed in most of the literature. However, sources like *Psychology of Intelligence Analysis* and *Spying Blind* reveal aspects of biases that may help explain why the headquarters model for local threat analysis still permeates the U.S. national intelligence capacity.[21] Additionally, Busch and Givens explore the quality of intelligence shared as part of recent national intelligence reform and explore the impact intelligence has had across the FSLTT domains.[22]

One common theme in the literature is how the very structure of the U.S. intelligence community may not facilitate intelligence sharing and cooperation at the local level. In addition to Dahl's article on NYPD's intelligence capability, other sources explain the intelligence community's structure and the types of intelligence it produces in an effort to see whether these concepts and techniques can be applied or to determine whether they are indeed being applied at the local level. For example, Dahl's *Intelligence*

---

[20] Richards J. Heuer, *Psychology of Intelligence Analysis* (Langley, VA: Center for the Study of Intelligence, 1999), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/.

[21] Zegart, *Spying Blind.*

[22] Nathan E. Busch and Austen D. Givens, "Information Sharing and Public-Private Partnerships: The Impact on Homeland Security," *The Homeland Security Review* 7, no. 2 (2013): 123–150.

and Surprise Attack theorizes that surprise attacks happen as a result of the failure to merge strategic and tactical intelligence. Policy makers tend to be briefed on strategic intelligence, while tactical intelligence may sound the actual local warning.[23] Another example, Lowenthal's *Intelligence from Secrets to Policy*, presents the composition and construction of the intelligence community along with the different types of intelligence capacities, from human intelligence (HUMINT) to signals intelligence (SIGINT).[24] In his book, Lowenthal also touches on post-9/11 intelligence reform, such as the elevation of the much overlooked open-source intelligence (OSINT) category as a full "INT" requiring the intelligence community to codify and standardize OSINT implementation across its various agencies.[25] The incorporation of a comprehensive, local, all-source intelligence capacity is a critical component to improving the ISE. However, Lowenthal falls short of agreeing with one of this thesis's critical arguments for intelligence reform, which is the need for the intelligence community to invest more heavily in local intelligence support programs. Investment in these local programs might help break up the "stovepipes" that he, Dahl, the 9/11 Commission, and other authors speak of as a central and enduring obstacle for integrated government-wide intelligence operations.

Last, the use of examples of local intelligence successes and failures, with an emphasis on how intelligence sharing and collaboration either helped or hindered the local agency operation, serves to elaborate issues referenced in earlier sources but with real-world impact. Cases described in sources like McGhee's master's thesis, "The Wicked Problem of Information Sharing" and cases such as the San Bernardino and Paris attacks provide examples of what works and does not work on varying scales of CT operations. [26] Additionally, interviews with local law enforcement executives, such as NYPD Deputy Commissioner of Intelligence John Miller on the quality of the ISE within

---

[23] Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington DC: Georgetown University Press, 2013), Kindle ed., 1–2.

[24] Lowenthal, *Secrets to Policy*, 431–433.

[25] Ibid.

[26] G. C. Sam McGhee, "The Wicked Problem of Information Sharing in Homeland Security: A Leadership Perspective" (master's thesis, Naval Postgraduate School, 2014), https://www.hsdl.org/?view&did=756782.

New York City are critical to this thesis. One scholarly interview with commentary from retired General Michael V. Hayden is included in this thesis and when combined with Posner's independent analysis of the 2004 IRTPA, the reader gains a more accurate sense of the challenges the ODNI and ISE face. [27] Future interviews with senior leaders from the ISE should be incorporated into the literature concerning this topic. In contrast, there seems to be a great number of primary and secondary government sources of information related to the strategic challenges of intelligence sharing. The greatest challenge in research for this thesis was narrowing the focus to relevant sources for local urban threat and field intelligence environs.

3. The SOF and NYPD Case Studies

A number of senior counterterrorism leaders from around the world have spoken about the "unprecedented" nature of the current terrorist threat environment. This demands a level of commitment to improving intelligence sharing that rivals the climate shortly after 9/11. Chapter III of the thesis focuses on practical solutions offered by field intelligence activities at the local level. Dahl's article, "Local Approaches to Counterterrorism," serves as one of the baseline sources for this section. [28] This thesis utilizes information revealing NYPD's Intelligence Unit and its comprehensive liaison intelligence officer program sourced from the interview for this thesis with John Miller and detailed by Dahl in "Local Approaches to Counterterrorism."

However, a variety of sources from the DOD special operations community, such as the *Special Warfare Journal*, contain valuable corollary and case study information offering possible alternative information sharing techniques for ISE consideration. While not a magic bullet, some of these techniques, integrated as part of a more comprehensive domestic intelligence program, may offer a practical fix to some ISE challenges. Authors Dahl, Lowenthal, Posner, and Zegart also touch on some of the proposed solutions, such as the creation of the ODNI, which DHS implemented, and others that have not been

[27] Posner, *Preventing Surprise*, 5–15.

[28] Dahl, "Local Approaches," 81–97.

implemented, such as the creation of a domestic intelligence agency. These sources focus on strategic-level information sharing solutions. This thesis seeks to merge both strategic and tactical techniques for a more comprehensive solution suite.

D. FRAMEWORK FOR EXPLORING THE ISE

This thesis argues that two major challenge areas remain for the ISE: national-level policy and focus as well as local-level access and implementation. Research for this thesis reveals that in these challenge areas, the ISE can be characterized by unclear and competing implementation strategies, a lack of alternative approaches to information sharing, and a lack of clear interagency policy. These areas should be addressed in a holistic way to improve counterterrorism functionality and access across multiple, disparate domains. Moreover, research for this thesis reveals that the ISE could be structured in a way to facilitate the continued integration of these challenges with the latest, most successful approaches to counterterrorism regardless of jurisdiction. What follows is the framework for the forthcoming discussion and the analysis in the chapters that follow.

1. National Level Challenges

The ISE's national-level challenges can be characterized by an overemphasis on intelligence community information-sharing reform within the national capital region, which narrowly focuses on federal agencies. Poor or non-existent implementation strategies to increase information sharing following the 2004 IRTPA mandate, has limited local agency access to high-quality classified information and facilities. There are several information-sharing mechanisms; however, many agencies have not fully complied with ISE reform initiatives, as detailed in the Government Accountability Office (GAO)'s high-risk report regarding government-wide information-sharing mechanisms.[29] Additionally, the program manager for ISE has limited capacities to address noncompliance with its issued strategies.

[29] GAO, *Establishing Effective Mechanisms*, 227–240.

2. Local Challenges

Local-level challenges to improving information-sharing for the ISE are mostly characterized by a failure to ensure integrated information-sharing processes and access across all entities operating at the local level. For instance, the overemphasis on existing structures, such as the Joint Terrorism Task Force and lower-quality unclassified intelligence, has led to the *appearance* of improvement in information-sharing at local levels. While there are excellent examples of integrated structures that facilitate precise and time-sensitive ISE operations, such as those of the NCTC, these are exclusively national capabilities. This is in part because the NCTC and other similar intelligence community structures—along with their vast sensitive compartmented information facilities, advanced analytic capacities, and interagency representation—are national-level organizations supporting national counterterrorism operations, but not necessarily local operations or investigations. At the local level, challenges still remain for organizations to access the same types of intelligence data that NCTC has at all classification levels. Furthermore, the program manager for ISE has no direct control over these local field intelligence assets and, therefore, cannot accurately track or ensure that field/local agencies have access to all intelligence community capabilities or are fully compliant under ISE legislation and policies.

3. SOF and NYPD Alternatives

In order to address my second thesis question regarding information sharing alternatives, the following question had to be researched: are there alternatives to how the ISE is structured and implemented that would improve local access to high-quality information? To find an answer, this thesis focuses on qualitative research, reflecting on two case studies that the author is intimately familiar with as a career intelligence officer. The first case study is of the SOF environment. SOF operators have employed operations and planning cells within counterterrorism environments for almost 20 years. The SOF approach organizes mission planning and operations cells with representatives from different support disciplines who bring their expertise and domain capacities, often in unique and innovative ways, to the SOF environment.

The second case study overviews the NYPD approach to intelligence. As our nation's largest police force, the NYPD has many unique programs that mirror SOF capabilities. Foremost is the how NYPD integrates national and international agencies into its intelligence and counterterrorism structures on a continuous basis. Furthermore, the NYPD, like SOF, manages these programs not as part of the ISE or its initiatives but through independent operational needs and experiences. The SOF technique in combination with the NYPD's local model could be part of a more integrated solution to help address the continued ISE challenges.

E. METHODOLOGY

This thesis explores the best practices of the SOF and NYPD and applies them to the historiographical analysis of ISE challenges explored in the thesis. The author uses primary and secondary source materials from official government resources as evidence outlining the current ISE challenges. Examples of these sources range from reports and other similar publications from the GAO, other government agencies, and scholars. This approach has the benefit of revealing what government agencies and other scholarly sources are saying about the ISE itself. However, there is little hard data detailing the relative successes or failures of the ISE outside firsthand accounts from these types of sources. The analysis presented in this thesis relies on the work of other experts and senior leaders in the field to characterize ISE as it is currently operating. Further empirical evidence includes an interview conducted with NYPD Deputy Commissioner for Intelligence John Miller and other testimony from senior leaders, such as former Boston Police Commissioner Ed Davis, who have been directly affected by the current state of the ISE.

1. Data Sources

This thesis reviews and compares government policy and reports as the primary sources. Secondary sources also include qualitative analysis and anecdotal commentary from academics and government agencies, such as congressional testimony, analyzing ISE-relevant policies and their effectiveness since the 2004 IRTPA. Last, there is growing literature recently published in media sources, such as Erik Dahl's article

describing NYPD's intelligence programs, detailing successful initiatives. These sources are also used in the solutions section and when combined with publications from the DOD's Joint Special Operations University, describe how the integration of specialized capabilities from the intelligence community can contribute to government-wide counterterrorism operations.

2. Limitations

Due to the amount of existing qualitative research, policy analysis, and congressional testimony on information sharing, this thesis does not provide another policy analysis on fusion centers or similar state-owned ISE capacities. The case study overview does not attempt to review fusion centers (urban, regional, or otherwise) since there has been a plethora of material written about this popular solution to the 2004 IRTPA. However, this thesis does address how fusion center ISE-related operations are either absent or have been inadequately implemented, leaving locals and stakeholders without ISE support. Additionally, with the exception of the interview conducted with NYPD's John Miller, this research plan avoided conducting interviews or other activities such as surveys, due to the depth and breadth of available published policy information including actual policies, policy critiques, and prior theses. Furthermore, due to interagency sensitivities and access limitations, this thesis avoids Federal Bureau of Investigation information-sharing policies, but it does discuss the organization's role in potential integrated solutions to the challenges within ISE. Additionally, this thesis focuses on the information-sharing challenges between the national and local levels. While there are similar issues with information sharing between these two groups and state-level organizations, the focus of this thesis remains with the under-explored national and local information sharing challenges. Finally, this research design does not explore the specific terrorism cases themselves but rather focuses on the intelligence sharing techniques and relevant programs alone.

3. Case Study Best Practices Overview

This research includes an overview and comparison of two case studies in an effort to examine them for potential solutions to the research questions. Specifically, the

NYPD and SOF methods of intelligence, information sharing, and counterterrorism operations planning are reviewed and compared with the aim to extract the best practices of each. In addition, analysis focused on the commonalities and differences between the NYPD and SOF models for CT information sharing.[30] The researcher then compared these commonalities to the analysis found in sources such as the GAO's High Threat Series, Dahl's articles on both the NYPD and the hunt for Bin Laden.[31] Finally, this thesis proposes a blending of the best practices of each that leverages existing national intelligence community capabilities to improve all-source intelligence and the ISE as a whole for local counterterrorism operators.

F. THESIS ORGANIZATION

Chapter II focuses on exploring the aforementioned ISE challenges. Chapter III reviews two cases, SOF and NYPD, which offer best practices that may offer solutions to the remaining ISE challenges. The concluding chapter ends with an exploration of the legal and political challenges that remain in implementing the solutions. It also explores what implementation of the solutions may look like from a local counterterrorism perspective.

[30] Stanley McChrystal et al., *Team of Teams: New Rules of Engagement for a Complex World* (New York: Penguin, 2015), Kindle ed.; Joint Chiefs of Staff, *National Intelligence Support to Joint Operations* (Joint Publication 2-02) (Washington, DC: Joint Chiefs of Staff, 1998), https://fas.org/irp/doddir/dod/jp2_02.pdf; Linda B. Williams, *Intelligence Support to Special Operations in the Global War on Terrorism* (Carlisle Barracks, PA: U.S. Army War College, 2004), handle.dtic.mil/100.2/ADA424015.

[31] Dahl, "Local Approaches."

II. THE INFORMATION SHARING ENVIRONMENT AND CHALLENGES FOR COUNTERTERRORISM

> Contrasted with the strong partnership by local, state and federal law enforcement at the crime scenes and command posts, there is a gap with information sharing at a higher level while there are still opportunities to intervene in the planning of these terrorist events. I speak specifically about the Joint Terrorism Task Forces (JTTF). The Boston Police Department has four members assigned to the JTTF in Boston. All have the appropriate security clearances and many of the Task Force Members have served in that capacity for a number of years. Information sharing with local law enforcement task force members needs to be improved.
>
> ——Edward F. Davis, Police Commissioner Boston Police Department before the Homeland Security and Government Affairs Committee United States Senate Wednesday, July 10, 2013[32]

A major part of the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA) focuses on information-sharing challenges and it has attempted to address them by creating the information-sharing environment (ISE). However, as described by organizations such as the Major Cities Chiefs Association (MCCA), since 9/11 the national ISE policy has been incompletely implemented at the local counterterrorism level.[33] Inconsistent implementation by ISE partners has led to gaps in strategic counterterrorism capabilities. Inconsistent local law enforcement access to innovative national intelligence collection and analysis capabilities has ultimately played a role in successful terrorist attacks from 2014 through early 2017. Testimony from local leaders and documentation from national police organizations have linked the problem to a lack of local intelligence collection and sharing prior to the attacks.

