

2017

A Duty to Share: The Opportunities and Obstacles of Federal Counterterrorism Intelligence Sharing with Nonfederal Fusion Centers

Jeffrey V. Gardner
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

 Part of the [Public Policy Commons](#)

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Jeffrey Gardner

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee

Dr. Eliesh Lane, Committee Chairperson,
Public Policy and Administration Faculty

Dr. David Milen, Committee Member,
Public Policy and Administration Faculty

Dr. Tanya Settles, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

A Duty to Share: The Opportunities and Obstacles of Federal Counterterrorism
Intelligence Sharing with Nonfederal Fusion Centers

by

Jeffrey V. Gardner

MS, National Intelligence University, 2005

MMAS, U.S. Army Command and General Staff College, 2004

MS, Troy University, 2001

BA, Norwich University, 1991

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2017

Abstract

Little is known about how effectively federal agencies share terrorism intelligence with state and local governments through fusion centers. As a result, there is a risk that local governments do not receive critical intelligence that would allow them to collaboratively prevent catastrophic terrorist attacks. Using Dawes' interagency information sharing model, the purpose of this exploratory case study was to evaluate how effectively federal agencies share terrorism intelligence with fusion centers. Data were collected through interviews with 25 senior leaders, federal agents deployed to fusion centers, and intelligence analysts in 5 fusion centers on the East Coast. These data were inductively coded and then subjected to a thematic analysis procedure. Findings indicated that, among these leaders, information sharing was hindered by both technology and inter-organizational relationships between the fusion centers and federal agencies. Participants also noted that obstacles to information sharing regarding classified data has not been sufficiently mitigated. Dawes' interagency information-sharing theory was found to be explanatory regarding intelligence sharing activities. Implications for positive social change include recommendations to the Department of Homeland Security to utilize Dawes' work on information sharing in order to alleviate the tension between federal and local agencies and remove obstacles, particularly related to classified intelligence related to counterterrorism. Doing so can be useful in developing policy recommendations to improve the dynamics between federal and local agencies, thereby allowing critical information to be shared with state and local governments in a proactive manner that may better protect communities.

A Duty to Share: The Opportunities and Obstacles of Federal Counterterrorism

Intelligence Sharing with Nonfederal Fusion Centers

by

Jeffrey V. Gardner

MS, National Intelligence University, 2005

MMAS, U.S. Army Command and General Staff College, 2004

MS, Troy University, 2001

BA, Norwich University, 1991

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2017

Dedication

This dissertation is dedicated to my God for *I can do everything through him who gives me strength*. Philippians 4:13

Acknowledgements

This dissertation would not have been possible if it were not for the cooperation and assistance of some key individuals. I want to thank all three of my committee members who mentored me in this long process and provided great inspiration. In particular, my chair, Dr Lane, was always encouraging and upbeat and greatly assisted in getting me through all the wickets. I would also like to thank Mr Mike Sena, the President of the National Fusion Center Association, who gave advice and advocated for this research to targeted fusion center directors.

I would like to thank the participants in this study who volunteered their time to be interviewed and contributed to furthering the body of empirical knowledge on fusion centers. I would also like to highlight a few very important individuals who went many steps farther to personally assist me with furthering this study. These few fusion center directors and federal agency embedded professionals not only took the risk of allowing me to conduct sensitive and controversial interviews of their personnel, but they went out of their way to provide introductions to other fusion centers, leveraging their professional contacts and putting their own personal reputations on the line to further this study. While I cannot name them due to our confidentiality and anonymity agreements, they know who they are, and I appreciate their trust in me and I wholeheartedly thank those great Americans for their assistance and professionalism.

Table of Contents

List of Tables	vi
List of Figures	vii
Chapter 1: Introduction to the Study.....	1
Background.....	1
Problem Statement.....	2
Purpose of Study.....	3
Research Outlook.....	4
Conceptual Framework.....	5
Research Questions.....	5
Limitation and Delimitations of Study	6
Definition of Key Terms.....	6
Data, Information, and Intelligence	6
Terrorism.....	8
State and Local.....	8
Significance of Study.....	9
Summary.....	10
Chapter 2: Literature Review	12
Introduction.....	12
Literature Search Strategy.....	12
Roles and Functions of Intelligence.....	14
The Intelligence Cycle	16

National and Foreign Intelligence.....	17
Operational, Tactical, and Actionable Intelligence.....	19
Domestic Intelligence and Homeland Security Information/Intelligence	21
The September 2001 al Qaeda Terrorist Attacks and Information-sharing	
Failures.....	24
Internal Federal Agency Information-Sharing Failures	24
Subfederal Information-sharing Failures	26
Terrorism Threats and Counterterrorism	27
Terrorism Threats to the Homeland.....	28
Countering Terrorism in the United States	30
Domestic Security and the Role of State and Local Agencies.....	32
Federalism and Intergovernmental Relations for Domestic Security	33
Interagency Challenges with Roles, Missions and Jurisdiction.....	35
Importance of State and Local Agencies in Combatting Terrorism	38
Domestic Counterterrorism Reforms	39
Creation of the Department of Homeland Security	40
Creation of the Director of National Intelligence	43
Creation of the National Security Branch within the FBI.....	45
Nonfederal Nonfederal Fusion Centers	52
History of Fusion Centers	53
Military Counterterrorism Fusion Centers.....	55
Fusion Centers Evolve	56

The Body of Fusion Center Research	58
Interorganizational Intelligence and Information-sharing	59
Theoretical Framework for Interorganizational Information-sharing.....	60
Domestic Counterterrorism Information-sharing	63
Obstacles to Domestic Interagency Information-sharing	65
Information-sharing Lapses at Fort Hood and Boston.....	68
Fusion Centers and Information-sharing	70
Fusion Centers and JTTFs	74
Summary	76
Chapter 3: Research Methodology.....	78
Introduction.....	78
Research Design.....	78
Site Selection, Sampling Size, and Participants.....	79
Site Selection and Sampling Size	80
Participants.....	82
Interviews.....	82
Data Collection and Analysis.....	83
Role of the Researcher, Bias Mitigation and Validity	84
Ethical Protection and Confidentiality of Participants.....	86
Data Storage.....	87
Conclusion	87
Chapter 4: Results.....	89

Introduction.....	89
Study Sample Process	89
Data Collection Method.....	91
Study Sample Description.....	94
Interview Questions Background.....	96
Analysis of the Data.....	96
Collective Participant Responses to Federal Terrorism Intel Sharing Questions.....	97
Comparison of Leader Responses to Other Fusion Center Personnel	117
Comparison of Responses by Profession: Intelligence vs Law Enforcement.....	118
Comparison of Responses by Longevity	119
Comparison of Responses by Type of Fusion Center.....	120
Validity, Credibility, and Confirmability.....	122
Findings and Enumeration	123
Research Question 1: How effectively are fusion centers receiving terrorism intelligence from federal agencies?.....	124
Research Question 2: What are the opportunities or benefits of federal CT info/intel sharing with fusion centers?	126
Research Question 3: What are the obstacles or barriers of federal CT info/intel sharing with fusion centers?	128
How federal sharing really occurs with fusion centers	131
Summary.....	133

Chapter 5: Discussion, Conclusions, and Recommendations	134
Introduction.....	134
Interpretation of Findings	134
Implications for Positive Social Change.....	138
Recommendations.....	139
Embed more federal representative from DHS and FBI in fusion centers	139
Embed more fusion center personnel in JTTFs	141
Assess the real mechanisms for intelligence sharing: Relationships	142
Focus fusion center directors on relationships.....	143
Employ open collaborative work environments	144
Improve tailoring intelligence for state and local partners	145
Mandate intelligence sharing on terrorism to state and local fusion centers	146
Recommendations for Future Research	146
Implications for Positive Social Change.....	149
Summary	150
References.....	152
Appendix A: Background Questions and Interview Questions	194
Appendix B: Participant Backgrounds By Site and Totals.....	197

List of Tables

Table 1. Overlapping Government Responsibilities in Domestic Security	37
Table 2. Categories of benefits and barriers associated with interagency information-sharing	61
Table 3. Study Participants by Fusion Center Role	94
Table 4. Interview questions subordination to research questions	123
Table 5. Obstacles to federal intelligence sharing with fusion centers	130

List of Figures

Figure 1. Data, information, and intelligence	7
Figure 2. Sharing with and within a fusion center	74

Chapter 1: Introduction to the Study

Background

On September 11, 2001, the terrorist attacks on the United States (abbreviated “9/11”) highlighted a number of gaps in the efforts of many different departments and agencies charged with securing the nation, as well as a lack of effective interagency and intergovernmental terrorism information-sharing. One of the many government reform efforts that these attacks brought about in the United States was the collection of 22 different federal domestic security agencies into a new Department of Homeland Security (DHS). The department was specifically tasked to prevent future terrorist attacks and to better share information on terrorism threats (U.S. Congress, 2002, PL 107–296 § 201, 9). DHS was also charged with ensuring that state and local officials received information from DHS as well as classified threat intelligence from other federal security agencies (Bush, 2003).

DHS thus began supporting the establishment and growth of multi-agency intelligence fusion centers owned and hosted by state and local officials around the country. These fusion centers were intended to provide a framework for subfederal agencies to be able to receive intelligence from federal agencies, and offer a mechanism to collect reports from agencies within the jurisdiction itself (Lewandowski, Carter & Campbell, 2017). The collective assemblage of DHS sponsored fusion centers owned by state and local agencies has evolved into an unofficial national network.

However, the Federal Bureau of Investigation (FBI) was not among the 22 federal domestic security agencies incorporated into DHS; they retained and actually greatly

amplified their preexisting role as the nation's domestic counterterrorism agency (Department of Justice, 2005; Treverton, 2008). In increasing their domestic counterterrorism efforts, the FBI rapidly expanded its separate network of Joint Terrorism Task Forces (JTTFs) around the country. This network has sometimes been in competition with fusion centers in disseminating information and intelligence to state and local officials (Cordner & Scarborough, 2010; Eack, 2008). The separate DHS and FBI information-sharing mandates and mechanisms overlap in multiple areas, which has created a bifurcated and ineffective dual track for federal counterterrorism information-sharing with subfederal security officials.

Problem Statement

Despite efforts by DHS and the FBI, a U.S. Government Accountability Office report found that “effective mechanisms for sharing information—a best practice in building successful information-sharing partnerships—had not been established” (Larence, 2009, p. 23). This is not a new problem; many public policy scholars, such as Dawes (1996), have found that “Despite the potential benefits, successful interagency information-sharing is difficult to achieve” (p. 379). Even today domestic counterterrorism interorganizational information-sharing remains suboptimal, as demonstrated by recent undetected terrorist activities like the 2009 Fort Hood attack, the attempted 2010 Times Square attack, the 2013 Boston marathon bombings and the March 2017 Review of Domestic Sharing of Counterterrorism Information (Mayer, Carafano, & Zuckerman, 2011; Reilly, 2013; McCaul & Keating, 2014; U. S. Department of Justice, 2017).

The 9/11 Commission Report stated that agencies needed to change the culture from a “need to know” mindset to one of having a “duty to share” this terrorism threat information that was acquired at taxpayer expense (Kean & Hamilton, 2004, p. 417). This study explored how federal agencies are fulfilling their duty to share terrorism information with state and local officials through the network of state and major urban area fusion centers. However, the literature review showed there is very little empirical research about this counterterrorism information-sharing and none that examined federal agencies sharing their terrorism information and intelligence with fusion centers. Thus, the problem is that the sharing of terrorist threat information and intelligence from federal agencies to state and local fusion centers remains suboptimal. This hampers the prevention of terrorism and presents vulnerabilities that have allowed catastrophes such as the 9/11 terrorist attacks and the 2013 Boston bombings to succeed (Barron, Lewis, Silberstein, & Shapiro, 2016; Kean & Hamilton, 2004; Reilly, 2013; Zamora, 2014).

Purpose of Study

The purpose of this study was to examine the opportunities and obstacles of sharing federal counterterrorism information with state and local officials. The research identified the prospects and barriers that the State and Local Fusion Center (SLFC) model provides for federal agency intelligence sharing with state and local partners about terrorist threats. This study examined the subfederal SLFC model to assess its viability as a framework for interorganizational domestic counterterrorism intelligence sharing from federal agencies to state and local partners. The study identified some of the effective sharing practices of SLFCs as well as the various impediments that prevent optimal

intelligence sharing. This study has significant implications for social change.

Information-sharing is a critical function that the government should be fully leveraging to improve homeland security and thus improve protection for citizens.

Research Outlook

Since a laboratory setting is not appropriate to study how these agencies interact, a qualitative case study was used to reach practitioners on their own terms and to examine a program or process in depth (Yin, 2009). The case study method allowed for the study of a bounded issue, such as domestic counterterrorism information-sharing, using multiple sites and multiple data sources (Maxwell, 2012).

This study was conducted as an exploratory qualitative case study. 25 officials at five fusion centers on the East Coast of the United States were interviewed. The fusion centers selected include a proportional mix of both state and regional major urban area fusion centers. Major U.S. cities are high-value targets for terrorists because they have significant population density and critical infrastructure. Conducting research at a major city also offers the opportunity to include a critical case and exemplar, where “if it doesn’t happen there, it won’t happen anywhere” (Patton, 2002, p. 236).

In order to gain access to the fusion centers and to enable participants to provide their candid opinions, the fusion centers and the interviewees will remain anonymous. Five individuals were interviewed at each site. Each participant was asked four main questions and eight amplifying questions, the interviews averaged 30 minutes. This qualitative research design with open-ended questions constituted a framework for analyzing responses discovering trends and patterns.

Conceptual Framework

This domestic interorganizational counterterrorism study was analyzed using Dawes (1996) conceptual framework of interagency information-sharing to identify the benefits and risks of intelligence sharing with nonfederal organizations. This study applied this theoretical model to ascertain how officials and analysts from various agencies represented within subfederal fusion centers view the opportunities of information-sharing as well as the obstacles or costs to more effective sharing. While other studies have looked at the benefits and risks of information-sharing, none have done so in relation to federal counterterrorism intelligence with state and local officials (Carter, Carter, Chermak & McGarrell, 2016; Drake, Steckler, & Koch, 2004; Bigdeli, Kamal, & Cesare, 2013; Graphia, 2010; Landsbergen & Wolken, 2001; Lewandowski, Carter & Campbell, 2017).

Research Questions

1. How effectively are fusion centers fulfilling their intended purpose of improving homeland security by receiving terrorism information and intelligence from federal agencies?
2. What are the opportunities in, or benefits of, federal counterterrorism intelligence sharing with fusion centers?
3. What are the obstacles or barriers to federal counterterrorism intelligence sharing with fusion centers?

Limitation and Delimitations of Study

The study has multiple delimitations related to the sensitive nature of domestic counterterrorism operations as well as ongoing intelligence and law enforcement operations. While a number of information technology systems and architectures are mentioned, this study is unclassified; it contains no information that is law enforcement sensitive (LES) and does not discuss how terrorism information is shared. This study is also limited to federal intelligence sharing with subfederal agencies and does not discuss how information or intelligence is analyzed or used within the fusion centers, nor how it is further disseminated.

Privacy and civil liberties have been a frequent issue with information and intelligence sharing, and they are a particularly controversial topic with regard to state and local fusion centers (German & Stanley, 2007; Hylton, 2009; Skahill, 2010). However, these topics have already been the subject of numerous studies; many government programs now exist to protect privacy and individual freedoms--along with significant oversight programs to monitor their progress. While not minimizing these very important topics, privacy and civil liberty issues were not addressed in this study.

Definition of Key Terms

Data, Information, and Intelligence

With government information-sharing, the terms *data*, *information*, and *intelligence* are often used interchangeably (Palmieri, 2005). But this is incorrect. There are significant differences between all three terms; having access to data from a federal agency is very different from sharing actionable intelligence (Treverton, 2008;

Department of Justice, 2006). Government agencies collect volumes of data from various and multiple sources, but much of it is not in a useful form. However, when that data is processed—for example, when documents or wire taps are translated from a foreign language—it is converted into information. However, this information is considered *raw* and it may or may not be useful in the context of homeland security. To make the information useful, a variety of other sources of information often need to be considered and analysis is needed to turn the information into intelligence. See Figure 1 for a depiction of these relationships.

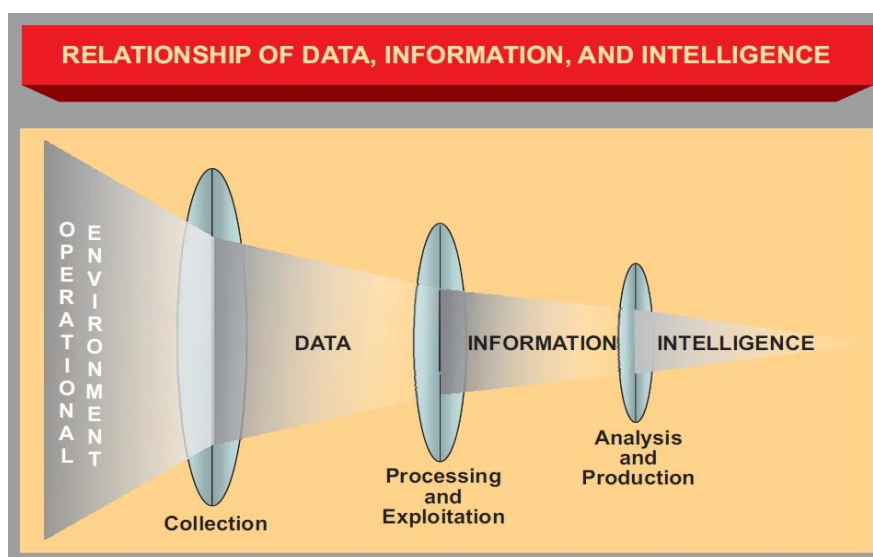


Figure 1. Data, information and intelligence. (Joint Chiefs of Staff, 2013, p. I-2).

The definition of intelligence provided by Carter (2009) to the Department of Justice for use by state and local law enforcement agencies states that intelligence means “Analysis of raw information to provide synergistic knowledge about a threat” (p. 10). This definition emphasizes intelligence as both a process and a product. Other aspects of intelligence are discussed in more detail in Chapter 2. For the purposes of this research,

intelligence means to convey sensitive information about threats (Tromblay, 2016). At times such intelligence will be fragmentary, such as a single report of suspicious activity by a particular individual, or it may be more refined, such as detailed analysis of terrorist attack trends or bomb-making techniques. Additionally, in the context of federal sharing with nonfederal fusion centers, there is an expectation that the intelligence these federal agencies share is always sensitive and often classified, so that recipients must have appropriate security clearances and secure means to receive it.

Terrorism

The United States Congress defines terrorism in law under Title 22 as a crime that is “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents” (U.S. Congress, 2012, 22 U.S. Code Chapter 38 § 2656fd). The Federal Bureau of Investigation (FBI) gets more specific and defines terrorism as “the unlawful use, or threatened use, of force or violence by a group or individual...to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives” (FBI, 2005, p. v). For the purpose of this research, this study used a hybrid definition for terrorism—the planned, threatened or use of illegitimate violence primarily against innocent people to achieve the psychological effect of fear or for political or other ideological purposes (Bruce, 2013, p. 27).

State and Local

There are many different descriptions for the subfederal levels of government. For the purpose of this research any major jurisdiction directly below the federal level such as

state, commonwealth or federal territory will be considered a state for definitional purposes. Any substate or jurisdiction smaller than a state such as a city, county, or tribal territory will be termed the local level. The terms city or major urban area are used interchangeably with the term local in this research.

Significance of Study

This study contributes to the body of knowledge by exploring the current state of intergovernmental terrorist threat information-sharing between federal agencies and state and local fusion centers. The 2012 National Strategy for Information-sharing and Safeguarding stated that connecting related information from different agencies “can mean the difference between identifying a threat during the planning stage or analyzing what could have been done to thwart the attack after it occurs” (National Security Council, 2012, p. 10). This study is significant as effective sharing of federal terrorism intelligence with state and local officials may have prevented terrorist attacks such as those on September 11th 2001, the 2009 Fort Hood Shooting, as well as the 2013 Boston Marathon Bombings (Reilly, 2013). By identifying the opportunities and obstacles to effective terrorism intelligence sharing this study advances the body of knowledge to better protect citizens.

Very little research into counterterrorism information-sharing exists, and no empirical research has studied the effectiveness of federal intelligence sharing with state and local officials. The topics of information-sharing and fusion centers have mainly been examined only in the briefest manner. Most studies into fusion centers examined dissemination and only down sharing to customers like state troopers (Ratcliffe &

Walden, 2010). Also, a fusion center study in 2016 stated, “Few scholars have gained access to fusion centers and begun to examine the intelligence process within these organizations” (Carter, Carter, Chermak & McGarrell, 2016, p.2).

Intelligence sharing with state and local officials is especially important to counter terrorism in this era of internet radicalization and the proliferation of the means to commit terrorist acts. As Larence (2011) stated that, “The federal government recognizes that fusion centers represent a critical source of local information about potential threats, including homegrown terrorism, and a means to disseminate terrorism-related information and intelligence from federal sources” (p. 10). This present study is significant because it reveals the barriers to effective counterterrorism information-sharing; if the barriers are mitigated, it would help to prevent future attacks and likely save lives.

Summary

Terrorists and their violent attacks on innocent Americans are a threat that will likely never go away (Treverton, 2008, p. 107). Thus, government agencies must continue to improve homeland security efforts and interorganizational cooperation among the agencies. This exploratory case study of fusion centers on the East Coast offered new knowledge about the effectiveness of sharing federal terrorism threat information with state and local officials. This is a unique area of research and is expected to identify the obstacles that prevent optimal sharing with nonfederal fusion centers. This examination of the critical issue of information and intelligence sharing between federal agencies and

subfederal fusions center offers an opportunity to significantly improve how citizens are protected in the United States.

Chapter 2: Literature Review

Introduction

This research addressed counterterrorism intelligence and information-sharing between federal agencies and subfederal state and local officials. Sharing terrorist threat information and intelligence from federal agencies with state and local fusion centers remains suboptimal; this hampers the prevention of terrorism and presents opportunities for terrorists as was seen on 9/11 and the more recent Boston Marathon bombings. The purpose of this research was to study the ability of fusion centers to serve as the focal point for federal counterterrorism information and intelligence sharing. In this chapter I reviewed the literature by looking at the role and function of intelligence, the information-sharing lapses that enabled the 9/11 attacks to succeed, terrorism threats and counterterrorism, and domestic security and the role of state and local agencies in homeland security. The chapter also addresses the literature on nonfederal fusion centers, domestic intelligence and information-sharing, as well as recent domestic counterterrorism failures. Most importantly, this section describes the empirical research in the field of domestic counterterrorism information-sharing and sets up the study to examine federal agencies' sharing of terrorism information and intelligence with fusion centers.

Literature Search Strategy

This literature review examined the research across numerous significant topics and fields relevant to the study: (a) intelligence for homeland security; (b) information-sharing failures related to the 9/11 terrorist attacks; (c) terrorist threats and domestic

counterterrorism; (d) domestic security and the role of state and local agencies; (e) history of nonfederal fusion centers; (f) domestic intelligence and information-sharing; (g) recent domestic counterterrorism information failures.

The review included aspects of the theoretical framework of interagency information-sharing. The theoretical model of interagency information-sharing analyzed the benefits and risks when agency officials are considering sharing information with other organizations. Finally, this literature review explored the existing research into fusion centers as it relates to effective interagency information-sharing from federal intelligence and law enforcement agencies.

The data were placed into categories to examine the role and function of intelligence, the information-sharing lapses that enabled the 9/11 attacks to succeed, terrorism threats and counterterrorism, and domestic security and the role of state and local agencies in homeland security. In this study, the following databases were used: Google Scholar, Academic Search Complete, International Security & Counter Terrorism Reference Center, Homeland Security Digital Library, Military and Government Collection, ProQuest Central and ProQuest Dissertations, Political Science Collection, Taylor Francis Online, Sage Publications, and JSTOR.

Since this research is in the field of public policy and administration, publications from government agencies were particularly important; they were gathered from the public websites of the following agencies: Department of Homeland Security (DHS), Department of Justice (DoJ), Federal Bureau of Investigation (FBI), Office of the Director of National Intelligence (ODNI), as well as the Library of Congress. The

reference lists and bibliographies of the studies I read and were further examined for additional sources. This harvesting continued until the relevance of the topics went beyond the scope of this study.

Examination of the literature was conducted using various the following search terms: *information-sharing, intelligence sharing, interagency information-sharing, interagency collaboration, 9/11 failures, domestic intelligence, law enforcement intelligence, fusion center, interagency communication, interorganizational communication, homeland security, domestic security, homeland security information-sharing, DHS information-sharing, FBI information-sharing, homeland security failures, terrorist threats, and domestic counterterrorism failures.*

Roles and Functions of Intelligence

Gaining knowledge about ones adversaries has been an essential function of rulers since biblical times. The United States first employed intelligence at home and abroad during the Revolutionary War, and this has continued to be an important government function to protect national interests and defend citizens from threats (Keegan, 2003). However, the use of the term intelligence by governments has multiple meanings. Carter (2004) described intelligence as primarily a product:

In the purest sense, intelligence is the end product of an analytic process that evaluates information collected from diverse sources; integrates the relevant information into a logical package; and produces a conclusion, estimate, or forecast...using the scientific approach to problem solving (that is, analysis).

Intelligence, therefore, is a synergistic product intended to provide meaningful and trustworthy actionable knowledge to...decision makers (p. 9).

While intelligence certainly is an intelligence product resulting from analysis, it is also a process—the intelligence cycle--and some use the term intelligence to mean intelligence organizations such as the agencies of the Intelligence Community overall (Carter, 2004, pp. 9-10; Bimfort, 1995, para. 9). While intelligence can be a process, product, or an agency, when it comes to the context of homeland security, intelligence plays a very important role. This highlights the point that “Information is only as valuable as our capacity to process, integrate, and interpret it” (Davis & Kayyem, 2014, para. 7).

Intelligence to protect the nation from threats includes a broad range of requirements that address both external foreign adversaries as well as domestic challenges such as homegrown extremism, which are predominantly a law enforcement concern. As Wheaton and Beerbower (2006) describe:

If intelligence, as a concept, is to mean anything at all, it should be large enough to contain not only the national security community but also the intelligence communities within business and law enforcement. Failure to establish such a comprehensive definition damages - perhaps fatally - the notion of intelligence itself (p. 327).

As described in Chapter 1, there are significant differences between the meaning of information and intelligence. This is also important in understanding the role of intelligence. As Palmieri (2005) states,

The first problem that confusing the terms “information” and “intelligence” caused was that many agencies employed so-called analysts who were either unaware of or untrained in analysis and who were merely collecting and disseminating raw data. In some agencies, the ability to search databases was considered sufficient for analysts in law enforcement; this was strictly a law enforcement interpretation of the position. (para. 6)

The Intelligence Cycle

The process of collecting information, analyzing it, and disseminating the resulting product it referred to as the intelligence process or intelligence cycle. Palmieri (2005) succinctly described this intelligence process stating, “The steps of the intelligence cycle include planning, collection, evaluation, collation and organization, analysis, production, dissemination, and feedback, which should spur more collection, at which point the cycle begins again” (para. 5). As Carter (2009) has written “This process provides mechanisms to ensure the consistent management of information that will be used to create intelligence” (p. 57). The intelligence cycle starts with identifying intelligence gaps or requirements and the whole point of the process is to ultimately deliver or disseminate intelligence products to decision makers in a timely manner (Joint Chiefs of Staff, 2013, p. I-5).

The intelligence process steps of collation and processing of data are important and often involve technical means or even the translation of what was collected into a useable format. Data are essentially raw information such as a list of unassociated phone numbers, which is of little value without being put in context. When these raw data are

processed, such as associating the phone numbers with the names of their owners, they then become information. When this information about the phone numbers and their owners is combined with other information such as the call locations and frequency of calls, analysis can be done to assess likely associations between these individuals and predict who the leader may be. This resulting product of analysis provides context and an assessment or prediction is only then is considered intelligence. Intelligence analytical products often factor in historical trends and employ multiple sources of information collected by various means. This intelligence process applies to all levels of government including national level strategic intelligence focused on foreign threats.

National and Foreign Intelligence

Intelligence related to adversaries overseas or the threats that enemy nations and other actors pose to the United States is generally considered national level intelligence as well as foreign intelligence. While the purpose of intelligence clearly serves the nation, there are many customers of intelligence efforts, and intelligence is often put into different categories based on the specialized needs of these different users of intelligence. For example, the President of the United States and his National Security Council use intelligence for decision making, but so do police officers protecting the streets of any major city. Some of the most commonly referred to customers of intelligence are at this national level in Washington, DC. The post-9/11 Intelligence reform law defined this category of national level intelligence for the purposes of national security in the U.S.

Code:

National Intelligence and the term ‘intelligence related to national security’ refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that...involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security. (U.S. Congress, 2004, IRTPA Section 1012, Public Law 108-458)

It is also common, at least in the military, to categorize intelligence based upon the three recognized levels of war that includes strategic, operational, and tactical. Strategic intelligence is generally collected by national level intelligence agencies, or provided to very senior civilian or military officials at the national level. The definition of strategic intelligence by the U.S. Joint Chiefs of Staff (2013) in the joint publication 2-0 on *Joint Intelligence* states:

National strategic intelligence is produced for the President, the National Security Council...and other U.S. Government departments and agencies. It is used to develop national strategy and policy, monitor the international and global situation, prepare military plans, determine major weapon systems and force structure requirements, and conduct strategic operations. (p. I-23)

While these military focused definitions are useful and important to understand, they do not directly translate for use in the homeland where monikers such as ‘strategic’ have very different meanings at the state and local levels. According to Canas (2012), strategic intelligence is that which is simply used to make predictions about the future,

even at the local levels, and he states “if the analysis predicts an emerging trend or pattern it is strategic intelligence” (p. 40). This leads to addressing the types of intelligence used for more tactical levels and the information needed to drive preemptive actions against terrorists.

Operational, Tactical, and Actionable Intelligence

In the U.S. military, operational and tactical intelligence supports the corresponding military commands at those levels. An example of operational level intelligence consists of supporting a senior military force commander responsible for overseeing an entire military campaign, like all joint operations in Afghanistan or against the Islamic State in Syrian and Iraq. An example of tactical intelligence would be the collection and analysis to support a small unit commander about to conduct an attack on a hill or an enemy entrenched in a city. Tactical intelligence is also a term that has meaning to law enforcement as well. One example of tactical intelligence in a domestic context would be using a small drone to check the roof of a bank before a SWAT team ascends to the roof to assault from the top down onto robbers who have taken hostages inside the building.

Actionable intelligence, as the name suggests, consists of detailed and timely intelligence reports that are specific enough to allow an agency to take action to prevent a crime or other event. In fact, the lack of actionable intelligence is the excuse most commonly heard to explain why the U.S. government did not go after al Qaeda long before 9/11 even though the terrorist group declared war against us and we knew where they were. The case of not attacking al Qaeda overseas before 9/11 due to lacking

actionable intelligence was outlined in the article by Shultz (2004) which described one main reason for not going was the lack of detailed intelligence on Osama Bin Laden's specific location for more than a brief moment in time, as well as the number of civilians in his vicinity (section 9, *No Actionable Intelligence*).

As mentioned in Chapter 1, there are relevant and significant differences between the terms information and intelligence as and having access to agency data is very different from sharing actionable intelligence (Palmieri, 2005, para. 6.). It is useful for the purposes of this study to look at exactly what is meant by actionable intelligence when it comes to terrorism. The U.S. military manual on counterterrorism describes five key elements of actionable intelligence as it relates to an HVI or high value individual as follows:

1. Location. Providing an ellipse radius or "vicinity of" location, if possible. Even a probable location is worthwhile.
2. Facilities. Providing useful data that can help identify the place when an HVI is involved, or where terrorist assets are located.
3. Time. Providing the time of a sighting or an event. Time, as with location, helps to establish patterns that are exploitable. Time is also useful in establishing potential evidence that may link an HVI to actual or planned terrorist events.
4. Travel. Providing information regarding movement and means of travel and other available details when they relate to HVIs.

5. Relationships/connections. Providing known or suspected family/tribal relationships that exhibit or have potential for greater trust...show possible linkages from COG (Center of Gravity)/critical capabilities to critical vulnerabilities. (JP 3-26, 2009, p.V-5)

Actionable intelligence is a term that does translate well across all levels of government and multiple agencies. This type of intelligence is a key aspect of this study as this is exactly the type of intelligence that is needed at the state and local level to address specific terrorism threats to provide for the ability to identify, prevent, interdict, or disrupt terrorist attacks. Actionable intelligence in a terrorism context brings the study back to look at the need for this type of information to be used in a domestic context.

