2023

Understanding Law Enforcement Counterterrorism Information Sharing in Homegrown Violent Extremism Cases

Danielle Corry
Walden University

Walden University

College of Health Sciences and Public Policy

This is to certify that the doctoral dissertation by

Danielle A. Corry

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. Jeffrey Bumgarner, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Joshua Ozymy, Committee Member,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2023

Abstract

Understanding Law Enforcement Counterterrorism Information Sharing

in Homegrown Violent Extremism Cases

by

Danielle A. Corry

MPA, University of Central Florida, 2005

BA, University of Florida, 2003

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

July 2023

Abstract

Local law enforcement agencies are charged with the responsibility to prevent terrorist events in the United States, including the emerging threat of homegrown violent extremism. Without the use of the terrorism prevention tool of information sharing, with other applicable state and federal law enforcement agencies, there continues to be a breakdown in the ability to prevent terrorist events, especially those associated with homegrown violent extremists, in the United States. This qualitative case study explores the information sharing process in law enforcement agencies by examining the recent Boston Marathon Bombing in Boston, Massachusetts that occurred in 2013. Five themes emerged from the analysis which both validate previous research and suggest that participants trust and rely that counterterrorism and/or homegrown violent extremism information would be shared with them if it were available. The study highlights that gaps remain in information sharing among law enforcement agencies, thus leaving the United States at risk for future terrorist attacks. The suggestions identified by this study, such as community policing and interagency working groups, have the ability to increase law enforcement information sharing for counterterrorism and homegrown violent extremist cases and can effect positive social change.

Understanding Law Enforcement Counterterrorism Information Sharing in Homegrown Violent Extremism Cases

by

Danielle A. Corry

MPA, University of Central Florida, 2005

BA, University of Florida, 2003

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

July 2023

Dedication

The endless hours of devotion of my PhD education and my dissertation would not have been possible without the support of my husband. Without his generous strength, I would not have been able to get through to the end. My lifelong pursuit of education would not have been possible without the powerful source of courage that my mother has always illustrated to me. She has truly showed me that motivation and the following of one's dreams has no bounds of gender, socio-economic status, or background. I dedicate my dissertation to my family. This process could not be possible without the feedback, encouragement, and guidance of my dissertation committee. I am truly thankful for all that I have learned in pursuit of my PhD.

Table of Contents

List of Tables

List of Figure

Chapter 1: Introduction to the Study

Since the terrorist attack that occurred in the United States on September 11, 2001, significant efforts have been devoted to terrorism prevention, including government counterterrorism funding for agencies, programs, equipment, and training for law enforcement at the federal, state and local levels. However, terrorist tactics, techniques, and procedures (TTPs) have adapted, and terrorist events have continued to occur on U.S. soil. Homegrown violent extremists (HVEs) are currently the most severe domestic terrorist threat (Comey, 2014), and in order to reduce their threat, coordination and communication between law enforcement agencies is fundamental. Based on studies of significant terrorist events in the United States since 2005, it has been noted that a primary gap in domestic terrorism prevention continues to be law enforcement information sharing (Department of Homeland Security, 2016; Gunaratna & Haynal, 2013; House of Representatives, 2014; Peled, 2016; Senate Committee on Homeland Security and Governmental Affairs, 2013). Without suitable counterterrorism information sharing, especially as it relates to HVEs, suspicious activities may not be disseminated in a timely manner, emerging threat information may not be compiled, active case information may not be represented properly, and terrorism likely will not be prevented (DHS, 2015a, 2016; Gunaratna & Haynal, 2013).

A lack of focus on the organizational boundaries of law enforcement agencies, as it applies to terrorism prevention information sharing with a focus on HVEs, is a key gap in academic literature. In this study, I used a recent terrorist event that occurred within the United States as a case study, the attack at the at the Boston Marathon in Boston,

Massachusetts on April 15, 2013, to explore the procedures of counterterrorism information sharing for local law enforcement agencies. In this research, I highlight how contingency theory can explain the organizational boundaries that may lead to a gap in information sharing between law enforcement agencies as it relates to counterterrorism information sharing with a HVE focus. The application of the results of this study can be implemented to terrorism prevention policy and planning procedures. The results can be used as a tool for decision makers to create actionable protocols for information sharing and allocate resources to information sharing technology for local law enforcement agencies, especially related to HVEs, as identified by the results.

Within this chapter, an overview of the background of the study will be provided that will explain the evolution of HVEs and the importance of local law enforcement agencies' ability to identify them and prevent their attacks. The conceptual framework, including research questions, scope, and methodology used to frame this study, is also explained within this chapter. Additionally, a list of key definitions and assumptions is provided.