---

[32] *Lessons Learned from the Boston Marathon Bombings: Preparing for and Responding to the Attack Hearing of Homeland Security and Government Affairs Committee United States Senate* (2013) (testimony of Edward F. Davis Police Commissioner Boston Police), https://www.hsgac.senate.gov/hearings/lessons-learned-from-the-boston-marathon-bombings-preparing-for-and-responding-to-the-attack.

[33] Major Cities Chiefs Association, *Criminal Intelligence Enterprise Initiative* (Major Cities Chiefs Association, 2012), https://majorcitieschiefs.com/pdf/news/mcca_criminal_intelligence_enterprise_initiative_20120329.pdf.

This chapter focuses on the specific ISE challenges that local field-based counterterrorism agencies face and critiques the ISE overall. Research reveals two main areas of ISE challenges: strategic, which are a result of national policies and how they have been implemented; and tactical, which local agencies face as a result of existing ISE implementation strategies. This thesis reviews the overarching ISE policies, its implementation strategy to date, as well as various assessments and actual testimony from senior leaders/subject matter experts on the impact these policies have had on local agencies.

A. NATIONAL LEVEL CHALLENGES

According to Dahl in "Local Approaches to Counterterrorism," the United States has been overly focused on national-level counterterrorism approaches that include favoring military and other governmental assets to detect and deter international terrorism plots.[34] Recent homeland attacks in Boston, San Bernardino, as well as Chelsea/Seaside suggest there is a growing trend in domestic terrorism that federal approaches have struggled to detect beforehand.[35] One can infer that the creation of the ISE by the 2004 IRTPA was designed to address all the intelligence-sharing concerns described in the *9/11 Commission Report*. The 9/11 Commission's recommendations focused on restructuring the intelligence community to reduce barriers to performing joint intelligence work, consolidating the divided management of national intelligence capabilities, developing common standards and practices across foreign and domestic intelligence community capacities, and reducing complexity to improve resource priorities.[36] The 9/11 Commission's recommendations led to several distinct actions: the creation of the Office of the Director of National Intelligence (ODNI) and the National

[34] Dahl, "Local Approaches," 82.

[35] Cities listed are located in the following states respectively: Massachusetts, California, New York, and New Jersey.

[36] National Commission on Terrorist Attacks upon the United States [9/11 Commission], *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* New York: W.W. Norton & Company, Inc. 2004).

Counterterrorism Center (NCTC) as well as an outline for the ISE concept.[37] Since the 2004 IRTPA, the ODNI has created the program manager for ISE, whose role is to establish policy standards and implementation guidance.[38] Three topics outline the strategic or national-level challenges remaining for ISE: gaps in ODNI authorities, the focus on national reform, and a lack of uniform classification standards for terrorism information.[39]

1. Gaps in the ODNI Mandate

The 2004 IRTPA represents the greatest restructuring of the intelligence community and strategic intelligence since the National Security Authorization Act of 1947 established them.[40] The 2004 IRTPA left intentional gaps in the ODNI authorities, which have led to inconsistent implementation as well as a lack of agency accountability. The ODNI lacks a mandate that all intelligence community agencies provide sister agencies access to counterterrorism intelligence. The result is a mixed bag of access across the homeland security environment whereby local law enforcement agencies, regardless of existing security clearance level, have no regular access to available classified intelligence holdings and analysis. For counterterrorism purposes, no single organization has complete knowledge of the full range of intelligence for a specific threat.[41]

Although the president has the final authority in ODNI actions toward cabinet-level intelligence agency heads, Section 1018 of the IRTPA has resulted in intelligence community partners ignoring the ODNI and its program manager's ISE guidance.

---

[37] Posner, *Preventing Surprise Attacks*, 59–61.

[38] Office of the Director of National Intelligence, Program Manager Information Sharing Environment [PM-ISE], *A Brief History of the Information Sharing Environment* (Washington, DC: Information Sharing Environment 2015), https://www.ise.gov/sites/default/files/Brief_History_of_the_ISE.pdf.

[39] U.S. Government Accountability Office [GAO], *Information Sharing Environment Better Road Map Needed to Guide Implementation and Investments* (GAO-11-455) (Washington, DC: U.S. Government Accountability Office, 2011), http://www.gao.gov/assets/330/321672.pdf.

[40] Michael V. Hayden, "The State of the Craft: Is Intelligence Reform Working?" *World Affairs*, September/October 2010, http://www.worldaffairsjournal.org/article/state-craft-intelligence-reform-working.

[41] Posner, *Preventing Surprise Attacks*, 60–61.

Michael V. Hayden, former director of the National Security Agency (NSA), summarizes the limitations of the ODNI more precisely:

> The DNI could not abrogate the authorities of the cabinet officers of departments in which elements of the intelligence community were located. Section 1018 of the IRTPA, as it was called, was a determined push to protect the secretary of defense's prerogatives when it came to his critical combat support agencies: the NSA, NGA [National Geospatial Intelligence Agency], and NRO [National Reconnaissance Office].[42]

Nevertheless, executive orders have attempted to address original weaknesses in the 2004 IRTPA. One of the first early attempts at addressing the law came in 2007–2008 with an amendment to Executive Order (EO) 12333.[43] Furthermore, in an attempt by the president to ensure intelligence sharing, according to EO 12333, the intelligence community

> shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating: (A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies.[44]

This section of EO 12333 is critical for establishing and maintaining ISE activities. However, the EO does not outline any penalties or systems of redress for agencies that ignore ODNI guidance in this area. Because the *DNI* cannot abrogate the authority of agency heads, independent agencies may simply ignore the program manager's intelligence dissemination programs and prioritize their own agency activities in countering terrorism threats.

---

42 Hayden, "The State of the Craft."

43 Ibid.

44 Exec. Order No. 12333, United States Intelligence Activities (as amended by Exec. Orders Nos. 13284 (2003), 13355 (2004) and 13470 (2008)), Code of Federal Regulations 73 FR 45325 (2008): 45323–45342, https://www.federalregister.gov/documents/2008/08/04/E8-17940/further-amendments-to-executive-order-12333-united-states-intelligence-activities. Exec. Order No. 12333 was amended on three subsequent occasions in the years 2003, 2004, and 2008.

2. Field Intelligence Limitations

Two of the five ISE stakeholder agencies identified by the program manager increased field or local-level ISE support, primarily by increasing field investigators, agents, analysts, and other personnel in specific locations.[45] However, while the NCTC and DNI have created domestic representative programs, the programs have resulted in relatively few officers actually stationed to high-threat areas. For instance as of early 2017, the NCTC's Domestic Liaison Program has only one regional representative covering territory from Maine to Delaware.[46] Additionally, while the joint terrorism task forces (JTTFs) are supplemented with additional analytic capacity during national and special local events as well as other elevated threat environments, the National Capital Region (NCR) predominantly receives the counterterrorism capabilities of the intelligence community.[47] Part of this challenge is the lack of trained field intelligence analysts who have access to and knowledge of the intelligence community capabilities available to the NCR-based NCTC, but in support of local counterterrorism operations. This absence of coordinated and integrated intelligence frameworks has led to field intelligence representatives developing their own processes that may be inconsistent with broader national and local initiatives. Ideally, the ODNI, along with the PM ISE, would have the regulatory and budgetary authority to revise the nation's field intelligence capacities, but the ODNI currently lacks legislative authority over these programs. The

---

[45] According to the GAO report 11-455, "The stakeholder agencies we reviewed are the five key agencies the Program Manager [ISE] identified, consistent with the Intelligence Reform Act, as critical to developing and implementing the ISE—the Departments of Homeland Security (DHS), Justice (DOJ), State (State), and Defense (DOD), as well as the Office of the Director of National Intelligence (ODNI). These agencies represent five information sharing communities that collect the homeland security, law enforcement, foreign affairs, defense, and intelligence information deemed critical for sharing in order to provide for homeland security." GAO, *Information Sharing Environment*, 7.

[46] *Hearing before the House Committee on Homeland Security, Understanding the Homeland Threat Landscape*, 112th Cong. (2012) (statement of Matthew G. Olsen), https://www.nctc.gov/docs/2012_07_25_HHS_Understanding_Homeland_Threat_Landscape.pdf. As of March 2017, NCTC's Domestic Representative program was now up to 11 representatives across major cities and regions in the United States. For more information, please see https://oig.justice.gov/reports/2017/a1721.pdf, 38.

[47] Edward Connors, *Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement* (Washington, DC: U.S. Department of Justice, Institute for Law and Justice, 2007), https://www.hsdl.org/?view&did=482649).

aforementioned limitations at the field level result in a dynamic wherein intelligence reform is concentrated in the NCR.

a. Classification Standards

Research conducted for this thesis, as well as interview information from John Miller, suggests that the intelligence community is still over-classifying terrorism-related information. While there are several information-sharing mechanisms through the PM ISE and through EOs 13356 and 13388, the intelligence community partners still have the ability to restrict other intelligence community and ISE partners from classified material, even for the purpose of counterterrorism.[48] As Posner elaborates in *Preventing Surprise Attacks*, the culture of the intelligence community still restricts increased sharing:

> Fear of penetration and leaks makes intelligence officers (and their services) reluctant to share information with each other fully and freely, which in turn makes it difficult to assemble scattered bits of information into a convincing mosaic. . . . This reluctance is not only ad hoc; it is codified in the different rules of different intelligence units [agencies] regarding access to classified information. The 2004 IRTPA did not empower the ODNI to prescribe uniform standards for classification.[49]

Uniform standards of classification across the intelligence community would essentially mean that all partners have a common set of rules by which to classify intelligence.

The ODNI and the Information Sharing Council (ISC) have observed that the overuse of originator control (ORCON) has negatively affected current ISE counterterrorism operations.[50] When an originator of classified intelligence uses

---

[48] PM ISE, *A Brief History*.

[49] Posner, *Preventing Surprise Attacks*, 102–103.

[50] The ODNI within its Intelligence Community Policy Guidance (ICPG) 710.1 memorandum defines ORCON as "a dissemination control marking" that restricts "the dissemination and extraction of information controlled by its originator." The ICPG further clarifies "Controls on the dissemination and use of classified national intelligence are necessary to protect intelligence sources, methods, and activities. The use of ORCON enables the originator to maintain knowledge, supervision, and control of the distribution of ORCON information beyond its original dissemination. Further dissemination of ORCON information requires advance permission from the originator. The ORCON marking shall be applied judiciously in accordance with this ICPG to ensure that classified national intelligence is disseminated appropriately without undue delay or restriction." Office of the Director of National Intelligence, *Application of Dissemination Controls: Originator Control* (Intelligence Community Policy Guidance 710.1) (Washington, DC: Office of the Director of National Intelligence, 2012), 2.

ORCON, it prevents other agencies from distributing the information beyond the original dissemination without approval from the originator.[51] A lack of uniform classification standards has enabled intelligence community agencies to continue using ORCON on terrorism intelligence. Currently, further dissemination of ORCON information requires advanced permission from the originator for every occurrence. Even when an agency receives permission to access ORCON material, it cannot pass that material along to its partner agencies without additional permissions from the originator.

This requirement for authorization prior to dissemination slows down the real-time sharing of intelligence and undermines field intelligence personnel by forcing them to coordinate intelligence-sharing activities with NCR-based approvers first. Additionally, the intelligence community's use of ORCON isolates certain ISE partners from specific terrorism information simply based on the department to which an agency belongs. For example, a DOD partner may have ORCON intelligence on a specific individual, but because it is marked ORCON, the DOD partner is restricted from using and/or disseminating the information in support of any non-DOD counterterrorism activities. Previous guidance from DNI has stated, "The ORCON marking shall be applied judiciously in accordance with this [intelligence community policy guidance] ICPG to ensure that classified national intelligence is disseminated appropriately without undue delay or restriction."[52] Given the DNI guidance to judiciously apply this control, ORCON is still applied inappropriately to classified terrorism intelligence. As NYPD's John Miller asked in an interview for this thesis,

> Now . . . [ORCON] makes sense on a number of levels if you're dealing in espionage, nuclear proliferation, a host of national security issues, but when you're dealing with terrorism, where the threat is to U.S. soil and to U.S. cities and to targets that are protected day-by-day by police, . . . how does this still make sense in the post-911 era?[53]

---

51 ODNI, *Application of Dissemination Controls*, 22.

52 Ibid.

53 John Miller (NYPD Deputy Commissioner for Intelligence and Counterterrorism), interview with author, October 17, 2016.

Miller argues that classification should not be used to restrict local law enforcement or intelligence community partners from accessing terrorism data even when one of the partners may choose to close a case. Overuse of ORCON and similar dissemination restrictions on terrorism intelligence damages the ability of counterterrorism operators to coordinate local threats that may span multiple jurisdictions. For example, if the FBI or intelligence community partner has information on a terrorism suspect but chooses not to the share information other ISE agencies that may encounter the suspect will have an incomplete intelligence picture of the potential threat that suspect poses. Recent terrorist attacks like those in Garland, Texas, and San Bernardino, California, highlight how the restriction of terrorism information can hurt investigations.

b. Focus on National Reform

The PM ISE is the principal authority for all ISE activities and generates an annual report to Congress outlining progress on GAO-mandated improvements.[54] However, there is no reporting mechanism or forum that encourages local agency feedback for local activities within the ISE.[55] Additionally, no local law enforcement agency or field intelligence activity is represented on the ISE's Information Sharing Council or Information Sharing and Access Interagency Policy Committee.[56] The absence of these connections at the local level is likely due in large part to the strategic-level focus of the PM ISE and the gaps left by weak implementation language within the 2004 IRTPA itself.