Domestic Intelligence and Homeland Security Information/Intelligence

Domestic intelligence of course is focused on internal threats within the country. However, domestic intelligence is more complicated than that. A useful description for domestic intelligence includes the following excerpt from a book titled *Remaking Domestic Intelligence* by former Federal Judge Richard Posner (2011) who stated it is,

intelligence concerning threats of major, politically motivated violence, or of equally grievous harm to national security, mounted within the nation's territorial limits, whether by international terrorists, homegrown terrorists, or spies or saboteurs employed by foreign nations. (p. 1)

While the intelligence process to produce intelligence for domestic users is similar to that of national strategic intelligence, there are also some significant

differences as well. A study by the RAND Corporation into domestic intelligence for counter terrorist described domestic intelligence as that which,

involves investigation of tips and other information about suspicious behavior to uncover who is involved and for what purpose. However, while law enforcement is focused on specific cases, domestic intelligence also includes exploratory activities designed to produce new leads and tips and to serve a broader warning function by building a strategic understanding of the domestic threat environment. (Leuschner, 2008, p.1)

During the Cold War with the global struggle against the Soviet Union and the threat of domestic Communists at home, intelligence and law enforcement agencies worked to counter these threats. However, there were few laws or regulations to govern these domestic security and surveillance activities and it resulted intelligence collection targeted against innocent Americans during this period. Numerous investigations later determined that intelligence and law enforcement agencies violated the privacy and constitutional rights of many citizens during this era (U.S. Senate, 1976, Church Committee Reports, Book II). When these violations became public, many laws and executive orders were then written in the 1970s to prevent more abuses as well as to specifically separate intelligence activities from law enforcement work (Best, 2007, pp. 2-3). Domestic intelligence implied a very negative meaning because of this earlier dark era.

A game changer for domestic intelligence and law enforcement came on 9/11. Judge Posner (2011) described how the FBI “turned in the most lackluster performance

of any agency in the run-up to 9/11, even though it had (and has) the primarily responsibility among police and intelligence services for preventing terrorists attacks on the nation from within” (p. 11). The 9/11 terrorist attacks were such an immediate and seminal event that views seemed to change overnight on the subject of domestic intelligence, and this turn-around is best evidenced by the passage of the USA PATRIOT ACT just days after the attack (Lerner, 2003). Rascoff (2010) described this resulting growth of domestic intelligence very aptly stating,

In the wake of 9/11, new government agencies with domestic intelligence responsibilities have been created, and others have been substantially retooled to focus on intelligence. State and local governments have also become heavily involved in domestic intelligence activities, either collaboratively with the federal government or independently. (p. 580)

The 9/11 was widely viewed as a “a failure of domestic intelligence, having been mounted from within the United States by terrorists who had been in this country for months--some intermittently for years” (Posner, 2011, p. 1). As a result of these attacks we also had the creation of the Department of Homeland Security, as well as the acceptance of the term Homeland Security Intelligence or HSI for some. While that term may not be accepted by all, the term “Homeland Security Information” is established in U.S. law and is defined as basically any information possessed by a federal, state, or local agency that related to the threat of or response to terrorist activity (6 USC 482(f)(1) 2006). The law goes on to describe homeland security information as that which is related to the ability to prevent, interdict, or disrupt terrorist attacks, which now brings

the study to the topic of how the U.S. failed to stop the 9/11 hijackers when it possessed information that may have prevented the attack.

The September 2001 al Qaeda Terrorist Attacks and Information-sharing Failures

The National Commission on Terrorist Attacks Upon the United States—also known as the 9-11 Commission – famously described the government failures that allowed 19 al Qaeda operatives to enter the country and hijack four civilian airlines and commit the deadliest terrorist attack in history. Much of these failures were on the part of large federal intelligence and law enforcement agencies. This section examines these federal failures as well as the implications for subfederal state and local agencies.

Internal Federal Agency Information-Sharing Failures

One of the government lapses that allowed the 9/11 attackers to enter the United States and travel around unmolested was the failure of federal intelligence and law enforcement agencies to share information with each other, the main thesis of the 9/11 Commission Report (Kean & Hamilton, 2004). One of the most famous lapses was the CIA not informing the FBI during the summer of 2001 about known al Qaeda terrorists not only possessing valid U.S. entrance visas, but actually being present in the United States at the time and, “none of the 50 to 60 CIA officials who could and should have watch-listed two of the 9/11 hijackers did so” (Zegart, 2008, para. 2). The 9/11 Commission Report stated these “fault lines in our government—between foreign intelligence and domestic intelligence” significantly contributed to the government’s inability to “connect the dots” and see the 9/11 attacks coming (Kean & Hamilton, 2004, p. xvii).

The failures leading to that attack were more than just not connecting dots. As Palmieri (2005) states, “the information to prevent the September 11, 2001, attacks was available, collected by someone, and stored somewhere; what was missing was the analysis that would have made all this information useful to decision makers” (para. 6). However accurate this statement may be, it assumes that this information was shared or at least available to analysts for them to examine and make an assessment, but it was not (Sims, 2007). The main reason information was not shared among federal agencies about al Qaeda and the hijackers being within in the country had to do with the divisions between agencies responsible for law enforcement and those who primarily collect and analyze intelligence.

The 9/11 Commissioners examined closely the so called ‘wall’ between law enforcement and intelligence which had resulted from a “widespread perception that statutory barriers restricted the flow of information” between intelligence and law enforcement agencies (Best, 2010, p. 14). This divide between these two government functions partly arose due to abuses by federal agencies during the Cold War, but also because of an attempt to keep the information from foreign intelligence and law enforcement separate. As Erwin (2013) wrote in a report for Congress on intelligence, “These barriers derived from the different uses of information collected by the two sets of agencies—foreign intelligence used for policymaking and military operations and law enforcement information to be used in judicial proceedings in the United States” (p. 17).

One of the key recommendations of the 9/11 Commission Report was to remove this ‘wall’ between intelligence and law enforcement that prevented the proper sharing of

information between agencies and contributed to the success of the nineteen suicide operatives on that day in 2001 (Kean and Hamilton, 2004, pp. 78-79). Congress did remove many limits on the sharing intelligence and law enforcement information with the USA PATRIOT Act of 2001, but “long-established practices have not been completely overcome” (Best, 2010, p. 7). However, we should ask ourselves what might have been the case if this information were shared within federal agencies as well as across the Nation with state and local officials.

Subfederal Information-sharing Failures

While the FBI did not know that al Qaeda terrorists were in the United States in the summer of 2001, a number of subfederal enforcement agencies had multiple interactions with the 9/11 hijackers. In fact three of the al Qaeda terrorists received speeding tickets, and two of those were in violation of their immigration status and the third had an arrest warrant out for failure to pay an earlier ticket (Bjelopera, 2011; Kean & Hamilton, 2004). When former White House Counterterrorism “Czar” Richard Clarke (2004) testified publicly to the 9/11 Commission that if he had been told in the summer of 2001 that some of these al Qaeda terrorists were in the U.S. he would have,

had the FBI release a press release with their names, with their descriptions, held a press conference, tried to get their names and pictures on the front page of every paper—America's Most Wanted, the evening news—and caused a successful nationwide manhunt for those two, two of the 19 hijackers. (p.110)

Even though no one was looking for the terrorists within the United States, multiple state and local police had interactions with the 9/11 terrorists, which could have

been significant had they been informed of the threat they posed. As Kobach (2004) stated,

One of the most disturbing aspects of the story of the September 11 terrorists is the fact that three of the hijackers were accosted by local police in routine law enforcement encounters. Had the federal government possessed information regarding their possible terrorist connections, and had that information been distributed to police officers...the terrorist plot might have been derailed. (p. 6)

It is appropriate to call these law enforcement encounters a failure to share and contributing factors to the 9/11 tragedy, especially since they were travelling under their true names. If Richard Clarke or the FBI had been told by the CIA about these terrorists being in the country, and had they taken the actions described, these might not have been routine traffic stops (Alexander & Mors, 2007). This is what the government must strive for and it leads the literature review to what terrorism threats there are to the homeland and how domestic counterterrorism is addressed.

Terrorism Threats and Counterterrorism

In Chapter 1, a hybrid definition for terrorism was outlined as the planned or use of illegitimate violence primarily against innocent people to achieve the psychological effect of fear or for political or other ideological purpose (Bruce, 2013). Unfortunately, terrorism has not subsided since 2001, but it has actually expanded and evolved. This section addresses threats to the homeland as well as counterterrorism within the nation.

Terrorism Threats to the Homeland

The terrorist threats to the U.S. from al Qaeda and similar overseas terrorist groups has remained high since 2001. Al Qaeda continually endeavored to attack the U.S. in number of ways, including multiple attempts on airliners using bombs planted in shoes, printer cartridges, and even explosive underwear (Biello, 2011). The United States and other nations aggressively attacked al Qaeda in Afghanistan and other places, but the threat did not dissolve. In 2009 al Qaeda also directly attempted to bomb the New York City subway system (Filler, 2010). While this type of international terrorism has been a concern since the 1970s, a more recent and troubling development has been the expansion of homegrown terrorism (Nelson & Bodurian, 2010). The terrorist threat evolved to include this domestic component where those residing in America became radicalized at home and have conducts attacks inspired by al Qaeda and other groups (Barron, Lewis, Silberstein, and Shapiro, 2016). One of the 9/11 Commission Co-Chairs, Lee Hamilton, described this type of threat by stating,

Al-Qaeda is much more diffuse than it was. There are pockets of strength of Al-Qaeda. So I think it remains a threat that is a serious one to the country...The threat that concerns us now in many ways is the home-grown terrorist, the American citizen if you would, who turns radical and subject to extremist ideology. This is the so-called lone wolf threat, and in many ways it's harder to detect than a more elaborate attack. (Alspaugh, 2011, para. 24)

These types of domestic attacks by radicalized U.S. resident greatly increased starting in 2009-2010 where “there were a dozen jihadist inspired homegrown terrorist

attacks and attempts by American citizens or legal immigrants (two attacks and 10 plots), which is a significant increase from the average of two attempts and no attacks the in seven previous years since 9/11” (Randol, 2010, p. 56). Domestic radicalization was previously seen as an issue mainly for Europe, but these attacks here at home caused many to recognize it is, “a bigger threat in the United States than originally believed” (Randol, 2010, p. 56).

A 2014 study by Hewitt outlining a chronology of terrorist plots and attacks since 9/11, “reveals...all were carried out by lone wolves or a group of friends...Most plots were by Islamist extremists (53%)...” (p. 66). Some of these attacks involved shootings as seen at Fort Hood in 2009, while others were bombings and attempted bombings like in New York’s Times Square in 2009 as well as the Boston Marathon in 2013. The New York City subway attempted attack was by core al Qaeda, while the Times Square attempt was by an al Qaeda affiliate, while Fort Hood and Boston were al Qaeda inspired lone wolf attacks. This means that “the threat is three-fold: from al-Qaeda ‘Core’; al-Qaeda's regional affiliates and allies; and homegrown extremists” (Silber & Frey, 2013, p. 129).

More recently are the developments of the former al Qaeda in Iraq branch, which has established itself as the self-proclaimed “Islamic State” and has seized significant territory in both Iraq and Syria and is often called the Islamic State of Iraq and Syria or ISIS (Laub, 2015). In 2015 this group greatly expanded terrorist attacks beyond the Middle East and directly struck out at Western targets such as a complex attack in Paris France by multiple small teams of shooters and suicide bombers who killed 130 and

wounded about 200 more in one night (Laub, 2015). This group also has brought online propaganda and recruiting to a new level and has inspired many homegrown attacks all over the world, to include a number here in the United States. The House Homeland Security Committee reported in January 2016 that the previous year had the highest terrorist threat level since 9/11, including the ISIS inspired attack in San Bernardino California that killed 14 in a single homegrown terrorist attack (House Homeland, 2016).

While homegrown terrorism has increased, we also cannot discount the most significant threat is the nexus between terrorism and weapons of mass destruction (WMDs), as the acquisition and potential use of these weapons has long been a stated goal of terrorist organizations like al Qaeda (Graham & Talent, 2008). While this is clearly not the most likely threat, the potential catastrophic results from a WMD attack require significant vigilance and collaborative counterterrorism efforts. The next section examines how terrorism is countered in the United States.

Countering Terrorism in the United States

As previously mentioned in this chapter, domestic Counterterrorism (CT) is primarily the role of the Federal Bureau of Investigation (U.S. Code Title 28, 2009, Sec .85). The FBI is the lead agency within the U.S. to investigate terrorism and disrupt any plots it may discover (Silber & Frey, 2013). However, countering these various terrorism threats within the United States is not something the FBI can do alone, so these efforts requires multiple agencies of the federal government, like national intelligence agencies, as well as close collaboration with state and local officials who are essentially the eyes and ears in communities (Ernst, 2014).

While terrorism is just a violent tactic employed for political or other purposes, it cannot be entirely eliminated any more than illegal narcotics can be eradicated. However, there are measures that can be employed to reduce radicalization and disrupt terror plots in the making (Rineheart, 2010). Domestic CT entails an all-inclusive approach and consists of measures to: counter radicalization, track suspected terrorists, deny them entry into the country, as well as efforts to deter, prevent, identify, pre-empt, and disrupt terrorist attacks using the full capabilities and resources of federal, state, local and tribal entities (White House, 2011).

As former Secretary of Homeland Security Janet Napolitano (2011) has stated, The realities of today's threat environment also means that State and local law enforcement officers will more often be in the first position to notice the signs of a planned attack. So our focus must be on aiding law enforcement and helping to provide them with the information and resources they need to secure their own communities from the threats they face. (p. 7)

According to statute and executive orders the FBI retains the leading role in domestic CT, and their capabilities have grown significantly since 9/11 with the bureau reprioritizing, refocusing and reorganizing to address this threat (Hoffman, Meese & Roemer, 2015). While many agencies and actors have a role in conducting or supporting domestic CT, striving for what the military called unity of effort requires, coordination not only at the apex of the federal government but also at the operational/tactical level, where response and intervention actions may be taken by diverse authorities acting independently or in coordination with each other.

This policy requires what is doctrinally known as unified action, also called the ‘whole of government approach’ by many interagency partners. (JP 3-26 CT, 2011, p. I-4)

However, this interagency approach with diverse and overlapping responsibilities, authorities, and jurisdictions has proved to be a significant obstacle to effective domestic CT, and the President even outlined this in the U.S. *National Strategy for Counterterrorism* stating that “Integrating and harmonizing the efforts of federal, state, local and tribal entities remains a challenge” (White House, 2011, p. 11). Although many in the public and private sector recognize the grave threat that terrorism poses to this Nation, cohesive counterterrorism remains elusive even 15 years after 9/11 (Vicinanze, 2015).

Domestic Security and the Role of State and Local Agencies

Domestic security within the United States Federal Republic is a complex and shared responsibility that spans all levels of government. The U.S. Constitution clearly outlines that some governmental roles are solely a national matter such as foreign policy and national defense. However, the 10th Amendment to the Constitution basically reserves all other powers not specified as national level for state governments to deal with at their level (Wright, 1990). For protection of citizens and preservation of life, the federal form of government in the United States primarily relies on local officials and first responders to provide this domestic security as a first resort (McCreight, 2015). Within the federal government alone there are approximately 40 U.S. government executive branch departments and agencies with a domestic security or response role, and

these agencies are not coordinated with each other nor are they adequately postured to collectively support officials at the state and local level (Wise & Nader, 2002, p. 45).

Federalism and Intergovernmental Relations for Domestic Security

The concept of federalism is about a power sharing arrangements between the national government and the respective state governments. Young (2015) writes that,

The original constitutional strategy for limiting national power and protecting state autonomy was the doctrine of enumerated powers. Article I, Section 8 lists explicitly confers certain powers on Congress; the Tenth Amendment then makes clear that the enumerated powers are it; whatever powers the Constitution doesn't confer remain with the States. (p. 8)

These enumerated and reserved powers provide for a very complicated domestic security environment in this Constitutional federated republic. The U.S. government can be looked at as a multifaceted "intergovernmental system" of three tiers that consist of federal, state, and local levels, and each level has some functions that overlap in numerous areas of domestic security (Mushkatel & Weschler, 1985, p. 49). Domestic security issues evolved during the two world wars and the Cold War, and now the threat of terrorism from abroad after 9/11 brought even more changes. In the new modern era of super-empowered non-state actors such as terrorist groups, "This federal-centric homeland security system we have right now is a single point of failure" (Morton, 2012, p. i).

The importance of state and local governments in internal security matters can be traced to the early days of this nation, and the "Constitution leaves with states, and the

states delegate to local governments, many of the broad police powers which naturally come into play” (Warmlesley and Schroeder, 1996, p. 242). While it is common practice that investigations and crises are managed at the lowest level possible, Wise (2006) noted that when state and local governments are overwhelmed, governors may request federal assistance. Ultimately domestic security is a collaborative effort among all three levels of government as, “no single actor enjoys sufficient authority or resources to compel action” (Chenoweth & Clarke, 2010, p. 498).

In 2006, Eisinger described the challenges of effective domestic counterterrorism by writing “The terror attacks of 9/11 exposed a federal system that was ill-prepared to craft and implement a coherent program to protect the nation’s cities...posed a set of challenges to the complex, decentralized division of functions among levels of government” (p. 537). Further, Mushkatel and Weschler (1985) stated that these domestic security and response situations “must be a cooperative intergovernmental venture. That is, our orientation is toward joint government efforts rather than domination by any single level of government” (p. 53). Thompson (2002) also described this critical intergovernmental challenge post 9/11 focused on how all levels of governments will individually and collectively perform homeland security” (p. 18).

The new paradigm of catastrophic terrorism threats from groups such as al Qaeda requires more highly effective governance which calls for “a new breed of collaborative federalism” (Kincaid & Cole, 2002, p. 181). Government security agencies from the federal level all the way down to the local level must be integrated in a manner that enables the collaborative prevention of all types of catastrophic events such as terrorist

attacks. However, this effective collaboration has been elusive and filled with tensions due to overlapping responsibilities, bureaucratic challenges as well as personality clashes.

Interagency Challenges with Roles, Missions and Jurisdiction

Some federal agencies—the FBI in particular—are famous for having frequent jurisdictional disputes with federal, state, and local law enforcement agencies. One Department of Justice audit stated “Historically, there had been no clear division of responsibilities. This often resulted in delays of criminal investigations because of jurisdictional disputes, and wasted resources because investigative work was often duplicated” (Department of Justice, 1996, Section I, para. 5). This situation became more complicated when the Department of Homeland Security was created after 9/11 to prevent terrorist attacks, but the FBI still retained the sole authority to investigate terrorism and disrupt terrorist attacks within the United States.

The FBI successfully fought to remain outside the DHS as it was being formed as a new agency, and the bifurcated nature of domestic security as it relates to terrorism remains in place today. The tension between these two agencies is famous and bureaucratic battles waged during and after as the FBI fought to stay out of the new DHS (Perrow, 2006). The first Secretary of Homeland Security, Tom Ridge (2009), stated that when it came to the FBI it “was a constant battle to convince them we weren’t the enemy” and he further wrote that the FBI “went out of its way to emasculate DHS” (pp. 161-162).

As a result of this separation and the continuing bifurcated arrangement, the FBI maintains over 100 JTTFs around the country while DHS sponsors 78 separate state and

local fusion centers (Randol, 2009b). Each of these separate inter-agency organizations overlaps and fights for limited federal funding which ends up limiting effectiveness of both (Lawrence, 2008, p. 8). The FBI retains their authorities, while DHS chooses to fund their own initiatives, and this leaves state and cities forced to separately interact with both federal agencies on terrorism issues. As of 2015, only 12 JTTFs and fusion centers have been combined or collocated (Hoffman, Meese, & Roemer, 2015).

A study of law enforcement interagency cooperation since 9/11 found that “[t]erritorial, jurisdictional and interpersonal conflicts also got in the way of efficient cooperation, both within between [*sic*] law enforcement agencies, and between the law enforcement and intelligence communities” (Middlemiss & Gupta, 2007, p. 139). These difficulties become further complicated when federal law enforcement agencies interact with the over 18,000 state and local agencies across the country, many of which have different agency cultures and may not have positive relationships among themselves for various reasons (Middlemiss & Gupta, 2007, p. 139; Domash, 2004, para. 18). There are even instances where state and local agencies have been caught in the middle of “turf wars” between federal agencies (Roebuck, 2009, para. 17). The FBI has also clashed with nonfederal agencies as well. Michael Sheehan the former deputy commissioner for counterterrorism at the New York Police Department and former ambassador at large for counterterrorism wrote in 2009 that

The FBI and New York Police Department remain engaged in a counterproductive bureaucratic struggle...clashed over releasing threat warnings to the public and to private-sector entities. The FBI claimed ownership of the

information (usually obtained by federal intelligence sources like the National Security Agency or the CIA) and wanted to dominate the podium at news conferences. (para. 4)

The tensions are not exclusive to the FBI, and Kahn (2009) wrote that DHS and the FBI fought over their roles during response to Hurricane Katrina, and stated that DHS has been under “continual inter- and intra-agency conflict. For example, Homeland Security and the Justice Department, which includes the FBI and DEA, both are tasked with gathering intelligence and sharing it with state and local law enforcement officials” (para. 4). This country has three levels of government and many different roles and functions performed across all levels. A snapshot of the overlapping government responsibilities with regard to domestic security is provided below in Table 1.

Table 1

Overlapping Government Responsibilities in Domestic Security

	Law Enforcement	Intelligence Sharing	Intelligence Collection	Security
Federal	FBI, ATF, Etc	DHS, FBI	Natl. Intel. Community	Dept. of Def. & DHS/FBI
State	State Police	Fusion Center	Citizens and Police reports	State police and Natl. Guard
City	City Police	Fusion Center	Citizens and Police reports	City Police

However, this chart does not fully depict all the overlapping roles and functions at each level, which might be best represented by a complex series of overlapping circles in

a Venn diagram. The 9/11 Commission Report outlined how these interagency tensions extend beyond just the wall between law enforcement and intelligence. Some of the clashes are based on the personalities involved, but many really stem from the conflicting and overlapping roles, missions and jurisdictions. This is unfortunate since federal, state and local officials have all strived to better protect citizens in this new age of terrorism.

Importance of State and Local Agencies in Combatting Terrorism

The 9/11 attacks were not only a wake-up call for the federal government to do better at countering terrorism, but it drove state and local governments to make terrorism a priority as well. Although terrorism cases may be under the purview of the FBI, all terrorist actions start out as a local issue. Also, the federal government asked state and local officials after 9/11 to ramp up security at possible terrorist targets and critical infrastructure such as bridges, nuclear power plants, and airports. Bjelopera and Randol (2010) emphasized the importance of these Nonfederal agencies when they wrote,

The role of state, local, and tribal law enforcement in detecting nascent terrorist plotting is particularly important, especially considering the challenges involved in detecting lone wolves and homegrown jihadist groups with few connections to larger terrorist organizations. Nine years after the 9/11 attacks, integrating state, local, and tribal law enforcement into the national counterterrorism effort continues to be an abiding concern of policymakers. (p. 4)

In order to effectively combat terrorism, local law enforcement officers need to be aware of signs of radicalization and realize that “terrorists are living all over the U.S. and they can be plotting an attack against a target even while living several states away”

(Ernst, 2014, para. 2). As Congressman McCaul (2014) stated in a House Homeland Security hearing, “State and Local police have a strong role in Counter Terrorism. They know the streets better than anybody and they know the local threats...They must know the terror threats in their own backyards” (p. 2).

One of the key lessons of the 9/11 attacks is that many government sectors must collaborate across the spectrum of law enforcement, security, and even first responders to develop “strategies as a multifaceted, layered approach, understanding that no single approach succeeds by itself” (Ellis, 2014, p. 220). Even Robert Mueller as the Director of the FBI at the time, stated that “No one agency or department can handle these diverse challenges” (Mueller, 2010, para. 24). While there have been efforts to improve interorganizational collaboration after 9/11, this history of interagency challenges and ‘bad blood’ between these entities remains an intergovernmental challenge when it comes to CT.

Domestic Counterterrorism Reforms

In response to the 9/11 attacks, a number of governmental reforms emerged to address weaknesses in securing the homeland. This section will outline some of the major reforms. Most significant to this study includes the creation of three new entities; the Department of Homeland Security; the Director of National Intelligence; and a National Security Branch within the FBI. Burch (2007) describes these post 9/11 reforms as,

The major change was the creation of the Department of Homeland Security with an intelligence charter. The U.S. government also adopted measures to implement intelligence coordination and improve identified shortfalls through the creation of

the Director for National Intelligence (DNI), the National Counter Terrorism Center (NCTC), and revamping the FBI's intelligence capability. (p. 16)

Each of these new entities have a role in preventing terrorism within the United States, and each of them all impact on state and local fusion centers.

Creation of the Department of Homeland Security

The most significant change in the organization of the U.S. government since the National Security Act of 1947 was the creation of the Department of Homeland Security which incorporated almost two dozen different government agencies and around 179,000 employees into a single agency (Perl, 2004). The government decided to consolidate into one large new agency many domestic protection functions such as "border and transportation security, effective response to domestic terrorism incidents, and ensuring homeland security" (Relyea, 2003, p. 617). The DHS was formed by collecting 22 different security, customs, immigration, and disaster assistance focused agencies together into one department (King, 2009, p. 152).

This newest government arm entails seven operating components or field agencies such as the U.S. Coast Guard, Customs and Border Protection (CBP), the Secret Service, and the Federal Emergency Management Agency (FEMA) (King, 2009, p. 155). This major reorganization merged myriad tasks of many diverse agencies in order to collect them under one large department (Huang, 2007). While a well-intentioned plan to better secure the nation through centralization, it was also criticized by some, including former White House Counterterrorism 'Czar' Richard Clarke (2004) who called it a "wiring diagram fix less able to deal with domestic security...for years to come" (p. 249).

The purpose to centralize these efforts was clearly intended to harmonize the domestic security functions and reduce interagency communication and coordination issues. However domestic security efforts overall are still highly disjointed with key federal security agencies like the Department of Defense (DOD), the Department of Justice (DOJ), and others remaining outside of the DHS organization (Lehrer, 2004, p. 85; Wise, 2006, p. 306). Kahn wrote in 2009 that for effective domestic counterterrorism there are many “external agencies and departments Homeland Security must coordinate with (the CIA, FBI, DEA, and Health and Human Services, among others)” (para 3). In describing this disconnect, Filler (2010) stated:

Since its inception, DHS has had to deal with federal agencies and authorities necessary to carry out the homeland security mission being kept outside the department... While DHS does play an important role in the current homeland security structure, it is a far cry from how it was marketed during its founding, as well as how it's perceived by the public today. (para. 15)

With all of these factors in mind it is important to note that although DHS has Homeland Security in its title, it is far from being a ‘one stop shopping’ agency for domestic security.

In addition to many key domestic security agencies being outside the organization, is the challenge of now harmonizing the separate and still often distinct efforts of the DHS components. Bringing together the U.S. Coast Guard and Customs Enforcement efforts under the same federal agency does not alleviate the many years of interagency tension between them or essentially eliminate conflicting roles and

jurisdictions by itself. In one way it can be stated that creating DHS the government only replaced interagency issues between these components and made them intra-agency challenges. This is especially the case since the Secretary of Homeland Security is not an operational position and he or she cannot order the field agencies to do anything (Ridge, 2009, p. 213). DHS is still striving to fully absorb all these different missions and cultures into a cohesive whole, and as one senior DHS official stated, “As post-9/11 operational necessity drove DHS’ formation from disparate legacy agencies, complex new departmental responsibilities obliged us to work together in enterprise fashion and forge a collaborative...culture” (Wagner, 2011, p. 3).

Two of the main functions of DHS that relate to fusion centers deal with the disbursement of federal funds to support state and local efforts to counter terrorism and information and intelligence sharing. As Caruson and MacManus (2006) stated, “DHS functions as the lead agency for the distribution of federal grant money and the locus of coordination between federal, state, and local governments” (p. 523). A number of these grants are used by states and major urban areas to fund their fusion centers. A completely different challenge DHS faces has to do with providing subfederal agencies with intelligence and information for countering terrorism.

The main limitation with DHS and intelligence has to do with the fact that it was specifically created not to be a domestic intelligence gathering agency, but to only analyze reports provided to it from other agencies (Randol, 2010). This has forced DHS to take a more non-traditional approach to ‘intelligence’ and to not just seek ‘state secrets’ but to also focus on the many thousands of routine, everyday observations and

activities such as suspicious activity reports (Chertoff, 2005). However, this means that for traditional and mainly classified intelligence, DHS has to principally rely on the many agencies that constitute the U.S. Intelligence Community. Another major centralization reform that came about as a reaction to the 9/11 attacks was the creation of a Director of National Intelligence to lead this community.

Creation of the Director of National Intelligence

One of the significant findings of the 9/11 Commission was that there was no true leadership over the constellation of intelligence agencies that had grown up during World War II and continued to grow during the Cold War (Kean & Hamilton, 2004; Zegart, 2005). The Director of the Central Intelligence Agency nominally held the title of “Director of Central Intelligence” that meant he was supposed to lead the whole community, but that title was next to empty as it came with no authority to direct other agencies—who already reported to Department heads of other major federal agencies (Gutjahr, 2005).

Based upon the recommendations of the 9/11 Commissioners and others, a new position of Director of National Intelligence or DNI was created (Hitz, 2012). However, this leadership issue was just one factor that attributed to the lack of effective intelligence to support the Nation, and in particular, effectively collaborate on terrorism threats across these many agencies and “Ensuring the integration of foreign and domestic intelligence collection and analysis, as the 9/11 Commission recommended, is one of the most important responsibilities given to the Office of the DNI” (McConnell, 2007, para. 6). Other issues had to do with uncoordinated multi-agency terrorism analytical efforts, and

the many different databases these various agencies each held independently on terrorists and terror groups (Best, 2011).

In light of these challenges, the government decided to simultaneously deal with the issues of terrorism analysis—the failure to ‘connect the dots’ about 9/11—and the need to bring together these terrorism databased in one fell swoop (Berkeley et al, 2012). The concept that first started as the Terrorism Threat Integration Center (TTIC), ended up evolving into the National Counterterrorism Center (NCTC) which was directly subordinated to the new Director of National Intelligence (Gutjahr, 2005). As Best (2011) stated in a report to Congress on the responsibilities of this new interagency government terrorism center,

Within the sprawling U.S. Intelligence Community, the National Counterterrorism Center (NCTC) was specifically established in 2004 to bring together all available information on terrorism, analyze the information, and provide warning of potential attacks on the U.S. (p. 1).

Another role for the Office of the DNI or ODNI, is the task to improve intelligence and information-sharing between and among different government agencies that have a role in countering terrorism. ODNI did this in cooperation with DHS and the Department of Justice by developing a government-wide information-sharing backbone called the Information-sharing Environment or ISE (Lahneman, 2004; Verton, 2011). The Intelligence Reform and Terrorism Prevention Act or IRTPA (2004) directed the establishment of the ISE as well as a Program Manager (PM) to plan for and manage the ISE to ensure information is shared across federal agencies. This PM-ISE establishes

standards, procedures, and instructions across the government to enable more effective terrorism information-sharing, and included in these efforts is the goal to better share intelligence and information with mission partners at the state and local levels (Paul, 2015).

These efforts to reform the Intelligence Community, and improve terrorism analysis and information-sharing have increased collaboration and access to some terrorism data. However, many challenges still remain as this study addressed. One of the challenges that creating DNI and NCTC did not address for the homeland is the limitation in the IRTPA which explicitly excludes NCTC from housing data on purely domestic terrorism, as that is under the purview of the FBI.

Creation of the National Security Branch within the FBI.

The FBI is a domestically focused agency, and it had a tortured history of poor relations with the CIA for example (Gorman, 2003). In the most basic sense, the CIA collected intelligence on threats overseas while the FBI focused on enforcing laws at home (Sales, 2010). These different missions resulted in “fault lines in our government—between foreign intelligence and domestic intelligence” which significantly contributed to the government’s inability to “connect the dots” and see the 9/11 attacks coming (Kean & Hamilton, 2004, p. xvii). The 9/11 Commission and other investigations of government terrorism efforts that went on before and during 2001 all identified many lapses on the part of the FBI. This agency was originally set up to deal with crime in a different era, so the many independent Field Offices in major cities around the country were not coordinated with or among each other, nor did headquarters have any real knowledge of

what investigations were going on inside these Field Offices as they were essentially “balkanized fiefdoms of the FBI” (Perrow, 2006, p. 22).