Background of the Study

After 09/11 occurred, counterterrorism resources were devoted to government agencies to detect, deter and respond to terrorists at a tremendous rate and new missions and organizations were created (Department of Homeland Security, 2016; Senate Committee on Homeland Security and Government Affairs, 2016). Local law enforcement agencies' counterterrorism roles were recognized as extremely important to the greater homeland security mission, and they were identified as the first line of defense

for terrorism prevention (Burruss, 2012; Haynes & Giblin, 2014; Peled; 2016). When the Department of Homeland Security (DHS) was created in 2003 (Homeland Security Act, 2002) and the National Counterterrorism Center (NCTC) was created in 2004 (Intelligence Reform and Terrorism Prevention Act, 2004), both in response to 09/11, one of their primary roles was assisting the facilitation of information and relationships for law enforcement agencies at the federal, state, and local levels so that they may work together to prevent terrorism (Homeland Security Act, 2002; Intelligence Reform and Terrorism Prevention Act, 2004). As information sharing still remained a primary national security gap in 2011, the *National Strategy for Counterterrorism* (2015) outlined the requirement for law enforcement agencies at all levels to increase their terrorism prevention capabilities. The *Strategy* broke down five mission areas vital for national counterterrorism preparedness, of which one was prevention (*National Strategy for Counterterrorism, 2015*).

As terrorist TTPs continue to evolve overseas, U.S. foreign and immigration policy shifted and has allowed for the capture and conviction of foreign-born individuals on the Federal Bureau of Investigation's (FBIs) terrorism watch list (Executive Order 13780, 2018). However, domestically, terrorist event TTPs have evolved to include U.S. citizens who learn about and are inspired by international terrorist group ideologies and are considered HVEs (Senate Committee on Homeland Security and Governmental Affairs, 2016). These types of terrorist events are extremely difficult for local law enforcement agencies to prevent due to the nature of the HVE not being affiliated with a

terrorist group or cell (FBI, 2013) and their use of technologies like social media and text messaging (Senate Committee on Homeland Security and Governmental Affairs, 2016).

Suspicious activity reporting (SAR) through government information systems is the manner in which federal, state, and local law enforcement agencies are required to report certain potential indicators of behavior that are criminal in nature, and may indicate something that leads to terrorism related activity (ISE-FS-200, v 1.5.5). Once an individual has more than one instance of being reported in the SAR database, a pattern may be detected and a law enforcement or intelligence agency will be able to use the information in an active investigation (Bjelopera, 2014; DHS, 2015; FBI, 2013). This type of information sharing is the most basic, but often the most vital and was noted as a gap in the Boston Marathon Bombing attack that occurred in April 2013 (Peled, 2016). An additional noteworthy information sharing gap identified in an Inspector General (2017) report was that state and local law enforcement agencies might not have the security clearances that they require to access the information systems to obtain certain information.

As HVEs continue to be a threat and TTPs continue to evolve, one recommendation for information sharing that is prevalent among academic literature and government agencies is community policing (Mondal & Hurwitz, 2012; Randol, 2012; Senate Committee on Homeland Security and Governmental Affairs, 2016). Community policing is the process where local law enforcement agencies educate local communities about TTPs and ask to be informed about suspicious behavior of individuals (Mondak & Hurwitz, 2012). An example of this is the DHS's "If you See Something, Say

Something" campaign, whereby this statement was made to the public to report suspicious terrorist related activities, persons or packages to their local law enforcement agency (DHS, n.d.). This type of information sharing can produce real-time threat information for law enforcement agencies (Bjelopera, 2014), but also can create the need for additional personnel with an intelligence analysis skill set and funding that some agencies do not have (RAND, 2016).

As domestic terrorist TTPs continue to evolve, it is vital that law enforcement agencies develop or maintain the terrorism prevention capability of information sharing (Ackerman, 2016; DHS, 2015; *National Strategy for Counterrorism*, 2011). This study provides a better understanding of why law enforcement agencies continue to have gaps in information sharing with domestic terrorism events (Ackerman, 2016; Bjelopera, 2014; House Homeland Security Committee, 2014;), specifically HVE events as illustrated with the Boston Marathon Bombing.

Even though it has been noted that there is a gap in information sharing, there remains to be a lack of academic literature surrounding the information sharing process and what information should be shared that would be deemed actionable to law enforcement agencies or counterterrorism HVE cases. This study expands upon those gaps in literature and explains the barriers to law enforcement HVE information sharing, exemplified by local law enforcement agencies leading up to and during the terrorist attack that occurred at the Boston Marathon in Boston, Massachusetts in April 2013.

Problem Statement

Information sharing remains a gap in the local law enforcement agency's ability to prevent HVE terrorism. Counterterrorism prevention measures begin at the local law enforcement level and the capability to deter an attack is a collaborative effort among all law enforcement agencies (DHS, 2015; *National Strategy for Counterterrorism, 2011;* Randol, 2013; Zuckerman et al., 2013). Even after 09/11, a gap of terrorism related information sharing has been highlighted across the nation, leaving the United States vulnerable to further attacks (Flinn, 2016; House of Representatives, 2014; DHS, 2016).