The 2004 IRTPA directs that the ODNI and NCTC must not be co-located with existing intelligence community facilities.[57] However, the IRPTA does not recommend that these organizations necessarily bring national-level intelligence capacity outside

54 PM ISE, *A Brief History*.

55 Intelligence Reform and Terrorism Prevention Act.

56 "ISE Governance," Program Manager Information Sharing Environment, accessed October 15, 2016, https://www.ise.gov/ise-governance.

57 Busch and Givens, "Information Sharing."

Washington, DC, to the local level.[58] In fact, while the ODNI and NCTC face the daunting challenge of interagency intelligence collection as well as analysis operations and reform, there is no legal mandate that these two agencies distribute their robust capabilities to high-threat local communities. Additionally, while some ISE partners have dedicated field intelligence representatives, the PM ISE has no direct control over these assets. Therefore, the national PM office for information sharing can neither accurately track nor ensure various field intelligence activities have appropriate accesses while remaining fully compliant with established ISE legislation and policies.[59] By focusing on intelligence community reform solely within Washington, DC region, the ISE has hampered the IRTPA's intent of improving counterterrorism information-sharing across the FSLTT domains. These domains are primarily found in local field areas, not in Washington, DC.

As an example of sustaining the continuum for national reform, two organizations have released reports that serve as important updates to the previous analysis for this thesis from 2016. In February 2017, the Government Accountability Office updated its High Risk Series report, GAO-17-317, by removing terrorism-related information sharing from its High-Risk List. The GAO goes on to state that the information was removed from the high-risk series due to the program manager for ISE achieving all nine of its actions items. However, the GAO does admit the continued challenges for the ISE:

> While this demonstrates significant and important progress, sharing terrorism-related information remains a constantly evolving work in progress that requires continued effort and attention from the Program Manager, departments, and agencies. Although no longer a high-risk issue, sharing terrorism-related information remains an area with some risk, and continues to be vitally important to homeland security, requiring ongoing

58 "Chairman McCaul's Inaugural "State of Homeland Security Address," House Committee on Homeland Security, December 7, 2016, https://homeland.house.gov/event/state-of-homeland-security-address.

59 GAO, *Establishing Effective Mechanisms*, 238.

> oversight as well as continuous improvement to identify and respond to changing threats and technology.[60]

The DHS Office of Inspector General (OIG) in its most recent report concerning domestic sharing of counterterrorism information outlines the continuing challenge that supports some of the analysis within this thesis:

> Updating or establishing new information sharing agreements among such entities should enhance coordination and collaboration, and reaffirm and formalize the roles and responsibilities of partners in the current information sharing environment. Similarly, although there is a national information sharing strategy, its implementation has been viewed to be uneven. The OIGs believe that the ODNI, DHS, and DOJ should review the interagency information sharing memorandum of understanding (MOU) and take necessary actions to update intelligence information sharing standards and processes among the departments, which we believe would result in better implementation of the strategy.[61]

Additionally, the March 2017 DHS OIG report possibly represents the most comprehensive government-sourced report on counterterrorism information sharing and the ISE to date. The author of this thesis recommends further analysis of OIG-17-49 for updating related thesis topics concerning the ISE.

B. LOCAL LEVEL ISE CHALLENGES

At the local level, ISE challenges are characterized by uneven access of local law enforcement to quality intelligence and a lack of enough experienced, trained intelligence analysts in the field. Regional fusion centers and the NCTC are examples of integrated structures that facilitate precise, time-sensitive dissemination of classified intelligence. However, the principal critique of the ISE in this section is that the NCTC's brand of classified data fusion remains exclusive to the NCR, far removed from the day-to-day

---

[60] U.S. Government Accountability Office [GAO], *Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others* (GAO-17-317), High-Risk Series (Washington, DC: U.S. Government Accountability Office, 2017), http://www.gao.gov/assets/690/682765.pdf, 2–8.

61 Inspectors General of the Intelligence Community, Department of Homeland Security and Department of Justice, *Review of Domestic Sharing of Counterterrorism Information* (OIG-17-49), March 2017, https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-49-Mar17.pdf, 2–8.

investigations and operations headed by local law enforcement agencies, despite the dramatic rise in local homegrown violent extremist cases since 2014.[62]

The FBI's JTTF program bears the brunt of tackling these terrorism cases within the nation's most densely populated urban regions. However, as suggested by former Boston Police Chief Edward F. Davis, even with cleared police officers on these JTTFs, not all intelligence is shared with the local non-FBI partners that support JTTF activities. This dynamic continues despite JTTFs having access to all strategic and tactical level intelligence related to the current terrorism environment.[63]

1. JTTF Control

The FBI-led JTTF structure serves as the homeland's principal domestic counterterrorism organization.[64] How intelligence is accessed, collated, analyzed, and disseminated at the local level greatly impacts who attains access. However, local JTTFs are wholly under the control of an FBI supervisory special agent. Under the existing JTTF structure, the supervisory FBI special agent solely decides who accesses all investigation-related information, often restricting access to investigation team members. Since the 2013 Boston Marathon bombing, the FBI has been criticized for not sharing intelligence prior to attacks or attempts.[65] One common theme in the criticism is that the perpetrators were at some point under FBI investigation with varying degrees of intelligence shared with local law enforcement prior to the attack.[66] Classified

---

62 Michael McCaul "The Terrorist Exodus: Resurgent Radicalism and the Threat to the West" (lecture, George Washington University, May 2016), https://homeland.house.gov/wp-content/uploads/2016/05/The-Terrorist-Exodus.pdf.

63 *Lessons Learned from the Boston Marathon*.

64 Federal Bureau of Investigation, "Joint Terrorism Task Forces," accessed January 15, 2017, https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces.

65 Chris Strohm, "FBI Gives Its Version of How the Orlando Shooter Slipped Through," *Bloomberg*, June 13, 2016, http://www.bloomberg.com/politics/articles/2016-06-13/law-enforcement-released-orlando-shooter-after-finding-no-threat.

66 Mark Berman, Ellen Nakashima, and Matt Zapotosky, "The FBI Looked into Suspected Bomber Ahmad Rahami in 2014 and Found No 'Ties to Terrorism,'" *Washington Post*, September 19, 2016, https://www.washingtonpost.com/news/post-nation/wp/2016/09/19/bombing-suspect-charged-with-attempted-murder-of-a-law-enforcement-officer-with-further-charges-expected/?utm_term=.445b66e78642.

information, such as the attackers' prior watchlisting status or communication with online jihadists, was not often shared in its entirety with the FBI's local law enforcement counterparts. As Dahl, Posner, Burch, and other scholars have suggested, these problems may reside in how domestic intelligence has been organized since the 2004 IRTPA created the ISE. Specifically, for the FBI as the principal domestic counterterrorism intelligence partner and ISE stakeholder, these problems reflect how the FBI prioritizes investigative approaches over intelligence.[67]

One of the PM ISE's primary missions is "supporting ISE partners to increasingly align policy, missions, and technology with their information sharing infrastructure at the domestic nexus of national security and public safety."[68] Though the FBI is one of the principal members of the ISE, the program manager is not ensuring FBI compliance with increased information sharing outside the JTTF structure. Perhaps the lack of PM oversight of individual members offers an explanation as to why the GAO is still critical of how the PM ISE is accomplishing its mission. The GAO has principally focused on the program manager's progress in architecture, frameworks, and policies for the 15 agencies identified as part of the ISE. Nevertheless, due to the language in the 2004 IRTPA and subsequent executive orders, the PM ISE does not have the ability to ensure that national-level ISE agencies comply with information-sharing goals. Additionally, while the FBI is part of the ISE, it continues to restrict access to information regarding counterterrorism cases and investigative decision making by local JTTF partner agencies, as described by former Boston Police Chief Edward F. Davis. Nonetheless, neither the GAO nor PM ISE acknowledges that local access to classified data is a critical priority to the ISE. Nor do they address the continued problems within FBI intelligence.

---

[67] Adam D. M. Svendsen, "The Federal Bureau of Investigation and Change: Addressing US Domestic Counter-terrorism Intelligence," *Intelligence and National Security* 27, no. 3 (2012): 371–397, doi: 10.1080/02684527.2012.668080.

[68] Program Manager Information Sharing Environment, *2016 Information Sharing Environment Annual Report to Congress* (Washington, DC: Program Manager Information Sharing Environment, 2016), http://www.ise.gov/annual-report/year-review.

2. Unclassified Intelligence Quality

As Busch and Givens describe, there is community consensus on the unprecedented amount of unclassified terrorism information available today.[69] Specific ISE initiatives have led DHS to create the Homeland Security Information Network (HSIN) for the dissemination of unclassified intelligence. Numerous other organizations have also created unclassified intelligence portals based on these same ISE frameworks.[70] By allowing access across the FSLTT community to sensitive but unclassified intelligence, HSIN partially meets the requirements set forth in a 2005 presidential memorandum concerning the information-sharing environment.[71] However, a requirement for access to classified intelligence by FSLTT partners does not exist in the 2004 IRTPA, the 2005 presidential memorandum, or other ISE publications. As Busch and Givens suggest in their article, current unclassified products lack operationally useful information as they omit "certain details to protect information sources and intelligence-gathering methods. But these omissions limit the utility of the information. Without a source, a recipient cannot make independent judgments about how credible or non-credible a piece of information is."[72]

Integrating classified intelligence into an all-source structured analysis program is instrumental in closing the current gaps in information sharing. Classified information does this in a variety of ways. First, classified intelligence can be used to provide leaders specific details on emergent terrorism capabilities and trends. Second, the most precise watchlisting data on individuals is classified. Third, integrating classified with unclassified intelligence creates a true all-source intelligence collection and analysis capability. This type of capability can lead to the production of high-quality integrated intelligence products that help drive more precise counterterrorism operations. Within

---

69 Busch and Givens, "Information Sharing," 8–9.

70 Ibid.

71 Office of the White House Press Secretary, *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment* (Washington, DC: White House, 2005), https://www.archives.gov/cui/training/awareness/includes/references/prsmem_121605.pdf.

72 Busch and Givens, "Information Sharing," 16.

counterterrorism, there is no doubt of the importance of integrated all-source intelligence that John Miller describes in his interview. Miller characterized NYPD's intelligence gathering and analysis approach, which leverages similar methods, sources, and techniques as the intelligence community. However, due to the need for driving rapid law enforcement operations and the limited number of cleared personnel, most police departments cannot integrate classified intelligence into similarly structured programs, effectively. [73] Yet providing classified intelligence to cleared intelligence analysis personnel and senior leaders for departments could drive strategic operations, if not joint interagency tactical operations.

Additionally, as early as 2003, the GAO published studies concerning the need for the information-sharing environment to include and increase the amount of classified intelligence available to state and local authorities.[74] With the passage of the Homeland Security Information Sharing Act in 2002, Congress also introduced the requirement to "share homeland security and classified information with . . . state and local governments." [75] Regardless, as of 2017, integrating classified and unclassified law enforcement information into fused intelligence products at the local level remains a challenge principally due to access-related issues for local agencies and federal field personnel alike.

On its webpage, the ISE has published the amended EO 13526, which provides the latest policy for handling classified information. While attempting to comply with Intelligence Community Directive (ICD) 501, which directs intelligence community activities for the "discovery and dissemination or retrieval of information within the intelligence community," EO 13526 does not stipulate or mandate routine access to

---

[73] Miller, interview with author.

[74] *Testimony Before the Committee on Government Reform, House of Representatives, SECURITY: Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues Statement of Robert F. Dacey, Director, Information Security Issues Randolph C. Hite, Director, Information Technology Architecture and Systems* (GAO-03-715T) (Washington, DC: U.S. Government Accountability Office, 2011), http://www.gao.gov/products/GAO-03-715T.

[75] Homeland Security Information Sharing Act, Pub. Law No. 107-296, 6 USC § 481 (2002), https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

classified information by local non–intelligence community partners. The executive order reads,

> In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with directives implementing this order and any procedure issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it.[76]

However as outlined above, there is one exception detailed in EO 13526 referring to "imminent threats," but as events such as those in Orlando and Chelsea/Seaside suggest, even this one exception may be routinely ignored at the local level.

While EO 13526 enables classified information sharing with local partner agencies, it does not provide the means to do so. The primary enabling capability that facilitates classified and integrated information sharing is a sensitive compartmented information facility (SCIF).[77] As described previously, integrated all-sources intelligence collection, analysis, and dissemination are best achieved within SCIF spaces. These spaces have secure, cross-domain network access to unclassified, secret, and top-secret sensitive compartmented information (TS/SCI). The ODNI provides further technical security requirements for these facilities but does stipulate that all SCIFs be "constructed, operated, and maintained for reciprocal use by intelligence community elements."[78] It is only in SCIFs that analysts can view unclassified, secret, and top-secret intelligence and brief it to stakeholders. Local interagency SCIFs would enable the type of fused all-source analytical production described earlier. These SCIFs could provide interagency access to unclassified and classified data alike for interagency intelligence personnel and

---

[76] Exec. Order No. 13526, Classified National Security Information, Federal Register 75, no. 2, (2010), https://www.archives.gov/files/isoo/pdf/cnsi-eo.pdf.