Functionally law enforcement agencies are very different from those who perform primarily intelligence roles, with the former being almost singularly focused on investigating and prosecuting crimes that have been committed, while the latter operates in the very grey area of trying to anticipate events and preempt them when possible (Gorman, 2003; Zegart, 2007). This results in divergent agency perspectives based on these different missions, which can also manifest itself in differing and often conflicting organizational cultures (Riebling, 2002). The FBI had a very strong law enforcement centric perspective and culture (Desai, 2005; Jeffreys-Jones, 2007). As a result of this mission and culture, U.S. Attorney Robert Mueller took over as Director of the FBI just days before 9/11, and he inherited a very antiquated agency with case files that were kept in shoe boxes dispersed among the many field offices around the country (Kean & Hamilton, 2004; Zegart, 2009).

While the 9/11 Commission and Congress felt the FBI had to change its culture, others said it was the mission that needed to change (Wyllie, 2011). When pressed by President Bush immediately after 9/11 to change the FBI’s focus from just investigating attacks after they happen to instead identifying threats and disrupting attacks in advance, Director Mueller replied “That’s our new mission, preventing attacks” (Bush, 2010, p. 145). However, some said the FBI was beyond repair and discussed ideas to start over or create a new domestic intelligence agency, so in an effort “To avoid dismemberment,

Mueller made bold promises to cure what ailed the FBI from within—rebuilding it into a modern, intelligence-driven enterprise” (Gellman, 2011, para. 10).

So the new top priority of the FBI became preventing terrorist attacks, and Director Mueller worked to steer the ship of the agency to focus on terrorism as the top priority (Bohm & Haley, 2012). However, changing culture is very challenging and takes time. So Director Mueller also made significant personnel changes to focus the Bureau more on intelligence and counterterrorism (Mueller, 2010). As a part of this effort, the FBI reinforced the Counterterrorism Division (CTD), and not only made terrorism its top investigative priority, it also

shifted resources to this area from its more traditional law enforcement activities, such as drug, white-collar, and violent crime. In addition to transferring hundreds of agents and support staff from criminal areas to counterterrorism, the FBI also subsequently hired thousands of additional agents, intelligence analysts, and other professional support staff to fulfill its mission. (Maurer, 2012, p. 1)

While a number of analysts and experts still felt that a new domestic intelligence agency should be created akin to the MI5 in the UK, both the 9/11 Commission and the Robb-Silberman ‘WMD’ Commission rejected these proposals (Cumming, 2005). The government had decided to instead reform the FBI into a law enforcement agency, but one with intelligence functions within the homeland. Director Mueller was able to make some strides to mold the Bureau to have a more preemptive mindset and be a better networked organization, but he could not do it alone, and changing the culture and organization were still very much a work in progress four years after 9/11 (Cumming,

2005). Ultimately it took a formal and public memorandum in 2005 from then President Bush to the Attorney General directing that he create a new National Security service within the FBI (Bush, 2005). In the memo, President Bush specified that this new ‘national security’ focused organization within the FBI would,

Combine the missions, capabilities, and resources of the counterterrorism, counterintelligence, and intelligence elements of the FBI into a new National Security Service...to build an FBI National Security Service workforce, including special agents, intelligence analysts, and as appropriate, other personnel, necessary to the effective performance of the national security missions of the FBI. (Bush, 2005, para. 4)

This memo ended up being the catalyst for creating the National Security Branch of the FBI which contains the Counterterrorism Division as well as counterintelligence and intelligence functions (Richelson, 2012). So, this change essentially reorganized the FBI into an agency with “two core functions: national security and criminal investigations” (Vizzard, 2008, p. 1080). In both of these areas the FBI strives to be a “threat-driven, intelligence-led organization. We are collecting, analyzing, and sharing intelligence to better understand all threats” (Mueller, 2010, para. 17).

The new National Security Branch of the FBI took an equal place in the Bureau alongside criminal investigations, a major organizational and cultural change (Cumming, 2005). One of the existing frameworks that was previously directly under each independent FBI Field Office, was the many Joint Terrorist Task Forces or JTTFs around the country. In this 2005 reorganization the Counterterror or CT Division was interjected

into the supervisory line for all JTTFs. Fuller (2008) described the history and post 9/11 growth of JTTFs,

The JTTF program was established by the FBI's CT division based on a 1980 New York City task force model that incorporated members from federal, state, and local law enforcement to combat an increasing number of terrorist bombings. Prior to 9/11, there were 35 JTTFs in existence throughout the United States. The FBI has since expanded the number of JTTFs to one at each of its 56 field offices and to approximately 46 of its annexes. (p. 4)

Fuller (2008) goes on to describe how there are more than 2,000 “non-FBI personnel from more than 600 federal, state, and local agencies currently participate on JTTFs in support of terrorist-related investigations” (p. 4). It is important to note the wording from Fuller in that he did not call the non-FBI personnel “members” of the JTTF, but stated they “participate” on JTTFs and “in support of” terrorism investigations – an important distinction. While created and describing these JTTFs as multiagency investigatory bodies, they are still formally part of the FBI, and “even though many agencies contribute to them, the FBI's ‘Joint Terrorism Task Forces’ are FBI-centric” (Desai, 2005, p. 61).

To supervise all these JTTFs and to provide a hub for their interactions, and new national level JTTF was stood up as a part of CTD. According to Fuller (2008), The FBI also created the National NJTTF (NJTTF), “a multiagency task force co-located with the National Counterterrorism Center in McLean, Virginia. The NJTTF serves as a point of

fusion for 44 federal, state, and local agencies, each providing full-time representatives and meeting daily to share timely CT-related information” (p. 4).

At their heart, these JTTFs are primarily focused on investigating terrorism cases, and have not proved to be a significant conduit for interagency information-sharing (Cordner & Scarborough, 2010). An example of the JTTFs being essentially an FBI organization is how the Bureau did not allow non-FBI ‘partners’ inside a JTTF to share information with anyone outside the JTTF without express permission. The FBI publicly acknowledged in a press release that stated, “JTTF-generated information may only be disseminated outside the structure of the JTTF (including to a member’s home agency) with the approval of the JTTF FBI supervisor” (FBI, 2009, para. 8). Those non-FBI personnel working in a JTTF are on “detailed” duty from their home agency and often referred to as detailees. A U.S. Senate Report (2011) about JTTFs stated the following:

The FBI's vision of JTTFs as being interagency information-sharing and operational coordination mechanisms is sound, but the...JTTF model has not fulfilled the vision completely in practice...JTTF detailees lack access to key databases. As a result, we have concerns that the culture of JTTFs may be that they are FBI investigative entities, with detailees to JTTFs essentially serving as additional personnel to augment the FBI. (p. 51)

FBI JTTFs are “a model for successful interagency coordination on a government wide basis” but just because JTTFs “have engaged in successful operations does not make the case that the U.S. has determined how best to share information within its law enforcement community or between the law enforcement community and its intelligence

agencies” (Middlemiss & Gupta, 2007, p. 141). While the FBI is the lead federal agency for domestic counterterrorism, that does not mean they are necessarily the best agency for sharing terrorism information with state and local officials. As the Senate Report (2011) found “we are concerned that JTTFs may not be fulfilling their intended role as interagency information-sharing and operational coordination mechanisms” (p. 87).

Assigning personnel to these JTTFs has been a challenge since arduous background investigations need to be completed to give detailees security clearances. There are also challenges with what work detailees are allowed to do and who the FBI really wants as participants in a JTTF. One study found that the FBI was looking for people just like them to be assigned, and a study by Zegart (2015) reported,

The FBI mainly wanted detailees to the JTTFs who were sworn federal law enforcement officers, which meant they could carry guns, wear badges, and were authorized to enforce all federal laws just like the FBI. In fact, the Pentagon had tried sending more skilled analysts and personnel with counterterrorism experience from the Army and Air Force years earlier. But because they were active duty personnel and not sworn federal law enforcement officers, Army and Air Force detailees were often relegated to clerical work on the task forces. (p. 45)

These drawbacks do not take away from the many successes that JTTFs have had, such as disrupting an attack on a shopping mall outside Chicago (McNeil, Carafano, & Zuckerman, 2011). However, Hitz (2012) notes that “Simply deputizing FBI and other law enforcement officers as intelligence professionals will not enable the intelligence community to overcome the bureaucratic stovepipes that have hindered interagency

cooperation in the past” (p. 255). As a result, “Calls for further FBI reforms have continued” (Burch, 2007, p. 16).

Today the FBI still has terrorism as its number one mission, but with the current threats from overseas groups as well as homegrown extremists recruited on the internet, the FBI clearly faces a significant shortfall in resources to deal with these manifold threats. This resource issue is most pressing with a lack of sufficient manpower and tools to investigate terrorism with FBI agents nationally than there are more police officers in New York City alone, and terrorism is only one of many federal crimes the Bureau has to deal with (Shedd, 2016). The FBI clearly cannot handle terrorism threats alone, and more and deeper partnerships are needed with state and local agencies.

In a recent follow up report to the 9/11 Commission, a detailed document and field study was done of the FBI and it found the continued widespread “perception that sharing with the Bureau is still too much of a one-way street” (Hoffman, Meese & Roemer, 2015, p. 83). However, some analysts and experts such as former DHS senior official Matt Mayer (2016) strongly advocated for the FBI JTTFs to be the lead and for fusion center to merge with them. While these reforms of the FBI in creating a National Security Branch and expanding JTTFs are important and admirable efforts, there is still clearly a need for nonfederal fusion centers which do focus on intelligence and information-sharing as a primary effort.

Nonfederal Fusion Centers

Subfederal fusion centers at the state and local levels started well before 2001, but the terrorist attacks of that year provided the catalyst for their rapid growth around the

country. Immediately after the 9/11 attacks the leaders of states and major urban areas received numerous—and often non-specific—federal warnings about possible al Qaeda terrorist threats. These subfederal leaders received only unclassified general warnings, and they also lacked the capability to effectively analyze these reports or put them into context to be relevant to their jurisdictions. Lacking specificity into these threats from the federal government and being without capability to analyze the threats were the dual catalysts that spurred on the spread of subfederal fusion centers after 9/11. Before examining the evolution of fusion centers, this literature review will first explore their beginnings in the 1980s and their growth after 9/11.

History of Fusion Centers

During the 1980s and 1990s a number of regions within the U.S. moved toward various forms of domestic intelligence fusion centers to counter the flow of illegal drugs into the country (Carter and Carter, 2009).

As Canas (2012) writes in *Homeland Security at the State Level*,

The popularity of such fusion centers reached a crest during the so-called ‘war on drugs’ in the mid-80s. Interagency centers such as the El Paso Intelligence Center (EPIC), the National Drug Intelligence Center (NDIC), and numerous state and regional crime Intelligence Centers were formed to facilitate the operational information needs of the law enforcement community (p. 36).

Another inspiration for law enforcement agencies to move toward a fusion center model was the Intelligence Led Policing (ILP) concept from the 1990s which focuses on gathering intelligence and conducting analysis to support proactive law enforcement

(Hylton, 2009; Lambert, 2010). At their heart, fusion centers work to bring together various agencies focused on a common problem that required information-sharing and analytical efforts. Shepard (2011), stated that “The concept of the fusion center is quite simple: to facilitate the sharing of homeland security related and crime-related information and intelligence within the law enforcement community” (p. 36). According to the Department of Justice (2005),

The principal role of the fusion center is to compile, blend, analyze, and disseminate criminal intelligence and other information (including but not limited to threat assessment, public safety, law enforcement, public health, social service, and public works) to support efforts to anticipate, identify, prevent, and/or monitor criminal activity. (p. 3)

After the 9/11 attacks and the many ominous warnings of potential follow on terrorist attacks, many governors and mayors felt they were not getting the intelligence and information they needed about terror threats from the federal government, so state and local fusion centers spread rapidly across the country (German & Stanley, 2007). Numerous states and major urban centers around the nation desired to improve their sharing of criminal information and to coordinate joint efforts. Carter and Carter (2009) described the intent of fusion centers “to marshal the resources and expertise of multiple agencies within the region to deal with cross-jurisdictional crime problems” (p. 1324). Fusion centers really started “as a national grassroots initiative” pushed by the demand signal from the state and local levels leaders, but it did not take long for the federal government to jump on board (Serrao, 2010).

Military Counterterrorism Fusion Centers

There are also counterterrorism fusion centers employed by the military which bring together many national intelligence agencies and military intelligence capabilities to successfully collect on and collaboratively analyze overseas terrorist groups. One well known example of a successful military fusion center effort was contributing to the defeat of al Qaeda in Iraq during the 2004-2011 timeframe (Lamb & Munsing, 2011). The concept is very similar to the intent for domestic counterterrorism fusion centers, and the idea came from the then Deputy Commander of Joint Special Operations Task Force 714, Rear Admiral William McRaven who said, “We need a joint interagency task force (JIATF)...we need CIA, we need FBI, we need everybody, all the three-letter intelligence agencies. If we don’t understand what CIA’s doing, or what FBI’s doing, or NSA, then we’re missing things. They have information we’re not seeing” (Shultz, 2016, p. 26).

The commander of Task Force 714, General Stanley McChrystal then had to convince each agency to join the JIATF and to “collaborate in a work environment of interdependency, cooperation, trust, and transparency” (Shultz, 2016, p.26). The commander “had to overcome the reluctance of other agencies to participate in building a counter network to tackle the metastasizing terrorist network assembled by Abu Musab al-Zarqawi in Iraq” (Henriksen, 2013, p.54). General McChrystal himself stated that the JIATF is,

a way to fuse the various intelligence agencies’ specialties in order to better understand the enemy. It would leverage the CIA’s ‘human intelligence’ from spies and sources; the National Security Agency’s intercepted signals; the FBI’s

forensic and investigative expertise; the Defense Intelligence Agency's military reach; and the National Geospatial-Intelligence Agency's (NGA) dazzling mapping ability (McChrystal, 2013).

Over time this approach worked and the JIATF became a true fusion center that was deployed overseas to bring together representative from all these various agencies to effectively collaborate intelligence on terrorist cells and leaders. Henriksen (2013) noted that the "natural tendency of the intelligence community is to hoard information" but General McChrystal "made his teams share intelligence" (p. 50). According to Lamb and Munsing (2011), it was the coupling of this collaborative all-source intelligence fusion center effort with targeted special operations raids became the secret weapon' that found and killed Zarqawi and eventually defeated al Qaeda in Iraq.

Fusion Centers Evolve

Similarly, domestic fusion centers after 9/11 were originally intended as clearing houses for threats and intelligence, and to 'connect the dots' and detect an actual terrorist plot (Apuzzo & Goldman, 2013). However, there was little that state and local agencies could do on their own without federal intelligence and information on terrorist threats. So fusion centers were "developed, in part, from a joint project with the federal intelligence community, including DHS and DOJ" (Serrao, 2010, para. 4). Although federal grant money came in from DHS for fusion centers "it did not take long to realize that, in most cities, the threat was not enough to justify all the manpower, money, and equipment. So in many states, the fusion center mission crept toward something broader" (Apuzzo & Goldman, 2013, p. 162).

While the original purpose for subfederal fusion centers after 9/11 was for sharing terrorism information, Larence (2008) wrote for the U.S. Government Accountability Office that the “majority of the centers had scopes of operations and missions that included more than just combating terrorism-related activities, such as a focus on all crimes or all hazards” (p. 3). As a result, many states and major urban areas have realistically co-located their fusions center with the functionally related Emergency Operations Centers (EOCs) in order to further improve cooperation (DHS/DOJ, 2010, p. 20).

Today there are 78 states and major urban regions that have formed their own fusion centers “...to share information and intelligence about terrorist threats, criminal activity, and other hazards” (Department of Homeland Security, 2010, p. 67). Rollins (2008) describes how state and local fusion centers take their broad array of locally gathered information from law enforcement, the public, and the private sector sources and it gets “fused with intelligence collected and produced by the federal Intelligence Community to better understand threat and assist in directing security resources” (pp. 5-6). The role and mission of each fusion center is based on the particular needs of each state or major urban area that owns it. This was discussed by the Washington DC fusion center director, Lee Wight (2015) who stated,

Each of the 78 centers is tailored uniquely to serve their particular area of responsibility...some fusion centers are investigative such as Boston....some are very tactical in their focus, i.e. case support for their local law enforcement agencies...we are strategic intelligence...more akin to operational intelligence,

i.e. regional trends and patterns is what we look at. Some centers are a watch, i.e. they report events and direct actions in the community. (Wight, 2015)

These fusion centers serve a significant function in providing a framework for agencies to share information and intelligence with state and local officials that did not exist before 9/11. As the Presidential Executive Order on intelligence activities says, State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments...when undertaking the collection and dissemination of information and intelligence to protect the United States. (Bush, 2008, Part 1)

The Body of Fusion Center Research

State and local fusion centers have been studied empirically by a number of researchers, since they are an important component of the homeland security enterprise. A significant number of studies and masters theses have addressed fusion centers including those from Carter, Carter, Chermak and McGarrell (2016), Carter, and Chermak (2012), Chen (2009), Coffey (2015), Comiskey (2008), Forsyth (2005), Fresenko (2010), Fries (2013), Fussell (2009), Graphia (2010), Harper (2009), Klem (2014), Ladner (2010), Larence (2008, 2010), Leavell (2007), Levin and Coburn (2012), McGregor (2010), Monahan (2009). Newbill (2008), Newkirk (2010), Regan and Monahan (2013, 2014, 2015), Rollins (2008), Saari (2010), Scott (2014), and Skahill (2010). As stated by Cilluffo, Clark, and Downing (2011), "Little empirical research,

however, has been done to study the weaving together of local, state, and federal counterterrorism efforts” (p. 1). Further, Taylor and Russel (2012) stated “Though fusion centers have been in operation for nearly a decade, there is a noticeable absence of information as to their effectiveness. Virtually no empirical evaluations have been conducted on them” (p. 195).

As described earlier in this chapter, state and local officials do have a critical role in protecting citizens in this federal republic with overlapping security responsibilities across all 3 levels of government. The FBI is not resourced to be able to deal with all the terrorist threats and reports that come in across the country, so this must be a collaborative effort. That is one of the main reasons why “these fusion centers have been created across the United States. Each is staffed with personnel from multiple agencies that help facilitate local, state, county and federal data sharing” (Serrao, 2010, para. 4).

Interorganizational Intelligence and Information-sharing

Interagency information-sharing is critical to the safety and security of this Nation. If the federal intelligence and law enforcement agencies had shared with each other what was known within their organizations about the al Qaeda terrorists before 9/11, and if this were then shared with state and local officials, it is very possible those attacks in 2001 could have been prevented (Zegart, 2009). While improvements certainly have been made since 9/11, interagency information-sharing is still very much a work in progress some 16 years later.

This issue is a significant challenge since sharing information among these numerous actors involves many overlapping statutory responsibilities, legal authorities,

and capabilities between these levels of government and multitude of agencies that pertain to countering terrorism (Imperial, 2005; Eack, 2008). However, these challenges are not completely unique to countering terrorism, as several other public sector functions have similar multi-agency and political challenges. This leads to the public administrative and policy theoretical framework that is employed in this study.

Theoretical Framework for Interorganizational Information-sharing

The study employed the theoretical framework of interagency information-sharing, in particular the opportunities it offers and the obstacles that prevent it from being effective. This theoretical basis is primarily derived from Sharon S. Dawes, Professor Emerita of Public Administration and Policy at the State University of New York at Albany. In 1996 Dawes conducted a study into the exchange of information between multiple agencies and published an article titled *Interagency Information-sharing: Expected Benefits, Manageable Risks* in the *Journal of Policy Analysis and Management*.

In short, her study was based on the premise that “sharing of program information among government agencies can help achieve important public benefits: increased productivity; improved policymaking; and integrated public services. Information-sharing, however, is often limited by technical, organizational, and political barriers” (Dawes, 1996, p. 377). This study examined the attitudes and opinions of government managers and showed they viewed interagency information-sharing to be beneficial and also revealed concerns about the organizational risks as well, and “The study proposes a theoretical model for understanding how policy, practice, and attitudes interact...to promote the benefits and mitigate the risks of sharing” (Dawes, 1996, p. 377). An

example of the Dawes theoretical framework as it relates to interorganizational information-sharing describes the technical, organizational and political aspects of both the benefits and barriers in Table 2.

Table 2

Categories of benefits and barriers associated with interagency information-sharing

Category	Benefits	Barriers
Technical	-Streamlined data management -Contributes to information infrastructure	-Incompatible technologies -Inconsistent data structures
Organizational	-Supports problem solving -Expands professional networks	-Organizational self-interest -Dominant professional frameworks
Political	-Supports domain-level action -Improves public accountability -Fosters program and service coordination	-External influences over decision-making -Power of agency discretion -Primacy of programs

Dawes, 1996, p. 378

This construct of interorganizational information-sharing was employed again by Zhang, Dawes, and Sarkis (2005), when they studied stakeholder expectations and how they are influenced by barriers and benefits to interorganizational information-sharing. These researchers stated, “It can be theorized that the expectation of benefits provides motivation for participants to engage in innovative efforts to share practice-related knowledge; while the expectation of barriers may undermine participants’ commitment to knowledge sharing initiatives and willingness to take risks” (Zhang, Dawes, & Sarkis, 2005, p. 549).

In 2009 Dawes employed this theoretical framework again with Cresswell and Pardo in an article titled *From 'Need to Know' to 'Need to Share': Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks*. In this latest study they identified that,

While public sector knowledge networks offer significant potential benefits for dealing with both wicked and tangled problems, our research suggests that they also face two sets of challenges that make them difficult to develop and sustain. One has to do with the nature of knowledge and the other with complexities of the boundaries to be navigated. (Dawes, Cresswell & Pardo 2009, p. 394)

It is evident that this model is relevant as a framework to study interagency information-sharing at fusion centers. Therefore, this research adapted Dawes (1996) theoretical framework to identify the opportunities and obstacles of federal interagency information sharing with nonfederal fusion centers. Clearly the greatest benefit of intelligence sharing in a homeland security context primarily comes from being able to share intelligence in order to collaboratively piece together available information and prevent terrorist attacks. Other opportunities and benefits also exist for domestic counterterrorism.

In regard to the barriers, some interagency literature offers a listing of various obstacles. One useful publication in this field is the 2009 military handbook titled *Interagency Teaming to Counter Irregular Threats*. This handbook includes some of these examples for barriers such as: legal, policy, procedural, lack of organizational mechanisms, classification/sensitivity, physical/virtual impediments, risk aversion,

inadequate incentives, organizational culture, and personality issues (U.S. Army Asymmetric Warfare Group, 2009). While this listing is not all-inclusive, it is a good starting point.

Domestic Counterterrorism Information-sharing

Sharing information and intelligence on terrorism for the homeland is a wicked problem due to the complexities of the different levels of government and the many various agencies involved (Dawes, Cresswell, & Pardo, 2009). Some of these challenges were mentioned in the 9/11 Commission Report, and some issues partially remedied in some new laws such as the USA PATRIOT ACT and the IRTPA (Adams, Nordhaus, & Shellenberger, 2011). The Homeland Security Act of 2002 made this interagency sharing of terrorism information a task for the new DHS and codified this role as,

To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States. (U.S. Code, 2002, PL 107–296 § 201, 9)

In order to accomplish this task, the Department of Homeland Security created what is now called the Office of Intelligence and Analysis (I&A). The former DHS Under Secretary for Intelligence and Analysis, Caryn Wagner (2010), testified to Congress about the importance of this intelligence and information-sharing role with partners at the state and local levels saying “It is our job to meaningfully convert what

may appear to be bits of unrelated information into a product that helps protect our communities...via a robust network of intelligence and law enforcement agencies participating in state and local fusion centers” (p. 3). Within this support component of DHS Headquarters is a State and Local Program Office (SLPO) and for the Office of Intelligence and Analysis itself,

I&A has a unique mandate within the Intelligence Community and is the federal government lead for sharing information and intelligence with state, local, tribal and territorial governments and the private sector. It is these nonfederal partners who now lead the Homeland Security Enterprise in preventing and responding to evolving threats to the homeland (U.S. DHS, 2015a, para. 9).

Former Secretary of Homeland Security Napolitano (2011) stated that, “DHS is intent on helping these fusion centers to develop their core capabilities to share and analyze information and to provide state and local law enforcement with useful, actionable information they can use to better protect their own communities” (p. 7). Former Under Secretary Wagner (2010) also described the establishment and importance of the Homeland Secure Data Network (HSDN), providing Secret-level intelligence and information capabilities to state and local partners, at fusion centers, and “This burgeoning network greatly expands two-way information-sharing flows between federal and nonfederal homeland security partners” (pp. 3-4). DHS has strived to make major improvement over the information-sharing infrastructure since virtually none existed before 9/11. However, there is still much room for improvement.

Obstacles to Domestic Interagency Information-sharing

Although the PATRIOT Act removed many obstacles that obstructed effective sharing of terrorism information between agencies, many other challenges remain. Some of these include organizational cultures, information technology, and other existing statutes that prohibit or impede effective interagency sharing (Sales, 2010). The PATRIOT Act and subsequent Foreign Intelligence Surveillance Act (FISA) adjustments did make it easier to share terrorism information between and among federal law enforcement agencies and the intelligence community, but it did not change the differing cultures that remain within respective agencies (Best, 2011). Organizational cultures and established practices remain a barrier to information-sharing between agencies. Olson (2008) discussed that law enforcement officials reluctantly share information among themselves let alone outsiders, “and the importance of protecting sources and methods within the intelligence community means that there are limits on how far any intelligence organization will go to share data” (p. 225-226).

The 9/11 Commission Report called for unity of effort in info sharing and stated, “The biggest impediment to all-source analysis--to a greater likelihood of connecting the dots--is the human or systematic resistance to sharing information” (Kean & Hamilton, 2004, p. 416). As the 9/11 Commission identified these gaps in terrorism information-sharing, they found insufficient mechanisms for effective sharing. The Commissioners also encountered traditional views that either everyone is responsible for information-sharing; or that it is up to intelligence workers themselves to decide whether they share information, resulting in “a ‘wait-and-see’ attitude in sharing information” (De Bruijn,

2006, p. 270). The many different organizational cultures and the interpersonal skills of the individuals involved remains a significant variable in interagency relations (Waugh & Streib, 2006). The 9/11 Commission Report specifically mentioned these agency cultural and interagency procedural dysfunctions as contributing factors in the U.S. government not preventing the 2001 terrorist attacks and they subsequently advocated for a change from the 'need to know' concept to a 'duty to share' mentality (Kean & Hamilton, 2004).

In relation to information technology impeding information-sharing, the former director of the Defense Intelligence Agency mentioned the difficulties of sharing when each agency operates their own information technology systems, which generally means agencies cannot access each other's data (Jacoby, 2002). James Clapper, the former Director of National Intelligence, declared during his confirmation hearing that he was "aghast at the state of information technology across the community, wondering why there's no single major combating-terrorism database with a robust search capacity instead of 50 some odd databases with varying degrees of technological sophistication" (Ambinder, 2010, para 3). While there have been great improvements in the area since 9/11, no optimal technological mechanism for intelligence sharing has been implemented.

In effect this makes most information-sharing a process of personal interactions between officials from different agencies. This generally requires a physical location where multiple agencies can exchange terrorism information, such as the National Counter Terrorism Center or NCTC was created to do (Best, 2010). Michael Leiter (2011), a former director of the NCTC, testified to Congress that interagency terrorism information-sharing has improved but "complex legal, policy, and technical issues as

well as the implementation of appropriate privacy, civil liberty, and security protections” still limits effective data sharing (pp. 6-7).

Other significant obstacles to effective counterterrorism include many remaining laws that prohibits or impede terrorism information-sharing between agencies. While the PATRIOT Act assisted in specifically allowing the sharing of information between some law enforcement agencies and intelligence agencies, it did not remove all of the impediments to effective domestic combating-terrorism. Significant obstacles remain for protecting citizens from determined terrorists such as agency cultures, incompatible and firewalled information technologies, and other laws that remain in effect. As Davis and Kayyem (2014) have written, “Often there are antiquated and bureaucratic barriers to information-sharing that serve no purpose and hinder the capacity of government to interpret different pieces of data from different sources” (paras. 3-5).

Some of the difficulties in sharing information among these numerous actors include the many overlapping laws, legal authorities, and differing capabilities between all three levels of government and the several agencies that have some role in terrorism (Imperial, 2005; Eack, 2008). Unfortunately, significant laws remain which prohibits or impedes terrorism information-sharing between agencies. Sales (2010) described some of these remaining statutory restrictions on information-sharing as the National Security Act of 1947 which bars the CIA from internal security functions and could prevent the CIA from sharing with federal law enforcement officials, the Posse Comitatus Act, which may prevent the Armed Forces from sharing information with domestic authorities. Sales

(2010) further states that the Privacy Act of 1974 which promotes individual privacy can also be a barrier since a

restrictive reading of the Act...could prevent, for example, U.S. Customs and Border Protection (Customs) from sharing data about arriving container ships with National Security Agency (NSA) officials who want to exploit it to screen for terrorist stowaways (pp. 1797-1798).

Pappas (2010) conducted a study about the condition of domestic terrorism information-sharing after 9/11 reforms, and found that agencies still fail to effectively share information and concluded that “it is clear that the change that was expected when enacting these laws has failed in many regards” (p. 15). A recent survey of key fusion center leaders across the country also found that they were not very satisfied with information-sharing (Carter, Carter, Chermak, & McGarrell, 2016). Despite the expansion of JTTFs, and the proliferation of fusion centers, “the United States still lacks a coherent national domestic intelligence collection effort” (Jenkins, 2011, p. 6). To find recent examples of failures in counterterrorism information-sharing within the United States, one need look no further than the terrorist attacks at Fort Hood and Boston.

Information-sharing Lapses at Fort Hood and Boston

Two post-9/11 events that could potentially have been prevented if more information been shared with relevant partners include the 2009 Fort Hood shooting by Army Major Nidal Hasan, and the Boston Marathon bombings in 2013 by the Tsarnaev brothers. In the case of Fort Hood, the FBI did not share with the military or with state and local officials in Texas that Major Hasan was making repeated email

communications with a known key al Qaeda figure in Yemen (Filler, 2010; Verton, 2011; Webster, 2012; Zegart, 2015). Had Hasan's military supervisors, counter-intelligence agents, or local officials been informed of this extremist activity, it is possible that other pieces of the puzzle could have been assembled to stop the attack (McCaul & Keating, 2014; Shane & Johnston, 2009; United States Senate Report, 2011).

In regard to the Boston Marathon bombings, a sole FBI Agent in the Boston JTTF looked into a report from Russia that Tamerlan Tsarnaev was a radicalized jihadist, but he did not share this information with anyone from state and local agencies (including those who were members of his own counterterrorism squad in the JTTF), or with either of the fusion centers—Boston Regional or Massachusetts (Bender & Bierman, 2014; Bodden, 2014; Davis & Kayyem, 2014; Etzioni, 2013; Evans, 2013; Inspector Generals, 2014; Reilly, 2013; Stokes, 2013). Had information been shared with local officials, even those local detectives from Boston within the JTTF, it is very possible that Tsarnaev could have been linked to two recent murders, or his later travel to Chechnya flagged and the attack potentially disrupted (McCaul & King, 2014; Viser, 2013; Zalkind, 2014). It is easy to second guess post facto, but the combined Inspector Generals of the Intelligence Community, the Department of Justice and the CIA stated it should have been shared with state and local officials (Inspector Generals, 2014).

Again, hindsight is always 20/20, but in both of the cases of Fort Hood and Boston, had this intelligence of a terrorist nature on Hasan and Tsarnaev been shared with appropriately cleared state and local officials, it is possible that the significant additional suspicious activity of these soon to be terrorists (that was not known or observed by the

FBI) could have all been collated with this federal intelligence and resulted in disrupting the attacks and many lives saved (Kranish, M., Bender, B., Murphy, S. P., & Bierman, N., 2013). Just as with 9/11, if state and local officials had known what federal law enforcement and intelligence agencies had known, then routine encounters with local law enforcement could have made the difference between life and death for unsuspecting innocent citizens.