Recent terrorist attacks in the United States, including the 2013 Boston Marathon bombing, were studied to determine what law enforcement and counterterrorism shortfalls occurred leading up the event. The House Homeland Security Committee (2014) found that the FBI and the local law enforcement agency in Boston, Massachusetts did not share vital information prior to the attack, including tips that may have helped to thwart the attack and there was a lack of ability of local police departments to gain access to certain databases to retrieve case specific information. Multiple studies have found an overlapping federal counterterrorism mission set (Foley, 2016; Inspector General, 2017; Peled, 2016) and a communication and political barrier to interagency communications (Foley, 2016; Peled, 2016; Pelfrey, 2014).

As terrorist TTPs continue to change, to include the rising trend of HVEs (Ackerman, 2016; DHS, 2015), it is increasingly important for law enforcement agencies to share case related information and suspicious activities in order to execute the terrorism prevention mission (Gunaratna & Haynal, 2013). Previous research continues to

highlight gaps in law enforcement information sharing at an interfederalist level; however, they do not identify what organizational shortfalls may lead to this barrier or how local enforcement agencies obtain HVE threat information from federal and state agencies. In this study, I explored how HVE information is obtained and shared in an interfederalist law enforcement setting, especially with regard to a local jurisdiction that experienced a terrorist attack in 2013.

Purpose of the Study

The purpose of this qualitative study is to understand how HVE terrorism prevention information is shared among law enforcement agencies. This study helps fill a gap in the body of research in the law enforcement HVE terrorism prevention information sharing environment. This case study explored the procedures agencies take with HVE terrorism information sharing and aimed to understand why local law enforcement agencies are not able to obtain HVE case information in a timely manner (Ackerman, 2016; Bjelopera, 2014; Gunaratna & Haynal, 2013; House Homeland Security Committee, 2014).

Research Questions

The research questions that are addressed in this study include the following:

RQ1: What level of HVE information is shared by federal agencies to local law enforcement agencies?

RQ2: What level of HVE information is shared by state agencies to local law enforcement agencies?

RQ3: What level of HVE information is shared with other local law enforcement agencies and law enforcement agencies?

Conceptual Framework

Contingency theory is the conceptual framework used for this study, as it seeks to explain how an agency adapts to changing environmental factors (Donaldson, 2001; Haynes & Giblin, 2014; Roberts et al., 2012). Donaldson (2001) indicated that organizations adapt to agency change over time to deal with contingencies in order to be effective. Effectiveness is a measure of performance or organizational success (Donaldson, 2001), and is applicable to law enforcement agencies in a multitude of ways. Roberts et al. (2012) explained that contingency theory can be applied to law enforcement agencies as they implement organizational changes and environmental factors to prepare for terrorism incidents, whereby terrorism prevention (in this context) is understood as a measure of how law enforcement agencies implement policies (p. 722).

The use of contingency theory in this study forms the basis for explaining the relationship between the terrorism prevention policy of information sharing within the jurisdiction of the local law enforcement agency that responded to the Boston Marathon Bombing and HVE terrorism prevention. Terrorism prevention in an interfederalist law enforcement context is applied to contingency theory by illustrating a measure of performance. This is further evident by answering the three research questions in this study, which were designed to answer how HVE terrorism prevention information is shared at the level of law enforcement between federal, state and local agencies.

Contingency theory and its components of organizational change and the environmental factors are explained further in Chapter 2.

Nature of the Study

This qualitative study uses a case study design. The focus of this approach was gaining in-depth knowledge of data in a natural setting (Hancock & Algozinne, 2015). A case study analysis was conducted using a local law enforcement agency, which was involved in responding to the HVE terrorism event at the Boston Marathon in 2013. Yin (2012) indicated that a case study design is helpful in applying the elements of a theory to a specific case. Additionally, case studies apply the analysis of a problem statement (Hancock & Algozzine, 2015) and the theoretical framework (Yin, 2012). This study pursues the understanding of HVE terrorism prevention information sharing at the local law enforcement level through the lens of contingency theory. The concepts within contingency theory, organization, and environment (Donaldson, 2001) are specifically applicable to this case study. This study explores how a local law enforcement agency applied the HVE terrorism prevention policy of information sharing to the specific case of the HVE terrorism event that took place at the Boston Marathon (Haynes & Giblin, 2014; Roberts et al., 2012; Yin, 2012).

I collected the data by conducting open-ended interviews with law enforcement personnel at a local law enforcement agency, conducted a simplified content analysis of documents within that agency, and also obtained finished reports from Congress related to the terrorist event in Boston, Massachusetts (Yin, 2012). Analysis and coding of the data followed with the development of themes and patterns (Yin, 2012). Finally, themes

that emerged from the sources of the data (interviews, documents, and reports) were analyzed and merged in order to write cohesive descriptions in the final report.

Definitions

Counterterrorism: For purposes of this study, counterterrorism is the collective goal of stopping an act of terrorism (DHS, 2015a).

Homegrown violent extremist (HVE): A HVE is a person living in the United States who is inspired by and acting upon the ideology of a terrorist group outside of the United States and is likely self-radicalized (FBI, 2013; Senate Committee on Homeland Security and Governmental Affairs, 2013).

Information sharing: Information sharing is the exchange of data or intelligence in an actionable timeframe with mission partners (DHS, 2015a; RAND, 2016).