[77] "What Is a SCIF or Sensitive Compartmented Information Facility," Adamo Construction Inc., accessed October 15, 2016, http://www.adamoconstruction.com/what-is-scif.php.

[78] Office of the Director of National Intelligence, *Sensitive Compartmented Information Facilities* (Intelligence Community Directive No. 705) (Washington, DC: Office of the Director of National Intelligence, 2010), https://www.dni.gov/files/documents/ICD/ICD_705_SCIFs.pdf.

are the physical manifestation of "improving protection while expanding access."[79] While integrated SCIFs exist, these are almost exclusively located in the NCR or on military installations and do not necessarily support local operations or investigations.[80]

3. SCIFs and Their Impact on Quality Intelligence

Local ISE members do not have access to the same types of intelligence data that are readily available to organizations like the NCTC. State and major urban area fusion centers and law enforcement intelligence units often lack a SCIF or other classified space with the necessary intelligence community systems to coordinate classified intelligence sharing.[81] In its publications, the PM ISE addresses neither SCIFs nor the personnel needed to run and work in these facilities. In its last annual report on fusion centers, DHS does not specifically mention SCIFs, yet it openly acknowledges the challenges of maintaining properly cleared personnel working in lower-level classified spaces and accessing the full range of available classified material.[82] DHS further explains in its *National Network of Fusion Centers Final Report* that fusion centers and the federal government should continue to facilitate access to classified systems and facilities that offer secret-level information through systems like the Homeland Security Defense Network (HSDN). However, the language that DHS uses to describe accessing classified information falls short of advocating that SCIFs are integrated into fusion centers or other local information-sharing facilities.[83] Additionally, it is impossible to construct and maintain a SCIF without the ability to maintain properly cleared personnel and without qualified onsite security personnel. Neither the PM ISE nor DHS addresses the relatively few SCIFs in the field and the role of a SCIF in improving the quality of shared data.

---

79 "Improving Protection While Expanding Access," Program Manager Information Sharing Environment, accessed December 18, 2016, https://www.ise.gov/resources/standards-guides-best-practices/improving-protection-while-expanding-access.

80 Posner, *Preventing Surprise Attacks*, 148.

81 U.S. Department of Homeland Security, *National Network of Fusion Centers Final Report* (Washington, DC: U.S. Department of Homeland Security, 2012), https://www.dhs.gov/sites/default/files/publications/2012%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf.

82 Ibid., 12–13.

83 Ibid., 13–14.

Data quality at the local level is a critical issue. Despite the ever-growing availability of controlled unclassified information (CUI), the intelligence community still over-classifies and thereby restricts the dissemination of relevant terrorist data to local operators.[84] Mechanisms are in place to access this classified information, but the best mechanism is the SCIF. Networks like HSDN are available outside SCIF spaces but still require other secured facilities to ensure proper protection of the data. While DHS acknowledges the need for an HSDN capability in fusion centers, routine access to the network and integration with higher classified data available through SCIFs is not occurring on a regular basis.[85] Additionally, unclassified data available through multiple unclassified platforms—such as HSIN, Law Enforcement Online, and Regional Information Sharing Systems Secure Cloud (RISSNET)—are also not being integrated with higher classified data. As Busch and Givens suggest, these systems highlight efforts that have improved information sharing.[86] However, the lack of enough personnel and the incredible volume of information they generate may actually be the reasons that many analysts still feel there are problems with information sharing. As previously mentioned, the NCTC and other federal agencies may have analysts and field liaisons that are properly cleared and have access to SCIFs and systems, but the volume of data may be overloading these analysts during routine operations.[87] These issues demonstrate that the ISE and related legislation are limited; they neither specify a requirement for secure facilities nor mandate that TS/SCI information be shared and produced at the local level. While there are a variety of problems surrounding the issue of increased local access to classified intelligence, including over-classification, local security clearances, and limited access, the PM ISE has been slow to address them.

---

84 Miller, interview.

85 Ibid., 12.

86 Busch and Givens, "Information Sharing," 8.

87 Ibid., 9–10.

C. CONCLUSION

This chapter has outlined the existing challenges currently impacting information sharing across the FSLTT stakeholders at field and local levels. The GAO, House Homeland Security Committee, and others within in the field agree that the challenges can be summarized as poor and/or conflicting strategic policy implementation, uneven access, and poor data integration at the local level. Technology hurdles that impact the quality of information those field analysts access and the resultant analysis they can perform foster this dynamic. More specifically, while the 2004 IRTPA led to the creation of several information-sharing initiatives, evidence still suggests that vital intelligence is not shared at the highest possible levels Additionally, intelligence assets in the field who are primarily responsible for sharing information are few and have far fewer capabilities than their NCR-based counterparts. This has contributed to a continuing issue of stove-piping intelligence, something that the 9/11 Commission and numerous other researchers following 9/11 have proven a core negative impact on domestic counterterrorism.[88] Post-9/11 reforms have focused on NCR-based intelligence community improvements and policy guidance, but the ISE has not fully engaged the FSLTT partners to ensure all available intelligence is being shared.[89] Furthermore, evidence suggests that the continued reliance on legacy structures like the JTTF and fusion centers has limited the sharing of pre-attack information with local law enforcement.[90] Figure 1 provides a notional graphic representing the imbalance within the current ISE.

88 Zegart, *Spying Blind*, 123.

89 9/11 Commission, *The 9/11 Commission Report*, 407–408.

90 David R. Johanson, II, "The Long and Winding Road: Post-9/11 Intelligence Reforms a Decade Later" (master's thesis, Naval Postgraduate School, 2013), 29–30.

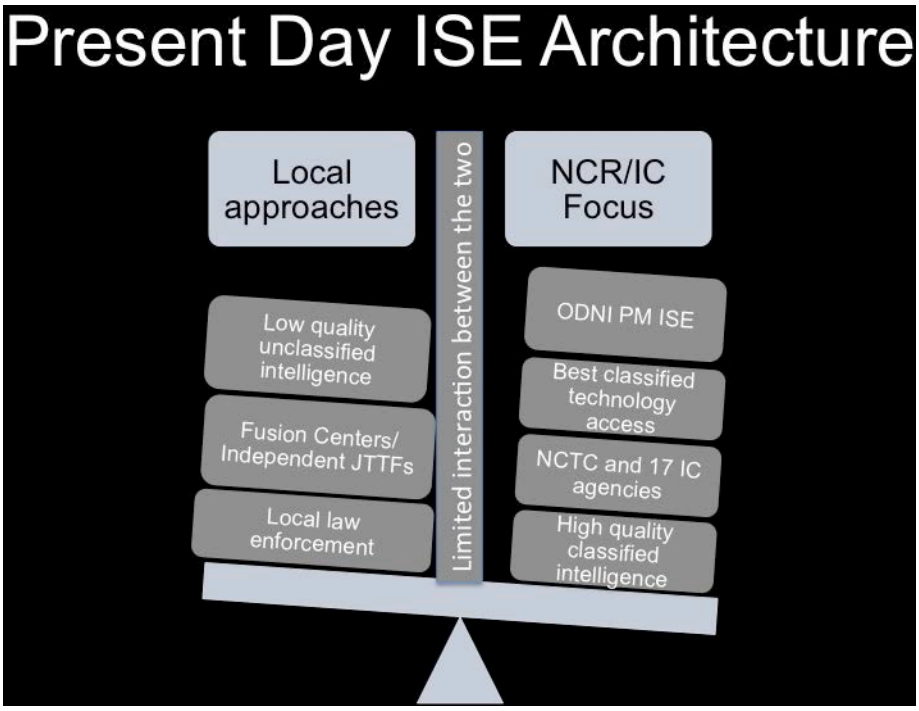

Figure 1. Present Day ISE Architecture

The next chapter introduces two case studies for consideration in addressing these enduring ISE challenges. The case studies focus on local and specialized approaches to counterterrorism that when merged with other existing ISE-related concepts may lead to meaningful ISE reform. Meaningful reform resembles a system in which the intelligence community no longer overwhelmingly bases its best counterterrorism capabilities, like the NCTC, within the NCR, but instead cultivates the capabilities and advantages that local approaches bring. This thesis concludes with an overview of the best practices that combine local and DOD approaches in a realistic way. However, this thesis is mindful of the political, resource, and funding limitations that currently exist.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MODELS TO ADDRESS ISE CHALLENGES

> Successful counterterrorism operations require robust, real-time information sharing. A data-point lost in the noise might be the key to disrupting a violent attack. Despite the enormous strides made in this area, more can be done to get the right information to the right people at the right time. After 9/11, intelligence fusion centers and more Joint Terrorism Task Forces were set up nationwide, recognizing that state and local law enforcement can be a force-multiplier in combating the threat. But they do not always have access to the critical information they need, which is why the U.S. government should redouble efforts to engage these frontline defenders in our counterterrorism efforts and facilitate two-way information sharing about threats.
>
> —Michael McCaul, Chair, House Homeland Security Committee, September 2016.[91]

When faced with complex problems, organizations require the ability to adapt and collaborate at unprecedented levels regardless of their status as federal, state, local, private, or commercial institutions.[92] The 2004 IRTPA created the ISE in an effort to address what the 9/11 Commission described as "lost opportunities" for the intelligence community and counterterrorism operations in terms of information-sharing reform.[93] The 9/11 Commission's conceptual recommendation for improving government-wide information sharing was to replace the traditional intelligence "need-to-know" presumption with a "need-to-share" culture.[94] Its primary recommendation led to the creation of the ODNI as an intelligence community chief officer to integrate information among all members and across all terrorism-related operations. Chapter II presented the challenges remaining for the ISE in terms of ensuring information-sharing across FSLTT

---

[91] Michael McCaul, *A National Strategy to Win the War against Islamist Terror* (Washington, DC: House Homeland Security Committee National Strategy, 2016), https://homeland.house.gov/wp-content/uploads/2016/09/A-National-Strategy-to-Win-the-War.pdf.

[92] McChrystal et al., *Team of Teams*.

[93] 9/11 Commission, *The 9/11 Commission Report*, 405.

[94] Ibid., 417.

communities. Chapter III attempts to address these challenges by reviewing and then analyzing the two models that, if endorsed by the ISE and FSLTT partners, could remedy some of the ISE's challenges. When the best practices of each model are combined, the SOF team-of-teams concept and the New York Police Department's intelligence unit, they form a framework contributing to an environment that fosters "robust, real-time information sharing" to the lowest operator level possible.[95]

A. THE SOF APPROACH

The first case study this thesis reviews is the special operations forces (SOF) model. As detailed in the *Special Operations Forces Reference Manual*, SOF "encompass[es] the use of small units in direct or indirect military actions focused on strategic or operational objectives. These actions require units with combinations of specialized personnel, equipment, and tactics that exceed the routine capabilities of conventional military forces."[96] These forces are augmented when deployed with a national intelligence support team (NIST) as well as other external and sometimes international capabilities to ensure mission success. These highly adaptable and flexible units have small footprints and operate under the "quiet professionals" mantra.[97] The following paragraphs review the overall SOF concepts and structure as well as NIST's background and capabilities. The structures and capabilities of the Combined Joint Special Operation Task Force (CJSOTF) and NIST were combined in Iraq in unique ways that provides examples of how they might be leveraged by the ISE. As acutely described in General Stanley McChrystal et al.'s *Team of Teams*, the CJSOTF hunted Al Qaida-in-Iraq and its leader Zarqawi from 2004 through 2007.[98]

---

95 McCaul, *A National Strategy*.

96 Joint Special Operations University [JSOU], *Special Operations Forces Reference Manual*, 4th ed. (MacDill AFB, FL: Joint Special Operations University Press, 2015), http://jsou.socom.mil/JSOU%20Publications/2015SOFRefManual_final_cc.pdf, I-1.

97 The SOF reference manual defines this as the best description of the SOF ethic and culture where conduct reflects not only on self but also the nation, where members are focused on contributing to missions at hand while part of an integrated team, unconcern over who gets credit but aware that much of what they do remains in the shadows. JSOU, *Special Operations*, I-1.

98 McChrystal et al., *Team of Teams*, 240–243.

1. SOF Concepts and Structure

Doctrinally, SOF teams are small units with specialized, task-organized capabilities that operate in complex, austere environments, augmented with external intelligence community capabilities.[99] These SOF units are flexible enough to be reshaped for a variety of missions and are designed to "ensure effective collaboration in joint, interagency, and combined operational environments."[100] Operational units range in size from 10 to 21 for Army Special Forces and Navy SEAL teams, and up to 110 members for Army Ranger battalions involving larger targets or missions.[101]

Special forces units are all designed to facilitate rapid and adaptive operations when augmented with various support elements, ranging from organic communications to legal and military intelligence detachments. External support elements also collaborate in a joint operations environment with other units and can be tasked by a joint geographic commander to provide support to other external units operating in the same mission or operational area. This augmentation strategy allows SOF units that do not have their own assets for certain disciplines but are needed for a given mission, for example aviation, to cross-leverage the SOF capabilities of other services under the joint command structure. The ability to augment units with national capabilities is the defining aspect of CJSOTF, which is described later in this chapter. The task force structure ensures mission success by pooling resources under one mechanism, despite being under separate military services when not operationally deployed.