Fusion Centers and Information-sharing

An essential element of any fusion center is the ability to receive intelligence and information. The DHS 2014 National Network of Fusion Centers Final Report states,

As focal points for the receipt, analysis, gathering, and dissemination of threat-related information between state, local, tribal, and territorial governments and the private sector, fusion centers are uniquely situated to provide critical information and subject matter expertise that allow federal law enforcement partners and the Intelligence Community (IC) to more effectively “connect the dots” and protect the homeland. (DHS, 2015b, p. iii)

It is important to note that information-sharing occurs on the top half of the vertical plane between federal and state entities, as well as horizontal sharing between multiple states and urban areas. These fusion centers can also become hubs for collaborative operations to “detect, prevent, investigate, and respond to criminal and terrorist activity” (Larence, 2008, p. 1). Sharing also occurs on the bottom half of the vertical plane where fusion centers disseminate to customers like state troopers, and well as receive reports from patrol officers and the public. Clearly, “A core purpose of a

fusion center is to facilitate the sharing of information across law enforcement and other public safety and private entities. Yet, information-sharing is one of the biggest obstacles to be overcome” (Teutsch, 2010).

The Department of Justice and Department of Homeland security baseline capabilities for fusion centers and the annual evaluation of them address as the first critical operating capability or COC as the receiving of information or intelligence to provide stakeholders with an accurate threat picture, outlined in these 5 factors:

COC 1 – Receive

1. Fusion center has approved plans, policies, or standard operating procedures (SOPs) for the receipt of federally-generated threat information
2. Fusion center has a plan, policy, or SOP that addresses the receipt and handling of National Terrorism Advisory System (NTAS) alerts
3. Fusion center personnel with a need to access classified information are cleared to at least the Secret level
4. Fusion center has access to sensitive but unclassified information systems
5. Fusion center has access to HSDN and/or FBINet (i.e. within fusion center or on-site). (2015 Annual Assessment, 2016, p. 20).

Fusion centers have improved significantly since 9/11 when the expansion began in earnest. DHS reported in January 2015 that the National Network of fusion centers continues to make progress and for the first time “all fusion centers have plans, policies, or standard operating procedures for all four Critical Operational Capabilities (COC)” (DHS, 2015b, p. iv). However, each fusion center is unique, and as has often been stated

at National Fusion Center Association events, “if you have seen one fusion center you have seen one fusion center” (Abold, Guidetti, & Keyer, 2012, p. 2). Since “no neat lines divide criminal and terrorist activities. This shows why fusion centers are so vital in helping agencies gain a more comprehensive picture of the threats they face” (Johnson, 2007, p. 29).

The problem is that these centers require information and intelligence to fuse. If agencies do not share, they are very limited in what they can analyze and warn state and local officials on. In early 2016 testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, the California Governors’ Homeland Security Advisor discussed improvements in information-sharing, but also described the less than optimal present condition. “While there exist significant improvements in collaboration and relationships among responders, there remains an overall lack of a comprehensive ‘unity of effort’ in our information-sharing environment” (Ghilarducci, 2016, p. 4). Further, the Business Executives for National Security reported in March 2016 that “information-sharing initiatives are frequently sub-optimized...MORE MUST BE DONE to institutionalize effective information-sharing programs between federal, state, and local partners, and to formalize the real-time sharing processes” (Barron, Lewis, Silberstein, & Shapiro, 2016, pp. 7-8).

A few studies have examined fusion centers and information-sharing such as Carter, Carter, Chermak and McGarrell (2016), Joyal (2012), Carabin (2011) and Graphia (2010). However, no studies have looked specifically at classified intelligence sharing, and none have singled out the sharing of intelligence from federal agencies down to state

and local fusion centers. Additionally, none of these studies have specifically addressed the sharing of intelligence for the purpose of countering domestic terrorism.

The studies that have asked research questions related to information-sharing only studied the concept of sharing in the most general sense. No study has completely factored in the many different ways and directions that fusion centers share, nor the many different categories of what information and intelligence is shared. For example, fusion centers share internally, externally, vertically, horizontally, and receive and transmit all types of information (data, information, and intelligence). The above mentioned previous research does not specify what exactly is meant by studying information-sharing in regard to fusion centers, nor do they specify if they are addressing intra-agency sharing or inter-agency sharing.

Taking the risk of oversimplify a highly complex sharing environment, figure #2 attempts to depict some of the many different directions and partners that fusion centers share with, both internally and externally. This graphic depiction highlights the focus of this research by placing sensitive intelligence sharing on terrorism from federal agencies to a hypothetical state fusion center as bold blue arrows.

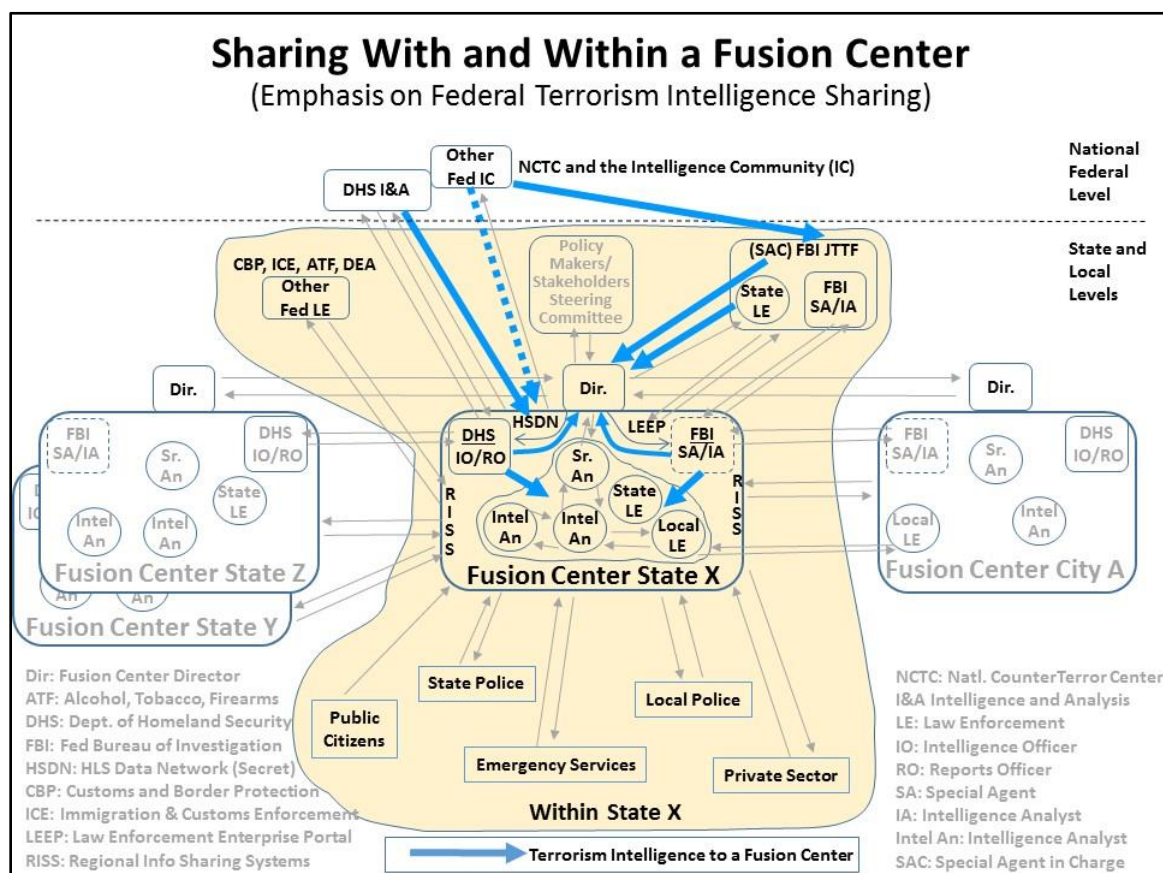


Figure 2. Sharing with and within a fusion center.

Fusion Centers and JTTFs

As previously mentioned in this chapter, a recent government commission investigating FBI practices found that many still view sharing with the FBI as a “one way street” and that means information goes to the FBI, not back out to partners (Hoffman, Meese & Roemer, 2015). On the other hand, some in the FBI feel that DHS sponsored fusion centers are misapplied and an inappropriate “diversion of critical resources and manpower” that should instead be allocated to the FBI for domestic counterterrorism (Verton, 2011, para 9). Some have described the FBI view as “an insurgent-like resistance to share certain streams of information with fusion centers and their main DHS

interface – the Office of Intelligence and Analysis (I&A) – due to the fact that active investigations have been compromised” (Verton, 2011, para 11).

In some instances, there has been effective FBI JTTF and fusion center information-sharing, but this has mainly been due to constructive personal relationships built between specific individuals within respective agencies that grew over time at certain locations (Apuzzo & Goldman, 2013). A core role now for each fusion center is to function as “a nerve center for all calls coming into the statewide terrorism tip line. Those with a suspected nexus to terrorism are forwarded to the JTTF for further investigation” (Johnson, 2007, p. 30). However, recent studies have shown the relationships between fusion centers and JTTFs are not necessarily healthy and effective (Carter, Carter, Chermak, & McGarrell. 2016; Mayer, 2016; Mitchiner, 2013).

Numerous studies and Congressional reports have described how the overlap between fusion centers and JTTFs was not well planned or deconflicted (Larence, 2008a; McCaul & King, 2013; Rollins, 2008). Since there is no overall plan or standard template for a JTTF or fusion center, this can “lead to duplication of effort and competition for mission and related resources” (Tromblay, 2015, p.141). As Filler (2010) has written,

State and regional intelligence fusion centers have evolved significantly as a place to pool multiple sources of intelligence within a region, but the next level of integration, such as between the FBI’s Field Intelligence Groups, Joint Terrorism Task Forces, fusion center analysts and local law enforcement remains unmet. Nor has a construct outlining how fusion centers across the country should

interoperate within a larger domestic intelligence framework been developed.

(para. 13)

The literature is clear that both fusion centers and interagency information-sharing have improved markedly since 9/11. However, the literature also identifies many interagency information-sharing obstacles and deficiencies. An appropriate theoretical framework to evaluate these phenomena is the Dawes (1996) model of interagency information-sharing to identify the benefits and barriers. No empirical research into how federal agencies share sensitive domestic counterterrorism intelligence with state and local officials through fusion centers exists, nor has this theoretical framework been employed to study fusion centers.

Summary

While improvements certainly have been made with interagency information-sharing, there are many issues that still need to be studied and analyzed for improvement. As this chapter addressed, fusion centers can and should serve a key role in domestic counterterrorism. The FBI cannot do it alone, and the state and local agencies have significant capabilities and the Constitutional responsibility to protect their citizens. While much has been written about fusion centers, none have empirically researched the issue of federal agencies sharing counterterrorism intelligence with subfederal fusion centers. All three levels of government have a true 'duty to share' terrorism intelligence to contribute to the collaborative effort that is necessary to stop both overseas terrorist groups and homegrown extremists. In order to prevent more attacks like 9/11, Fort Hood,

and Boston, it is essential to identify the key opportunities and obstacles to domestic counterterrorism information-sharing at fusion centers.

This chapter examined the issues revolving around intelligence, the interagency information-sharing failures, the challenges of domestic security in this federal intergovernmental system, counterterrorism reforms, and the history and growth fusion centers themselves. This chapter also identified the interorganizational knowledge sharing theoretical framework upon which the proposed study is built, as well as the domestic counterterrorism information-sharing challenges, the role of fusion centers and information-sharing as well as this topic being a gap in the literature. Chapter 3 outlines and discusses the methodology of this study, research questions, population, data analysis procedures, instrumentation, and ethical considerations.

Chapter 3: Research Methodology

Introduction

This chapter will outline the methodology used to examine the opportunities and obstacles of federal counterterrorism information-sharing with state and local fusion centers. Fusion centers are a rich topic for a qualitative, intergovernmental information-sharing research study. Each fusion center hosts various agencies from multiple levels of government, all combined at one location, including representation of the federal agencies themselves. The purpose of this study was to examine the opportunities and obstacles of sharing federal counterterrorism information with state and local fusion centers. This research advances the understanding of aspects of public policy as it relates to homeland security and fill an important gap in the literature on information-sharing to combat terrorism. Specifically, how effective does the state and local fusion center model provides for federal agency intelligence and information-sharing with state and local partners on terrorist threats.

This chapter covers the following topics: methodology, research questions, role of the researcher, data collection, selection of participants, interview protocol, data analysis, ethical considerations, and credibility and reliability.

Research Design

I used a qualitative case study to examine how federal agencies share information and intelligence with fusion centers on terrorist threats that are likely impact their jurisdictions. With this empirical and pragmatic methodology, I was able to reach practitioners in their own setting and to examine, in depth, how the agencies interact

(Yin, 2009; Stake, 1995). Case study research offers the chance to explore a narrow topic based on multiple sources within the context of the phenomenon (Baškarada, 2014; Hancock & Algozzine, 2006).

Based on Yin's (2003) suggestions, I examined documents and records; the focus, however, was on interviews of experts working in a fusion center. Thus, interviews of individuals from different agencies at five fusion centers provided multiple perspectives on the subject and yielded the data needed to answer the following research questions:

1. How effectively are fusion centers fulfilling their intended purpose of improving homeland security by receiving terrorism information and intelligence from federal agencies?
2. What are the opportunities in, or benefits of, federal counterterrorism intelligence sharing with fusion centers?
3. What are the obstacles or barriers to federal counterterrorism intelligence sharing with fusion centers?

Site Selection, Sampling Size, and Participants

This selected research design employed an exploratory case study analysis of five state and local level fusion centers in the East Coast region of the United States. Any region of the country can provide an appropriate sampling of fusion centers, however most of the major al Qaeda terrorist attacks and attempts since the 1990s have been on the East Coast (Mayer, Carafano & Zuckerman, 2011). Additionally, the East Coast of the United States is the location of the national capitol where all these federal agencies are headquartered. The proximity to the capitol makes it more likely to have participants

in state and local fusion centers who will have interacted with federal officials, and they may therefore know more about the opportunities and obstacles of interagency information-sharing.

Site Selection and Sampling Size

Of the 78 total recognized fusion centers, there are 23 nonfederal fusion centers across the 16 states on the East Coast of the United States and every state in the East has at least one fusion center. Two of these East Coast states have three fusion centers (one for the state and two regional fusion centers), and two states have two fusion centers (one for the state and one major urban area). The East Coast is also home to the nation's capital, and there is a regional fusion center supporting the District of Columbia.

Researching 5 fusion centers therefore entails 22% of the total East Coast fusion centers.

Fusion center sites were selected for research based upon criteria to ensure different locations were visited to offer various perspectives from across the spectrum of jurisdictional and regional environments. This included researching fusion centers in the south as well as those from the north of the country, as well as both large and small states were selected. Fusion centers from both the state level and local/regional levels were proportionally selected. Of the 78 nonfederal fusion centers, there are currently 53 state level (68%) and 25 major urban area (32%) fusion centers spread throughout the country, so this study therefore researched 3 at the state level (60%), and 2 fusion centers for major urban areas (40%) (Carter, Carter, Chermak & McGarrell, 2016).

Fusion center research sites were further selected from across the spectrum of the three principal functions (or types) fusion centers as described by Wight (2015),

including those that are investigative in focus, centers that are principally analytical, and those with a watch function. This sampling of 5 fusion centers also includes two major U.S. cities with a significant critical infrastructure and regional importance. A major urban area presents a frequent target of terrorists with high value, so these fusion centers serve as a critical example of information-sharing where “if it doesn't happen there, it won't happen anywhere” (Patton, 2002, p. 236).

An additional factor for site selection criterion was that the fusion center director or even higher government official had to approve researching their fusion center. This was a significant challenge due to the sensitive nature of ongoing domestic counterterrorism operations as well as the significant controversy still surrounding fusion centers by some detractors in Congress and the private sector (German & Stanley, 2007; Levin & Coburn, 2012). Additionally, this research was not government sponsored, without compensation, and completely voluntary for both the centers and individual participants. Further, a recent fusion center researcher had sullied the potential participant pool by conducting interviews and then writing up very negative finding and naming the centers visited in the process (McQuade, 2016). Not every fusion center that was approached agreed to participate, so the next center on the list was approached based upon the criteria until all 5 were completed. During the recruiting process it was vital to assure both the leadership of prospective fusion centers and individual participants that confidentiality and anonymity would be maintained.

Participants

Interviews were conducted with 4-5 officials or analysts performing various roles and representing different agencies at each of the participating fusion center sites. All participants were identified as those with insider access, and only individuals who actually work within the fusion center itself were interviewed. Individuals targeted for interviews at each fusion center included personnel in the following positions: Fusion Center Director or Deputy; Fusion Center Intelligence Analyst; DHS Intelligence Officer/Reports Officer; FBI Special Agent or FBI Intelligence Analyst (or liaison to the fusion center); as well as analysts or other officials assigned to the fusion center from other federal, state, or local agencies. Only fusion centers that are formally recognized by both DHS and the National Fusion Center Association (NFCA) at the time of data collection were considered. Contact information for each fusion center is publicly available both on the DHS website (<https://www.dhs.gov/fusion-center-locations-and-contact-information>) and the NFCA website (<https://nfcausa.org/default.aspx/MenuItemID/117/MenuGroup/Public+Home.htm>).

Interviews

King (1994) states the goal of a qualitative research interview is to “see the research topic from the perspective of the interviewee, and to understand how and why he or she comes to have this particular perspective” (p. 14). To effectively interview personnel in fusion centers, this research employed a hybrid approach that included both a structured interview with the same questions asked of each participant at each center, as well as time for an open-ended discussion about information-sharing issues. Patton

(2002) describes this as a combined approach where one employs a “standardized format by specifying certain key questions exactly as they must be asked while leaving other items as topics to be explored at the interviewer’s discretion” (p. 347).

These voluntary interviews were conducted either in person or telephonically, and were designed to highlight the various perspectives from different individuals representing many different agencies and separate fusion centers. In-person ‘face to face’ interviews are preferred, but telephone interviews may be employed. Each interview lasted approximately 30 minutes, with the participants being asked both specified and open-ended questions. This does not count the time spent in discussions with fusion center personnel before and after the interviews discussing information-sharing and touring the facilities. Appendix A includes the list interview questions which were derived from the research questions and the theoretical framework of Dawes (1996) interagency information-sharing.

Data Collection and Analysis

The data were primarily collected during site visits and interviews as described above. The interviews were recorded and the notes and recordings were transcribed for analysis. Participants were also offered the opportunity to provide input at the end of the interview to ensure their perspectives were accurately recorded and to ask questions of the researcher. The assembled data from interviews was analyzed for word trends and themes using NVivo qualitative data analysis software (NVivo v11). This software is specifically designed for unstructured qualitative data, and it assisted in processing and categorizing the information using an “open” coding method (Bazeley, 2012). This

malleable method enables the researcher to code without many restrictions in order to effectively identify patterns in the research.

The open coding method is appropriate for conducting exploratory research such as this, as it allows the researcher additional flexibility for discovery. The analysis of the text based qualitative data using NVivo also provided results such as word frequency and as well as comparisons by job function, agency, location (Bazeley, & Jackson, 2013). Some anticipated themes for obstacles to interagency information-sharing included bureaucracy, personalities, compartmentalization, fear of leaks, and ownership. Through this data collection on fusion centers and subsequent analysis, this study identified both opportunities and obstacles to intelligence and information-sharing from federal agencies to state and local officials.

Role of the Researcher, Bias Mitigation and Validity

Qualitative research is interpretive and involves the researcher interacting with participants to study their experiences and perceptions and that the researcher should also provide their own background and past experiences (Maxwell, 2012). A researcher experienced in the field of study can be an advantage when it comes to having credibility with the participants and may also facilitate gaining entry and permission to research on site. However, researcher experience in the field can also have pitfalls that need to be overcome such as bias and preconceived notions.

I personally brought many years of experience working in the Intelligence field as well as being a retired U.S. Army Lieutenant Colonel to the project. I also have been a member of a military fusion center in a war zone that brought together many different

agencies in order to combat terrorism. During the research, I also served as a University Assistant Professor of Homeland Security. While I have not worked in a domestic fusion center, and have no relationships with any of them, my experiences and titles did assist in getting permission from fusion centers to conduct research. This also provided credibility as a researcher with the participants as a fellow practitioner. However, these experiences also shaped my views, and this potential bias needed to be mitigated.

In an effort to reduce and mitigate experiential bias, steps were taken to ensure my personal views and perceptions did not influence or compromise the study. The first step was to state that there is no conflict of interest with this study, I had no personal interest in the results of the study—either professionally or financially (Maxwell, 2012). This research was purely for academic inquiry and solely about a topic I am interested in learning more about in order to assist in closing the gap in the literature. I had no preconceived notions about what the findings will be and am open minded and willing to take the research where it leads – not lead the research based on any preexisting ideas.

The next step to ensure bias was not interjected into the research was the dissertation committee itself. One of the roles of dissertation committee members is to hold the researcher accountable to the scientific method make sure bias is not interjected into the study (Miles & Huberman, 1994). This was accomplished during periodic dissertation reviews, updates with the dissertation chair, and during oral defenses.

The validity, credibility, and confirmability of the research was ensured through employing multiple strategies to maintain the high standards of quality and integrity. These strategies included variation in participant selection, reflexivity, and dissertation

committee review (Anney, 2014). Participant variation was employed by ensuring that interviewees come from varying positions within fusion centers such as interviewing individuals from the upper-level leadership, from mid-level leaders, and with those doing most of the work such as investigators and analysts. Reflexivity was employed by using a field journal for “creating transparency in the research process, and explore the impact of critical self-reflection (Ortlipp, 2008, p. 695). Also, the open coding results will be specified in Chapter 4 to ensure that another researcher can duplicate this study and achieve same results.

Ethical Protection and Confidentiality of Participants

This research involved interviews where participation was strictly voluntary and completely anonymous. There was no solicitation of protected populations, and participant employment at a highly secure fusion center made that possibility highly unlikely. The identity of both the fusion center sites visited as well as the names of individual participants will remain anonymous. No participant personal information such as names or contact information was recorded. Anonymity is important to ensure that the participants can share their experiences and perspectives freely without concern for retribution or other implications.

Data collection methods and confidentiality were thoroughly explained to the participants, as well as to the leadership at each fusion center in advance. The only identifying information on participants that was recorded included: the type of fusion center (state level or major urban area), the job function or role such as “Analyst” or

“Federal Agency Liaison” and all data gathered in this study will be kept confidential. At no time are individual participants or the identity of fusion centers researched disclosed.

Additionally, no research was conducted until approved by the Institutional Review Board was secured. Walden University’s approval number for this study is 07-18-16-0192667. Further, no research was undertaken until cooperation agreements for the study were secured from fusion center leadership at each location. Before any participant interviews, volunteers were briefed on the study and provided with informed consent forms. The participants were not subjected to any risk, and they were given the opportunity to ask questions, as well as the freedom decline participation at any time.

Data Storage

Data collected during this study were stored electronically on a password-encrypted computer located in a secured area with monitored alarms. All notes from interviews were transferred to text based electronic files. Any publicly available hard copy materials provided by fusion centers were scanned in and retained as secure electronic files, just as data collected during interviews. In accordance with the standard University Institutional Review Board practices, all research documentation will be maintained for a period five years and then destroyed.

Conclusion

The case study method provided an effective qualitative research approach that allows for the study of this bounded issue of domestic counterterrorism information-sharing using interviews at multiple sites and of various agencies. Larence (2011) stated that,

The federal government recognizes that fusion centers represent a critical source of local information about potential threats, including homegrown terrorism, and a means to disseminate terrorism-related information and intelligence from federal sources. DHS, which has a statutory lead for state and local information-sharing...has taken steps to partner with and leverage fusion centers. (p. 10)

Fusion centers are a major facet of the local efforts to protect the U.S. because the “ability of local government agencies to effectively utilize technologies to share information constitutes a critical element in nationwide efforts to fight terrorism” (Akbulut, et al, 2009, p. 143). However, many barriers to effective information-sharing exist and fusion centers “have not achieved fully integrated and reliable communication and collaboration mechanisms” (Joyal, 2012, p.368). While some research on fusion centers exists, Carter and Carter (2009) found “fusion centers are so new that there has been no empirical assessment of their effectiveness” (p. 1336). This research contributes to closing this gap in empirical research using a qualitative case study framework consisting of expert interviews of fusion center personnel.

Chapter 4: Results

Introduction

The research assessed how effectively fusion centers are fulfilling their intended purpose: to improve homeland security by receiving terrorism information and intelligence from federal agencies. Data on federal counterterrorism information-sharing was collected through interviews conducted at five fusion centers on the East Coast of the United States. This chapter presents the interview data gathered from the fusion centers, including both state level and major urban areas; the chapter also presents the patterns, research findings, and resulting analysis of the data.

Study Sample Process

Gaining access to fusion centers to collect data proved to be the most challenging part of the research process. This was due to three reasons: (a) the sensitivity of the intelligence and law enforcement work going on inside fusion centers, (b) the controversial perceptions about domestic intelligence, and (c) recent interview-based research in which negative findings were published, participants were directly named, and the centers were shamed. This challenge was eventually overcome due to (a) my experience as an intelligence professional, and the (b) relationships established with personnel in fusion centers during the course of research. This study would have likely ended with only two centers visited were it not for the direct intervention by some helpful and interested fusion center directors and federal agency personnel who took a personal interest in this study and assisted with outreach.

After sending participation requests to fusion centers in the East Coast, the target area, I was ultimately able to gain access to five centers that were willing to participate in the study. As described in Chapter 2, this sampling included three state fusion centers and two major urban areas. Researching 60% and 40%, they closely matched the national percentages of 68% and 32% respectively for the ratio of fusion centers compared to state and local centers. Two of the states were large and had multiple counties, multiple JTTFs, and major urban areas; the third state was smaller.

Five personnel from each of the five centers were recruited for interviews, for a total of 25 participants. Participation in the study was strictly voluntary and interviewees were informed they could withdraw at any time during the process. However, all volunteers fully participated in the process. Each answered all of the background questions and all 12 interview questions. Participants included upper level management such as directors and deputy directors, middle level management such as senior analysts and federal agency representative, as well as those in nonsupervisory positions such as analysts and investigators. All participants were actually working within a fusion center at the time of data collection and came from various positions within each center.

From the five fusion centers participating in the study, I was able to recruit personnel from agencies across all three levels of government spanning federal, state, and local levels. Participants were specifically selected because they encompassed a variety of backgrounds to include state and local law enforcement officers and investigators, federal agents and intelligence officers, as well as intelligence analysts from state and local agencies. At each fusion center I was able to interview at least one person from each

of the three targeted sub-categories within each fusion center including senior leadership, federal representatives, and intelligence analysts. These participants provided firsthand knowledge directly related to federal level intelligence sharing with their respective fusion center. It is for this reason that each of the participants from all three levels of government and across this span of duties and responsibility levels were recruited to be interviewed for this study.

Data Collection Method

Data collection occurred through interviews mainly conducted on-site and in-person with the 25 research participants conducted in August and September 2016. The interviews were all performed in-private, one-on-one and recorded via an Olympus digital recording device. This allowed for ease of transcription and facilitated the researcher being able to actively listen to the answers. Four of the five fusion centers were visited by the researcher to conduct face to face interviews, and one fusion center was researched by conducting telephone interviews. Additionally, the researcher visited two different fusion centers a few years earlier (one state and one regional) unrelated to data collection. This offered the researcher an overall qualitative context of 6 total fusion centers physically visited (four researched for this study) spanning from New England to Florida, and only one site researched virtually/telephonically.

Each participant in the study was asked six background questions which provided the needed data to identify the interviewee career field, position in the center, leadership level and longevity. Twelve interview questions to ascertain their experiences and views on federal counterterrorism information-sharing with their respective fusion center. Due

to the sensitive and potentially controversial nature of this study, third parties were not allowed to observe or listen to the interviews, which also ensured anonymity and that the participants would feel free to express their opinions. Each fusion center and individual participants were assured their identities would remain confidential and the study findings would not attribute collected data to any location or specific person. Additionally, the participants were advised during recruiting and informed consent processes that the study would remain at the unclassified level and not get into technical details involved with the information technology or systems involved in federal intelligence sharing on terrorism.

As the researcher, I did not interject my personal views and opinions during the interview process, and made a point to keep my expressions neutral as not to influence the interviewee. This helped to ensure that participants answers were their own and not influenced by any researcher opinions or biases. The duration of interviews ranged between 20 and 50 minutes, with the average time close to the planned 30 minutes. The variability between the interview length was mainly based on how much individual participants wanted to talk about each question, as well as the participants' experience level with and passion about interagency information-sharing. Each participant provided detailed responses on federal intelligence sharing with their fusion center, and their own thoughts about the opportunities and obstacles for effective terrorism intelligence sharing.

By actually visiting four of the five centers researched, I was able to gain rich context into fusion centers by conducting the research on-site. Not only was I able to spend at least one day at each facility, visits to some centers spanned multiple days,

which provided me with an opportunity to see those centers in operation. While I did not participate in any analysis or closed door meetings, I did observe all the various workspaces, offices, conference rooms as well as some interactions between analysts, agents, investigators and fusion center leaders. This was further contextualized by my own personal experiences serving in a military counterterrorism fusion center overseas. Having context from my own fusion center experience coupled with observations of state and local fusion centers in action assisted in framing recommendations for this research.

During discussions with these 25 participants, I learned indirectly about other challenges and successes from other fusion centers that were mentioned in the interviews. This is due to the national network of fusion centers being a network of networks where directors, senior analysis and others are often in contact with one another (see Figure 2. Sharing With and Within a fusion center). While the five fusion centers participating in this research generally had very positive relationships with their corresponding JTTFs, multiple participants mentioned accounts of dysfunctional relationships and a serious lack of sharing from JTTFs. Collecting these examples of deep and rich data from participants as well as observations could not have been gained from quantitative surveys or by solely conducting telephone interviews.

Immediately after each interview, the recordings were reviewed and transcribed into a Microsoft Word document. Each document was sorted by location and participant number (Site A, B, etc and Participant 1, 2, etc). Additionally, each interview form included the background information for further analysis such as position within the fusion center, years at that center, leadership level, etc. (see Appendix A for the list of

background questions). All interview files on participants were saved on a password-encrypted computer and organized according to the fusion center site files. At the conclusion of researching all five fusion centers, interview data was compiled and analyzed.

Study Sample Description

The individuals targeted for interviews were those working in counterterrorism related functions within the fusion centers, or secondarily those who could benefit from federal intelligence sharing on terrorism threats. Based upon recruitment process and background questioning, the composition of the 25 participants consisted of 11 law enforcement professionals (44%) and 14 intelligence professionals (56%). The years of experience of the participants in their respective career fields ranged from 1 to over 20 years, with the average being 14.4 years. See Table 3 on Study Participant Roles below, and more details in Appendix B: Participant Background By Site and Totals.

Table 3

Study Participants by Fusion Center Role

	Site A	Site B	Site C	Site D	Site E	Total
Director/deputy director	1	1	1	1	1	5
Senior Intelligence Analyst	0	0	1	1	1	3
DHS representative	1	1	1	1	1	5
FBI representative	1	0	0	1	0	2
Detective or investigator	1	0	0	1	1	3
Intelligence/criminal analyst	1	3	2	0	1	7
						25

The study sample included five upper-level leaders with the director or deputy director being interviewed at every fusion center (four directors and one deputy). Also,

eight middle or lower level supervisors participated and 12 nonsupervisory personnel giving the breakdown of 52% leadership and 48% non-leaders. The participants came from all three levels of government with 7 from federal agencies (28%), ten from the state level (40%) and eight from the local or city level (32%). The participants' total longevity of service in the fusion centers researched spanned from less than one to over ten years, averaging out to 4.68 years for all participants. This is a significant amount of time considering the frequency of rotating in fusion center personnel and the fact that fusion centers have only become relatively mainstream since 2004. Interestingly, the newest fusion center participant interviewed (less than a year) was a former New York City Police Officer who previously worked in the famous NYPD Intelligence Division and actively worked counterterrorism cases before moving to a new city and joining a fusion center as an analyst.

At each fusion center the expressed goal was to interview a diverse set of only five participants at each center for consistency of data. These individuals were targeted based on their role in the center (directors, federal representatives, investigators, and analysts) and across the spectrum of levels of government (federal, state, and local) as well as leadership and non-leaders. For the seven federal representatives there was a DHS representative at each center interviewed and only two from the FBI. This limited number of FBI representatives interviewed also directly matched the limited amount of time FBI personnel spend at fusion centers with most only being present about two days a week and in one fusion center the FBI position was vacant. The FBI rarely assigns personnel to a fusion center on a permanent basis, and most often conducting liaison with the fusion

center is an additional duty on top of their primary position within a nearby FBI field office or JTTF. All participants were actively working in a state or local fusion center at the time of research. A few participants mentioned having worked in more than one fusion center, although this was not a specific background question.