Local law enforcement: A local law enforcement agency is a police department, sheriff's office, or other municipality police agency that is charged with the prevention of crime.

Tactics, techniques, and procedures (TTP): TTPs in terrorism research and analysis is the approach to understanding the evolution to how a specific terrorist group or threat actor behave, what they target(s), the resources they have to attack with, weapons they have acquired or wish to acquire, and an approximate approach of attack (Sullivan & Bauer, 2008).

Terrorism prevention: Terrorism prevention refers to the measures taken to stop terrorism and terrorist attacks from occurring, including threat detection, information sharing, and other prevention techniques mentioned within this study (DHS, 2015a).

Assumptions

Inherent in this qualitative approach are assumptions regarding the nature of reality and how it is known. This study is an examination of the lack of an early warning or communication system which provides the ability to inform law enforcement about the Boston Marathon Bombing before it happened. Federal, state, and local law agencies were operating in the area, and ideally, they should have synchronized operations and provided preventative alerts to avert the HVE event that took place at the Boston Marathon. However, it is assumed that the individuals involved in the information sharing activities (through use of various communication systems explored in Chapter 2) will give a strong indication as to why the failures occurred.

The reality, or the ontological assumption, is that the lack of information sharing prior to the attack increased the vulnerability to a terrorist attack. The description of the pattern of behavior relies on both the ontological reality and the epistemological one. Equally important is how these patterns continue to prevail. If the information sharing processes applicable to HVE notifications are going to be successful in field operations, we must identify these patterns that are based on how reality is perceived and how knowledge about them takes place.

These assumptions are embedded in an interpretive framework. The framework used in this study is a social constructivist one (Creswell, 2012). This framework allows

the researcher to explore what the participants have idealized about the nature, forms and expressions of HVE. Contingency theory is the theoretical framework used for this study, as it is the best-suited approach to examine the outside influences on law enforcement agencies, with various levels of political and other cogs, and how these impact the performance of the organization (Donaldson, 2001; Haynes & Giblin, 2014).

Scope and Delimitations

This study focused on terrorism prevention and not terrorism preparedness. Preparedness literature, in the scope of homeland security, typically adds two additional steps to terrorism prevention, including responding to and recovery from a terrorism event. Additionally, when law enforcement is mentioned within this study, the scope is focused on a counterterrorism or terrorism prevention role within those agencies.

Study Limitations

One limitation of this study is that the data were collected in one jurisdiction in a high profile HVE case. The police department jurisdiction in Boston, Massachusetts is a large sized municipality, and the results can be learned from and applied to (Yin, 2012) other jurisdictions. Data derived from a single case can be seen by some as a limitation (Creswell, 2009).

Significance of the Study

Information sharing is continually highlighted as a major shortfall by policymakers and researchers in law enforcement counterterrorism prevention capabilities (Gunaratna & Haynal, 2013; House of Representatives, 2014; Inserra, 2015;), but the additional step of providing recommendations on how to rectify the problem are

not made, especially as it relates to HVE events. This study is well-timed and can be applied to the understanding of the HVE terrorism information sharing process, the potential information sharing shortfalls and providing policy recommendations by closely examining a case of a local law enforcement agency that recently responded to an HVE event.

This study bridges the gap between identifying the need to improve information sharing and determining the means to share the counterterrorism information through the results of the qualitative data derived from case study. The implications for positive social change to which this study can contribute include applying the results in an actionable manner with law enforcement agencies so that they may see how to better exchange HVE information with each other. Additionally, the results from this study can be used by policymakers to fill gaps in national security by taking the next step in implementing tools to better assist law enforcement agencies to share HVE information in order to prevent terrorism.

Summary and Transition

This study highlights the prevalence of HVE terrorism information sharing gaps among law enforcement agencies and the continued role it has on the United States' national security. Since 09/11, even though it has continually been identified as a gap, information sharing between law enforcement agencies at the federal, state, and local levels has continued to be a primary concern among Congressional committees and academic researchers (Foley, 2016; Haynes and Giblin, 2014; House of Representatives, 2014; Randol, 2013). As identified by the FBI (2014), HVEs are the current greatest

threat to the homeland and are the hardest to track for law enforcement agencies at every level, which makes information sharing even more vital (Ackerman, 2016; Bjelopera, 2014; Comey, 2014; Gunaratna & Haynal, 2013).

This chapter provides an overview of this qualitative case study of the Boston Marathon Bombing HVE attack in Boston, Massachusetts in 2013. The use of contingency theory is used to answer the research questions about inter-federalist law enforcement HVE terrorist information sharing. This study can assist policy makers by providing policy recommendations and fill gaps in the HVE terrorism information sharing academic literature.