One of the best practices of modern-day SOF is the joint planning process and the operations planning cell. The joint operational planning process is required for most counterterrorism and/or unconventional missions involving a joint task force.[102] The process occurs in a networked, collaborative environment that relies on routine dialogue

---

99 JSOU, *Special Operations*, I-7.

100 Ibid.

101 Ibid.

102 Joint Chiefs of Staff [JCS], *Joint Task Force Headquarters* (Joint Publication 3-33) (Washington, DC: Joint Chiefs of Staff, 2012), http://www.dtic.mil/doctrine/new_pubs/jp3-33.pdf, ix–6.

among senior leaders across multiple planning levels.[103] The primary goal of this type of planning is to provide clear strategic guidance through frequent interaction to promote early understanding of mission objectives and intelligence requirements. The intent of SOF mission planning is to consider a wide-range of mission-related aspects from assumptions and risks to considerations and other factors that form the elements of the overall operational design.[104] This operational design leads to detailed mission analysis, course of action (COA) development, war gaming, COA comparison, and other decision-supporting processes prior to mission rehearsals. The planning cells are just one aspect of the overall joint planning group but may comprise sub cells that incorporate both operational and intelligence disciplines to analyze all aspects of potential missions.[105] The final result provides SOF and task force commanders with comprehensive, detailed, and flexible operations plans that help them make informed decisions from a variety of options. Lastly, through task organization, SOF mission planning and operations cells imbed representatives, including NIST members, from different support disciplines.[106] Figure 2 offers an example of SOF structures in a joint operational planning environment.

103 Joint Chiefs of Staff, *Joint Tactics, Techniques, and Procedures for Special Operations Targeting and Mission Planning* (Joint Publication 3-05.2) (Washington, DC: Joint Chiefs of Staff, 2003), http://www.bits.de/NRANEU/others/jp-doctrine/jp3_05_2.pdf, I-7.

104 Ibid.

105 Ibid., ix–11.

106 JCS, *National Intelligence Support to Joint Operations*, 20.

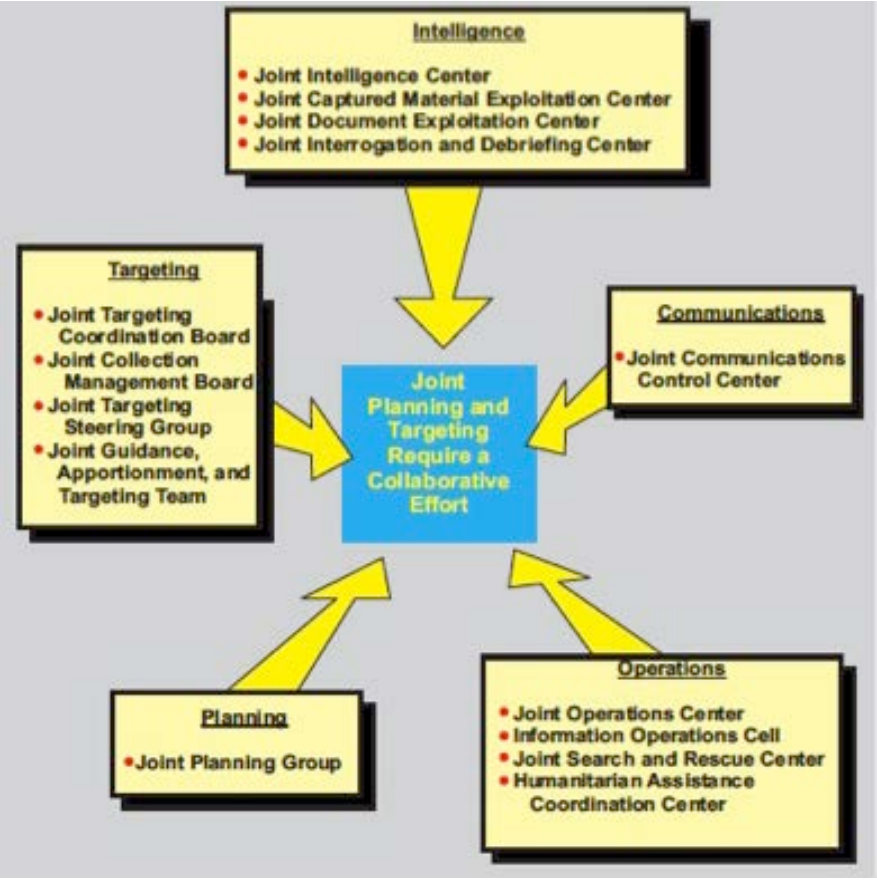

Figure 2. Theater-Level Planning and Targeting for Organizational Structures[107]

2. NIST Concepts and Structure

The NIST concept has its origins in the early 1990s when the DOD reimagined how its military forces deployed to support multiple simultaneous "low-intensity" conflicts around the world once mission needs exceeded the capabilities of ordinary military units.[108] The intelligence community had to innovate to support these new types of continuous operations in a world of "disorder."[109] NIST was one of the innovations to

[107] Source: JCS, *Joint Task Force Headquarters*, ix–6.

[108] James M. Lose, "National Intelligence Support Teams, Fulfilling a Crucial Role," Central Intelligence Agency, accessed October 15, 2017, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter99-00/art8.html.

[109] Ibid.

support operations in the 1990s and into the early 2000s. The Joint Chiefs describes the NIST best, "The NIST is a nationally sourced team of intelligence and communications experts from Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), and other agencies. The NIST's purpose is to provide a national-level, deployable all-source intelligence team" for task force commanders." [110] NIST may comprise various intelligence community personnel from the DIA, NSA, NGA, and CIA. These personnel are deployed upon request by a joint task force (JTF) commander to "facilitate the flow of timely all-source intelligence between a JTF and Washington" during various types of crisis operations.[111]

Participating national intelligence community partners send one to 20 volunteers to deployed NIST elements. These trained individuals have a tailored combination of skills and report to a team chief who is selected by the Joint Staff J-2 based on nominations from the intelligence community.[112] NIST has an integrated communication structure that leverages both unique agency and operation command capabilities.[113] And since NIST is deployed in support of a task force commander, thee teams perform functions at his or her behest. All intelligence generated in support of the JTF is made available to the respective parent organizations, the Joint Staff J-2, and ideally, the rest of the intelligence community depending on classification restrictions. However, the CIA member of NIST has the ability to make quick dissemination determinations of previously reviewed ORCON material. This tactical dissemination capability is key to facilitating intelligence sharing at the local level and back through the rest of the intelligence community. Additionally, NIST members can also determine secondary and

110 JCS, *Joint Task Force Headquarters*, II-5.

111 JCS, *National Intelligence Support to Joint Teams*, V-6.

112 According to JCS Joint Publication 2-01, the J-2 is defined as the intelligence directorate of a joint staff and in charge of the national military joint intelligence center. JCS *National Intelligence*, V-6; Joint Chiefs of Staff [JCS], *Joint and National Intelligence Support to Military Operations* (Joint Publication 2-01) (Washington, DC: Joint Chiefs of Staff, 2004), http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf.

113 Ibid., V-7.

follow-on product dissemination.[114] NIST cells are meant to deploy only for limited durations not exceeding 90 days and are intended to train theater intelligence assets once operations transition from crisis to "sustained operations."[115]

NIST capabilities ensure joint intelligence operations integrate unique military services and national intelligence capacities into a unified effort. Such capabilities align with Joint Chiefs intent by ensuring commanders receive accurate and timely intelligence that drives JTF operations and shapes long-term sustainment by "[surpassing] any single organization's effort." [116] One of the best practices NIST has achieved has been providing each member and the JTF commander intimate knowledge of parent-agency resources and capabilities. The NIST has provided dynamic intelligence over the years, supporting a variety of combat operations overseas, each with unique operational considerations. However, JTF commanders are concerned about the potential for intelligence community micromanagement and operational leaks, which often coincide with NIST deployers coordinating with their respective headquarters. However, JTF commanders can direct exactly when and how NIST members communicate with their headquarters. For example, in 1995, NIST members supporting Task Force Eagle in Bosnia were ordered not to disseminate information that was relevant to ongoing or future operations.[117]

3. Team of Teams

As General Stanley McChrystal et al. describes in *Team of Teams*, "The greatest innovations have not come from a lone inventor or from solving problems in a top-down, command-and-control style. Instead, the great successes—the creation of the computer, transistor, microchip, Internet—come from a 'team of teams' working together in pursuit of a common goal."[118] In Iraq following the 2003 invasion, in one of the nation's most

---

114 Ibid.

115 JCS, *Joint and National Intelligence*, II-16.

116 Ibid., I-1.

117 Lose, "National Intelligence Support Teams."

118 McChrystal et al., *Team of Teams*, Foreword.

complex counterterrorism environments, NIST augments alone were not enough to support successful JTF missions. Multiple NIST-type elements were integrated into a wider concept, the team of teams. The new team-of-teams concept leveraged and merged the full extent of the United States' elite special forces and national intelligence with other, similar international capabilities. In *Team of Teams*, General McChrystal et al. illustrate how traditional SOF/NIST concepts became rigid and inadaptable to a new, complex fight.[119] This section reviews the team-of-teams concept and structure as well as synopsizes how it evolved into a reimagined combination of existing SOF and NIST capabilities.

a. Justification for Concept

In the complex operating environment of Operation Iraqi Freedom (OIF) in 2003–2004, SOF units experienced significant challenges to information/intelligence sharing.[120] Despite SOF units being the elite of the elite in counterterrorism operations, the system had significant flaws. Operators complained of not receiving intelligence that was relevant to their missions as well as not receiving follow-up analysis from data that they previously captured.[121] Supporting analysts complained that recoveries from operations had little intelligence value and did not fit with the established intelligence requirements.[122] Additionally, the intelligence community did not facilitate rapid analysis and response, a critical step to drive follow-up operations, even when evidence of value was recovered. Such a dynamic can be described as a hierarchical, vertical organizational structure whereby operators and others at the lowest or more tactical levels of the task force are disconnected from the best support assets. Additionally, those support assets may be placed in positions to compete with each other rather than to collaborate on the overall outcome of the mission.

---

119 Ibid.

120 Williams, *Intelligence Support to Special Operation*, 14–16.

121 McChrystal et al. *Team of Teams*. 119–121.

122 Ibid.

b. Concept Structure

General McChrystal et al. detail operational challenges such as those outlined in the previous section in his first-person account from his time as the commanding officer of the CJSOTF for OIF. One of the themes expressed in *Team of Teams* is the scalable team approach, which allows individual teams to address complex issues with more adaptability than any top-down process ever could. General McChrystal et al. describe the reasoning behind this approach:

> The solution we devised was a "team of teams"—an organization within which the relationships between constituent teams resembled those between individuals on a single team: teams that had traditionally resided in separate silos would now have to become fused to one another via trust and purpose.[123]

The CJSOTF environment for Iraq combined U.S. SOF with international Special Forces elements, eventually building up to 7,000 members for a complete task force.[124] Teams within the CJSOTF were tasked with gathering and applying intelligence. This intelligence was eventually fused into a daily briefing for all task force members and their component agencies. This briefing was securely broadcast as a virtual teleconference not only to all member organizations of the CJSTOF but also to the supporting intelligence community partners. While briefings of this nature are not unique and occur fairly regularly across a variety of domains in homeland security and the intelligence community, the unique culture of this operations and intelligence or "O&I" briefing called for and promoted an environment where anyone in attendance could present intelligence they felt was relevant to CJSOTF missions.[125] In other words, anyone could present and counter-argue intelligence and planning analysis. In fact, McChrystal's leadership style encouraged this cultural change. The culture shift of the O&I briefing replaced the "need-to-know" approach with a "need-to-share" culture. The change in culture sought to build trust by placing operators directly in contact with intelligence

123 Ibid., 132.

124 Ibid., 128.

125 Ibid., 164.

analysts while facilitating regular/routine communication between all CJSOTF members.[126] This shift created a wide-open communication structure that fostered what McChrystal et al. call "a holistic understanding of the interaction between all the moving parts. Everyone has to see the system in its entirety for the plan to work."[127] Within the scope of overall taskforce objectives, operators, and lower-level leaders also require empowerment to act on insights gained as part of this team-of-teams O&I process.[128]

c. SOF, NIST, and Team of Teams Combined

Lastly, while the combined SOF, NIST, and CJSOTF programs eventually experienced great success in degrading AQI and eliminating its leader, Zarqawi, for a variety of reasons, this new team-of-teams concept ended prematurely. Expense, force commitment, and overall leadership turnover likely drove this unique restructuring of the CJSOTF model to its conclusion. Nevertheless, commonalities and best practices drawn from the team-of-teams concept are applicable as solutions to ISE challenges. The team-of-teams concept combined elite SOF, NIST, and other national and international capabilities with regular communication within the taskforce while maintaining a constant secure communication capability to national parent organization.[129] Furthermore, operational planning combined imbedded intelligence analysts with operators and collectors resulted in holistic planning and a successful decentralized leadership style.[130] While empowered to make insights and take actions within their own sphere of influence for the overall mission, all taskforce members became knowledgeable and invested in the overall operational outcome.[131] The O&I brief synchronized CJSOTF activities by bringing together both the latest intelligence with the latest mission developments for real-time situational awareness that drove future operations.

---

[126] Ibid., 138–139, 140.

[127] Ibid., 141.

[128] Ibid., 244.

[129] Ibid., 163–164.

[130] Ibid., 166.

[131] Ibid., Foreword.

B. THE NYPD APPROACH

In "Local Approaches," Dahl provides an appropriate overview of why alternative counterterrorism strategies are needed. He writes, "International security against terrorism is profoundly affected by domestic and local policies, and national defense against terrorism is best achieved through local approaches."[132] This section details the most comprehensive local approach for terrorism-related information sharing in the country, the NYPD model. It reviews the NYPD's Intelligence Bureau, Intelligence Support and foreign liaison officer programs, and its Sentry and SHIELD programs. When combined, these programs offer the most comprehensive suite of intelligence collection and dissemination programs by a local law enforcement agency in the country.