Interview Questions Background

The questions asked during the interview were derived from the three research questions and solely focused on federal intelligence sharing with state and local fusion centers on terrorist threats. The 12 interview questions, were primarily formed from the Dawes (1996) interagency information-sharing theoretical framework and aligned to focus on benefits and barriers to this intelligence sharing on terrorism with fusion centers (for all 12 interview questions, see Appendix A). In accordance with Dawes theory the questions were designed to give interviewees a framework to discuss their practitioners' perspective on federal terrorism intelligence sharing with their fusion centers. The emphasis was on identifying the benefits and opportunity of intelligence sharing with the fusion center as well as specifying the barriers, obstacles and risks of the same specific sharing dynamic. The questions were contextualized around terrorism intelligence as well as the role the fusion center plays in countering terrorism. All of the participants seemed to immediately comprehend the questions and a number of expert participants commented afterward that the questions were very good and thought provoking.

Analysis of the Data

The data analysis occurred after the completion of all interviews and the compiling of all transcripts into NVivo (version 11). All participant interviews were

added into NVivo as “sources” and then categories as “cases” and given person “attributes” to match the 6 background questions “classifications” by case. Then the interview questions were added as “nodes” and the data were analyzed by each question and through the aspect of each factor such as profession, role, longevity and type agency.

Through the analysis by interview question, it was apparent that explicit themes as well as less obvious patterns were revealed in the interview data. There were also trends and patterns revealed based upon background factors. Additionally, all 12 interview questions were subordinated to the three research questions and coded and analyzed based upon the research questions focused on Dawes (1996) interagency sharing theory.

Themes and patterns presented themselves collectively for all participants as well as other trends based upon background factors such as: those participants in a leadership position and longevity within a center, responses based on years of experience in the career field, and responses based on position within the fusion center. However, there were no patterns or differences between the various levels of leadership within fusion center managers and supervisors (only differences between leaders vs non-leaders).

Collective Participant Responses to Federal Terrorism Intel Sharing Questions

For this research, the questions focused on gaining qualitative data on the perceptions of federal counterterrorism information-sharing with these nonfederal fusion centers. This study focused on asking how well is the federal government sharing terrorism intelligence with fusion centers, in what ways are they sharing it, what obstructs sharing, and what could make this sharing more effective. The responses from all the

participants collectively revealed clear trends in the interview data on these benefits and barriers. However, some questions yielded a range of answers based additional factors, such as differences between sites based upon the specific and distinct roles of different fusion centers. The following represents a summary of the 12 questions and the thrusts of the collective participant responses (henceforth referred to as P1-P25) with key excerpts provided for each interview question as exemplars.

Q1. What role does your fusion center play in counterterrorism?

Participants from each of the fusion centers mentioned at least two aspects in countering terrorism. The first role is receiving and vetting suspicious activity reports, and the second is disseminating relevant terrorism bulletins and other products to those who need it – mainly police and other first responders. Interestingly, this role in vetting suspicious activity reports evolved over time as most fusion centers started before the baseline capabilities came out in 2008 starting the formalization of suspicious activity reporting (Department of Justice, 2008). A representative participant response was,

Here at this center, the major role played in terms of counterterrorism is the one that is played in most centers across the country in the sense that suspicious activity reports (SARs) that come in are vetted and...as soon as the SARs come in and there's a potential for terrorism related behavior it automatically goes to the JTTF and database checks are run at the state level at the local level based on the fact that here in this state much of that information is available, the access that the state analysts have here at the this center includes basically all the local law

enforcement databases for the state and they're all kind of aggregated, so those checks happen here.

Aside from these two consistent counterterrorism roles for all sites, there was a range of additional responses to this question based upon the distinct missions of each individual fusion center. The fusions centers that are purely analytical mentioned the additional role of contextualizing federal reporting and other information into tailored and meaningful products for their customers – not just passing on federal bulletins. One example includes analyzing recent terrorist attacks overseas and in the United States to support preparing police and emergency services to be able to detect and better respond if similar attacks occur in their jurisdiction.

Some fusion centers also had additional counterterrorism responsibilities if the center has an investigative role or an operational component with terrorism functions under the fusion center director. For example, some fusion centers are not just analytical but also have detectives or investigators to actively explore suspicious activity – normally in coordination with the local JTTF. These fusion centers with more than analytical roles have collection assets or sources they can task for intelligence purposes, which gives them more of terrorism role than passively receiving federal intelligence or suspicious activity reports from citizens. At least one fusion center also commanded an operational law enforcement arm with an active counterterrorism related mission and had close cooperation with federal law enforcement agencies. Also, some fusion centers have a “watch” function where they monitor events using close circuit cameras or other live reporting as well as coordinating response actions.

Q2. How has receiving federal information and intelligence in your fusion center been useful in countering terrorism?

Participants responded that federal information and intelligence on terrorist threats was “invaluable” to their terrorism mission. A key role mentioned in interviews is that receiving this federal intelligence allowed them to have situational awareness on threats coming from overseas, as well as details of terrorist trends and patterns that they otherwise would not be aware of. A participant response representative of this includes, “We gain better understanding of the threats that we face, the kind of these things that are happening both nationally and internationally and try to develop a vision of it being replicated here within the state, which helps us mitigate threats.”

Participants in fusion centers with a focus on analysis were quick to mention how this federal sharing provided them the ability to deliver valuable products to their customers. Participants also mentioned how receiving this intelligence allowed them to keep their stakeholders and policymakers informed about terrorism overall and the specific terrorist threats to their jurisdiction. In fact, this reason was the original catalyst for the growth of nonfederal fusion centers around the country after 9/11.

Receiving this federal intelligence allows fusion centers to have visibility into terrorism threats from both the domestic and overseas fronts that they do not have themselves. Multiple participants mentioned the vast and well-funded resources that that federal government has at its disposal to address terrorism threats, which state and local agencies do not have—nor are they resourced to build. Participants mentioned federal agencies in the 17 member U.S. intelligence community, the many federal law

enforcement agencies, as well as the many intelligence sources and databases at the federal level. Although a few participants with a lot of fusion center experience noted that receiving federal intelligence in fusion centers has not been as significant as initially thought it would be, which may also partially explain the evolution of most fusion centers from primarily terrorism to an all-crimes, all-hazards focus.

Q3. What are the opportunities or benefits of federal Counter Terrorism (CT) info/intel sharing with fusion centers?

This question was answered in various ways depending upon the participant's role in the fusion center, as well as the mission of the fusion center at each particular site. The most notable responses were along the lines of the overall cause for fusion centers to rapidly expand in the mid-2000s in the first place – that sharing federal intelligence with state and local officials can help prevent terrorist attacks such as 9/11. Multiple practitioners mentioned how sharing with a fusion center can better ensure state and local police are able to be on the lookout for specific activities when it comes to terrorism. This is a benefit to everyone from the federal level down to the local levels, and even citizens themselves. to be able to fill in those gaps that we would never otherwise be able to fill.

Question 3 also generated interesting discussions about different roles in domestic counterterrorism as well as which agencies benefit from interagency sharing. The question was originally intended to elicit views about how this top down sharing benefits the nonfederal fusion centers who receive the intelligence, which many participants emphasized. However, this question elicited responses describing many other benefits within and without the fusion center, addressing all 360 degrees (see Figure 2 on the

directions of sharing within and with fusion centers). Multiple participants explained that fusion centers greatly benefited from the sharing, but that federal agencies such as the FBI benefited as well since fusion centers generally focus on analysis and dissemination while JTTFs focus on investigations and disruptions of terrorist plots. For example, many participants discussed the rise in homegrown terrorism and the difficulty in identifying those on the path to radicalization. By sharing with fusion centers the federal government is extending their network and making it increasingly capable of informing those with the ability to get the word out and to educate people on what to report using resources like as the 18,000 fusion liaison officers around the country (Stewart, 2016).

A major benefit to fusion centers is the ability to leverage the massive resources federal agencies have that fusion centers do not have. The most significant benefit to sharing with fusion centers is the ability to collaborate and pool resources in order to support counter terrorism in their jurisdiction. While federal intelligence and law enforcement agencies are well funded and they have a lot of capabilities and databases, they are also stretched very thin domestically. One participant response highlighting this point was,

Obviously the federal government has a lot more resources and they have confidential informants and all these are other resources that we don't have, so we can leverage those resources that as a local government agency we would never be able to afford or commit our resources to and bring that to bear on the threats and the hazards that we have here in the region. So having that connection is really important.

Q4. What are the obstacles or barriers of federal CT info/intel sharing with fusion centers?

More than half of the participants answered this question by first mentioning multiple obstacles to sharing stemming from aspects of the sensitive and classified nature of federal terrorism intelligence. While, these practitioners clearly recognized the need to keep this sensitive information within appropriate channels and only to those possessing security clearances, there were still many existing barriers regarding secrecy. The main barrier mentioned by the vast majority of participants is that receiving this classified federal terrorism intelligence in the fusion center does them little practical good when they cannot share it with those they feel most need it – patrol officers and other customers who do not have any security clearances. Participants discussed that even when they receive this sensitive intelligence, they are not authorized to extract or reword any classified information from the reports to disseminate it to others who need it even for their awareness. A representative participant response was,

I would just say the one that stands out to me is just the clearance issues, because if you don't have a clearance you can't get that information to attend a meeting even, but then if you do, what do you do with that information if you're stakeholders don't have a clearance? So I have all this now but how do I apply it—I can't share that.

Other obstacles to sharing with fusion centers include the technological and physical components. Multiple participants discussed the great difficulty in getting access to federal intelligence systems at the secret level, and the challenges in searching those

systems for anything in their region. They also discussed the lack of content available on the Secret level Homeland Security Data Network (HSDN) and state and local agencies only have access to a very small portion of the entire federal government Secret level databases. Another physical barrier to sharing is the fact that state and local officials are not allowed to certify facilities or systems for secure operations, and everything is driven by the slow federal bureaucracy. As a case in point, one fusion center visited was operating completely at the unclassified level due to change in location many months earlier. Multiple participants complained about the difficulty getting access to federal classified systems and databases, and maintaining that access once granted.

Another obstacle is the lack of available intelligence products relevant for their jurisdiction. An example provided was that NCTC has a site on HSDN but it is nearly empty, the vast majority of terrorism intelligence at the federal level is above Secret and not available on HSDN (or on the other sensitive but unclassified systems that fusion centers can access). These federal intelligence reports either cannot be downgraded to the secret only level, or NCTC and other agencies are just not sanitizing these reports to make them available to state and local analysts in fusion centers.

One fusion center director stated that the main obstacle to effective intelligence sharing for that particular center is the lack of Top Secret / Sensitive Compartmented Information (TS/SCI) security clearances and TS/SCI facilities for fusion center analysts. However, many other participants at multiple fusion centers were doubtful that more sensitive information above the Secret level would even be useful to a state or regional fusion center. As of this writing the DHS is currently under Congressional mandate to

study the value of providing Top Secret clearances to officials in state and local fusion centers (McCaul, 2015).

On this point, multiple participants highlighted the difficulty of utilizing of reports shared with a fusion center at only the Secret level information, unless it had an unclassified summary or “tearline” embodied within the report that could be shared with partners who need to know but do not have a secret clearance. Very few ‘customers’ of fusion center reporting and disseminated products have a Secret clearance, which is another barrier mentioned by many participants. Fusion center participants generally stated that all reporting and products from their center have to be unclassified.

Another barrier mentioned by participants involved the organizational cultures and personality dependent aspects of intelligence sharing. While a number of fusion centers studied currently have very good relationships with their corresponding JTTFs, the participants made it clear that this was due in large part to the existing interpersonal relationships between fusion center directors and JTTF supervisory special agents. It was also highlighted by participants that the current senior leadership of the FBI and DHS were pushing for increased interagency sharing to the lowest levels. However, this has not always been the case, and there are still enduring negative perspectives about intelligence sharing. Participants from each of the five sites mentioned that one barrier to sharing is the view by some in federal agencies that state and local fusion centers are either untrained or unable to either properly handle classified intelligence, or that they would not know what to do with it. This was described by one participant as the “Barney Fife” view of state and local agencies, and it is difficult to overcome.

Multiple participants also discussed the often negative impact that the cultures of different agencies and career fields have on effective sharing. For example, some law enforcement professionals described how their career field holds an almost automatic suspicion of those who do not carry a badge and a gun. It was specifically mentioned that it took time to overcome this distrust and that a fusion center should not send an analyst as a liaison or detailee to a law enforcement centric JTTF, but to send a law enforcement professional.

Finally, one of the most impactful barriers mentioned by participants is the lack of federal agency personnel actually working within fusion center. Participants at each fusion center researched stated that the main sharing from the federal level comes from the federal personnel working in or liaising with their fusion center. However, none were satisfied with either the number of personnel present or the amount of time those assigned from federal agencies were available to them in person. All 18 state and local participants interviewed held their federal agency counterparts working with them in extremely high regard. However, many feds working in their centers often had tasks requiring them to travel outside of the fusion center, or they had to spend significant time in federal offices not co-located with the fusion center. Multiple participants felt strongly that one representative each from DHS and FBI was not enough to effectively support their fusion center and some were seeking more embedded representatives. Interviewees mentioned Congressional limits which limit the total number of DHS Intelligence Officers in fusion centers, resulting in some centers losing their most important vehicle for intelligence sharing (United States Congress, H.R.3503, 2015).

Q5. What can or should be done to remove or mitigate these obstacles, barriers, and risks that impede effective sharing of federal terrorism information and intelligence sharing with state and local fusion centers?

Most participants answered this question by directly addressing the barriers and obstacles they listed for Question 4. One frequent suggestion by participants was to increase the number of federal representatives in fusion centers. By embedding more federal personnel it addressed almost every single barrier or obstacle mentioned by the participants. For example, having more feds represented in the fusion center from DHS and the FBI would increase the number of individuals who can knowledgeably access federal systems and databases to look for what is relevant to their jurisdiction. This also increases the number of people in the fusion center whom leaders, investigators, and analysts can ask questions about terrorism issues and reports and also have more representation from these agencies in meeting and other fusion center work. While it is true that virtual sharing can occur over a computer or phone, it was made very clear by the participants that the vast majority of sharing occurs in person and the thrust of perceptions by participants was that “you can’t share if you are not there.” A response representing this line was “I think maybe one way to remove these barriers is co-locating people. So you have someone you know detailed to the JTTF and that helpful because you're operating in a secure environment.”

Another example of how to remove or mitigate these barriers is to ensure that the right people are selected for interagency exchanges. Instead of sending an intelligence analyst to a JTTF, send a state or local law enforcement officer who would be much more

likely to have information shared with them based upon the common bonds shared by serving law enforcement professionals that are “in the club” than those outsiders. In fact, the theme of establishing or building trust came up often.

Another way to overcome sharing obstacles mentioned by participants is increasing the production of “tearline” reports from the Feds to state and local fusion centers. These reports contain the essence of the threat information without the sensitive sources and methods information at the top of the report that gets torn off and not shared. One fusion center senior analyst mentioning knowing about tearlines and the process to create one, but that the center had not received any. Federal terrorism information and intelligence coming in is either classified and cannot be shared or unclassified and ready for dissemination, but with no real value to analysts or their customers. General information that the threat from terrorists is high during any particular period is not very valuable to fusion centers and often is “watered down” to the point of being elementary and almost pointless.

Q6. Which federal intelligence, security, and law enforcement agencies share info and intel on terrorism with your fusion center?

All 18 state and local participants answer this question by saying that DHS was the number one and most consistent federal agency that shares with their fusion center. DHS representatives themselves highlighted that sharing is a major role for DHS. Next participants most frequently listed the FBI as the second federal agency sharing with their center. Others federal agencies mentioned include the NCTC, CIA, ICE, ATF, DEA, the Secret Service, and Homeland Security Investigations (HSI). A representative fusion

center participant response on these agencies was “The bulk of the information comes from FBI and DHS So there may be some things that come from other agencies but it would be typically be through the FBI or via DHS.”

This point on other federal agencies sharing through DHS or the FBI means most federal agencies other than DHS and FBI that share with fusion centers generally do so second hand. For example, NCTC databases are accessible via HSDN, not by having NCTC personnel in a fusion center (at least in any center visited as a part of this study). If I were to repeat this research I would clarify this question to ask “which agencies directly share with your fusion center” and possibly ask an additional question about which agency reports or databases are accessible to your center. Although asked about agency sharing, some participants immediately personified organizational sharing by discussing the individual agency representatives by name who shared the most with them in their center. This further reinforced the point about most sharing is really about people and not organizations or systems.

For these five east coast fusion centers there were some particularities of having national borders within their jurisdictions. For example, these border region fusion centers also mentioned interactions with DHS field agencies like the U.S. Coast Guard or Customs and Border Protection, which may not likely be the case in the heartland of America. Some of these federal agencies interacted directly with fusion center. As an example, I was simultaneously visiting one center at the same time as HSI. Interestingly, there is a legislative proposal in Congress at the time of this writing to study the value of

placing representatives from these DHS border related agencies in state and local fusion centers (McCaul, 2015).

Q7. How would fusion centers be different if there was no sharing of federal CT info/intel?

This question caused the most visceral reactions from participants with the clear majority making comments that fusion centers would “die on the vine” or be “dead in the water” without this federal intelligence being shared with them. Additional representative participant responses include “I think the fusion centers would cease to exist” and “We'd be blind.” Some participants furthered commented that without this federal sharing it ignores all the recent counterterrorism lessons learned and setback counterterrorism efforts with representative responses including,

Actually going backwards compared to where we would be going back to 9/11 where you know the information's out there, dangling out there somewhere but nobody is able to grab it and put pieces together make sure that all entities of law enforcement whether it be at the federal state or local level are informed in order to make decisions as far as the safety of the citizens of the U.S.

A minority of participants thought fusion centers would still continue, but that the residual mission would only deal with average state and local crimes, and the federal government would have to deal with terrorism threats by themselves. Example participant responses along these lines includes “I think that over time you see a quick erosion of anything even remotely related to national security focus and back down into community your traditional criminal activity focus” and “We would just be a crime center.”

Some participants commented that without federal intel their stakeholders and customers would be without this reporting, or policymakers would have to go directly to feds to get intelligence terrorism threats without the benefit of state and local context. No participants reacted in a positive way to this question or felt it was a good idea. It was clear that almost all saw the lack of federal sharing on terrorism threats as the death knell for fusion centers and that neither JTTFs nor the FBI can do it alone.

Q8. How would fusion centers be different if they had extensive access and sharing of federal CT info/intel?

This answer generated a spectrum of responses that spanned from those who felt there would be little difference to those who saw this hypothetical future as revolutionary. The few participants who felt there would be little difference for fusion centers were generally the same participants who feel that their fusion center already receives this type of information. However, participants also felt that if this extensive and detailed intelligence were available to fusion centers it would require significantly more resources and time to integrate that information. As it stands now, fusion centers mainly have access to their own state and local systems and databases, and a very small amount of federal intelligence at the secret level. However, if the vast amounts of federal intelligence were accessible, there is not enough time to search, nor enough analysts to access it all. A representative response for this question was “There are limited resources we have a limited number of people and even if opened-up the floodgates I don't think there's enough hours in the day and number of people to be fully explore all that information.”

Additionally, very few personnel in fusion centers have security clearance above the secret level that would allow them access to this intelligence even if systems were in place to do so. Some participants again raised the point about the difficulty of using any relevant intelligence they did find if they had access to this Top Secret information. An interesting participant response to this question was,

There's absolutely nothing that you can do with that information, because when you're going to the Top Secret level you're talking about methods of collection. You're talking about how the information was collected” and “we don't need to know source details we just need to know there's a threat and the details of the threat but we don't need to know like the sourcing of it. So I think it's a good thing that they don't we don't have access to go in to into the databases just kind of like at our own will.

Interestingly, most of the experienced participants were firm in their opinion that they do not want this level or depth of access to massive federal intelligence databases. The practitioners with the most fusion center experience and career longevity stated they would prefer to instead have more federal personnel embedded with them who can access these federal systems and tell them what they need to know, not try to search for what they think they need themselves. A representative response along these lines was “Instead of having deep access I'd rather have an extra FBI analyst... I mean I'd rather have a body here. You know be able to tap into that.”

All participants were cognizant that having access to these federal intelligence databases an FBI case files would require a lot more resources than what they currently

have, and that it would be a significant risk to have so many people exposed regularly to this sensitive intelligence (nor do they have facilities or systems above secret anyway). A number of participants also commented that they have no practical use for this intelligence anyway since they cannot integrate it into their products or share it with any of their customers (many of which do not even have a Secret clearance).

Q9. Should federal security agencies share info/intel with fusion centers or should they share with a different organization in your jurisdiction (such as a JTTF)?

This question generated mainly straightforward answers that this intelligence should definitely come into the fusion center in some form. Participants noted that it is a critical role of a fusion center to disseminate terrorism information to lowest possible levels of first responders, but they cannot fulfill this role if intelligence was not shared with them to do so. A concise participant response on this point was “All the federal, like high level information is being worked at the Top Secret level by federal agencies like CIA, NSA, Homeland Security, FBI, and all of that information is sent down to local JTTF offices...we might not get the full information because a lot of it is Top Secret.”

It was recognized that JTTFs are the lead investigative bodies in the U.S. for investigating and countering terrorism, and that JTTFs are in receipt of this intelligence already – as they should be. However, participants were united in the view that this terrorism intelligence should also be shared with the fusion centers as well. As a result, this question was most often answered with the response that terrorism intelligence should go to both fusion centers and JTTFs. A representative participant response from a fusion center senior intelligence analyst was:

I feel that information should be shared with us. Lots of times we've not had that issue, but I know in speaking with other fusion centers that's been a big problem if it gets to the JTTF, you may or may not have a component on that JTTF that can share that information with you as a fusion center, so I'm a proponent that information be shared with the fusion center because basically that's why fusion centers were created in the first place, they are supposed to be that bridge.

The answers to this question also generated discussion on the different roles that fusion centers play and their differences with JTTFs. Participants discussed their focus as a center for vetting of suspicious activity reports which are then forwarded on to the JTTF if they seemed credible or met certain criteria. However, non-leadership participants made it clear that they rarely heard anything back from JTTFs, while fusion center upper level leaders were periodically briefed on intelligence and ongoing investigations.

Another representative participant response was "JTTFs have a lot of local and state agencies collocated but I don't think they reach out to or have as many stakeholders in their operation as we might. given our network of contacts around the region, so I think it makes sense to share it with both. Some overlap but really different purposes." Interestingly, in a few of the fusion centers with the closest relationships with their respective JTTFs, the participants at those sites saw themselves as so connected between the two organizations that they were basically two facets of the same counterterror node. Some participants plainly stated this by saying "I see no difference between our fusion center and the JTTF here."

Q10. As called for in the 2012 National Strategy for Information-sharing, are federal agencies “sharing the right information with the right people at the right time” in your view? For example, do you receive information about terrorist threats in general or actionable intelligence on specific individuals or cases?

There were a wide variances of perspectives from participants in answering this question with some replying they felt they do get what they need in a timely manner and most commenting they do not get specific or actionable intelligence. Some representative participant responses include “The answer is generally yes. It's not at the right time sometimes or delays and sometimes we find out after the fact about a terrorism related investigation” as well as “I think it feels more general and I think specific stuff more probably ends up going to a JTTF to investigate and carry out.”

Subsequent analysis of these replies using NVivo 11 revealed that the differences in perspective on this question have to do with the type of fusion center (analytical vs investigative) as well as the role the participant plays in the fusion center (leader vs non-leader). This will be addressed in more detail below in comparative responses by type center and leader vs non-leader. Additionally, responses to this question will be further addressed in findings by research question.

Q11. Other than the obstacles and barriers to federal terrorism information already described, are there other risks to this information-sharing?

This question most often generated a discussion of the risks to intelligence sharing such as the potential for information becoming public or “leaking” out. There was also a wide variance of perspective on answering this question with some feeling there certainly

are risks to sharing and other feeling the risks are minimal and at times overexaggerated by those not in a fusion center.

A representative participant responses that risks are minimal was “I think it's absurd to imply that there is a risk to over sharing and I guess there's crusty agents out there that will tell you more stories about their case getting blown because it got leaked to the wrong place but, I haven't seen that happen, I haven't seen a real example of that.”

However, other recognized the risks and one fusion center director stated:

There's obviously risks, risk of compromise, risks of oversharing or risk of ending up harming investigations, but we are very draconian in our information-sharing processes, we have to be very deliberate. Unfortunately, there are humans involved and sometimes people don't understand or don't follow procedures.

Q12. What have been the most useful sharing mechanisms from the federal government for information and intelligence on terrorist threats; systems such as Homeland Security Data Network (HSDN), FBI Law Enforcement Online (LEO)/FBI Net, or embedded personnel in your fusion center and interagency liaison meetings?

This question mainly asked the participants to not only describe what they viewed as the most effective sharing mechanisms overall, but to also compare technological sharing with interpersonal sharing. 24 out of 25 participants clearly identified people and interpersonal relationships as by far the most effective sharing mechanism. Most participants were also very emphatic on this point and made comments including the following “a hundred percent the people” and “personal relationships” or “People, hands down” or “physical like having a physical body in the fusion center to me is absolutely

the best way to get information whether it's coming or going I think it clears up a lot of miscommunication or inconsistencies” as well as “The most useful sharing mechanism by far is having people co-located” and “It's really hard to justify the bosses. It's hard to write it into budgets. But fusion centers downward and fusion centers upward. I think they live and die on relationships.”

Comparison of Leader Responses to Other Fusion Center Personnel

Participant responses based upon being a leader or non-leadership members of fusion centers was the first interesting trend discovered during analysis. Fusion center leaders including upper-level leaders such as directors or deputy directors as well as supervisors in fusion centers viewed intelligence sharing from the federal government much more positively than the non-leadership members of the same fusion centers (those who do the daily work). Fusion center directors often described as a positive development how often they were being “briefed” about ongoing FBI terrorism investigations in their jurisdictions. However, non-leadership fusion center personnel such as analysts and investigators often commented on this did not constitute intelligence sharing in their mind since the directors left those meetings (or phone calls) with nothing in their hands or anything they could share with the rest of their fusion center. The fusion center non-leaders had a much less positive view of the state of terrorism intelligence sharing since they are accessing classified government secure networks with little valuable intelligence to do their jobs while fusion center directors are “in the know” but can’t share with them to inform fusion center work. This finding was consistent across all five sites researched

regardless of the type of fusion center or the size of their jurisdiction, and was a very interesting discovery not mentioned in any previous research.

Comparison of Responses by Profession: Intelligence vs Law Enforcement

There were few substantive differences between participant responses based upon only their career field when it came to the core issues of benefits and barriers to sharing with fusion centers. Both types of professionals shared common views overall of what was holding up effective sharing and what would improve it. However, there were some differences when it came to their level of intensity of their beliefs. For example, both law enforcement professionals and intelligence professionals felt that people were the most important sharing mechanism with systems being secondary. However, law enforcement professionals responded immediately and were highly emphatic on this point and left no doubt as to their views about the supremacy of personal relationship as the most important aspect of sharing. When intelligence professionals answered the same question they also came down on the side of people as most effective for sharing, but only after hesitation or reflection and they seemed to hold this view to a less intense degree than law enforcement professionals.

For example, law enforcement professionals would answer the question on the most important sharing mechanism with statements like “hands-down its people” or “people 100%” while intelligence professionals would answer with a reply along the lines of “people are most effective, but I still want access to the systems.” These differences are likely due to the necessity for law enforcement professionals to rely upon people to succeed in their careers such as the use of witness testimony and confidential informants.

Intelligence analysts on the other hand predominantly rely on written reports and second hand sources and methods that are accessible in databases and often remove them for direct contact with the people gathering this mainly human derived intelligence.

Comparison of Responses by Longevity

Participant responses based upon both longevity in their career field and within the fusion center provided some interesting patterns regardless of the site researched. Those individuals with many years of longevity in their career field were more understanding and realistic about what can really be expected from the type of information which could or should be shared with fusion centers. Those long serving professionals and those with the longest service within fusion centers were aware of the extreme sensitivity of case specific information and a number knew of instances where investigations had been compromised. Senior law enforcement officers and analysts stated that this will probably never happen, nor were they interested in investing the time to try to search those complex systems even if they were allowed access. These veteran law enforcement officers and senior analysts were generally satisfied with the overall level intelligence sharing.

However, more junior participants and those with less career experience were less understanding and more expectant of what can or should be shared with them as far as specificity and actionable intelligence. These less experienced individuals felt the strongest that intelligence of a specific and actionable nature was not being shared with their fusion center. State and local junior intelligence analysts were also the individuals

most eager to have access to FBI case files and sensitive databases on individuals under investigation.

Additionally, those with longevity in fusion centers greater than 3 years had interesting perspectives based upon experiences with different federal agency personally being assigned to their fusion center and evolving relationships between their fusion center and JTTFs. These long serving professionals emphasized trust building between individuals from other agencies (particularly with the FBI) and they saw FBI representatives to their fusion center come and go. These professionals were very thankful for the near daily interactions with DHS representative and critical of the fact that FBI personal were only “part time” in the fusion center (on average 2 days a week across all fusion centers visited). The strong view of the participants in this research is that periodic participation is very inadequate and state and local participants expressed the desire to have both DHS and FBI representatives in their fusion centers on a daily basis.

Comparison of Responses by Type of Fusion Center

While there is no standard fusion center, there were two common counter-terrorism roles for each fusion center researched for this study. These include receiving and vetting suspicious activity reports from both public and official sources, as well as the function of dissemination terrorism warning information to those who need – primarily patrol officers. Beyond those two functions there was significant variance in the fusion center roles relating to domestic terrorism. Fusion centers focus on analysis of trends and disseminating as much unclassified information as possible. Other fusion

centers have taken on a significant out-reach and training role focusing on getting the word out to both law enforcement agencies as well as the private sector on how to best report on and prepare for terrorist activity.

Separate from these analytical and dissemination driven centers, some fusion centers researched are also investigative in nature or contain an operational component with a terrorism related mission. These fusion centers with an ‘on the ground’ role to play in terrorism had a very close and symbiotic relationship with the JTTF (and to a lesser degree with DHS operational agencies such as CBP and the Coast Guard). Additionally, the intelligence needs of centers with an investigatory or operational role are different than ones that are purely analytical or have a watch function. Analytical centers mainly received general information on terrorism from the federal government, such as how recent attacks in the U.S. and Europe were undertaken. Investigative and operational centers receive more specific intelligence on individual cases within their jurisdiction. It is likely this difference is due to the need to synchronize investigations and de-conflict potential operations.

At the outset of this research I envisioned there would be differences in the perspectives between state fusion center and those for major urban areas. However, in the context of sharing of federal intelligence on terrorism there was no discernable divergence based upon level of government. In fact, there were also no notable differences in federal intelligence sharing between large state and small states, so there were no findings based solely upon the size of a jurisdiction for a fusion center. However, there were differences based upon the different fusion center missions and exact role each

plays in countering terrorism with regard to federal sharing with them. For example, fusion centers that generally focus only on analysis and providing products to their stakeholders most often only reported getting general terrorism information from the federal government. However, fusion centers with an investigative role or an operational component with a terrorism related mission reported receiving actionable intelligence on specific cases and specific individuals of terrorist interest very often.

Validity, Credibility, and Confirmability

This study strived for validity, credibility, and confirmability of the research by employing objective techniques to ensure integrity and scholarly quality. These strategies included variation in research site selection, consistent participant selection based upon background, reflexivity, and dissertation committee review (Anney, 2014). Research sites were selected to include large and small states and local fusion centers to match the national proportions. Participants were specifically recruited based upon backgrounds that were followed consistently at each site researched. For example, variation was employed by ensuring that interviewees came from varying positions within fusion centers, and at each center the same type of background was recruited. Additionally, exactly five individuals were interviewed at each site for consistency. Reflexivity was also employed by using a field journal and notes for critical self-reflection (Ortlipp, 2008). Confirmability and dependability were ensured by specifying these procedures, the sample population, and site selection criteria all explained in detail so another researcher can duplicate this study and get same results.

Findings and Enumeration

This section of Chapter 4 presents some of the main findings from researching intelligence sharing at these fusion centers. The answers from the participants clearly demonstrated the Dawes (1996) theory of interagency information-sharing provided an effective framework to analyze the obstacles and opportunities of federal terrorism intelligence sharing with nonfederal fusion centers. The participant answers outlined both benefits and barriers of federal terrorism information-sharing with fusion centers.