Chapter 2: Literature Review

Introduction

Local law enforcement agencies are charged with responding to domestic terrorist attacks and assisting state and federal agencies in preventing them through the process of information sharing. Federal, state, and local law enforcement agencies are guided through counterterrorism policies that require them to share information for terrorism prevention purposes (Davis, 2016). However, as identified by multiple noteworthy domestic terrorism incidents that have occurred in the United States since September 11, 2001, information sharing continues to be a key gap in local law enforcement terrorism prevention capabilities, especially as it relates to HVEs, (Randol, 2013; Roberts et al., 2012; Senate Committee on Homeland Security and Governmental Affairs, 2013; Steinbach, 2016; Wormeli, 2014) and is explored in depth within this study. As indicated within the following literature review, there is a gap in the scholarly literature regarding law enforcement information sharing as it relates to homegrown violent extremism.

This chapter begins by providing a detailed account of the literature search strategy utilized, followed by a synthesis of the academic literature and federal government publications on the most recent domestic terrorist attacks. The literature review is organized into sections that include an in-depth look at federal counterterrorism policy since 09/11 and the language it instills on local law enforcement agencies. The timeline of policy iterations and how they progress to include mention of HVEs is provided within this section. Next, a synthesis of both academic and policy literature on information sharing is detailed in this chapter. Even though information sharing is

prescribed as a counterterrorism prevention method within national policy documents, it also deems its own section due the importance of the noted continued gap in law enforcement action. A section on terrorism prevention is also detailed in this chapter, a synthesis of academic literature as it relates to these topics is provided, and the theoretical foundation that this study is based upon is included.

Literature Search Strategy

Many of the resources used in the literature review were derived through an organizational approach that included partitioning subtopics. The process began by searching the keywords law enforcement and terrorism prevention in the ABI/INFORM database in order to gain a cursory understanding of the literature in the field. After obtaining the peer-reviewed articles that were applicable to this study, I created a Google Scholar search parameter that alerted me of any new scholarly publications with the same keywords. Because the scholarly research that focused on local law enforcement and terrorism prevention was mostly related to countries outside of the United States or were more than 10 years old, additional keyword search terms were added. As I continued through the literature review, I was able to narrow down the parameters of the importance of law enforcement information sharing and HVEs in the current counterterrorism climate. Therefore, I narrowed the literature review keyword combination search parameters to law enforcement and HVEs and law enforcement and information sharing while searching in the SAGE Journals and Criminal Justice databases.

The next step taken in the literature search strategy was obtaining all applicable federal counterterrorism, terrorism prevention, and law enforcement information sharing

policies at the federal and interagency levels. This process was taken using the FindLaw, Federal Register, and FDSys databases. Federal agency websites were also searched. I also reviewed dissertations using ProQuest in order to ensure no other dissertations were published on the same topic area. The databases were checked frequently to determine if new material using this study's keywords were published or updated policies were released. This chapter includes the literature identified within this review. The keywords used included *terrorism, law enforcement, terrorism prevention, contingency theory, homegrown violent extremism,* and *information sharing.*

Disclosure of Researcher Bias

In order to adequately illustrate objectivity, a discussion about my professional background as it relates to this research is important. I have worked for the U.S. federal government in several capacities including writing intelligence policy, as an intelligence analyst, assisting state and local agencies with complying with federal mandates, and as a counterintelligence special agent, where I worked with federal, state, and local agencies. Therefore, my professional experience with and passion for the topic matter of this study has the ability to bias the way that I framed questions that I asked during the data collection of the case study. However, I took specific note of this and was careful not to allow my background to influence this study. Additionally, my professional background could also frame my writing style and the way that I make assumptions about the topics of interagency communication and information sharing. I have paid particular attention to this potential bias and have made note to reflect only the words used by the participants

in this study and to keep an open mind when conducting the literature review and analysis.

Counterterrorism Policy

In order to have a clear representation of the nuances in law enforcement counterterrorism policy, the policy evolution since 09/11 is important to highlight. In 2002, the *Homeland Security Act of 2002* established the creation of the DHS, which streamlined several services and agencies and responded to a new level of threat as a result of 09/11 (Homeland Security Act, 2002). The *Intelligence Reform and Terrorism Prevention Act of 2004* established the Office of the Director of National Intelligence to oversee the intelligence community and the sharing of terrorism related intelligence (Intelligence Reform and Terrorism Prevention Act, 2004). Among other requirements in the Act, it outlined the need to share terrorism information with all levels of government electronically, specifically in a way that can assist with investigations and analysis, and in a manner that all levels of personnel can access no matter what security clearance they maintain (Intelligence Reform and Terrorism Prevention Act, 2004). This policy was published only 3 years after 09/11, but it clearly delineated requirements for information sharing for law enforcement and intelligence agencies in a straightforward manner.

The Presidential Policy Directive – 8 (PPD-8) was created under the Obama administration to provide policy guidance for the whole of government and private citizens on how to respond to and recover from threats to the nation's security, including terrorism and natural disasters. DHS built upon PPD-8 and created the *National Preparedness Goal* in 2011 and then the second edition in 2015, which superseded that

policy. The *National Preparedness Goal* (2015) is an implementation plan that provides an overview of how the federal, state and local government and communities should coordinate their efforts to achieve five core capabilities. One of the five core capabilities highlighted within the *National Preparedness Goal* (2015) is terrorism prevention, where collaboration and information sharing is stated as necessary to achieving the goal.