1. Intelligence Bureau

The NYPD Intelligence Bureau offers potential solutions to remaining ISE challenges. The NYPD has one of the most comprehensive law enforcement intelligence programs in the country. This should not come as a surprise given that the NYPD is the nation's largest police force with over 40,000 uniformed and civilian personnel.[133] As Dahl states, NYPD's model leverages the resources of local law enforcement and combines them with an unmatched relationship with the local population it is assigned to protect.[134] Prior to 9/11, the NYPD had no organization that specialized in terrorism-related intelligence even though the Intelligence Bureau "focused on protecting dignitaries and developing criminal intelligence."[135] Today, the Intelligence Bureau incorporates an operational counterterrorism division, civilian analysts, an intelligence support program formed from external FSLT agencies, and a foreign liaison officer program. The Intelligence Bureau also established and hosts at least two programs vital to

132 Dahl, "Local Approaches," 81–97.

133 Miller, interview.

134 Dahl, "Local Approaches," 83–84.

135 Ibid., 85.

information/intelligence sharing across law enforcement and public/private domains: the Sentry and SHIELD programs.[136]

According to Dahl, the NYPD's Intelligence Bureau is unique and its functions the envy of national intelligence community agencies and major metropolitan police forces alike. Its personnel range from uniformed field intelligence officers (FIOs) assigned to each of its precincts to the civilian analysts that are part of its Analytic Unit. Civilians who are part of the Analytic Unit are recruited from the intelligence community, NCTC, CIA and other government organizations and research centers. These civilian analysts also have advanced degrees and are recruited from our nation's top universities and research institutions.[137] Uniformed FIOs serve as "core collection" officers who gather information about possible ties to radicalization and follow up on leads developed from reports or other intelligence collection sources like social media. [138] This local human intelligence (HUMINT) capacity surpasses that of any ordinary police department and leverages the very population it serves to protect. As John Miller describes in the interview conducted for this thesis, the NYPD is now a "majority minority," meaning it has successfully recruited its ranks from the melting pot of the city's diverse population.[139] The NYPD's diversity gives its intelligence capacity organic language skills and an unsurpassed local cultural knowledge. The precinct FIOs and investigating detectives communicate directly with the civilians of the Analytic Unit to work cases jointly, assist with research, and then coordinate with external agency officers of the Intelligence Support Program (ISP), which is collocated with the Analytic Unit.

2. Intelligence Support Program

The NYPD's ISP hosts over 30 federal, state, local, and international partners that, in addition to working for their respective agencies in the city, also have part-time

[136] The NYPD SHIELD program is not an acronym. NYPD has described this program in multiple and various forums but does not define it as an acronym but does always capitalize it in the method used in this thesis.

[137] Ibid.

[138] Ibid.

[139] Miller, interview.

desk hours with the NYPD Intelligence Unit and a 24/7 communications capability to support crisis and special event operations. Participation is voluntary by the agency; however, external agencies jump at the opportunity to participate in order to have access to the NYPD programs that are collocated. Collocated within NYPD intelligence spaces are programs such as the Lower Manhattan Security Initiative (LMSI) and the High Intensity Drug Trafficking Area (HIDTA) cell. The ISP program co-leverages the same personnel and analytical capabilities for an integrated all-source (unclassified) approach to local investigations.

Both HIDTA and LMSI have the added advantage of leveraging NYPD's best technologies, all of which are accessible through the ISP program. Thousands of private and public security cameras, license plate readers, and other technologies, such as advanced facial recognition analysis, are monitored 24/7 by NYPD's operations centers and are part of their "Domain Awareness System," which streams all information back to the local and regional operations centers.[140] NYPD's John Miller describes the impact these programs have had: "A level of networking, a tightness of weaving that law enforcement fabric together across borders and cultures … has been extraordinarily productive and important."[141] Finally, agencies that participate in the ISP can also bring in their own unique unclassified systems and databases to augment access to NYPD. These databases give analysts and liaison officers assigned to the ISP, cross-domain capabilities that mirror or even rival the capabilities of national intelligence community organizations.

3. Liaison Program

One of the more contentious programs NYPD created after 9/11 has been its foreign liaison officer program.[142] The program involved posting uniformed NYPD officers in now 13 different foreign countries or foreign-based organizations around the

[140] Dahl, "Local Approaches," 85–86.

[141] Miller, interview.

[142] Dahl, "Local Approaches," 86.

world.[143] While the NYPD liaison officers are based at foreign posts, they do not investigate foreign crimes and not authorized to conduct typical law enforcement collection in their host countries. However, NYPD's liaison officers serve the vital function of facilitating information flow between the NYPD and foreign, local police department hosts with an emphasis on examining potential threats to NYC. These liaison officers are also based in organizations such as EUROPOL and Interpol, which focus on transnational crime and terrorism. Having officers embedded in these organizations avoids having to station officers in 60–100 different countries. As Miller described during his interview, "We've got people in Interpol and Europol because that's one-stop shopping."[144]

However, the program is not without criticism, mostly from federal agencies. Dahl describes this tension:

> Especially in the first few years after the programme was initiated, the international programme led to conflicts between the NYPD and the FBI, which maintains its own Legal Attaches, or "Legats," around the world. One such turf struggle occurred after a terrorist bombing in Madrid, Spain, in 2004, when the NYPD sent an intelligence liaison team to Spain without consulting with the FBI.[145]

Criticism from federal agencies such as the FBI often centers on the need for "one voice" for foreign-based U.S. law enforcement to reduce confusion on the part of the foreign host country. Relying solely on one federal agency to conduct foreign law enforcement liaisons restricts the dissemination of information collected during the investigative process.

To its credit, the NYPD has leveraged the information it has gathered through its foreign liaisons to the mutual benefit of the NYPD and their hosts, by publishing products of intelligence value that are shared not only locally and nationally. The NYPD also shares its analysis with the foreign partner law enforcement organizations. The

---

143 Miller, interview.

144 Ibid.

145 Dahl, "Local Approaches," 86.

greatest success of NYPD's foreign liaison officer program occurred during the terrorist attacks in Mumbai in 2008.[146] Although the NYPD did not have an officer already based in India, it was able to send an experienced senior officer who had previously visited India on official business. The officer was sent to India while the attacks were still ongoing and that officer was able to relay near real-time information back to NYC officials regarding the tactics used in the attacks.[147] Bureau leaders then used this information to assess NYPD's Emergency Services Unit (ESU) and the department took steps to improve its specific capabilities designed to defeat a similar attack if perpetrated in New York. Additionally, the Intelligence Bureau produced and shared an analysis of the attacks through its SHIELD program to city and nationwide private businesses.[148]

4. Sentry and SHIELD Programs

The reporting that the above programs tap into still largely depends on official sources and investigations. In order to expand its collection capabilities into more private and public organizations, the NYPD created the Sentry and SHIELD programs. These programs combined bring together hundreds of organizations from across the city, country, and world to share the latest intelligence analysis, best practices, and training all in the name of increased networking. Once a year, the NYPD hosts Sentry program members in a conference at NYPD headquarters where over a 158 state and local law enforcement agencies attend and share data on the latest gang, narcotics, and other criminal trends in a secure environment.[149] Agendas for the conference in previous years have featured a variety of speakers from organizations like the Texas Department of Public Safety, Pennsylvania State Police, and the U.S. Military Academy at West Point. These speakers have also presented material on a wide range of topics, from counterterrorism best practices to jihadist messaging to drug cartels.[150] John Miller

---

146 Ibid., 87.

147 Ibid.

148 Ibid.

149 "Operation Sentry: A Counterterrorism Coalition," *NYPD News*, November 10, 2015, http://nypdnews.com/2015/11/operation-sentry-a-counterterrorism-coalition.

150 Ibid.

outlines how the NYPD leverages these types of briefings, "We have Sentry members do their own presentations. When this started, it was built to be the NYPD's network. We brought the FBI, Secret Service, ATF into it on the idea that all our networks need to touch."[151] The NYPD's multiagency approach enables a wider range of varying analysis that can influence and be incorporated into their counterterrorism strategies.

While the Sentry program largely hosts other official law enforcement and government agencies, the NYPD recognizes the informational and networking value of inviting public and private institutions to the information-sharing table as well. Its SHIELD program is the standard for partnership and outreach: "NYPD Shield program exemplifies public-private sector information as well as vertical information sharing. NYPD Shield enlists local business owners to be the 'eyes and ears' of the NYPD in identifying potential terrorist threats."[152] While on the surface the sharing of intelligence may just seem as another top-down or vertical process where agencies 'preach' at business owners and share low-quality trend data, but it's much more. By bringing in business and industry partners who are the potential targets of terrorists' activity, the NYPD is also encouraging horizontal information sharing that builds trust and 'routineness' to the information sharing.[153] This is how the NYPD links privately owned security cameras and other privately held data collection methods to its Lower Manhattan Security Initiative program among others, and in exchange, businesses receive access to NYPD Intelligence and threat briefings from invited guest speakers such as the NCTC, the ODNI, or FBI.[154] John Miller outlines the importance of NYPD's interagency approach: "That's where we get access to the kinds of information that all of those industries have their own expertise in that we could never match."[155] The dynamic creates a secondary effect in that business owners now trust their local precincts more and reach out to city officials more frequently on local issues.

---

[151] Miller, interview.

[152] Busch and Givens, "Information Sharing," 5.

[153] Ibid.

[154] Ibid.

[155] Miller, interview.

5. NYPD Information Sharing

The NYPD approach to information consists of horizontal and vertical sharing across the various components of its Intelligence Bureau: the Intelligence Support, foreign liaison officer, and the Sentry and SHIELD programs. All work together to provide the best analysis to aid investigations and operational planning but also to drive an unmatched level of public/private information sharing. While not all local law enforcement has the resources that NYPD does, similar local law enforcement driven programs are scalable and can serve as examples for smaller local agencies to emulate.[156] Given the successful terrorism cases the NYPD approach has solved, when combined with other information sharing best practices, many domestic local agencies could leverage similar concepts in their counterterrorism fight.[157]

C. ANALYSIS AND CONCLUSION

The implications for solving some the ISE challenges by both models could be profound. The success of both the SOF and NYPD models for information sharing largely centers around building trust and fostering a sense of shared investment in successful operational outcomes. Both models build structures that rely primarily on fitting the right personnel in the right collaborative environment, facilitated by the right technology to cross interagency divides. Both models recruit the best of the best, meaning the most experienced and skilled personnel, to participate. Both foster open lines of horizontal cross-agency communication and vertical lines of communication with external intelligence community partners as well as their respective stakeholders. Both models combine and pool resources with external supporting agencies since both recognize that no single agency can complete the mission on its own. Both models demonstrate how operators within each serve as intelligence collectors and users. Both models leverage the skills of their operators at building relationships with their respective local target communities as means to gathering better intelligence through cultivating

156 Dahl, "Local Approaches," 92.

157 Ibid., 88–89.

local trust. All of these best practices have built interagency and interdisciplinary trust, something rarely seen in domestic counterterrorism operations.

However, the ISE mandate did not lead to the creation of the models referenced nor did ISE representatives directly participate in or created these structures. In fact, research for this thesis revealed little if any recognition of ISE PM connections to the models themselves. The models arose out of unique and local operational demands to meet specific threats and/or missions. Therein lies the most significant challenge for the ISE: its own connectivity to unique missions and local operational needs. For example, in New York, while fusion centers like the New York State Intelligence Center (NYSIC) have been created, endorsed, and improved under the auspices of the ISE, NYPD's intelligence model is not part of the national fusion center network.[158] The PM ISE is greatly involved with ensuring intelligence community participation in the NCTC and other national-level classified terrorism intelligence collaboration. But the ISE was not involved with the team-of-teams operations that were under local military commander control. While the PM ISE has influence over national intelligence community information sharing initiatives, their role in how the intelligence community jointly participates in military operations is limited. Intelligence sharing for military operations is largely determined by established joint military policy and not the ODNI, the 2004 IRTPA, or by current PM ISE guidance.

158 Ibid., 87.

IV. INFORMATION SHARING ENVIRONMENT: THE WAY FORWARD

This thesis combined policy and case study analysis with anecdotal commentary from senior leaders on the current state of the ISE for local field counterterrorism operations. The findings reveal the need for a reimagined homeland information-sharing environment. Senator Michael McCaul, NYPD's John Miller, Erik Dahl and other scholars, as well as senior leaders all agree that current intelligence support for the domestic counterterrorism environment needs improvement. The author of this thesis imagines a collaborative counterterrorism environment wherein all FSLTT capabilities are leveraged. To accomplish this objective, current mechanisms—fusion centers, the NCTC, the JTTF, and field intelligence liaisons established following 9/11—must all be combined in a way that builds trust among the "owners" of these capabilities.

Merging both the team-of-teams and NYPD models in their entirety would be almost impossible for a variety of reasons. The models would likely face implementation difficulties, from associated costs to command and control. Additionally, domestic implementation of several team-of-teams concepts would also likely face restrictions under the Posse Comitatus Act, which limits direct DOD support to domestic, civilian law enforcement communities but does not outright prevent it. However, blending the best practices of each model with ISE endorsement could pave the way for reducing the strategic, tactical, and technological challenges that persist and impede domestic information sharing. Strategically, the ISE would have to acknowledge that not all information sharing can or should be controlled through Washington, instead endorsing a more decentralized approach by issuing policy and funding guidance that advocates for sending national capabilities where they are needed most—the field.