These findings focus on the 3 research questions this study employed revolving around the Dawes (1996) framework of interagency information-sharing. For the purposes of data coding and analysis the 12 interview questions were individually subordinated to the most relevant research question. This facilitated focusing the research around the Dawes model as shown in Table 4 below.

Table 4

Interview questions subordination to research questions

RQ1: How effectively are fusion centers receiving terrorism intelligence from federal agencies?

1. What role does your fusion center play in counterterrorism?
6. Which federal intelligence, security, and law enforcement agencies share info and intel on terrorism with your fusion center?
10. Are federal agencies “sharing the right information with the right people at the right time”? Do you receive general threat information or actionable intelligence on specific individuals or cases?
12. What have been the most useful sharing mechanisms from the federal government on terrorist threats.

RQ2: Opportunities of federal intelligence sharing with fusion centers

-
-
2. How has receiving federal information and intelligence in your fusion center been useful in countering terrorism?
 3. What are the opportunities or benefits of federal Counter Terrorism (CT) info/intel sharing with fusion centers?
 8. How would fusion centers be different if they had extensive access and sharing of federal CT info/intel?
 9. Should federal security agencies share info/intel with fusion centers or should they share with a different organization in your jurisdiction (such as a JTTF)?

RQ3: The main obstacles to intelligence sharing with fusion centers

4. What are the obstacles or barriers of federal CT info/intel sharing with fusion centers?
 5. What can or should be done to remove or mitigate these obstacles, barriers, and risks that impede effective sharing of federal terrorism information and intelligence sharing with state and local fusion centers?
 7. How would fusion centers be different if there was no sharing of federal CT intel?
 11. Are there other risks to this information-sharing?
-

Research Question 1: How effectively are fusion centers receiving terrorism intelligence from federal agencies?

The first research question this study sought to answer was: how effectively are fusion centers fulfilling their intended purpose to improve homeland security by receiving terrorism information and intelligence from federal agencies? As mentioned above this research question was pre-coded in NVivo by grouping the nodes of all participant responses to questions 1, 6, 10 and 12. Codes that emerged from analysis included effectiveness, limited sharing and means of sharing.

The answer to this research question is that fusion centers can be effective sharing mechanisms, as demonstrated in the interviews of 25 participants from five east coast fusion centers, but the level of effectiveness depends on at least two factors. These factors are the mission of each fusion center and the organizational and personal relationships between federal agencies and key officials within the jurisdiction.

When it comes to the mission and role of a fusion center there was a distinct difference between the perspectives of the effectiveness of sharing from federal agencies based upon what that fusion center actually does as it related to counterterrorism. As discussed in Chapter 2 there are a number of fusion centers varieties such as those which are investigatory, analytical, and those with a watch function. The responses in this study showed if the fusion center has only an analytical role then the respective perceptions of intelligence sharing by those in that center were noticeably lower than those of fusion centers with a counterterrorism operational component or investigative role. Participants in analytical only fusion centers rarely mentioned receiving actionable intelligence or specific case information. This makes sense as why would an analytical only center need actionable intelligence or case specific information if they have no action to take or investigation to deconflict?

So the effectiveness of fusion centers in receiving intelligence varies depending on the role and mission of the fusion center. Therefore the intelligence needs of each center in terms of specificity and timeliness vary accordingly. When developing assessments for federal intelligence sharing with state and local fusion centers these different missions and roles need to be factored in.

Organizational and personal relationships between the fusion center and key federal agencies was just as important, although much less tangible. It is very difficult to measure personal relationships, but as many participants emphasized, it can be the most important factor in how much or what kind of intelligence is shared with a fusion center. The organizational and personal relationships with federal agencies and officials within the jurisdiction is a very multifaceted factor since it includes many different components such as the personal relationships between the fusion center director and senior FBI officials in the city or state, the level of trust fusion center personnel have with their embedded federal representatives from DHS and the FBI, as well as the quality of state and local liaisons or embeds in federal agencies such as JTTFs.

These personal relationships are extremely hard to get right and even harder to measure, especially for the entire national network of fusion centers. Additionally, personal relationships are also very perishable and even good relationships may vanish when a new fusion center director or FBI SAC is assigned. But that does not mean it should be left off fusion center assessments as it currently is.

Research Question 2: What are the opportunities or benefits of federal CT info/intel sharing with fusion centers?

As mentioned earlier in this chapter, this research question was pre-coded in NVivo by grouping the nodes from participant responses to questions 2, 3, 8 and 9. Two primary codes that emerged during analysis on opportunities or benefits of sharing intelligence with fusion centers included preventing terrorist attacks and being able to disseminate to state and local users such as police and other first responders. Additional

codes that emerged included having access to more intelligence sources and the ability for state and local analysts to have context for national and international events as well as terrorist trends and patterns.

The predominant benefits to sharing federal terrorism intelligence with fusion centers immediately mentioned by participants is the ability to fuse federal intelligence with state and local knowledge to stop terrorist attacks. If state and local officials are aware of the specific intelligence available to federal agencies they can be on the lookout for known individuals or search the state and local records based on this information. This was witnessed by the researcher during a visit to a state fusion center during an east coast wide manhunt for terrorist suspect Ahmad Khan Rahami who had just allegedly bombed multiple cities in NY and NJ wounding over 30 people and was still at-large (U.S. Attorney's Office Southern NY, 2016). Federal authorities shared what they knew about Rahami with fusion centers as well as an associated license plate. Fusion center officials in the state fusion center being visited immediately sent this information out to all state police on patrol (and local agencies) and programmed it into the automatic license plate readers on patrol cars and other locations in the state. Terrorist suspect Ahmad Rahami was apprehended while the researcher was still on-site at the fusion center. However, if Rahami was driving and had passed a license plate reader, it would have immediately shown the benefit of federal intelligence sharing with the national network of fusion centers.

In the context of Dawes (1996) model, the main benefits and opportunities are also just as heavily focused on the organizational and political components as were the

obstacles, and less on the third factor of technology. These research findings clearly deemphasized technical barriers in interviews with participants. However, there was an emphatic request for more embedded federal representatives and changes to policies and procedures when it comes to sharing (which are both organizational and political). The participants mentioned many benefits that fit the Dawes (1996) theoretical framework such as fostering program and service coordination.

These findings also show that while there is room for improvement on the technology side, the focus is on what can be gained through more extensive in-person contacts. Participants emphasized that agency personnel across all three levels of government to exchange information to better secure the American people in a collaborative manner. This falls exactly into the premise of improved and integrated government services through interagency information-sharing described by Dawes (1996).

Research Question 3: What are the obstacles or barriers of federal CT info/intel sharing with fusion centers?

This final research question was pre-coded in NVivo by grouping the nodes of all participant responses to questions 4, 5, 7 and eleven. During analysis emerging codes included classification, interpersonal, organizational, and policies and procedures. There was also a code created for facilities, but this was a relatively minor barrier mentioned compared to the other four codes that emerged.

There were four major thrusts that participants outlined when it comes to identifying the most significant barriers to effective intelligence sharing from federal

agencies down to fusion centers. These four obstacles can be listed plainly as clearance, culture, policy and personality, or C2P2. The 'clearance' obstacles addresses all the issues surrounding the sharing restrictions and excuses about sensitive sources and methods and ongoing investigations that keeps intelligence from being shared. This "need to know" mentality was a contributing factor in 9/11 and other terrorists attacks like Fort Hood and the Boston marathon bombing.

The culture aspect focuses on organizational perspective of entities like the FBI where the long standing views of sharing it that it happens "to" the FBI but little comes "from" them to partners. This organizational culture is improving according to participants, but is still a significant barrier from the state and local perspective. This is closely linked to the 'policy' barrier where having a 'duty to share' has still not been manifested into organizational policies and procedures to enable highly effective terrorism sharing (not just after a case is closed). Multiple participants mentioned pre-9/11 policies of information-sharing restrictions and lack of access to reports and data continue to hinder effecting collaboration between federal agencies and state and local fusion centers.

The final main barrier revolves around the personality of individuals involved in sharing federal information both within and adjacent to fusion centers. The major players for fusion centers are the FBI Special Agents in Charge (SACs) of FBI field offices and JTTF supervisory agents in their jurisdictions. These FBI officials hold significant sway over what will be shared with fusion centers and they set the atmosphere for both the FBI personnel and interagency detailees working under their organizations.

Numerous participants mentioned significant sharing differences (both positive and negative) based solely upon a change in the FBI SAC in their jurisdiction. This also highlights the great importance of the personal relationships between these SACs and fusion center directors. Every upper-level fusion center leader interviewed placed significant emphasis on their personal interactions with the FBI SAC as well as the frequency and depth of sharing. However, personality is also the most intangible aspect of sharing and the most difficult to overcome if key leader personalities are not in-sync between these agencies. Table 5 below lists these obstacles, a brief description, and representative participant responses.

Table 5

Obstacles to federal intelligence sharing with fusion centers

Title	Obstacle or Barrier description	Representative participant quote
Clearance	Fusion centers are at the Secret level only and many stakeholders and ‘customers’ have no clearance	“There’s information on the federal level that’s classified, it cannot be shared down”
Culture	Federal intelligence agency cultures do not emphasize sharing	“Institutional culture sucks...trying to get information from my federal partners is like pulling teeth”
Policy	Policies still emphasize “need to know” not a “duty to share”	“...if it goes to the JTTF we may never hear about it...we are not getting all the information”
Personality	What to share and how much to share with fusion centers is highly reliant on interpersonal relationships, especially with the FBI	“...it still tends to be personality dependent, so if the FBI SAC is supportive of the role of fusion centers then you have a pretty good relationship”

In the context of Dawes (1996) model, these barriers and obstacles are focused heavily on the organizational and political components, and less on the third factor of technology. This is an interesting finding since the emphasis in the literature and federal statutes surrounding sharing with fusion centers only focuses the technical aspects, as if incompatible technologies are the problem. However, the real barriers to sharing shown from this research are that the organizational and political factors are the real obstacles. As a case in point, fusion centers have access to the secure communications technology, but it is the interagency relationships and government policies preventing that technology from carrying any meaningful and actionable intelligence on them (such as terrorism tear lines relevant to their jurisdiction).

The research has shown that effective sharing of terrorism intelligence primarily occurs in these five fusion centers mainly through personal contacts. Further, this research has identified that the four most significant obstacles or barriers to effective intelligence sharing with nonfederal fusion centers are clearance, culture, policy and personality. In the context of Dawes theoretical framework, these four major obstacles all fall within the factors of organizational or political barriers and none predominantly technical in nature.

How federal sharing really occurs with fusion centers

The finding of this research is that intelligence sharing is not principally focused on technology, but is really about people. This is an important finding as the only current official measures of sharing with state and local officials focus solely on systems to share. The fusion center baseline capabilities by DOJ and DHS discuss the ability to

receive federal information solely based on having the computer systems in place within the fusion center, as well as making sure it is connected to HSIN and HSDN/FBInet. In plain terms, it asks do you have the computer, it is set up, does it turn on, and does it have connectivity? The reality is these systems reflect only a minority of intelligence sharing, and these systems are not considered the most important element according to every participant in this study save one. The critical operating capabilities do reflect the much more important question about receiving federal intelligence on terrorism, which is, do you have representatives from the DHS and FBI embedded in your center on a near daily basis to share intelligence with you?

These federal officials embedded within a fusion center are the key to federal intelligence sharing with state and local officials. These individuals know what is going on with their respective agencies and they know the federal information systems and exactly how to find what is needed for the fusion center. These federal representatives are also tied into their home agencies and counterparts within the state and within their networks to know what is going on (well beyond what is known in a fusion center) and are able to share what they can with at least the fusion center director.

This research finding that information-sharing is more about personal interactions than systems is not a new discovery by itself. The point of virtual or telephonic collaboration being far inferior to personal contact has been empirically demonstrated many times (Kraut, Fussell, Brennan, & Siegel, 2002). This research established twofold findings in this regard. The first outcome to emerge is the premise of personal contact is not just for sales or business, but that it is just as important (or even more so) in the

context of federal intelligence sharing with fusion centers. The second outcome to emerge is the finding about the great importance of embedded federal personnel in fusion centers has not been addressed as the key to effectiveness of this sharing dynamic. In fact, the DOJ and DHS baseline capabilities and subsequent annual assessments ignore this point completely when requiring fusion centers have the ability to receive information from federal partners by only addressing clearances and systems and not addressing the more essential aspect of embedded federal personnel. Additionally, the much more recent National Fusion Center Strategy from 2014 also has a focus on intelligence sharing systems and does not address embedded federal representatives either.

Summary

The findings in this research shows that fusion centers can contribute to stopping terrorist attacks if intelligence is effectively shared with them in a timely manner. The main barriers to effective intelligence sharing according to participants are clearance, culture, policy and personality. Fusion center leaders think the state of intelligence sharing is more effective than those doing the work for them in the fusion centers. Importantly, federal terrorism intelligence sharing with fusion centers is really about people, not systems or technology. In fact, every participant but one identified personal interactions as the most effective mechanism for sharing terrorism intelligence with fusion centers and highlighted their embedded federal representatives.

Chapter 5 offers final insights as well as policy recommendations and potential topics for future research.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

Since 9/11, every U.S. state except Wyoming, and many major urban areas, have established fusion centers to promote information-sharing by bringing together intelligence from a variety of sources and thus better protecting its citizens from terrorists and other significant threats. One of the most important sources of intelligence for fusion centers is the kind of sensitive intelligence on terrorist threats that can come only from federal intelligence and law enforcement agencies. Despite this sharing imperative, research has shown providing terrorism intelligence to fusion centers remains sub-optimal. This study sought to find out (a) how effectively federal agencies are sharing intelligence with fusion centers, (b) the sharing opportunities and obstacles, and (c) the best practices that might be shared.

Interpretation of Findings

Terrorists are a particularly difficult intelligence target because they organize as clandestine networks, hide within open societies, act alone or kill without notice (Sims, 2007). For this reason, it is important that agents of the federal government share as much as possible on terrorists with the affected jurisdictions and work together to stop them. By interviewing participants from five East Coast fusion centers, I was able to identify the benefits and barriers to intelligence sharing as well as answer the research questions on how effectively these centers are serving their purpose as a hub of terrorism intelligence sharing.

The barriers to intelligence sharing identified here, based on Dawes theoretical framework, are principally organizational and policy in nature; the barriers revolve around clearance, culture, policy, and personality. The benefits of federal intelligence sharing with state and local fusion centers is that citizens are better protected and terrorism is collaboratively countered. Although important and useful, terrorism intelligence sharing is not principally about access to databases or information technology. Sharing is primarily about (a) interagency organizational relationships within a jurisdiction and (b) between key personnel from agencies with a role in counterterrorism.

A point here can be made about the Boston bombings and information-sharing. As mentioned in Chapter 2, the FBI agent investigating Tamerlan Tsarnaev did not discuss the assessment with any state or local officials, including those on his squad from the Boston Police in the JTTF. However, he did file his report in the FBI's Guardian system, which members of the JTTF had access to. But this is not sharing because it does not involve dissemination to those in the JTTF or offer a mechanism to push the information out to those in the jurisdiction might want to know. Massachusetts Congressman William Keating wrote a letter to FBI Director James Comey in July 2013 about this lack of sharing within the JTTF. He wrote: "these local officials could not search the database for something they did not know existed" (Keating, 2013, p. 3).

The findings in this study about the critical importance of personal relationships and embedded personnel to enable interagency intelligence sharing and collaborative countermeasures makes the Special Operations fusion center more relevant to domestic

fusion centers than might seem obvious. The JIATF model described in Chapter 2 that worked so well to defeat al Qaeda in Iraq in the mid to late 2000s is an important case that offers some considerations and best practices for domestic fusion centers. As General McChrystal stated,

proximity to Washington also had costs. The Beltway culture compelled, or allowed, the agencies to be less collaborative. Valuable information that might slide across a table downrange had to cross miles and clear bureaucratic hurdles back in the States. In Washington, the myriad essential but competing priorities, from bureaucracy to family life, always slowed action. For this reason, the JIATF would bring analysts from each agency into the same literal tent—and that tent would be on a base in Afghanistan or Iraq. Obviously, this would enable intelligence to be analyzed downrange, close to the fight, making the process faster and the information potentially more relevant. Less obvious but more important, having the analysts live and operate forward, teamed with counterparts from other agencies, decreased the gravitational pull of their headquarters back in D.C. and dramatically increased the sense of shared mission and purpose. It was extraordinarily powerful for analysts to share information, to brief operators on their assessments, to hear the rotors of an assault force launching on their information, and then to debrief together after the operation. (McChrystal, 2013)

This sense of shared purpose and mission focus, which I personally experienced in the JIATF under General McChrystal, I also witnessed in the narratives of the embedded federal agency representatives from all five fusion centers researched. These

individuals are federal employees reporting to supervisors in Washington (or closer by), but they became full-fledged “teammates” with their fellow fusion center members and this is mutually beneficial for many reasons. The embedded federal representatives (from both the FBI and DHS) has not only earned the trust of their state and local partners, but they fully understood the intelligence needs of the fusion center (and their stakeholders) in ways that cannot be achieved from the outside. This is how intelligence is really shared, person to person, and this is not reflected in existing fusion center assessments.

Interagency relationship building is very difficult with conflicting or overlapping organizational responsibilities and cultures as well as personalities getting in the way. As General McChrystal (2013) described,

No alliance could be as infuriating or as productive as my relationship with the CIA... more than once, my most trusted subordinates had to stop me, in moments of utter frustration, from severing all ties with our ‘Agency brothers,’ repeating back to me my own guidance to preserve our relationships through specific conflicts...; ours had to be a unified fight.

In seeking to achieve this unified fight for the homeland, we have to set the conditions to do so and embed more federal representatives in fusion centers, which will be a key policy recommendation of this study. This will not be easy, as even General McChrystal serving as a high ranking commando general officer in Iraq with the President’s ear and focused on the number one terrorist threat at the time (al Qaeda in Iraq) he had great difficulty bringing together the necessary interagency intelligence

players to join his JIATF (Henricksen, 2013). However, this is what is needed to address the terrorism threat we face today here at home.

Implications for Positive Social Change

Overcoming the barriers to counterterrorism interagency intelligence sharing can significantly impact major aspects of our society in ensuring a collaborative approach to counterterrorism. This can only be achieved if it is based on a solid foundation of terrorism intelligence sharing across all 3 levels of government. By effectively sharing terrorism intelligence vertically and horizontally among partner agencies is the only way to stop the complex threats the nation faces from both international terrorists and homegrown extremists (Schmitt, 2011). We cannot go back to the way it was before 9/11 where a failure to effectively share resulted in a massive tragedy.

A specific example where getting this sharing ‘right’ could have averted disaster is the case of NY/NJ terrorist suspect Rahami mentioned earlier in this chapter. On the morning of September 19th 2016 I observed a fusion center in action during an East Coast wide manhunt for this suspect. That day counterterrorism intelligence from federal agencies was quickly disseminated out to every state police officer on patrol (and directly to their cruisers) as well was programmed into license plate readers. One can only imagine if this network of fusion centers had been in place before 9/11 and federal agencies had shared what they knew about the al Qaeda hijackers already here in America months before that fateful day.

This research contributed to the body of knowledge on fusion center with empirical evidence and original findings on how federal intelligence is actually shared

with state and local officials, and how it can be improved. If the policies and procedures are enacted and federal personnel are embedded full-time to enable effective terrorism intelligence sharing with nonfederal fusion centers, then significant social change can be gained through increased abilities to counter terrorist attacks within the homeland. This research intends to positively influence improved national security through policies that reflect the importance of fusion center federal manning as the crux of intelligence sharing (over systems) and the need to develop and assess personal relationships between key individuals and organizations with leading counterterrorism roles in protecting our citizens.

Recommendations

This research has identified a number of best practices where effective federal terrorism intelligence sharing was reported by participants. Additionally, some specific policy recommendations identified through conducting this research that can improve terrorism intelligence sharing. These best practices along with specific policy recommendations are addressed below.

Embed more federal representative from DHS and FBI in fusion centers

Participants in the study were highly appreciative of each individual federal representative embedded in their fusion center and all emphasized how important these individuals are for effective intelligence sharing. Most participants would rather have these federal representative in their fusion centers than having information systems allowing them to access federal intelligence. In fact, these federal personnel themselves were listed as the most effective sharing mechanism for intelligence on terrorists within

their jurisdiction. When asked which federal agencies share with their center, some participants immediately personalized the question and replied by naming the individual embeds on a first name basis. The participants were also clear that they want more federal representatives in their center; both more representatives and to have them for more time.

These federal representatives, such as the DHS intelligence officers, also often have some responsibilities outside the fusion center since they often represent the entire 17 agency consortium of the U.S. Intelligence Community to that state or locality. Multiple participants complained that when their DHS person was out (for whatever reason), they felt significantly hampered in their state or local mission. So most fusion centers would greatly benefit from a having a second full time DHS person embedded in the form of an intelligence analyst—a more junior person working under the supervision of the DHS Intelligence Officer or Senior Reports Officer (SRO). This framework offers more depth in key federal representatives in the fusion centers and allows the DHS representative to perform outreach or training in the jurisdiction as well as provide total job coverage (in the event of illness, conference, or vacation, etc).

This same model of a 2 person federal liaison team should be used for the FBI representation with a full time FBI Special Agent and full time FBI Intelligence Analyst embedded in each fusion centers. This recommendation would significantly increase manning as the FBI generally sends only liaisons to fusion centers on a part time and as an additional or supplementary duty to investigative or analytical work for the local FBI field office (not full-time embedded). Several participants discussed the different pros

and cons of having an FBI Agent representing the bureau versus an FBI Intelligence Analyst, so the optimal solution is to send both according to participants.

In sum, every recognized fusion center should have at least one DHS IO or RO and at least one full time FBI Intelligence Analyst or Special Agent. None of the 5-fusion centers researched had an arrangement of this kind. Based upon the fusion centers' operational capabilities and mission, more of these federal representatives may be required. At least one fusion center was striving for two full time representatives from each agency for a total of four. The optimal footprint in a fusion center would be a DHS Intelligence Officer, a DHS Intelligence Analyst, an FBI Special Agent and an FBI Intelligence Analysts. This is the best solution to support fusion centers, although this is a significant federal resource commitment and currently legislatively constrained, at least for DHS according to participants.

Embed more fusion center personnel in JTTFs

Just as having more federal representative embedded in fusion centers, much can be gained by having more state and local representatives in JTTFs. Fusion center directors mentioned being proud of their own personnel detailed to JTTFs in their jurisdiction, and this is a strong bond for intelligence sharing. However, multiple non-leadership participants working in fusion centers emphasized how these detailed individuals are not allow to share intelligence about ongoing investigations due to operational sensitivities (for the most part). It should also be emphasized that overcoming organizational culture can be eased by sending "the right person" as a fusion center

representative who can most easily earn the trust of the FBI Agents and other law enforcement professionals in key positions in the JTTF.

The theme of establishing or building trust was mentioned often by participants in this study, and some investigators confessed to having bias against analysts (who do not have a badge or carry a gun). This same bias is famous in the FBI, and a fusion center director may benefit more in the long run by sending a detective or investigator to be their representative to a JTTF than even their best intelligence analyst for this reason. Also, sending a police officer or detective to the JTTF who reports to the fusion center director and where that relationship is strong will help facilitate the JTTF to fusion center organizational relationship as well.

Assess the real mechanisms for intelligence sharing: Relationships

The fusion center baseline capabilities only assess systems and not where most information-sharing really occurs, with embedded personnel (both within the centers and from the center to critical nodes like JTTFs). Information systems required for sharing should not be eliminated, but the emphasis for assessing intelligence sharing with fusion centers should be refocused on people and organizational relationships. There is no mention in fusion center assessments now of the all-important role of people in sharing, and this needs to be addressed and made a priority. Not only do fusion centers need federal embeds from DHS and FBI, they need to be increased in number and they need to be quality individuals with training and solid relationships back to their home federal agency. Priority should be placed on who is sent from federal agencies to the fusion centers, as a number of state and local participants complained about being sent “the JV

team” to their fusion center where (the FBI in particular) viewed fusion center duty as a less than desirable assignment.

Focus fusion center directors on relationships

Leading a fusion center is a difficult and complex job requiring the ability to form a cohesive team from a highly diverse conglomeration of analysts, agents, investigators and emergency services personnel—many of whom probably do not directly work for them. Couple this complexity with the necessity to establish and maintain very effective personal and professional relationships with a constellation of federal (and other) agencies and you have a glimpse of the day in the life of fusion center director. Fusion center directors discussed how different this type of assignment is compared to traditional police work. Directors participating in this study shared how they personally felt unprepared at the beginning of their assignment to succeed. Some felt that after several years they had finally figured out their jobs but were only at this point highly effective and now subject to rotation to a different job.

Two fusion center directors commented without prompting that the process to select, train, and assign new fusion center directors is less than optimal. Although a law enforcement professional himself, one fusion center director stated the job is so specialized and complex that the position should probably be filled by an intelligence professional. At any rate, when selecting and training fusion center directors, the most important aspect should be the personality component according to this research. If people and relationships are the most effective sharing mechanisms, then directors should be selected based on their leadership and interpersonal skills. Fusion center directors

should primarily focus on team building within the fusion center and relationships building with the many federal partners and other stakeholders in the jurisdiction.

A recommendation for fusion center personnel is to deliberately plan unofficial and social interactions both internally and with the key external partners. These interactions will do more to establish personal bonds and build trust more than work interactions and meetings. I would suggest fusion center directors prioritize getting out of the center frequently for personal and focused engagements to build and sustain critical relationships supporting the fusion center mission. Within the fusion center they could plan team-building events like team sports, going to the shooting range together, and occasional outings like a fusion center barbeque. These activities may sound trivial, but as multiple participants pointed out, it is too late to start a relationship or begin to build trust once a crisis occurs.

Employ open collaborative work environments

In order to actually fuse diverse agencies and different types of information it requires a collaborative working environment within a fusion center. If analysts and agents have to navigate a labyrinth of cubicles or are constantly going up and down stairs, that serves as a physical barrier to effective sharing and collaboration. Also, people can't collaborate well if they are stuck behind a vault all day while analysts and investigators toil away in an unclassified pen, or worse, their individual cubicle. Some fusion centers are set up well and others were hampered by their physical environments. If domestic counterterrorism is important to a jurisdiction then I recommend establishing more open architecture work spaces to enable this collaboration. Since personal relationships as so

important to sharing, there should also be multiple social spaces like a well-stocked and aesthetic break room, an outdoor patio or gazebo to allow critical social bonds to build.

Improve tailoring intelligence for state and local partners

Another recommendation is that federal intelligence can be better tailored to the requirements of state and local partners. Multiple participants complained about the vast amounts of unhelpful information available to them in the classified and unclassified federal systems. Most fusion center participants rarely access these systems to do their jobs and some purposely avoid it. There is very little in there that pertains to their jurisdiction. Intelligence needs to be pushed to those who need it, not just searchable as few know what may or may not be in there relating to them. It is not just a duty to share, but a question we often asked ourselves in the military: who else needs to know this? When appropriate and valuable to a jurisdiction, federal agencies should push intelligence to the fusion center.

As an example, participants mentioned that NCTC Current (a federal terrorism database) is now available on HSDN at the Secret level, but they said very little useful intelligence is accessible in that system. The vast majority of federal terrorism intelligence is maintained at the top secret level and not available to fusion centers. While participants do not accuse anyone of purposely withholding intelligence from fusion centers, there also does not seem to be a significant effort to downgrade this vast intelligence to the Secret level for dissemination to state and local partners either. An aspect of this recommendation is to aggressively push down to state and local fusion centers what they need to know using a secret level 'tear-line' report.

Mandate intelligence sharing on terrorism to state and local fusion centers

A final recommendation to overcome sub-optimal federal intelligence sharing with nonfederal fusion centers is to direct that this intelligence be shared. Mandating federal agencies share intelligence on terrorist threats may be the only way to overcome many of the barriers like personal relationships and organizational culture. Requiring that intelligence be shared with fusion centers is like psychologists having a duty to report patients to law enforcement who are a threat to themselves or others. Having Congress pass a law that mandates intelligence on terrorism be disseminated to nonfederal fusion centers would move the nation literally toward a “a duty to share” paradigm.

Recommendations for Future Research

This study was conducted as an exploratory case study “aimed at generating hypotheses for later investigation” (Baškarada, 2014, p. 5). One proposition of this study is that personal interactions are the most important sharing mechanism, as evidenced by participant interviews. This was a new finding and one that calls for further research as no other study has identified this as the primary factor with intelligence sharing and fusion centers.

Additional findings from this study can be further researched based on differing locations and research methodologies. Replicating this study using the same methodologies and research questions in a different region of the country can further confirm the findings or adjust them based on other locational factors. This concept could entail repeating the qualitative case study approach by conducting interviews in other regions of the country such as the west coast, gulf coast, or middle America. For

example, the fusion center in Chicago was not researched or visited (as it is not on the East Coast). However, it was mentioned by a participant as a positive example where a fusion center is housed in a secure federal facility and can access Top Secret and compartmented government intelligence. By studying other regions of the country further research may reveal other unknown factors or different interactions of factors that cannot be known until studied.

Another way to expand upon this research is to employ additional research approaches. A second potential future study concept could include conducting this same study quantitatively across the entire country using surveys. Several existing research studies on fusion centers used this quantitative approach, but none of them focused specifically on intelligence sharing from federal agencies down to the state and local officials. Creating a quantitative research instrument based upon the interview questions from this research study but employed across the nation could generate some interesting findings. If significantly more time and resources were applied, a mixed methods approach may also reap new or interesting findings that expand on this qualitative exploratory case study.

However, repeating this study across the country solely by using quantitative surveys could be much less effective than approaches which also employ in person interviews. There were many perspectives shared that interviewees would not have been as likely to write down on a survey and send in. Also, several participants were recruited based on establishing a level of trust with them that is not possible with mass distribution of impersonal surveys. For example, gaining entrance to fusion centers for this research

was done by first establishing rapport and some degree of trust with each fusion center director. Then, every individual interviewed for the study knew my intelligence background as well as my employment teaching Homeland Security college courses. This greatly assisted in gaining entrance and recruiting individuals to participate. Those interviewees then advocated participation in the study to other members of their fusion center or their own personal network of contacts at other fusion centers. Once done with their own interview, completed participants then recommended to onsite coworkers and off-site contacts in other fusion centers to allow me to interview them. The rapport establishment and trust building with interviewees was passed on to others and following fusion centers which generated momentum. It is unlikely that an impersonal survey can establish even this surface level of trust or elicit perspectives on a sensitive topic like terrorism intelligence sharing.

Another consideration for future research could include focusing on the organizational relationships within fusion centers and between fusion centers and other organizations. As this study highlighted in Figure 2 *Sharing With and Within a fusion center*, there are many different types and directions (both internally and externally) where sharing occurs related to fusion centers. While this study only focused on the vertical and singular direction of federal intelligence sharing with fusion centers, it would be interesting to learn from an in-depth study trying to map out in detail the sharing that was depicted in figure 2 both within a fusion center (or centers) and between fusion centers and the many key other organizations they interact with on the outside.

Another new and interesting line of research related to this study could include adjusting the same research questions that focused on fusion centers to instead address the role of JTTFs in terrorism intelligence sharing. FBI JTTFs were not directly studied as a part of this research, but their role and the importance of the relationship between fusion centers and JTTF became very evident. JTTFs primarily serve as interagency counterterrorism investigative bodies, but they also are advanced as a mechanism to share terrorism information and intelligence. For this possible future study, it would make sense to start with another exploratory qualitative case study of JTTFs on the east coast, including those who's jurisdiction is an entire state and those focused on a single urban region.

Implications for Positive Social Change

Overcoming the barriers to counterterrorism interagency intelligence sharing can significantly impact major aspects of our society in ensuring a collaborative approach to counterterrorism. This can only be achieved if it is based on a solid foundation of terrorism intelligence sharing across all 3 levels of government. By effectively sharing terrorism intelligence vertically and horizontally among partner agencies is the only way to stop the complex threats the nation faces from both international terrorists and homegrown extremists. We cannot go back to the way it was before 9/11 where a failure to effectively share resulted in a massive tragedy.

This study contributed to the body of knowledge on fusion center with significant and original findings on how federal intelligence is actually shared with state and local officials, and how it can be improved. If the policies and procedures are put into

enactment and federal personnel are embedded full-time to enable effective terrorism intelligence sharing with nonfederal fusion centers, then significant social change can be gained through increased abilities to counter terrorist attacks within the homeland. This research intends to positively influence improved national security through policies that reflect the importance of fusion center federal manning as the crux of intelligence sharing (over systems) and the need to develop and assess personal relationships between key individuals and organizations with leading counterterrorism roles in protecting our citizens.