Executive Order 13780 (2018) is the subsequent administration's legislation aimed at countering foreign terrorists and focuses primarily on DHS and the Department of Justice's (DOJ's) coordination and response to foreign terrorist entry to the United States. This counterterrorism policy focuses primarily on keeping foreign nationals from certain high-risk countries out of the United States and concludes with the request for information sharing from states to DHS and DOJ (Executive Order No. 13780, 2018). Unlike several other preceding policies, this one specifically provides a bottom-up approach to counterterrorism information sharing, where federal agencies are designated with the responsibility to lead terrorism investigations and response (Executive Order No. 13780, 2018).

Kassop (2013) argued that counterterrorism policies, at the national level, are created based on political influences and executive branch appointees are an extension of that political influence. Waxman (2012) noted that while federalism is attempted with these counterterrorism policies, the implementation is mostly uneven across jurisdictions due to various state and local laws that apply to law enforcement counterterrorism (i.e., surveillance, intelligence collection, etc.). The next iteration of counterterrorism policies

became focused more on countering violent extremism and less on counterterrorism, due to political complexities and the evolution of the policy process (Heydemann, 2014).

Countering Violent Extremism

Empowering Local Partners to Prevent Violent Extremism in the United States (2011 and updated 2016) was created to provide a guideline for communities, local law enforcement, and federal agencies to approach the goal of preventing violent extremism in the United States. In his 2014 Congressional Research Report, Bjelopera explained that the government's CVE effort was essentially following a domestic terrorist counter-radicalization model, whereby a path from risky behavior or interactions, then radicalization to terrorism is ultimately where it leads. The CVE policy includes incorporating communities at-risk of being targeted by radical groups, training law enforcement agencies to prevent violent extremism, and stopping radical propaganda (*Empowering Local Partners to Prevent Violent Extremism in the United States*, 2016). Bjelopera (2014) noted that the New York Police Department and the FBI both maintained their own versions of a domestic CVE model, where they incorporate community programs and specifically maintain engagement efforts in Muslim communities, anticipating to be notified of any suspicious activities. The prevention of HVEs is overseen by the Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States 2016 (SIP).

In 2015, there was a significant increase in domestic terrorism events and plots that were either carried out by or inspired by radical extremist groups, thereby beginning the conversation for counterterrorism policy reform and a more streamlined approach to

countering extremism (Inserra, 2015). The Heritage Group made several policy recommendations to Congress including that a static office within DHS be created to lead an interagency effort to coordinate the response to counter violent extremism (Heritage Group, 2015). *Empowering Local Partners to Prevent Violent Extremism in the United States* (2015) is focused on local agencies and community groups, indicating their importance in information sharing and preventing violent extremism (*Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*, 2016). DHS, in turn, took action and created an agency-wide *Department of Homeland Security Strategy for Countering Violent Extremism* (2016), in coordination with the DOJ, to reach out to other federal agencies, communities, academia, and local jurisdictions to counter violent extremism.

Information Sharing

Information sharing is pivotal to the process of terrorism prevention, and the continued lack of actionable information sharing among law enforcement agencies related to counterterrorism continues to be a national security risk (Carney, 2015; Foley, 2016; Peled, 2016). Since 09/11, lawmakers have made information sharing a legislative priority, leaving project managers to create several national-level programmatic, network, or policy tools including: the Homeland Security Information Sharing Network, Fusion Centers, and the Information Sharing Environment (Peled, 2016). The following federal agencies have a domestic counterterrorism, CVE mission: the DOJ, the FBI, DHS, and the Department of Defense. However, there is no lead agency responsible from an operational perspective, which can add to the information sharing confusion (CRS, 2014;

Heritage Group, 2015). After a review of counterterrorism information sharing breakdowns, the FBI and DHS reported that they have overlaps in their missions and both feel that coordination and information sharing is conducted based on relationships (Inspectors General, 2017).

A theoretical model was proposed in Dawes's (1996) seminal empirical study on how state program managers share information among agencies and the nuances involved in such endeavors. Within this model, benefits and barriers to sharing information were explored in three categories of information: technical, organizational, and political (Dawes, 1996). Several policy focused recommendations from this study include the following: a formal legal structure is needed for information sharing to be implemented properly, information technology needs to be in place, and administrative protocols are required for proper information sharing (Dawes, 1996, p. 392). In their summative paper, which provides an overview of scholarly literature on information sharing in the public sector, Yang and Maxwell (2011) identified three main types of information sharing: 1) interpersonal, 2) intra-organizational, and 3) inter-organizational. Yang and Maxwell noted that barriers to information sharing within and between agencies can be removed by promoting an organizational culture that rewards information sharing and promotes leadership that does the same. This article provides an excellent synopsis of recommendations from timely studies related to information sharing. Yang and Maxwell also posited a complex model that incorporates Dawes's three categories of information and the three types of information sharing they identified in their article.