Local information sharing initiatives need an advocate that can incorporate their best practices into national programs and capabilities. Tactically, the ISE would have to endorse local initiatives such as the NYPD and begin to change overly restrictive policies limiting the involvement of local law enforcement agencies in nationwide domestic intelligence activities and information sharing. In many ways, this has already begun, by

having organizations like the Major City Chiefs Association and the NYPD liaise with agencies and leaders in Washington. However, the ISE must require all federal agencies, the FBI in particular, to share more information with the local jurisdictions they support. As discussed in Chapter II, given the gaps in authority under the 2004 IRTPA and subsequent executive orders, Congress and the White House have to collaborate on revising existing law to grant ODNI and PM ISE the necessary authority to enforce accountability for any ISE solutions. Part of any revisions to these laws and executive orders would also need to include language endorsing local law enforcement participation in PM ISE's various advisory councils as well. This chapter reviews the remaining challenges for blending the models.

A. BEST PRACTICES OVERVIEW

A common failure in counterterrorism was evident in the case of the 2013 Boston Marathon bombing and in other cases since then: one agency wrongly determined that the subject of interest was no threat. This decision was not carried out in a collaborative fashion among all FSLTT partners whose jurisdictions were the targets of these attacks, but rather in a stove-piped, top-down approach by a federal entity. The best practices from the models discussed in Chapter III would mitigate this problem by making all aspects of an investigation into these individuals' parts of a collaborative interagency cell. Cells of this kind would feature highly specialized multijurisdictional operators working alongside the nation's best intelligence capabilities. Teams would have the latest technology and communications capacities to facilitate rapid intelligence collection, analysis, and sharing to drive the prevention operation. The collective cells would have the responsibility to keep local and national senior decision makers routinely informed about operations and relevant intelligence that has influenced the decision-making process. Ultimately, the cells would have an empowered command structure with one common operational goal: preventing attacks instead of case investigation.

This concept will take time to build, and it will be particularly important to build trust among all partner agencies and disciplines. At all levels of government, mistakes may be made, such as leaks of classified information, but preventing the loss of life in

another terrorist attack on U.S. soil demands that intelligence and law enforcement communities reimagine how they counter terrorism. Gone should be the days of single agencies having sole responsibility for domestic counterterrorism operations since evidence has established that one agency—one structure alone—cannot handle the overwhelming number of terrorist and HVE cases. The national intelligence community must realize that there are alternatives to dealing with the overwhelming volume of intelligence data on its own. National intelligence partners should be forced to broaden their capabilities by incorporating local law enforcement collection and analysis in a way that considers alternative theories. At times when a specific domestic threat is not imminent, the intelligence community should invest in regular joint analysis and trend briefings on global terrorist tactics with local partner agencies.

One of the critical recommendations of this thesis is to ban the use of the ORCON dissemination control for all terrorism-related intelligence. Currently, the 2004 IRTPA allows for intelligence agencies to ignore specific guidance from the White House and ODNI to share terrorism intelligence, regardless of classification, to the lowest levels possible across the ISE domains. However, the 2004 IRTPA provides a legal loophole that intelligence agencies exploit to restrict dissemination of terrorism data despite the legislation's intent to increase terrorism data sharing. Banning ORCON would at least allow federal field intelligence officers to share classified intelligence more routinely with cleared senior NYPD personnel and open the door to merge the SOF and NYPD models for sharing information both horizontally and vertically.

By leveraging the most successful, specialized, adaptable capabilities the homeland has to offer, the HSE will be better suited to address the challenges to ISE that remain today. However, this will take investment by all agencies. All must contribute not only their best personnel but also their best facilities, tactics, methods, technology, funding, and intelligence. Since terrorism crosses all jurisdictions and existing law already provides the legal authorities for sharing terrorism intelligence across these boundaries, ensuring compliance should be only a matter of national prioritization, and local-level acceptance. The PM ISE could be the national body if existing policies were rewritten to promote FSLTT partner participation. This thesis offers four core

recommendations that need implementing before moving this type of interagency collaboration forward: revise existing (1) ODNI/PM ISE and (2) intelligence community authorities, (3) update the language of the Posse Comitatus Act to enable the use of SOF in advisory roles to local law enforcement, and (4) solicit local law enforcement input and investment in a new ISE.

B. RECOMMENDATIONS

Research for this thesis included an interview conducted with the NYPD's DCI John Miller, who revealed the complexity within the offices of the DNI and PM ISE. The 2004 IRTPA and follow-on executive orders, including EO 12333, leave gaps in the authority of the ODNI to hold the intelligence community accountable. Additionally, the PM ISE wears two hats as it "lives halfway in between the White House and ODNI."[159] Revising the 2004 IRPTA and EO 12333 as well as housing the PM ISE in the executive branch's National Security Council (NSC) could help solidify the authorities and encourage compliance of ISE members.

1. Rewrite the 2004 IRTPA

It may be time to amend the 2004 IRTPA based on feedback from senior intelligence officials, considering that no members of the House Intelligence Committees served as principle authors when it was written 13 years ago.[160] Although Congress struggles to agree with the executive branch, it should consider repealing or revising section 1018 of the legislation because it prevents the DNI from abrogating the authorities of the intelligence community's department heads.[161] Eliminating or revising this provision would provide the DNI direct control over the intelligence community and ensure compliance is enforced through a single office, at least for all intelligence community operations involving terrorism. Additionally, the IRTPA would have to include new language that details specific types of information to be shared as part of the

159 Miller, interview.

160 Hayden, "State of the Craft."

161 Ibid.

ISE, including raw and finished data, local law enforcement data, and foreign government data.[162] Then, intelligence community agencies would have to legally comply with established ODNI policies and guidance on all ISE activities or risk budgetary and legal penalties.

However, a change in this role for the ODNI would conflict with the role of the Under Secretary of Defense for Intelligence (USDI), who currently serves as the DOD's senior intelligence official and has line-item control over some of the intelligence community's largest intelligence agencies such as the NSA.[163] True change for the authorities of the ODNI may require either eliminating this position by the Congressional Armed Services Committee or amending EO 12333 to clarify the USDI portfolio. This recommendation would then have the effect that Lederman describes as "clarifying the accountability for the intelligence community's performance," which is important for intelligence sharing reform.[164]

2. Update EO 12333

The authors of the 2004 IRPTA wanted to leave responsibility for determining the relationship between the ODNI and the intelligence community agency leads to the president.[165] However, EO 12333 was updated in 2003, 2004, and 2008 with language reinforcing the IRPTA guidance that the ODNI not abrogate the authority of the intelligence community heads.[166] To implement the recommendations of this thesis, EO 12333 needs updating again. That update should include language extending the authority of the ODNI over intelligence community classification standards and information dissemination controls, banning the use of ORCON for all terrorism intelligence, and

---

162 James Burch, "The Domestic Intelligence Gap: Progress Since 9/11?," *Homeland Security Affairs XII Proceedings of the 2008 Center for Homeland Defense and Security Annual Conference* (April 2008): 14, https://www.hsaj.org/articles/129.

163 Ibid.

164 Gordon Nathaniel Lederman, "Restructuring the Intelligence Community," in *The Future of American Intelligence*, ed. Peter Berkowitz (Palo Alto CA: Hoover Institution Press, 2005), 80.

165 Burch, "Domestic Intelligence Gap," 14.

166 Hayden, "State of the Craft."

extending oversight over military intelligence capabilities to support domestic terrorism threats. The Foreign Intelligence and Surveillance Act (FISA) and the USA PATRIOT Act specify the types of intelligence that can be collected on U.S. persons and explains what can be shared with local law enforcement and intelligence agencies respectively.[167] However, more specific guidance is needed to increase the sharing of classified intelligence with FSLTT partners.[168] Since EO 12333 provides the primary executive authority over the intelligence community, perhaps it should provide details on how the ODNI and PM ISE implement the strategy.

3. Update Posse Comitatus Act, Title 10, and Title 50

The Posse Comitatus Act of 1878 specifically permits only the president to authorize the use of federal military forces for law enforcement within domestic boundaries and then only under "exigent circumstances."[169] But the Act does not outright prevent the use of intelligence assets domestically.[170] Today, the executive and legislative branches closely review requests for direct DOD support to civilian law enforcement agencies.[171] Given the age of the statute, its authors likely had not conceived of the need to use intelligence assets to protect U.S. citizens from terrorism. Perhaps it is time Posse Comitatus be revised to include language specific to the problem set this thesis addresses. An update to Posse Comitatus should include language that allows for the use of both state active duty (SAD) personnel in homeland security roles and highly trained SOF personnel to augment existing counterterrorism capabilities.[172] As with JTF Empire Shield, under presidential authorization, military forces could augment local law

---

167 Foreign Intelligence Surveillance Act of 1978, Public Law 95–511; 92 Stat. 1783; approved October 25, 1978 as amended through Pub. Law No. 114–23, enacted June 2, 2015; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. Law. No. 107-56, 115 Stat. 272 (2001).

168 Burch, "Domestic Intelligence Gap," 5, 21.

169 John B. Alexander, *Convergence: SOF and Civilian Law Enforcement* (Report 10-6) (Washington, DC: Joint Special Operations University, 2010), https://www.hsdl.org/?view&did=692827.

170 Ibid., 4.

171 JCS, JP *Joint Task Force Headquarters*, VI-1.

172 State of New York, *Joint Task Force Empire Shield* (New York: State of New York, 2017), http://dmna.ny.gov/blog/resources/jtfes_info.pdf.

enforcement at all major airports and other critical infrastructure locations. An additional provision to Posse Comitatus should also allow SOF capabilities to augment various CT missions supporting local enforcement on individuals with a nexus to terrorism in either an advisory/training capacity or in supporting actual prevent/capture missions.[173]

Additionally, in order to support intelligence-reform, Title 10 and Title 50 likely need modification. Both Title 10 and 50 clarify the roles of the U.S. Secretary of Defense. Title 10 describes the authorities of the DOD for military operations while Title 50 describes the extent of intelligence activities in covert versus overt operations.[174] While Title 10 currently allows for the establishment of state and federal military coordination in support of JTTFs, further authorities may be needed for establishing collaborative planning and operational cells across FSLTT domains.[175] Combining these authorities for counterterrorism purposes would allow highly trained SOF operators to serve as advisors to local partners' interdiction and counterterrorism operations while also leveraging the teams-of-teams concept with integrated intelligence community support. Each entity would then retain its authority under existing law. When cells disagree on intelligence and operational decision making for any given target, a briefing at the highest classification possible for all senior leader stakeholders would aid the final operational decision-making process. The roles of NSA and DIA also need revisiting in a revised Title 50. Title 50 establishes and defines the authorities of two of the largest intelligence agencies. Along with EO 12333, Title 50 could enable these intelligence agencies to leverage their vast capabilities to support domestic counterterrorism operations under a hybrid SOF–local law enforcement model.[176]

There may be an added mutual benefit to this type of augmented SOF–local law enforcement relationship. In *Convergence: SOF and Civilian Law Enforcement*, Jon B. Alexander describes how the escalation of threat actor capabilities, both foreign and

---

173 Ibid.

174 Andru E. Wall, "Demystifying the Title 10-Tile 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 3, no. 1 (2011): 100.

175 JCS, *Joint Task Force Headquarters*, E-1, E-2.

176 Wall, "Demystifying," 99.

domestic, has blurred the lines between wholly military and law enforcement capabilities.[177] To meet the growing challenge of gathering intelligence and targeting terrorist networks, SOF has had to seek law enforcement–style warrants for the first time in history. In foreign sustainment operations, SOF has also been involved in law enforcement–style policing operations.[178] Both missions are not something SOF has ever trained for in the past.[179] Domestically, law enforcement agencies have encountered extremely well-armed threat actors and have had to deploy military-style capabilities without the benefit of the highly specialized training SOF receives. By updating Posse Comitatus, Title 10, and Title 50 of the U.S. Code, the SOF and law enforcement communities could forge better joint training and operational relationships that add to the capabilities of their independent but related missions.

4. Revise PM ISE's Roles

Today, while some lone intelligence community agencies share intelligence, they still tend to make operational decisions independent of a joint environment. A revamped PM ISE should aid intelligence sharing with local officials as part of the National Security Council or the National Intelligence Council. In addition, the PM ISE should review highly classified intelligence community intelligence on international and domestic threats and direct that intelligence to the hybrid SOF–law enforcement cells, which could then begin real-time mission planning. Moreover, a new ODNI with improved authorities could ensure intelligence community compliance with PM ISE tasking. As previously discussed, a revised information-sharing concept works only if local jurisdictions have more access to SCIFs and more collaboration with field intelligence assets across the FSLTT domain. Then, the PM ISE would move from being a policy advocate to having a more hands-on role of implementing and directing information sharing. The counterterrorism community has the technology to

177 Alexander, *Convergence*, 4–5.

178 Ibid., 27–29.

179 Ibid.

communicate in real-time across the globe; it should be able to communicate locally and collaborate on local terrorism threats.

C. FINAL CONSIDERATIONS

This thesis considers the current global and national terrorism threat as one that has grown only since 9/11. Successful domestic terrorist attacks in the years 2014 through 2017 have revealed cracks in the current approach to domestic counterterrorism. Yet our nation has experienced success internationally in targeting terrorists using the team-of-teams approach. This thesis has proposed a more unified approach to counterterrorism that merges the best capabilities from military, federal, and local approaches. To accomplish reform, the nation needs to rebuild trust in the intelligence community, solidify the roles of the ODNI and PM ISE, and build on operational successes. Opponents of the proposed changes to ODNI may argue that to do so would effectively eliminate the capability for intelligence community agencies to disagree independently with the ODNI. This may lead to entrenching hierarchical relationships between the ODNI and the intelligence community heads, thereby hurting collaboration and alternative analysis. Perhaps any legislative update of ODNI authorities over the intelligence community heads need only include language relevant to information-sharing equity. Congress could give the ODNI budgetary authority over intelligence-community information-sharing programs while developing options for increased research and development in multi-domain information-sharing technologies. By having control over all budgetary decisions for information sharing in the intelligence community, the ODNI and its ISE PM would have clearer accountability for information sharing lapses and a faster ability to reform or develop domestic information-sharing programs.