Summary

This exploratory case study into terrorism intelligence sharing with nonfederal fusion centers has identified several tangible barriers preventing effective sharing such as clearance, culture, policy and personality. The study also detailed of many of the benefits to our nation in better protecting citizens that can be gained in overcoming these obstacles. Changing policies to enable sharing and emphasizing the importance of personal contacts and embedded federal personnel (over systems) is an important finding that should become reflected in both state and local programs as well as federal fusion center funding and statutes.

Finally, this was an academic study and the researcher is aware that many of these policy recommendations may be resource intensive or difficult to enact. However, is it important to reflect on these recommendations now and not after the next major terrorist attack with hundreds of American killed in another preventable catastrophe that could

have been stopped if federal agencies had only been more effective at fulfilling its duty to share the intelligence in its possession with state and local partners.

References

- Abold, J. L., Guidetti, R., & Keyer, D. (2012, June). Strengthening the Value of the National Network of Fusion Centers by Leveraging Specialization: Defining “Centers of Analytical Excellence.” *Homeland Security Affairs* 8(7). Retrieved from <https://www.hsaj.org/articles/223>
- Adams, N., Nordhaus, T., & Shellenberger, M. (2011). *Counterterrorism since 9/11: Evaluating the Efficacy of Controversial Tactics*. Oakland, CA: The Breakthrough Institute. Retrieved from http://thebreakthrough.org/images/pdfs/CCT_Report_revised-3-31-11a.pdf
- Akbulut, A. Y., Kelle, P., Pawlowski, S.D., Schneider, H., & Looney, C.A. (2009). To share or not to share? Examining the factors influencing local agency electronic information-sharing. *International Journal of Business Information Systems*, 4(2), 143 - 172.
- Alexander, E. R., (1995). *How organizations act together: Interorganizational coordination in Theory and Practice*. Amsterdam: Gordon and Beach Publishers.
- Alexander, D. C. & Mors, T. (2007). Best Practices in Identifying Terrorists During Traffic Stops and On Calls for Service, *Crime & Justice International*, 23 (99), 4-12.
- Alspaugh, C. (2011, September 11). Lee Hamilton reflects on 9/11 Commission work. *The New Republic*. Retrieved from http://www.therepublic.com/view/local_story/Lee_Hamilton_reflects_on_9_11__1315737691

- Apuzzo, M. & Goldman, A. (2013). *Enemies Within: Inside the NYPD's Secret Spying Unit and the Bin Laden's Final Plot Against America*. New York, NY: Simon and Schuster.
- Baca, L. (2008, September 24). Testimony of Sheriff, Los Angeles County U.S. Congress, House Committee on Homeland Security, Subcommittee on Intelligence, Information-sharing, and Terrorism Risk Assessment, A Report Card on Homeland Security Information-sharing.
- Baker, T. (2010, August 23). Intelligence-led policing: Leadership, strategies & tactics. What is a law enforcement fusion center? *Security Debrief*. Retrieved from <http://securitydebrief.com/2010/08/23/what-is-a-law-enforcement-fusion-center/>
- Baker, V. (2013). *Information-sharing among public safety agencies*. (Order No. 3550653, Walden University). ProQuest Dissertations and Theses, 145. Retrieved from <http://search.proquest.com/docview/1287062257?accountid=14872>.
- Barron, T., Lewis, J., Silberstein, A. and Shapiro, S. (2016, March). Domestic Security Revisited: An Update on the Progress U.S. Intelligence and Law Enforcement Agencies Have Made in Confronting a Dynamic Domestic Threat Landscape. Business Executives for National Security (BENS). Retrieved from http://www.bens.org/file/DomesticSecurityRevisited_March2016.pdf
- Baškarada, S. (2014). Qualitative Case Study Guidelines. *The Qualitative Report*, 19(24), 1-18.
- Bazeley, P. (2012). NVivo 10 Reference Guide, Research Support. Retrieved from http://www.researchsupport.com.au/NV_10_notes.pdf

- Bazeley, P. & Jackson, K. (Eds). (2013). *Qualitative Data Analysis with NVivo* (2nd ed.), Thousand Oaks, CA: Sage Publications.
- Bender, B. (2013, April 25). FBI did not alert state's anti-terror unit to its probe of suspected bomber in 2011. *The Boston Globe*. Retrieved from <http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html>
- Berkeley, A. R., Bush, W., Heasley, P.G., Nicholson, J.B., Reid, J.A., and Wallace, M.J. (2012, January). *Intelligence Information-sharing Final Report and Recommendations*, National Infrastructure Advisory Council, Retrieved from <http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf>
- Best, R. A. Jr. (2007, February 13). *Sharing Law Enforcement and Intelligence Information: The Congressional Role*. Congressional Research Service Report to Congress (Report # RL33873). Retrieved from http://assets.opencrs.com/rpts/RL33873_20070213.pdf
- Best, R. A. Jr. (2010, July 9). Intelligence issues for Congress. *Congressional Research Service*. Report RL33539. Retrieved from <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA525366>
- Best, R. A. Jr. (2011, December). The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns. *Congressional Research*

- Service*. Report RL41022. Retrieved from <https://www.fas.org/sgp/crs/intel/R41022.pdf>
- Biello, D. (2011, September 9.). The Next Attack? Terrorists' Attempts to Hijack Technology. *Scientific American*. Retrieved from <http://www.scientificamerican.com/article/terrorist-attack-possibilities/>
- Bigdeli, A.Z., Kamal, M., and Cesare, S. (2013). Information-sharing through inter-organisational systems in local government, *Transforming Government: People, Process and Policy*, 7(2), 148 – 176.
- Bimfort, M. T. (1995). A Definition of Intelligence. *Center for the Study of Intelligence, Central Intelligence Agency*. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol2no4/html/v02i4a08p_0001.htm
- Bjelopera, J. P. (2011). Terrorism Information-sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress, CRS Report R40901. Retrieved from <http://fpc.state.gov/documents/organization/166837.pdf>
- Bjelopera, J. P. (2012). The Domestic Terrorist Threat: Background and Issues for Congress, R42536, Congressional Research Service.
- Bjelopera, J. P. & Randol, M. A. (2010). American jihadist terrorism: Combating a complex threat. *Congressional Research Service*. Report R 41416. Retrieved from http://assets.opencrs.com/rpts/R41416_20101207.pdf
- Bodden, V. (2014). *The Boston Marathon Bombing*. Minneapolis, MN: ABDO Publishing.

- Bumgarner, J. (2006). *Federal agents: The growth of federal law enforcement in America*. Santa Barbara, CA: Greenwood.
- Bruce, G. (2013). Definition of Terrorism Social and Political Effects. *Journal of Military & Veterans' Health*, 21(2), 26-30.
- Budinger, Z. B. & Smith, J. H. (2011). Ten Years After 9/11: A Status Report on Information-sharing. Statements before the Senate Committee on Homeland Security and Governmental Affairs.
- Burch, J. (2007, June), A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and Their Implications for Homeland Security. *Homeland Security Affairs*, 3(21). Retrieved from <http://www.hsaj.org/?article=3.2.2>
- Bush, G. W. (2003). Memorandum on Strengthening the Ability of the Department of Justice to Meet Challenges to the Security of the Nation. Retrieved from <http://georgewbush-whitehouse.archives.gov/news/releases/2005/06/text/20050629-1.html>
- Bush, G. W. (2003, July 29). *Executive Order 13311, Homeland Security Information-sharing*, Federal Register/ Vol. 68, No. 147. Retrieved from <http://www.gpo.gov/fdsys/pkg/FR-2003-07-31/pdf/03-19675.pdf>
- Bush, G. W. (2008). *Executive Order 12333: United States Intelligence Activities*. Retrieved from <https://www.cia.gov/about-cia/eo12333.html>
- Bush, G. W. (2010). *Decision Points*. New York, NY: Crown Publishers.

- Canas, D. (2012). *Homeland Security at the State Level: A Primer on State Homeland Security Programs*. Anchor House. Bloomington: IN.
- Cardillo, R. (2010). Intelligence community reform. *Studies in Intelligence* 54(3), 1-7.
Retrieved from <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-54-no.-3/pdfs/ExtractCardillo%20IC%20Reform-Cultural%20Evolution.pdf>
- Carter, D. L. (2004). *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, U.S. Department of Justice. Retrieved from <http://www.cops.usdoj.gov/pdf/e09042536.pdf>
- Carter, D. L., and Carter, J. G. (2009). The intelligence fusion process for state, local, and tribal law enforcement. *Criminal Justice and Behavior*, 36(12), 1323-1339.
- Carter, J., & Chermak, S. (2012). Evidence-based intelligence practices: Examining the role of fusion centers as a critical source of information. *Evidence-based Counterterrorism Policy* 3: 65–88.
- Carter, J. G., Carter, D. L., Chermak, S., and McGarrell, E. (2016, May). Law Enforcement Fusion Centers: Cultivating an Information-sharing Environment while Safeguarding Privacy. *Journal of Police and Criminal Psychology*. pp 1-17. doi 10.1007/s11896-016-9199-4.
- Caruson, K., & MacManus, S. A. (2006). Mandates and management challenges in the trenches: An intergovernmental perspective on homeland security. *Public Administration Review*, 66(4), 522-536.

- Chen, Y. R. (2009). *Tell Me What I Need to Know: What Mayors and Governors Want from Their Fusion Center*. Naval Postgraduate School Masters Thesis. Retrieved from <http://calhoun.nps.edu/handle/10945/4570>
- Chertoff, M. (2005, July 13). Secretary of Homeland Security. U.S. DHS Second Stage Review Remarks. Retrieved from http://www.dhs.gov/xnews/speeches/speech_0255.shtm
- Cilluffo, F. J., Clark, J. R., & Downing, M. P. (2011, September). Counterterrorism intelligence: Law enforcement perspectives. *The George Washington University Homeland Security Policy Institute*. Retrieved from <http://www.gwumc.edu/hspi/policy/HSPI%20Research%20Brief%20-%20Counterterrorism%20Intelligence.pdf>
- Clarke, R. A. (2004, March 24). Testimony to the 9/11 Commission. Retrieved from http://govinfo.library.unt.edu/911/archive/hearing8/9-11Commission_Hearing_2004-03-24.pdf
- Coffey, A. (2015, October). Evaluating Intelligence and Information-sharing Networks: Examples from a Study of the National Network of Fusion Centers. George Washington University Issue Brief # 2015-04. Retrieved from <https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CoffeyFusionCenterPaper-CCHS.pdf>
- Comiskey, J. G. (2010, March). *Effective State, Local, and Tribal Police Intelligence: The New York City Police Department's Intelligence Enterprise-A Smart Practice*.

Naval Postgraduate School Masters Thesis. Retrieved from

<http://calhoun.nps.edu/handle/10945/5460>

Cordner, G., & Scarborough, K. (2010). Information-sharing: Exploring the intersection of policing with national and military intelligence. *Homeland Security Affairs*, 6(1). Retrieved from <https://www.hsaj.org/articles/92>

Cresswell, A.M., Pardo, T. A., Canestraro, D.S., Dawes, S.S., (2005). Why Assess Information-sharing Capability? *Center for Technology in Government*, Retrieved from http://www.ctg.albany.edu/publications/guides/why_assess/why_assess.pdf

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Cumming, A. (2005, August 16). Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress. *Congressional Research Service Report RL33033*. Retrieved from <https://www.fas.org/sgp/crs/intel/RL33033.pdf>

Davis, P. (2010). Connecting the Dots at the Local Level: Fusion centers Make Homeland Security a State, City and County Affair. *Journal of Counterterrorism & Homeland Security International* 16(3), 8-10. International Security & Counter Terrorism Reference Center.

Davis, E. & Kayyem, J. (2014, April 15). Would better data have helped? *The Boston Globe*, Retrieved from <http://www.bostonglobe.com/opinion/2014/04/15/better-data-management-can-solve-crime-and-other-problem/hqshiNwRO9Fqs7FFTCUC8K/story.html>

- Dawes, S. S. (1996). Interagency information-sharing: Expected benefits, manageable risks. *Journal of Policy Analysis & Management*, 15(3), 377-394.
- Dawes, S. S., Cresswell, A. M., & Pardo, T. A. (2009). From 'Need to Know' to 'Need to Share': Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks. *Public Administration Review*, (3). 391.
- De Bruijn, H. (2006). One fight, one team: the 9/11 commission report on intelligence, fragmentation and information. *Public Administration*, 84(2), 267-287.
doi:10.1111/j.1467-9299.2006.00002.x
- Desai, S. B. (2005, February 1). Solving the Interagency Puzzle. *Policy Review* (129). 57-72.
- Domash, S. F. (2004, September). How to work with the feds. *Police Magazine*.
Retrieved from <http://www.policemag.com/Channel/Patrol/Articles/Print/Story/2004/09/How-to-Work-with-the-Feds.aspx>
- Drake, D.B., Steckler, N.A., & Koch, M.J. (2004). Information-sharing in and Across Government Agencies. *Social Science Computer Review* 22(1), 67-84. doi: 10.1177/0894439303259889.
- Eack, K. D. (2008). State and local fusion centers: Emerging trends and issues. *Homeland Security Affairs*, Supplement 2. Retrieved from <http://www.hsaj.org/?special:fullarticle=supplement.2.3>
- Eisinger, P. (2006). Imperfect federalism: The intergovernmental partnership for homeland security. *Public Administration Review*, 66(4), 537-545.

- Ernst, M. (2014, March 20). *How local and state cops fit into counterterrorism*. P1 (Police One) First Person. Retrieved from <https://www.policeone.com/counterterrorism/articles/6994276-How-local-and-state-cops-fit-into-counterterrorism/>
- Erwin, M. C. (2013). *Intelligence Issues for Congress*. Congressional Research Service. Retrieved from <http://www.fas.org/sgp/crs/intel/RL33539.pdf>
- Etzioni, A. (2013, May 29). The Danger of Overcorrecting on Terror, *The National Interest*. Retrieved from <http://nationalinterest.org/commentary/the-danger-overcorrecting-terror-8525>
- Evans, R. (2013). *Policy implementation in homeland security: Implementing open source intelligence policies within state run fusion centers*. (Order No. 3552221, Walden University). ProQuest Dissertations and Theses, 149. Retrieved from <http://search.proquest.com/docview/1294161960?accountid=14872>.
- Federal Bureau of Investigation (2005), *Terrorism 2002-2005*, Retrieved from <http://www.fbi.gov/stats-services/publications/terrorism-2002-2005>
- Federal Bureau of Investigation (FBI). (2009, November 11). Investigation continues into Fort Hood shooting. *FBI National Press Office*. Retrieved from <http://www.fbi.gov/news/pressrel/press-releases/investigation-continues-into-fort-hood-shooting>
- Fenske, D. (2008). All enemies, foreign and domestic: Erasing the distinction between foreign and domestic intelligence gathering under the fourth amendment. *Northwestern University Law Review*, 102(1), 343-381.

- Filler, J. (2010, February 15). The disconnect between DHS and the homeland security mission. *Emergency Management*. Retrieved from <http://www.emergencymgmt.com/emergency-blogs/homeland/The-Disconnect-between-DHS.html>
- Filler, J. (2010, March 23). Analysis: Collecting and Sharing Information Is Not Enough. *Emergency Management*. Retrieved from <http://www.emergencymgmt.com/safety/Collecting-Sharing-Information.html>
- Forsyth, W. A. (2005, September). *State and Local Intelligence Fusion Centers: An Evaluative Approach in Modeling a State Fusion Center*. Naval Postgraduate School Masters Thesis. Retrieved from <https://calhoun.nps.edu/handle/10945/2044>
- Fresenko, V. L. (2010, December). *Social Media Integration into State-Operated Fusion Centers and Local Law Enforcement: Potential Uses and Challenges*. Naval Postgraduate School Masters Thesis. Retrieved from <http://calhoun.nps.edu/handle/10945/4996>
- Fries, T. (2013, March). *Fusion Center and Federalism: Erosion or Enhancement*. Naval Postgraduate School Masters Thesis. Retrieved from <http://hdl.handle.net/10945/32821>
- Fuller, G. (2008). Joint Terrorism Task Forces: Protecting DOD from Terrorist Attacks. *The Guardian*, 10(1). Retrieved from <https://www.hsdl.org/?view&did=486223>

- Fussell, C., Hough, T., & Pederson, M. D. (2009, December). *What makes Fusion Cells effective?* Naval Postgraduate School Masters Thesis. Retrieved from <http://calhoun.nps.edu/handle/10945/4438>
- Garicano, L., & Posner, R. (2005). Intelligence reform since 9/11: An organizational economics perspective. *Journal of Economic Perspectives*, 19(4). Retrieved from <http://www.jstor.org/stable/4134960>
- Gellman, B. (2011, May). Is the FBI up to the job 10 years after 9/11? *Time Magazine* 177(18) Retrieved from <http://www.time.com/time/magazine/article/0,9171,2068082,00.html>
- German, M. and Stanley J. (2007, December). What's Wrong with Fusion Centers? *American Civil Liberties Union*. Retrieved from https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf
- Ghilarducci, M. (2016, February 2). Frontline Response to Terrorism in America. Testimony to the U.S. Senate Committee on Homeland Security and Governmental Affairs. Retrieved from <http://www.hsgac.senate.gov/download/testimony-ghilarducci-2016-02-02>.
- Gil-Garcia, J.R., Guler, A., Pardo, T.A. and Burke, G.B. (2010), "Trust in government cross-boundary information-sharing initiatives: identifying the determinants", System Sciences HICSS 2010 43rd Hawaii International Conference on 5-8 January, IEEE Computer Society, p. 1.
- Gorman, S. (2003, August 1). FBI, CIA remain worlds apart. *National Journal*. Retrieved from <http://www.govexec.com/dailyfed/0803/080103nj1.htm>

- Graphia, R. D. (2010). An exploratory study of the perceived utility and effectiveness of state fusion centers. PhD Dissertation Rutgers University; Graduate School – Newark. Retrieved from <http://dx.doi.org/doi:10.7282/T3BG2P4V>
- Graham, B. and Talent, J. (2008). World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism. Retrieved from http://digital.library.unt.edu/ark:/67531/metadc123525/m2/1/high_res_d/10942265.pdf
- Gutjahr, M. H. (2005). *The Intelligence Archipelago: The Community's Struggle to Reform in the Globalized Era*. National Intelligence University. Retrieved from http://ni-u.edu/ni_press/pdf/The_Intelligence_Archipelago.pdf
- Harper, J. L. (2009, December). *Fusion center privacy policies: does one size fit all?* Naval Postgraduate School Masters Thesis. Retrieved from <http://calhoun.nps.edu/handle/10945/4431>
- Hatter, H. B. (2011, March 7). The tech that makes anti-terrorism tip lines effective. *GCN Magazine*. Retrieved from <http://gcn.com/articles/2011/03/07/feature-3-fusion-center-main.aspx>
- Henriksen, T. (2013, July). Eyes, Ears, and Daggers: Special Operations Forces and the Central Intelligence Agency in America's Security. *Joint Special Operations University*. Retrieved from <http://jsou.socom.mil/JSOU%20Publications/SOF-CIA%20Roles%20by%20Henriksen.pdf>

- Hewitt, C. (2014). Law Enforcement Tactics and Their Effectiveness in Dealing with American Terrorism: Organizations, Autonomous Cells, and Lone Wolves. *Terrorism and Political Violence*, 1(26), 58-68.
- Hitz, F. P. (2012). U.S. intelligence in the wake of September 11: The rise of the spy commando and reorganized operational capabilities. *Harvard Journal of Law & Public Policy*, 35(1). Retrieved from <http://heinonline.org/HOL/LandingPage?handle=hein.journals/hjlp35&div=19&id=&page=>
- Hoffman, B., Meese, E. and Roemer, T. J. (2015, March). *The FBI: Protecting the Homeland in the 21st Century: Report of the Congressionally-directed 9/11 Review Commission to the Director of the Federal Bureau of Investigation*. Retrieved from <https://www.fbi.gov/stats-services/publications/protecting-the-homeland-in-the-21st-century>
- Homeland Security Intelligence Council (2011). Intelligence to protect the homeland: ...taking stock ten years later and looking ahead. *Intelligence and National Security Alliance*. Retrieved from http://images.magnetmail.net/images/clients/INSA/attach/INSA_Homeland_Security_Intelligence.pdf
- House Homeland Security Committee. U.S. Congress. (2016, January). *Terror Snapshot*. Retrieved from <https://homeland.house.gov/wp-content/uploads/2016/01/HSC-Terror-Threat-Snapshot.pdf>
- Huang, M. P. (2007). After reorganization: a leadership journey. *The Public Manager*, 36(1), 67-69.

- Hylton, H. (2009, March 9). Fusion Centers: Giving Cops Too Much Information? *Time*. Retrieved from <http://www.time.com/time/nation/article/0,8599,1883101,00.html>
- Imperial, M. T. (2005). Using collaboration as a governance strategy: Lessons from six watershed management programs. *Administration and Society*, 37(3), 281–320.
- Inspector Generals of the Intelligence Community, Central Intelligence Agency, Department of Justice, and Department of Homeland Security (2014, April 10). *Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombings*. Retrieved from <http://www.justice.gov/oig/reports/2014/s1404.pdf>
- Intelligence Reform and Terrorism Prevention Act of 2004. Public Law 108–458, 118 STAT. 3639, codified as amended at 50 USC 401 note. Retrieved from <http://www.nctc.gov/docs/irtpa.pdf>
- Interagency Threat Assessment and Coordination Group. (2011, March). *Intelligence Guide for First Responders*. 2nd Ed. Retrieved from http://ise.gov/sites/default/files/ITACG_Guide_2ed.pdf
- Jackson, B. A. (ed). (2009). The challenge of domestic intelligence in a free society: A Multidisciplinary Look at the creation of a U.S. domestic counterterrorism intelligence Agency. RAND. Retrieved from http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG804.pdf
- Jeffreys-Jones, R. (2007). *The FBI: A history*. Binghamton, NY: Vail-Ballou.
- Joint Chiefs of Staff. (2013, October 22). Joint Publication 2-0: Joint Intelligence.

Joint Chiefs of Staff. (2009, November 13). Joint Publication 3-26: Counterterrorism.

Johnson, B. R. (2007). A Look at Fusion Centers: Working Together to Protect America.

FBI Law Enforcement Bulletin, 76(12), pp. 28-32. Retrieved from

<http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2007-pdfs/dec07leb.pdf>

Joyal, R. G. (2010). Are fusion centers achieving their intended purposes? findings from a qualitative study on the internal efficacy of state fusion centers. *IALEIA Journal*, 19(1), 54-76.

Joyal, R. G., (2012, December). How far have we come? Information-sharing, interagency collaboration, and trust within the law enforcement community.

Criminal Justice Studies, 25(4), 357–370.

Kahn, L. H. (2009, June 9). The problems with the Department of Homeland Security.

Bulletin of the Atomic Scientists. Retrieved from <http://www.thebulletin.org/web-edition/columnists/laura-h-kahn/the-problems-the-department-of-homeland-security>

Kaplan, E. (2007, February 22). Backgrounder: Fusion centers. The Council on Foreign

Relations. Retrieved from <http://www.cfr.org/intelligence/fusion-centers/p12689>

Kean, T.H., & Hamilton, L.H., & et al. (2004, July 22). *The 9/11 Commission Report*.

Retrieved from <http://www.9-11commission.gov/report/911Report.pdf>

Keating, W. H. (2013, July 31). Letter to FBI Director James Comey. Retrieved from

<http://heavy.com/news/2013/07/bill-keating-letter-fbi-boston-bombings/>

- Keegan, J. (2003). *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*. Random House. New York: NY.
- Kincaid, J., & Cole, R. (2002, September). Issues of federalism in response to terrorism. *Public Administration Review*, 62. 181-193.
- King, C. B. III. (2009). The Department of Homeland Security: An organization in transition. *Joint Forces Quarterly*, 55. Retrieved from <https://digitalndulibrary.ndu.edu/cdm4/document.php?CISOROOT=/ndupress&CISOPTR=39478&REC=5>
- Klem, N. (2014, December). The national network of fusion centers: Perception and reality. Naval Postgraduate School Masters Thesis. Retrieved from <https://calhoun.nps.edu/handle/10945/44598>
- Kobach, K. W. (2004, June). State and Local Authority to Enforce Immigration Law: A Unified Approach for Stopping Terrorists, *The Center for Immigration Studies Backgrounder*. Retrieved from <http://www.cis.org/sites/cis.org/files/articles/2004/back604.pdf>
- Kranish, M., Bender, B., Murphy, S. P., & Bierman, N. (2013, April 25). Data-sharing troubles raise questions in Marathon case: 2 separate watch lists named Boston suspect. *The Boston Globe*. Retrieved from <https://www.bostonglobe.com/news/nation/2013/04/24/government-terrorism-information-sharing-program-rated-high-risk-despite-years-effort-since/3ImcHIZOaPKfeeBYTAXRHN/story.html>

- Kraut, R. E., Fussell, S. R., Brennan, S. E. and Siegel, J. (2002). Understanding Effects of Proximity on Collaboration: Implications for Technologies to Support Remote Collaborative Work. In P. Hinds, and S. Kiesler, (Eds.), *Distributed work* (137-158). Cambridge, MA: MIT Press.
- Kumar, R. (2013). Lessons from Boston bombing: need for strategic creativity in counter-terrorism. *S. Rajaratnam School of International Studies*, Retrieved from <http://hdl.handle.net/10220/18872>
- Kumar, K. & Van Dissel, H. G. (1996). Sustainable collaboration: Managing conflict and cooperation in interorganizational systems. *MIS Quarterly*, 20(3), 279-300.
- Lamb, C. J. & Munsing, E. (2011, March). Secret Weapon: High-value Target Teams as an Organizational Innovation. National Defense University. Institute for National Strategic Studies, Perspectives #4. Retrieved from www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA540046
- Ladner, R. D. (2010, December). A Trusted National Fusion Center Network: Are Baseline Capabilities and Accreditation Needed? Naval Postgraduate School Masters Thesis. Retrieved from <http://calhoun.nps.edu/handle/10945/5215>
- Lahneman, W. J. (2004). Knowledge sharing in the intelligence community after 9/11. *International Journal of Intelligence and CounterIntelligence*, 17(4), 614-633. doi: 10.1080/08850600490496425
- Lambert, D. (2010, December). Intelligence-Led Policing in a Fusion Center. *FBI Law Enforcement Bulletin*. Retrieved from http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/Dec2010/intelligence_feature

- Landsbergen, D. Jr & Wolken, G. Jr (2001), Realizing the promise: government information systems and the fourth generation of information technology. *Public Administration Review*, 61(2), 206-220.
- Laub, Z. (2015, November 16). *The Islamic State. CFR Backgrounder*. The Council on Foreign Relations. Retrieved from <http://www.cfr.org/iraq/islamic-state/p14811>
- Lawrence, E. (2008a). Homeland Security: Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers. *Government Accounting Office Report GAO-08-636T*. Retrieved from <http://www.gao.gov/new.items/d08636t.pdf>
- Larence, E. (2008b, April 17). Homeland security: Federal efforts are helping to address some challenges faced by state and local fusion centers. United States Government Accountability Office, Report GAO-08-636T. Retrieved from <http://www.gao.gov/assets/120/119734.pdf>
- Larence, E. (2009, December). Information-sharing: Federal agencies are sharing border and terrorism information with local and tribal law enforcement agencies, but additional efforts are needed. GAO-10-41. *Government Accountability Office*. Retrieved from <http://www.gao.gov/new.items/d1041.pdf>
- Larence, E. (2010, September). Information-sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results. GAO-10-972. *Government Accountability Office*. Retrieved from <http://www.gao.gov/assets/320/310268.pdf>

- Larence, E. (2011). Information-sharing: Progress made and challenges remaining in sharing terrorism-related information. GAO-12-144A. *Government Accountability Office*. Retrieved from <http://www.gao.gov/new.items/d12144t.pdf>
- Larence, E. (2013). Information-sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective. GAO-13-233. *Government Accountability Office*. Retrieved from <http://www.gao.gov/assets/660/652995.pdf>
- Larence, E. (2014). Information-sharing: DHS Is Assessing Fusion Center Capabilities and Results, but Needs to More Accurately Account for Federal Funding Provided to Centers. GAO-15-155: *Government Accountability Office*. Retrieved from <http://www.gao.gov/assets/670/666760.pdf>
- Leavell, R. (2007, March). Evolution of Regional Counterterrorism Centers within a National Counterterrorism Network. Naval Postgraduate School Thesis. Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/3010/07Mar_Leavell.pdf
- Lehrer, E. (2004, Summer). The homeland security bureaucracy. *The Public Interest*, 156, 71-92
- Lewandowski, C., Carter J. G., and Campbell, W. L. (2017) The role of people in information-sharing: perceptions from an analytic unit of a regional fusion center, *Police Practice and Research*, 18:2, 174-193, doi: 10.1080/15614263.2016.1250631

- Lerner, C. S. (2003) The USA PATRIOT Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement, 11 *George Mason Law Review*, 493, pp. 524–26
- Leuschner, K. J. (2008). Should the United States Establish a Dedicated Domestic Intelligence Agency for Counterterrorism? RAND Research Brief. Retrieved from http://www.rand.org/content/dam/rand/pubs/research_briefs/2008/RAND_RB9369.pdf
- Levin, C. and Coburn, T. (2012, October 2). *Federal support for and involvement in state and local fusion centers*. Majority and Minority Staffs Report of the U. S. Senate Permanent Subcommittee on Investigations. Retrieved from <https://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04>
- Logan, G. (ed). (2010). *Homeland Security and Intelligence*. Santa Barbara, CA: Praeger Publications.
- Mandoli, G. R. (2006, September). The sandbox strategy: The why and how of federal law enforcement integration. Naval Post-Graduate School unpublished Master's Thesis. Retrieved from http://edocs.nps.edu/npspubs/scholarly/theses/2006/Sep/06Sep_Mandoli.pdf
- Marks, D. E., & Sun, I. Y. (2007). The impact of 9/11 on organizational development among state and local law enforcement agencies. *Journal of Contemporary Criminal Justice*, 23(2), 159-173. doi: 10.1177/1043986207301364

- Maurer, D. C. (2012, April 16). FBI Counterterrorism: Vacancies Have Declined, but FBI Has Not Assessed the Long-Term Sustainability of Its Strategy for Addressing Vacancies. *Government Accountability Office Report GAO-12-533*. Retrieved from <http://www.gao.gov/assets/600/590147.pdf>
- Maxwell, J. A. (2012). *Qualitative Research Design: An Interactive Approach*. Sage: Thousand Oaks, CA.
- Mayer, M. A., Carafano, J. J., and Zuckerman, J. (2011). *Homeland Security 4.0: Overcoming Centralization, Complacency, and Politics*, The Heritage Foundation. Retrieved from <http://www.heritage.org/research/reports/2011/08/homeland-security-4-0-overcoming-centralization-complacency-and-politics>
- Mayer, M. A. (2016, March). *Consolidate Domestic Intelligence Entities Under the FBI*. American Enterprise institute. Retrieved from <https://www.aei.org/wp-content/uploads/2016/03/Fusion-Center.pdf>
- McCaul, M. (2014), U.S. House of Representatives Committee on Homeland Security Hearing, *The Boston Marathon Bombings, One Year On: A Look Back to Look Forward*. Retrieved from <http://homeland.house.gov/sites/homeland.house.gov/files/documents/04-09-14%20McCaul%20Open.pdf>
- McCaul, M. (2015, November 2). *Department of Homeland Security Support to Fusion Centers Act of 2015*. U.S. House of Representatives. Retrieved from <https://www.congress.gov/114/crpt/hrpt322/CRPT-114hrpt322.pdf>
- McCaul, M. and Keating, B. (2014, March 27), *How did Tsarnaev go off FBI radar?* *The Boston Globe*, Retrieved from

<http://www.bostonglobe.com/opinion/2014/03/27/missed-opportunities-lessons-learned-year-after-marathon-bombings/ztVLvM1SFyzaVtf1oI6AyN/story.html>

McCaul, M. and King, P. (2013, March), Majority Staff Report on the National Network of Fusion Centers. U.S. House of Representatives Homeland Security Committee Report. Retrieved from <https://www.archives.gov/files/isoo/oversight-groups/sltps-pac/staff-report-on-fusion-networks-2013.pdf>

McCaul, M. and King, P. (2014, March), The Road to Boston: Counterterrorism Challenges and Lessons from the Marathon Bombings. U.S. House of Representative Homeland Security Committee Report. Retrieved from <https://homeland.house.gov/files/documents/Boston-Bombings-Report.pdf>

McConnell, M. (2007). Overhauling intelligence. *Foreign Affairs* 86(4), 49 – 58.