Jackson et al. (2017) conducted a study aimed at creating a tool to measure the effectiveness of interagency information sharing on criminal justice outcomes, where the study notes the potential application to counterterrorism information sharing. This study focused primarily on information sharing systems across jurisdictions and how they impact specific cases and investigations but noted the complexity with measuring the effectiveness of information sharing (Jackson et al., 2017). In their study, Roberts et al. (2012) indicated that while sharing information between law enforcement agencies at the federal, state, and local level is important to preventing terrorism, so is the proper implementation of technology platforms and the interoperability among agencies (Roberts et al., 2012, p. 739). Drake et al. (2004) expanded on Dawes's (1996) study to seek to understand the role of subcultures in federal agencies with regard to information sharing. This study examined three federal agencies, exploring their use of various sources of data, the interoperability of information systems, and different type of data that subcultures develop within each agency (Drake et al., 2004). The subcultures identified within Drake et al.'s study include: bureaucratic, political, and scientific, where they note that sharing information between these subcultures can even be difficult in the same government agency because of educational, cultural, or trust backgrounds.

The 2013 Boston Marathon bombing highlights continued information sharing gaps between the FBI and local law enforcement, as noted in *The Road to Boston: Counterterrorism Challenges and Lessons from the Marathon Bombings* ,which indicates that the FBI did not share relevant case related information with the local police

department (House of Representatives, 2014). The following is a list of information sharing mechanisms that federal counterterrorism/CVE established:

Fusion Centers

In an effort to co-locate federal, state and local law enforcement agencies after 09/11 so that they could share information in one space and build upon each other's intelligence, fusion centers were created in several cities around the country (Chermak, et al., 2013). Fusion Centers are sometimes physically located at a federal agency in an effort to save operational budgets, and are staffed by several different federal, state and local agencies on an ad-hoc basis (Inspectors General, 2017). Most personnel are required to have a security clearance and training to obtain and synthesize information processed through a fusion center (Bjelopera, 2014; Inspectors General, 2017). Among other tasks, fusion center personnel are responsible for disseminating finished reports to relevant state and local agencies. However, if there is a lack of knowledge regarding the correct person who needs the relevant information or if there is no proper security clearance and/or information technology infrastructure between the two agencies than an information sharing gap exists (Bjelopera, 2014; Inspectors General, 2017).

Homeland Security Information Network (HSIN)

HSIN is an information system network that DHS created to provide sensitive, but unclassified information for homeland security or counterterrorism related topics (Peled, 2016). DHS currently operates HSIN at fusion centers, law enforcement agencies, and DHS locations to provide cross-jurisdictional finished reports (DHS, n.d.).

Information Sharing Environment (ISE)

The ISE is both a policy and a program created as a result of the George W. Bush administration's mandate from the *Intelligence Reform and Terrorism Prevention Act of 2004*. The purpose of the ISE was to create an actionable capability plan to organize all jurisdictional elements across the country with a counterterrorism mission (Intelligence Reform and Terrorism Prevention Act, 2004). It included the creation of a working group, which acts as a strategic think-tank and oversight element for information sharing (ISE-FS-200).

Resistance to Sharing Information

Federalism has aided in the creation of multiple agencies at every level of government with terrorism prevention responsibilities (Foley, 2016). The law enforcement agencies in the United States were created purposely in a decentralized structure so that there would not be large police organizations with jurisdiction over small towns (Berkley, 1970). Additionally, a decentralized law enforcement structure ensures that there is no single agency responsible for failure of a single law enforcement issue (Berkley, 1970). However, today, law enforcement agencies at the federal, state, and local levels all maintain a counterterrorism and HVE prevention role which require the need to share information (CRS, 2014; DHS, 2015b; SIP;).

It has been suggested that the gap in information sharing between law enforcement agencies at each level continues due to mistrust, but it is necessary to continue to strengthen the mechanisms of trust in order to develop a strategy to exchange structured information (Carney, 2015). Dawes (1996) notes that a network of formal and

informal networks existing within agencies themselves can sometimes make them resist sharing information in order to hold onto their power (p. 381). Bureaucracy within agencies and a resistance to change procedures are two other notions that are put forth as continued counterterrorism information sharing gaps after 09/11 (Foley, 2016; Inspector's General, 2017;). Peled (2016) adds that agencies sometimes resist sharing counterterrorism information with each other because it can show that they have overlapping missions and they may lose control of future distribution of their data and access to budgets.

Suspicious Activity Reporting (SAR)

Information Sharing Environment – Function Standard – Suspicious Activity Reporting Version 1.5.5 (ISE-FS-200) is a policy document that provides guidelines for the processes and procedures for agencies, with a counterterrorism mission, to report suspicious behavior or warning information. There is a national SAR Data Repository (SDR) where personnel submit their SAR reports and the information is only shared with appropriate agencies (ISE-FS-200). A SAR is a standard report where law enforcement agencies are required to submit terrorism-related suspicious activity, tip or warning information. This suspicious information can include individuals taking photographs of sensitive infrastructure, the purchase of certain chemicals or precursors to bombs, receiving tips from communities about suspicious persons, etc. (Hewitt, 2014). The SDR maintains the SAR in one central area in an effort to reduce privacy law and First Amendment violation concerns (ISE-FS-200). SAR submissions increased by 96% between fiscal year 2012 and fiscal year 2015 (Inspector Generals, 2017).