For agencies at the local level, existing intelligence-sharing mechanisms work. One case study in particular highlights what can be accomplished through the PM ISE's office. Hocevar et al. reviewed the role the PM ISE had in sponsoring a framework called multimodal information sharing team (MIST), for collaborative information-sharing

across the transportation port domain.[180] The MIST program was designed to bring the multiple stakeholders across the Port of Baltimore's interdependent transportation domain into one intelligence-sharing framework. As the sponsor for MIST workshops, PM ISE held several meetings and made recommendations that helped actualize its core objectives:

- Advance responsible information sharing to further counterterrorism and homeland security missions.
- Improve nationwide decision making by transforming information ownership to stewardship.
- Promote partnerships across federal, state, local and tribal governments, the private sector and internationally.[181]

Over 30 organizations participated in the workshops, which helped the Port of Baltimore identify core information sources, systems, and approaches to better share sensitive but unclassified (SBU) information.[182] While similar information-sharing forums alone fall short of the recommendations of this thesis, the MIST framework does demonstrate the hands-on approach the PM ISE would take if a national SOF–law enforcement cell concept came to fruition. The PM ISE could operationalize the MIST model on a national scale to increase multimodal information-sharing across the nation. However, as successful as MIST was, its achievements in increasing information sharing in the Baltimore Port were confined to that narrow domain. The strategic, tactical, and technological challenges that remain for the ISE should be addressed by updating several pieces of related legislation, subsequent orders, and policies as previously outlined.

Lastly, reimagining counterterrorism operations means that no single federal agency would be responsible for terrorism investigations and prevention. However, reform may mean a more collaborative multiagency approach with an interdependent,

180 Susan Page Hocevar et al., *Multimodal Information Sharing Team (Mist)—Port of Baltimore Industry and Public Sector Cooperation for Information Sharing* (Naval Postgraduate School, Monterey, CA, 2012), http://calhoun.nps.edu/handle/10945/30398, 1. Note: Port multimodal domains can best be defined as multiple modes of transportation (aviation, maritime, surface, rail, etc.) that intersect and cross-leverage the maritime port domain, as describes in the above referenced thesis.

181 Ibid., 2.

182 Ibid.

multijurisdictional mission area that combines the nation's best operators and collaborative activities. As John Miller explains, "Everything that's working right now is working really well."[183] Nevertheless, Miller suggests the culture of the intelligence community needs to change as there is still a strong belief that "information is power."[184] Until that dynamic across government changes, the potential political will to enforce implementation and compliance for intelligence-sharing reform is unlikely. Programs such as the intelligence community's A-Space, Razor, and Catalyst, as outlined by Miller, were designed to help analysts share and communicate with one another.[185] However, following the noteworthy cases involving leaks of national security intelligence, these programs have been shuttered.

Perhaps deliberate and comprehensive intelligence reform could reignite investment in new technologies that enable collaboration while protect classified national security intelligence from leaks and espionage. In a recent interview for a WNYC podcast, Miller encapsulates some of the complexities regarding intelligence reform:

> If you look at the history of intelligence and policing … having rules and structure, even rules that … make your job harder sometimes, those rules are your friend. Intelligence collection in a free and democratic society without strict rules always ends up running aground.[186]

Intelligence reform must strike a careful balance between enabling collection and collaboration—yet occur within the limits of protecting the freedoms that our Constitution guarantees.

---

[183] Miller, interview.

[184] Ibid.

[185] Ibid.

[186] Preet Bharara. interview with John Miller, *Stay Tuned with Preet*, October 5, 2017, http://www.wnyc.org/shows/preetbharara?modal=queue-history.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alexander, John B. *Convergence: SOF and Civilian Law Enforcement* (Report 10-6). Washington, DC: Joint Special Operations University, 2010. https://www.hsdl.org/?view&did=692827.

Berman, Mark, Ellen Nakashima, and Matt Zapotosky. "The FBI Looked into Suspected Bomber Ahmad Rahami in 2014 and Found No 'Ties to Terrorism.'" *Washington Post*, September 19, 2016. https://www.washingtonpost.com/news/post-nation/wp/2016/09/19/bombing-suspect-charged-with-attempted-murder-of-a-law-enforcement-officer-with-further-charges-expected/?utm_term=.445b66e78642.

Bjelopera, Jerome P. *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress* (CRS Report No. 7-5700). Washington, DC: Congressional Research Service, 2011. https://fas.org/sgp/crs/intel/R40901.pdf.

Bowling, Zach. "DNI: Fiscal Challenges and Snowden Leaks Created 'Perfect Storm.'" *Homeland Security Today*, September 30, 2014. http://www.hstoday.us/single-article/dni-fiscal-challenges-and-snowden-leaks-created-perfect-storm/de6feaa607915b03c637cbcafb32cb1e.html.

Burch, James. "The Domestic Intelligence Gap: Progress Since 9/11?" *Homeland Security Affairs XII Proceedings of the 2008 Center for Homeland Defense and Security Annual Conference* (April 2008). https://www.hsaj.org/articles/129.

Busch, Nathan E., and Austen D. Givens. "Information Sharing and Public-Private Partnerships: The Impact on Homeland Security." *The Homeland Security Review* 7, no. 2 (2013): 123–150.

Connors, Edward. *Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement*. Washington, DC: U.S. Department of Justice, Institute for Law and Justice, 2007. https://www.hsdl.org/?view&did=482649.

Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond*. Washington DC: Georgetown University Press, 2013. Kindle edition.

———. "Local Approaches to Counterterrorism: The New York Police Department Model." *Journal of Policing, Intelligence and Counter Terrorism* 9, no. 2 (2014): 81–97.

Gerber, Burton, and Jennifer E. Sims. *Transforming U.S. Intelligence*. Washington DC: Georgetown University Press, 2005. Kindle edition.

Heuer, Richards J. *Psychology of Intelligence Analysis*. Langley, VA: Center for the Study of Intelligence, 1999. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/.

Hocevar, Susan Page, Wendy Walsh, Anita Salem, and Lyla Englehorn. *Multimodal Information Sharing Team (Mist)—Port of Baltimore Industry and Public Sector Cooperation for Information Sharing*. Naval Postgraduate School, Monterey, CA, 2012. http://calhoun.nps.edu/handle/10945/30398.

House Committee on Homeland Security. "Chairman McCaul's Inaugural "State of Homeland Security Address." December 7, 2016. https://homeland.house.gov/event/state-of-homeland-security-address.

———. "The Islamist Terror Threat." *Terror Threat Snapshot* (November 2015). https://homeland.house.gov/wp-content/uploads/2015/11/November-Terror-Threat-Snapshot.pdf.

Joint Chiefs of Staff. *Joint and National Intelligence Support to Military Operations* (Joint Publication 2-01). Washington, DC: Joint Chiefs of Staff, 2004. http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf.

———. *Joint Intelligence* (Joint Publication 2-0). Washington, DC: Joint Chiefs of Joint Staff, 2013. http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.

———. *Joint Tactics, Techniques, and Procedures for Special Operations Targeting and Mission Planning* (Joint Publication 3-05.2). Washington, DC: Joint Chiefs of Staff, 2003. http://www.bits.de/NRANEU/others/jp-doctrine/jp3_05_2.pdf.

———. *Joint Task Force Headquarters* (Joint Publication 3-33). Washington, DC: Joint Chiefs of Staff, 2012. http://www.dtic.mil/doctrine/new_pubs/jp3-33.pdf.

———. *National Intelligence Support to Joint Operations* (Joint Publication 2-02). Washington, DC: Joint Chiefs of Staff, 1998. https://fas.org/irp/doddir/dod/jp2_02.pdf.

Joint Special Operations University. *Special Operations Forces Reference Manual*. 4th ed. MacDill AFB, FL: Joint Special Operations University Press, 2015. http://jsou.socom.mil/JSOU%20Publications/2015SOFRefManual_final_cc.pdf.

Johanson, II, David R. "The Long and Winding Road: Post-9/11 Intelligence Reforms a Decade Later." Master's thesis, Naval Postgraduate School, 2013.

Lederman, Gordon Nathaniel. "Restructuring the Intelligence Community." In *The Future of American Intelligence*, edited Peter Berkowitz, 65–102. Palo Alto, CA: Hoover Institution Press, 2005.

Lose, James M. “National Intelligence Support Teams, Fulfilling a Crucial Role.” Central Intelligence Agency. Accessed October 15, 2017. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter99-00/art8.html.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington DC: CQ Press, 2011. Kindle edition.

Major Cities Chiefs Association. *Criminal Intelligence Enterprise Initiative*. Major Cities Chiefs Association, 2012. https://majorcitieschiefs.com/pdf/news/mcca_criminal_intelligence_enterprise_initiative_20120329.pdf.

McCaul, Michael. “The Terrorist Exodus: Resurgent Radicalism and the Threat to the West.” Lecture, George Washington University, May 2016. https://homeland.house.gov/wp-content/uploads/2016/05/The-Terrorist-Exodus.pdf.

———. *A National Strategy to Win the War against Islamist Terror*. Washington, DC: House Homeland Security Committee National Strategy, 2016. https://homeland.house.gov/wp-content/uploads/2016/09/A-National-Strategy-to-Win-the-War.pdf.

McChrystal, Stanley, Tatum Collins, David Silverman, and Chris Fussell. *Team of Teams: New Rules of Engagement for a Complex World*. New York: Penguin, 2015. Kindle edition.

McGhee, G. C. Sam. “The Wicked Problem of Information Sharing in Homeland Security: A Leadership Perspective.” Master’s thesis, Naval Postgraduate School, 2014. https://www.hsdl.org/?view&did=756782.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton & Company, Inc. 2004.

NYPD News. “Operation Sentry: A Counterterrorism Coalition.” November 10, 2015. http://nypdnews.com/2015/11/operation-sentry-a-counterterrorism-coalition.

Posner, Richard A. *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11*. Lantham, MD: Rowman & Littlefield Publishing Inc., 2005.

Program Manager Information Sharing Environment. *2016 Information Sharing Environment Annual Report to Congress*. Washington, DC: Program Manager Information Sharing Environment, 2016. http://www.ise.gov/annual-report/year-review.

Office of the Director of National Intelligence. *Application of Dissemination Controls: Originator Control* (Intelligence Community Policy Guidance 710.1). Washington, DC: Office of the Director of National Intelligence, 2012.

———. *The National Intelligence Strategy of the United States of America*. Washington, DC: Office of the Director of National Intelligence, 2014. http://www.dni.gov/files/documents/2014_NIS_Publication.pdf.

———. *The National Intelligence Strategy of the United States of America Transformation through Integration and Innovation*. Washington, DC: Office of the Director of National Intelligence, 2005. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/NISOctober2005.pdf.

———. *Sensitive Compartmented Information Facilities* (Intelligence Community Directive No. 705). Washington, DC: Office of the Director of National Intelligence, 2010. https://www.dni.gov/files/documents/ICD/ICD_705_SCIFs.pdf.

Office of the Director of National Intelligence, Program Manager Information Sharing Environment. *A Brief History of the Information Sharing Environment*. Washington, DC: Information Sharing Environment 2015. https://www.ise.gov/sites/default/files/Brief_History_of_the_ISE.pdf.

Office of the White House Press Secretary. *Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment*. Washington, DC: White House, 2005. https://www.archives.gov/cui/training/awareness/includes/references/prsmem_121605.pdf.

State of New York. *Joint Task Force Empire Shield*. New York: State of New York, 2017. http://dmna.ny.gov/blog/resources/jtfes_info.pdf.

Strohm, Chris. "FBI Gives Its Version of How the Orlando Shooter Slipped Through." *Bloomberg*, June 13, 2016. http://www.bloomberg.com/politics/articles/2016-06-13/law-enforcement-released-orlando-shooter-after-finding-no-threat.

Svendsen, Adam D. M. "The Federal Bureau of Investigation and Change: Addressing US Domestic Counter-terrorism Intelligence." *Intelligence and National Security* 27, no. 3 (2012): 371–397. doi: 10.1080/02684527.2012.668080.

U.S. Department of Homeland Security. *The 2014 Quadrennial Homeland Security Review Report*. Washington, DC: U.S. Department of Homeland Security, 2014. https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

———. *National Network of Fusion Centers Final Report*. Washington, DC: U.S. Department of Homeland Security, 2012. https://www.dhs.gov/sites/default/files/publications/2012%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf.

U.S. Government Accountability Office. *Information Sharing Environment Better Road Map Needed to Guide Implementation and Investments* (GAO-11-455). Washington, DC: U.S. Government Accountability Office, 2011. http://www.gao.gov/assets/330/321672.pdf.

———. *Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others* (GAO-17-317). High-Risk Series. Washington, DC: U.S. Government Accountability Office, 2017. http://www.gao.gov/assets/690/682765.pdf.

———. *High-Risk Series an Update, Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland* (GAO 15-290). Washington, DC: U.S. Government Accountability Office, 2015. http://www.gao.gov/assets/670/668415.pdf.

Wall, Andru E. "Demystifying the Title 10-Tile 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harvard National Security Journal* 3, no. 1 (2011): 85–142.

Williams, Linda B. *Intelligence Support to Special Operations in the Global War on Terrorism*. Carlisle Barracks, PA: U.S. Army War College, 2004. handle.dtic.mil/100.2/ADA424015.

Zegart, Amy B. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton: Princeton University Press, 2009. Kindle edition.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California