McCreight, R. (2015). Constitutional Authority in Crisis: Examining a State Governor's Emergency Powers. *Journal of Homeland Security and Emergency Management*, 12(1), pp. 23-42. doi:10.1515/jhsem-2014-0095

MacGregor, D. S. (2010). Fusion 2.0: the next generation of fusion in California: aligning state and regional fusion centers. Naval Postgraduate School Masters Thesis. Retrieved from <http://calhoun.nps.edu/handle/10945/5396>

McNeill, J. B., Carafano, J. J. and Zuckerman, J. (2011). 39 Terror Plots Foiled Since 9/11: Examining Counterterrorism's Success Stories. *The Heritage Foundation Backgrounder #2556 on Terrorism*. Retrieved from http://www.heritage.org/research/reports/2011/05/39-terror-plots-foiled-since-911-examining-counterterrorisms-success-stories#_ftnref57

- McQuade, B. (2016, July 19). The Puzzle of Intelligence Expertise: Spaces of Intelligence Analysis and the Production of “Political” Knowledge. *Qualitative Sociology*, pp 1-19.
- Middlemiss, A. D. & Gupta, N. (2007). U.S. interagency law enforcement cooperation since September 11, 2001: Improvements and results. *Journal of Financial Crime*, 14(2), 138.
- Mitchiner, C. C. (2013). Department of Homeland Security and Fusion Centers, an Unfused Network. Strategy Research Project, U.S. Army War College. Retrieved from <http://www.dtic.mil/dtic/tr/fulltext/u2/a589473.pdf>
- Monahan, T. (2009) The murky world of 'Fusion Centers', *Criminal Justice Matters* 75(1), 20 – 21. Retrieved from <http://www.scribd.com/doc/21970772/Murky-World-of-Fusion-Centers-2009>
- Monahan, T. & Palmer N.A. (2009). The Emerging Politics of DHS Fusion Centers. *Security Dialogue*, 40(6), 617-636. doi: 10.1177/0967010609350314
- Morton, J. F. (2012). *Next-Generation Homeland Security: Network Federalism and the Course to National Preparedness*. Annapolis, MD: Naval Institute Press.
- Mueller, R. S. (2010, October 6). *Countering the Terrorism Threat*. Director of the Federal Bureau of Investigation, speech to the Preparedness Group Conference <https://www.fbi.gov/news/speeches/countering-the-terrorism-threat>
- Mushkatel, A. H., & Weschler, L. F. (1985). Emergency management and the intergovernmental system. *Public Administration Review*, 45, 49-56.

- Napolitano, J. (2011, February 11). Testimony Before the United States House of Representatives Committee on Homeland Security, “Understanding the Homeland Threat Landscape – Considerations for the 112th Congress”. Retrieved from <http://www.gpo.gov/fdsys/pkg/CHRG-112hrg72212/pdf/CHRG-112hrg72212.pdf>
- National Security Council (2007). National Strategy for Information-sharing: Successes and Challenges in Improving Terrorism-related Information. Washington, DC: The Whitehouse. Retrieved from: http://georgewbushwhitehouse.archives.gov/nsc/infosharing/NSIS_book.pdf
- National Security Council (2012). National Strategy for Information-sharing and Safeguarding. Washington, DC: The Whitehouse. Retrieved from http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf
- Negroponete, J. D.; Wittenstein, E. M. (2009). Urgency, Opportunity, and Frustration: Implementing the Intelligence Reform and Terrorism Prevention Act of 2004. *Yale Law & Policy Review*. 28(2). Pp. 379-417.
- Nelson, R. and Bodurian, B. (2010, March). *A Growing Terrorist Threat? Assessing “Homegrown” Extremism in the United States*. Center for Strategic and International Studies. Retrieved from http://csis.org/files/publication/100304_Nelson_GrowingTerroristThreat_Web.pdf
- Newbill, R. (2008, June). *Intelligence Sharing, Fusion Centers, and Homeland Security*. U.S.A.F Institute of Technology, Retrieved from handle.dtic.mil/100.2/ADA488163

- Newkirk, A. B. (2010) The Rise of the Fusion-Intelligence Complex: A critique of political surveillance after 9/11. *Surveillance & Society*, 8(1), 43-60. Retrieved from <http://surveillance-and-society.org/ojs/index.php/journal/article/view/fusion/fusion>
- O'Connor, T. R. (2006). Intelligence Led Policing and Transnational Justice. *Journal of the Institute of Justice and International Studies*. (6), 233-239. ISSN 1538-7909
- Olson, W. (2008). Interagency coordination: The normal accident or the essence of indecision. *U.S. Army Strategic Studies Institute*. Retrieved from <http://www.strategicstudiesinstitute.army.mil/pdf/PUB896.pdf>
- Palmieri, L. M. (2005, June). Information vs. Intelligence: What Police Executives Need to Know. *The Police Chief Magazine*, 72(6).
- Pappas, M. J. (2010). Department of Homeland Security and Information-sharing: Is it Working. Unpublished U.S. Army War College Masters Thesis. Retrieved from <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA520018&Location=U2&doc=GetTRDoc.pdf>
- Patel, D. M. and Olson, S. (2012). *Information-sharing and Collaboration: Applications to Biosurveillance*. The National Academies Press. Washington, D.C. Retrieved from <http://biosurveillance.typepad.com/files/iom-nbic-reports.pdf>
- Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage Publications.
- Paul, K. (2015). *2015 ISE Annual Report to Congress*. Information-sharing Environment. Retrieved from

https://www.ise.gov/sites/default/files/FINAL_ISE_Annual_Report_2015_FOR_WEB_0.pdf

- Perl, R. (2004). The Department of Homeland Security: Background and challenges. In *Terrorism: Reducing Vulnerabilities and Improving Responses: U.S - Russian Workshop Proceedings* (pp. 176-184). Washington, DC: The National Academies Press.
- Perrow, C. (2006, April). The Disaster after 9/11: The Department of Homeland Security and the Intelligence Reorganization. *Homeland Security Affairs* 1(2). Retrieved from <https://www.hsaj.org/articles/174>
- Plecas, D., McCormick, A. V., Levine, J., Neal, P., and Cohen, I. M. (2011). Evidence-based solution to information-sharing between law enforcement agencies, *Policing: An International Journal of Police Strategies & Management*, 34(1), pp.120- 134.
- Posner, R. A. (2011). *Remaking domestic intelligence*. Hoover Press. CA: Stanford.
- Randol, M. A. (2009a). Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches. Congressional Research Service. Retrieved from http://assets.opencrs.com/rpts/RL33616_20090114.pdf
- Randol, M. A. (2009b). The department of homeland security intelligence enterprise: Operational overview and oversight challenges for Congress. Congressional Research Service Report #R40602. Retrieved from http://assets.opencrs.com/rpts/R40602_20100319.pdf

- Randol, M. A. (2010). The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress. Congressional Research Service. Retrieved from http://assets.opencrs.com/rpts/R40602_20100319.pdf
- Rascoff, S. J. (2009). Domesticating Intelligence. *Southern California Law Review*, 83, pp. 575-648.
- Rascoff, S. J. (2010). The Law of Homegrown (Counter) Terrorism (2010). *Texas Law Review*, 88, pp. 1715-1749.
- Riebling, M. (2002). *Wedge: From Pearl Harbor to 9/11: How the secret war between the FBI and CIA has endangered national security*. New York: New York, NY: Simon & Schuster.
- Regan, P. and Monahan, T. (2013). Beyond counterterrorism: Data sharing, privacy and organizational histories of DHS Fusion Centers. *International Journal of E-Politics* 4 (3): 1–14. DOI: 10.4018/jep.2013070101.
- Regan, P. and Monahan, T (2014). Fusion center accountability and intergovernmental information-sharing. *Publius: The Journal of Federalism* 44(3): 475–498.
- Regan, P., Monahan, T, and Craven, K. (2015). Constructing the suspicious: Data production, circulation, and interpretation by DHS fusion centers. *Administration and Society* 47(6): 740–762. DOI: 10.1177/0095399713513141.
- Relyea, H. C. (2004). Homeland security and information-sharing: Federal policy considerations. *Government Information Quarterly*, 21(4), 420-438.

- Reilly, S. (2013, April 29). Boston bombing renews focus on gaps in information-sharing. *Federal Times* 49(7), 4-4. Retrieved from <http://archive.federaltimes.com/article/20130426/DEPARTMENTS03/304260002/Boston-bombing-renews-focus-gaps-information-sharing>
- Richelson, J. T. (2012, July 19). Documenting the FBI: Declassified Documents Provide New Detail on Confronting the Terrorist Threat – from al-Qaeda to Skinheads. *National Security Archive Electronic Briefing Book No. 386*. Retrieved from <http://nsarchive.gwu.edu/NSAEBB/NSAEBB386/>
- Ridge, T. (2009). *The test of our times: America under siege and how we can be safe again*. New York, N.Y: St. Martin's Press.
- Riegle, R. (2009, April 1). *The Future of Fusion Centers: Potential Promise and Dangers*, Testimony before the House Committee on Homeland Security. Retrieved from http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm
- Rineheart, J. (2010). Counterterrorism and Counterinsurgency. *Perspectives On Terrorism*, 4(5). Retrieved from <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/122/249>
- Roberts, P. (2008, Summer). Dispersed federalism as a new regional governance for homeland security. *Publius*, 38(3), 416-444.
- Robinson, N. & Disley, E. (2010). *Incentives and Challenges for Information-sharing in the Context of Network and Information Security*. European Network and

Information Security Agency. Retrieved from

http://www.rand.org/pubs/external_publications/EP201200167.html

Roebuck, R. (2009, June 18). ICE, DEA vow to cooperate in efforts against drug trafficking: Federal agencies often caught in border turf wars, studies show. *The Monitor*. Retrieved from <http://www.themonitor.com/articles/ice-27790-drug-agencies.html>

Rollins, J. (2008, January 18). *Fusion Centers: Issues and Options for Congress*. Congressional Research Service Report for Congress (Report #RL34070). Retrieved from http://assets.opencrs.com/rpts/RL34070_20080118.pdf

Rosenbach, E. (2008). The incisive fight: recommendations for improving counterterrorism intelligence. *The ANNALS of the American Academy of Political and Social Science*, 618(1), 133-147. doi:10.1177/0002716208316947

Saari, S. C. (2010, December). Fusion centers securing America's heartland from threats. Naval Postgraduate School Thesis. Retrieved from <http://hdl.handle.net/10945/5053>

Sales, N. A. (2010a, February) Share and Share Alike: Intelligence Agencies and Information-sharing, *The George Washington Law Review*, 78(2), 279-352. Retrieved from <http://groups.law.gwu.edu/lr/articlepdf/78-2-sales.pdf>

Sales, N. A. (2010b). Mending walls: Information-sharing after the USA Patriot Act. *Texas Law Review*, 88, 1795-1854.

- Schmitt, E. (2011, February 10). Lawmakers hear of threat by domestic terrorists. *The New York Times*, Retrieved from <http://www.nytimes.com/2011/02/10/us/politics/10terror.html>
- Schnedar, C. A. (2011). Acting Inspector General, U.S. Department of Justice Statement before the U.S. House of Representatives concerning “Oversight of Department of Justice and Department of Commerce,” February 9, 2011. Retrieved from <http://www.justice.gov/oig/testimony/t1102.pdf>
- Scott, E. F. (2014, November). *Integrating Fusion Centers and Law Enforcement in Utilization of the Intelligence Cycle*. Masters Thesis, American Public University. Retrieved from <http://digitalcommons.apus.edu/cgi/viewcontent.cgi?article=1093&context=theses>
- Shultz, R. (2016, May). Military Innovation in War: It Takes a Learning Organization—A Case Study of Task Force 714 in Iraq, *Joint Special Operations University*, Report 16-6. Retrieved from jsou.socom.mil/JSOU%20Publications/MilitaryInCVM29Apr16.pdf
- Sims, J. (2007). Intelligence to counter terror: The importance of all-source fusion. *Intelligence & National Security*, 22(1), 38-56. doi:10.1080/02684520701200772
- Seamon, R. H. and Gardner, W. D. (2005) The *PATRIOT Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL’Y 319, pp. 458–63.

- Serrao, S. (2010, August 23). What is a Law Enforcement Fusion Center? *Security Debrief*. Retrieved from <http://securitydebrief.com/2010/08/23/what-is-a-law-enforcement-fusion-center/>
- Shedd, D. (2016, August 25). Facing the New Reality of Homegrown Terrorism. The Cipher Brief. Retrieved from <https://www.thecipherbrief.com/column/strategic-view/facing-new-reality-homegrown-terrorism-1089>
- Shane, S. & Johnston, D. (2009, November 12). Questions, not alarms, met exchanges with cleric. *The New York Times*. Retrieved from <http://www.nytimes.com/2009/11/12/us/12inquire.html>
- Sheehan, M.A. (2009, September 26), "The Hatfields and McCoys of Counterterrorism," *The New York Times*, Retrieved from <http://www.nytimes.com/2009/09/27/opinion/27sheehan.html>
- Shepherd, D. (2011, January). The role of the private sector in fusion centers. *Security*, 48(1), 36-39.
- Shiffman, G. M., Sciara-Rippeon, N., and Gee, M. (2010, February). Managing the Dots: The Challenges of Intelligence Sharing for the Homeland Security Enterprise, Center for Peace and Security Studies. Retrieved from http://www1.georgetown.edu/sfs/cpass/center/research/publications/ManagingtheDots_1.pdf
- Shepherd, D. (2011, January). The role of the private sector in fusion centers. *Security*, 48(1), 36-39.

- Shultz, R. H. (2004, January 26). Showstoppers: Nine reasons why we never sent our Special Operations Forces after al Qaeda before 9/11. *The Weekly Standard*. Retrieved from <http://www.weeklystandard.com/showstoppers/article/4846>
- Silber, M. D. (2012, June). Who Will Defend the Defenders? *Commentary Magazine*. Retrieved from <http://www.commentarymagazine.com/article/who-will-defend-the-defenders/>
- Silber, M. and Frey, A. (2013, November). Detect, Disrupt, and Detain: Local Law Enforcement's Critical Role in Combatting Homegrown Extremism and the Evolving Terrorist Threat. *Fordham Urban Law Journal*. 41(1), 217-176.
- Silberman, L. H., and Robb, C. S. (2005 March 31), Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (The WMD Commission), Report to the President of the United States. Retrieved from http://www.wmd.gov/report/wmd_report.pdf.
- Skahill, T. M. (2010, December). *Striking the Right Balance Fusion Centers and Privacy*. Naval Postgraduate School Masters thesis. Retrieved from <http://calhoun.nps.edu/handle/10945/5243>
- Stake, R. E. (1995). *The Art of Case Study Research*. Sage: Thousand Oaks, CA
- Steiner, J. E. (2010). Improving homeland security at the state level--Needed: State-level, integrated intelligence enterprises. *Studies in Intelligence*, 53(3). Retrieved from <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-53-no.-3/improving-homeland-security-at-the-state-level.html>

- Steiner, J. E. (2015). *Homeland Security and Intelligence*. Thousand Oaks, CA: Sage Publications.
- Stewart, C. (2016, September 9). Combating terrorism: Five things to know about a fusion center. <http://www.mydaytondailynews.com/news/news/local/five-things-to-know-about-a-fusion-center/nsTpP/>
- Stokes, R. L. (2013). Employing the intelligence cycle process model within the Homeland Security Enterprise. Naval Postgraduate School Thesis. Retrieved from http://calhoun.nps.edu/public/bitstream/handle/10945/39018/13Dec_Stokes_Roger.pdf?sequence=1
- Stone, K. E. (2014). Creating an information-sharing and analysis center: A case study of the North Central Texas Fusion Center. The University of Texas at Dallas PhD Dissertation. UMI Dissertations Publishing. Retrieved from <http://search.proquest.com/docview/1548325736>
- Taylor, R. W., & Russel, A. L. (2012). The Failure of Police 'Fusion' Centers and the Concept of a National Intelligence Sharing Plan. *Police Practice & Research*, 13(2), 184-200. doi: 10.1080/15614263.2011.581448.
- Teutsch, K. (2010, May). Addressing National Security Concerns in an All-Hazards Threat Environment. *Homeland Security Journal*. Retrieved from <http://www.homelandsecurity.org/journal/BrowseArticles.aspx?catid=1>
- Thompson, F. J. (2002). Homeland security: The state and local crucible. *Public Administration Review*, 62, 18-20.

- Treverton, G. F. (2002). *Intelligence, Law Enforcement and Homeland Security*. The Century Foundation. Retrieved from http://tcf.org/publications/2002/8/pb278/get_pdf
- Treverton, G. F. (2008). *Reorganizing Domestic U.S. Intelligence*. RAND Corporation. Retrieved from http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG767.pdf
- Tromblay, D. E. (2016). *The U.S. Domestic Intelligence Enterprise: History, Development, and Operations*. CRC Press: New York.
- United States Army Asymmetric Warfare Group. (2009, December). *Interagency Teaming to Counter Irregular Threats*. Fort Meade, MD Retrieved from <https://info.publicintelligence.net/APL-InteragencyTeaming.pdf>
- U.S. Attorney's Office Southern New York. (2016, November 16). Ahmad Khan Rahimi Indicted In Manhattan Federal Court On Terrorism Charges. Retrieved from <https://www.justice.gov/usao-sdny/pr/ahmad-khan-rahimi-indicted-manhattan-federal-court-terrorism-charges>
- United States Code, Title 28, Section .85 (2009). *Organization of the Department of Justice*. Retrieved from http://edocket.access.gpo.gov/cfr_2009/julqtr/28cfr0.85.htm
- United States Code, (2002). *The Homeland Security Act of 2002*. Public Law 107–296 107th Congress. Retrieved from https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

- United States Congress. (2002). Homeland Security Act. Public Law 107–296. Retrieved from http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf
- United States Congress. (2004, December 17). Intelligence Reform and Terrorism Prevention Act of 2004. PUBLIC LAW 108–458—DEC. 17, 2004. Retrieved from <http://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf>
- United States Congress. (2007). Implementing Recommendations of the 9/11 Commission Act of 2007. Retrieved from <http://intelligence.senate.gov/laws/pl11053.pdf>
- United States Congress (2011). Hearing on The DHS Intelligence Enterprise- Past, Present, and Future. Retrieved from <http://homeland.house.gov/hearing/hearing-dhs-intelligence-enterprise-past-present-and-future>
- United States Congress. (2012). U.S. Code Title 22, Foreign Relations and Intercourse. Retrieved from <http://uscode.house.gov/browse/prelim@title22>
- United States Congress. (2015). H.R.3503 - Department of Homeland Security Support to Fusion Centers Act of 2015; 114th Congress (2015-2016). Retrieved from <https://www.congress.gov/bill/114th-congress/house-bill/3503/text>
- United States Department of Homeland Security. (2008, December). *Department of Homeland Security Concept of Operations for Interaction with State and Local Fusion Centers*. Retrieved from <http://fas.org/irp/agency/dhs/conops.pdf>

- United States Department of Homeland Security. (2010, February 1). *Quadrennial Homeland Security Review Report*. Retrieved from http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf
- United States Department of Homeland Security. (2015a, July). *Office of Intelligence and Analysis Mission*. Retrieved from <http://www.dhs.gov/office-intelligence-and-analysis-mission>
- United States Department of Homeland Security. (2015b, January). *2014 National Network of Fusion Centers Final Report*. Retrieved from http://www.dhs.gov/sites/default/files/publications/2014%20National%20Network%20of%20Fusion%20Centers%20Final%20Report_1.pdf
- United States Department of Homeland Security. (2016, April). *2015 National Network of Fusion Centers Final Report*. Retrieved from <https://www.dhs.gov/sites/default/files/publications/2015%20Final%20Report%20Section%20508%20Compliant.pdf>
- United States Department of Homeland Security / Department of Justice DHS/DOJ. (2010, May). Considerations for Fusion Center and emergency operations center coordination; Comprehensive preparedness guide 502. Retrieved from http://www.fema.gov/pdf/about/divisions/npd/cpg_502_eoc-fusion_final_7_20_2010.pdf
- United States Department of Justice. (1996, September). *Criminal Justice in Indian Country Audit Report*. Office of the Inspector General. Retrieved from <https://oig.justice.gov/reports/plus/a9616/>

United States Department of Justice (2008). Fusion Center Baseline Capabilities.

Retrieved from http://www.it.ojp.gov/documents/d/fusion_center_guidelines.pdf

United States Department of Justice (2004). A Review of the FBI's Handling's of Intelligence Information Related to the September 11 Attacks. Office of the Inspector General. Retrieved from

<http://www.justice.gov/oig/special/0506/final.pdf>

United States Department of Justice (2005a, June). The Department of Justice's Terrorism Task Forces. Office of the Inspector General Report # I-2005-007

Retrieved from <http://www.justice.gov/oig/reports/plus/e0507/final.pdf>

United States Department of Justice. (2005b, July). Fusion center guidelines: Developing and sharing information and intelligence in a new world. Retrieved from

http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

United States Department of Justice. (2006, August). *Fusion Center Guidelines:*

Developing and Sharing Information and Intelligence in a New Era. Bureau of Justice Assistance. Retrieved from http://www.it.ojp.gov/documents/fusion_center_guidelines.pdf

United States Department of Justice (2004, November). A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks. Retrieved from

<http://www.justice.gov/oig/special/0506/final.pdf>

United States Department of Justice. (2009). Navigating Your Agency's Path to Intelligence-Led Policing. Bureau of Justice Assistance, Retrieved from

<http://www.it.ojp.gov/docdownloader.aspx?ddid=1082>

- United States Department of Justice. (2017, March). *Review of Domestic Sharing of Counterterrorism Information*, Office of the Inspector General Audit Division Report 17-21. Retrieved from <https://oig.justice.gov/reports/2017/a1721.pdf>
- United States Senate. (1976). Church Committee Reports. *Book II: Intelligence Activities and the Rights of Americans*, Retrieved from http://www.aarclibrary.org/publib/contents/church/contents_church_reports_book2.htm
- United States Senate Report. (2011, February). *A ticking time bomb: Counterterrorism lessons from the U.S. Government's failure to prevent the Fort Hood Attack*. Committee on Homeland Security and Governmental Affairs. Retrieved from http://hsgac.senate.gov/public/_files/Fort_Hood/FortHoodReport.pdf
- Verton, D. (2011, October 24). Government Data Centers Under Fire. *BreakingGov*. Retrieved from <http://breakinggov.com/2011/10/24/government-data-centers-under-fire/>
- Vicinanzo, A. (2015, March 3). Gaps In Info Sharing Continue To Hinder Counterterrorism Efforts. *Homeland Security Today*. Retrieved from <http://www.hstoday.us/briefings/daily-news-analysis/single-article/gaps-in-info-sharing-continue-to-hinder-counterterrorism-efforts/b365f132d73fa2a44e1966dfbee3340a.html>
- Viser, M. (2013, May 9). Tensions emerge over lack of Tsarnaev information shared between FBI, local authorities. *The Boston Globe*. Retrieved from <http://archive.boston.com/politicalintelligence/2013/05/09/tensions-emerge-over->

lack-tsarnaev-information-shared-between-fbi-local-
authorities/c0JqORZNBkQJomxbODmwVK/story.html

Vizzard, W. J. (2008). The FBI, A hundred-year retrospective. *Public Administration Review*, 68(6), 1079-1086. doi: 10.1111/j.1540-6210.2008.00956

Wagner, C. (2010, March 4). Statement to the U.S. Congress, House Committee on Appropriations, Subcommittee on Homeland Security, DHS Intelligence Programs and the Effectiveness of State and local Fusion Centers. Retrieved from http://democrats.appropriations.house.gov/images/stories/pdf/Caryn_Wagner-3-4-10.pdf

Wagner, C. (2011, June 1). Statement to the U.S. Congress, House Committee on Homeland Security, The DHS Intelligence Enterprise- Past, Present, and Future. Retrieved from <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Wagner.pdf>

Waugh, W. L. Jr, & Streib, G. (2006). Collaboration and leadership for effective emergency management. *Public Administration Review*, 66, 131-139.

Webster, W. (2012, July). *Final Report of the William H. Webster Commission on the FBI, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009*. Retrieved from <https://www.fbi.gov/news/pressrel/press-releases/final-report-of-the-william-h.-webster-commission>

White House, (2011, June). National Strategy for Counterterrorism. Retrieved from http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf

- Wight, L. (2015, December 3). Securing the Homeland: Information-sharing and the Role of Law Enforcement. Presentation to the Potomac Institute for Policy Studies. Retrieved from <http://www.potomacinstitute.org/featured-news/1870-law-enforcement-seminar>
- Wilson, J. Q., & DiIulio, J.J., Jr. (1995). *American Government Institutions and Policies*. Washington, DC: Heath and Company, p. A-49 as quoted in Boyd, E. (1997) *American Federalism, 1776 to 1997: Significant Events*. Retrieved from <http://usa.usembassy.de/etexts/gov/federal.htm#1>
- Wise, C. R., & Nader, R., (2002, September). Organizing the Federal System for Homeland Security: Problems, Issues, and Dilemmas. *Public Administration Review*, 62, 44-58.
- Wise, C. R. (2006). Organizing for homeland security after Katrina: Is adaptive management what's missing? *Public Administration Review*, 66(3), 302-318.
- Wright, D. S. (1990). Federalism, intergovernmental relations, and intergovernmental management: Historical reflections and conceptual comparisons. *Public Administration Review*, 50 (2), 168-178.
- Wyllie, D. (2011, September 11). 10 years after 9/11: Police counterterrorism, then and now. *PoliceOne.com News*. Retrieved from <https://www.policeone.com/terrorism/articles/4348766-10-years-after-9-11-Police-counterterrorism-then-and-now/>
- Yin, R.K. (2002). *Case Study Research: Design and Methods* (3rd ed.). Thousand Oaks, CA: Sage Publications.

- Young, E. A. (2015, March 3). Federalism as a Constitutional Principle. *University of Cincinnati Law Review*, Forthcoming. Retrieved from http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2573338_code86281.pdf?abstractid=2573338&mirid=1&type=2
- Zalkind, S. (2014, April 4). Five myths about the Boston Marathon bombing. The Washington Post. Retrieved from http://www.washingtonpost.com/opinions/five-myths-about-the-boston-marathon-bombing/2014/04/04/0d0c8470-b9b2-11e3-9a05-c739f29ccb08_story.html
- Zamora, M. F. (2014). Intelligence Failures: Matters of Homeland and National Security. *Journal of Homeland and National Security Perspectives*, 1 (1), 49-65.
- Zegart, A. (2005). September 11 and the adaptation failure of U.S. Intelligence agencies. *International Security*, 29(4), 78-111. doi:10.1162/isec.2005.29.4.78
- Zegart, A. (2008, May). CIA Chronicles. *Foreign Affairs*, 87(3). Retrieved from <https://www.foreignaffairs.com/articles/united-states/2008-05-03/cia-chronicles>
- Zegart, A. (2009). *Spying blind: The CIA, the FBI, and the origins of 9/11*. Princeton, NJ: Princeton University Press.
- Zegart, A. (2015). Insider Threats and Organizational Root Causes: The 2009 Fort Hood Terrorist Attack. *Parameters* 45(2), 35-46.
- Zhang, J., Dawes, S. S., & Sarkis, J. (2005). Exploring stakeholders' expectations of the benefits and barriers of e-government knowledge sharing. *Journal of Enterprise Information Management*, 18(5), 548-567.

Appendix A: Background Questions and Interview Questions

Participant Background Questions:

1. What is your profession / career field (Law enforcement, intelligence, etc)?
2. How many years have you worked in this career field?
1-3; 4- 5; 6 – 8; 9 – 12; 13 – 16; 17 – 21; 20+
3. What is your position within the fusion center?
4. How many years have you worked at this particular fusion center?
Less than 1; 1 – 3; 4 – 6; 6 – 11; 12+
5. Are you in a leadership/supervisory position within the fusion center?
(If “Yes”) Upper-Level (Director, Deputy Dir); Middle-Level (Lieutenant, etc);
Lower-Level (Senior Analyst, Detective, etc)
6. What level of government does your agency fall under? (federal, state, local)

Interview Questions

1. The January 2015 National Network of Fusion Centers Final Report found that over 96% of fusion centers have involvement in counterterrorism in their mission focus.
What role does your fusion center play in counterterrorism?
2. How has receiving federal information and intelligence in your fusion center been useful in countering terrorism?
3. What are the opportunities or benefits of federal Counter Terrorism (CT) info/intel sharing with fusion centers?

4. What are the obstacles or barriers of federal CT info/intel sharing with fusion centers?
5. What can or should be done to remove or mitigate these obstacles, barriers, and risks that impede effective sharing of federal terrorism information and intelligence sharing with state and local fusion centers?
6. Which federal intelligence, security, and law enforcement agencies share info and intel on terrorism with your fusion center?
7. How would fusion centers be different if there was no sharing of federal CT info/intel?
8. How would fusion centers be different if they had extensive access and sharing of federal CT info/intel? (examples include access to FBI case files of ongoing terrorism investigations in your area, current intelligence agency threat streams, and warning of suspected terrorism related travel in your area, foreign fighters returning from overseas conflict zones, radicalized citizens)
9. Should federal security agencies share info/intel with fusion centers or should they share with a different organization in your jurisdiction (such as a JTTF)?
10. As called for in the 2012 National Strategy for Information-sharing, are federal agencies “sharing the right information with the right people at the right time” in your view? For example, do you receive information about terrorist threats in general or actionable intelligence on specific individuals or cases?
11. Other than the obstacles and barriers to federal terrorism information already described, are there other risks to this information-sharing?

12. What have been the most useful sharing mechanisms from the federal government for information and intelligence on terrorist threats; those described in the DOJ/DHS baseline capabilities assessment such as Homeland Security Data Network (HSDN), Homeland Security Information Network Intelligence Community of Interest (HSIN-Intel), FBI Law Enforcement Online (LEO)/FBI Net, or other mechanisms to receive terrorism info and intel in your fusion center such as liaison meetings, video-conferences, periodic visits, telephone calls, etc.

Appendix B: Participant Backgrounds By Site and Totals

Site A	Site B	Site C	Site D	Site E	Totals	% of Total	5 per Site; 25 Total Participants
1. Profession / career field							
2	1	3	3	3	12	48%	Law Enforcement
3	4	2	2	2	13	52%	Intelligence
2. Years in career field							
1	1	0	0	1	3	12%	1 to 3 (2)
0	1	0	0	0	1	4%	4 to 5 (4.5)
0	1	1	0	1	3	12%	6 to 8 (7)
0	2	1	1	0	4	16%	9 to 12 (10.5)
0	0	1	3	0	4	16%	13 to 16 (14.5)
1	0	0	0	0	1	4%	17 to 21 (19)
3	0	2	1	3	9	36%	20+ (22)
17.4	9.2	15.2	15.2	15	14.4	Average years in career field	
3. Position within Center							
1	1	1	1	1	5	20%	Director / Deputy Director
0	0	1	1	1	3	12%	Analytical Supervisor
1	1	1	1	1	5	20%	DHS Representative (Intel or Reports Off)
1	0	0	1	0	2	8%	FBI Representative (Special Agent or Intel)
0	0	1	0	0	1	4%	Criminal Analyst
1	3	1	0	1	6	24%	Intelligence Analyst
1	0	0	1	1	3	12%	Law Enforcement Officer / Investigator
4. Years at this fusion center							
0	2	0	0	0	2	8%	Less than one (1)
1	2	2	1	1	7	28%	1-3 (2)
2	1	2	3	2	10	40%	4-6 (5)
2	0	1	1	2	6	24%	6-11 (8.5) [none in 12+]
5.8	2.2	4.5	5.1	5.8	4.68	Average for years at this fusion center	
5. Supervisory position							
1	1	1	1	1	5	13 (52%)	Upper leadership
0	0	1	2	1	4		Mid Level Leadership
2	1	0	0	1	4		Lower level supervisor/Provides Direction
2	3	3	2	2	12	48%	Non-supervisor
6. Level of Govt Agency Falls Under							
2	1	1	2	1	7	28%	Federal
2	0	4	0	4	10	40%	State
1	4	0	3	0	8	32%	Local