In Foley's (2016) study, he suggests that the overlap in counterterrorism responsibilities in federal, state, and local law enforcement agencies in the U.S. has caused "informal routines" (p. 159), where the work among agencies is conducted through interpersonal relationships that are personality driven. In his research, Foley (2016) conversely presents that the law enforcement counterterrorism information sharing roles in the United Kingdom are more formal and structured, due to a more centralized government structure. It is noted that the nature of the American government system, at each level, is compartmentalized due to the built in checks and balances, making it inherently unnatural to share information outside of an agency (Peled, 2016). Foley (2016, p. 155) discusses agencies difficulty to adapt to a new organizational culture of information sharing and equally difficult may be related to their responding to terrorism related information sharing. In Peled's (2016) research, he notes, "counterterrorism agencies are designed to be reliable, consistent, and predictable rather than change with the times" (p. 676).

Terrorism Prevention and HVEs

The terrorism literature has, in large part, discussed terrorism as one cumulative kind of behavior. Terrorism is a tactic that comes in different forms, and it is both theoretically and practically restrictive to treat all forms of terrorism as though they were the same (Combs, 2017). Scholars have noted the benefits of examining specific targets and tactics separately. Additionally, scholars have indicated that behaviors are not equal in all circumstances, as some have created typologies within terrorist tactics (Perliger, et al., 2016). It is important to disaggregate terrorism into specific behaviors yet target and

tactic selections are not made entirely independently of one another (Perliger at al., 2016).

Counterterrorism measures that protect particular targets or prevent specific tactics present obstacles to terrorist groups (FBI, 2013). Some targets have been hardened or protected in such a way that specific tactics have been largely stopped, such as installing metal detectors at airports and increased security at special events (Hewitt, 2014). In response to information about security measures, a terrorist group may revise its targets or learn a new way of attacking the same target (Miller, 2013).

Beyond protecting targets and preventing tactics, both scholars and policymakers have directed their focus in determining how to counter radicalization before a terrorist act has occurred. Davies (2016) argues that violent extremist behavior can be addressed prior to inception through education in a community. An emerging field in international academia called Preventing Violent Extremism – Education (PVE-E) is taught in universities as a program (Davies, 2016) aimed at discovery for the cause and removal of violent ideologies in neighborhoods (Davies, 2016; Heydemann, 2014). Fink (2014) notes that the CVE field is rooted in both the counter radicalization and conflict resolution fields, and also posits that it is the evolution of traditional counterterrorism.

As identified in the previous policy section, a White House level strategy was developed to address a standardized approach for preventing violent extremism at the local level in the U.S. (*Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*, 2016). A federal level CVE Task Force was created to execute this plan and was instructed to do the following:

> Community collaboration with state and local law enforcement can address gang violence, hate crimes, and other public safety issues, including violent extremism. Federal departments and agencies, in partnership with state and local law enforcement, will encourage and expand successful community policing models and increase their scope to also address recruitment and radicalization to violent extremism (*Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*, 2016, pg. 9).

Horgan (2014) argues that CVE efforts should never be seen as a "top-down" (p. 3) issue, but a community driven matter to be addressed if one is to think they can actually approach countering extremist behavior. Parker (2014) presents that the current research in CVE is helpful in garnering "insights" (p. 3), but it should not be seen as applicable in peacekeeping approaches or answers to the actual problems at hand. Academics seem to agree that the field of CVE has much to explore before the application of research principles should be implemented in the field (Davies, 2016; Horgan, 2014; Parker; 2014).

In 2015 alone, 57 HVE events or plots occurred in the U.S. (The Heritage Foundation). HVEs are the current greatest threat to the homeland and one of the most difficult to detect (Comey, 2014). Because HVEs are inspired by ideologies of terrorist groups outside of the United States, the radicalization process is different than typical terrorists; HVEs can be self-radicalized using the Internet (Cohen, 2016). The use of social media is used as a recruitment tool to inspire HVEs, and as TTPs continue to change, it is increasingly more difficult for law enforcement to detect and prevent attacks

(*ISIL Online*, 2016). HVEs can become radicalized in a short amount of time, and, in most cases, are self-trained (Cohen, 2016). Much like intelligence agents target and recruit spies, international terrorist groups are using social media tools to identify specific people and recruit them to carry out attacks in the name of a terrorist ideology (Cohen, 2016; *ISIL Online*, 2016).

In an effort to determine if terrorism events can be predicted and prevented, LaFree & Bersani (2014) studied domestic terrorist attacks from 1990 to 2011 using the Global Terrorism Database data set. Their study found that these terrorist events were planned primarily in non-urban locations and carried out in counties across the United States with a high level of urbanization and foreign-born inhabitants with instability and a high degree of language disparity (LaFree & Bersani, 2014). Pelfrey (2014) notes that as HVEs have become an increasing threat, he builds on Lafree & Bersani's (2014) work and suggests that local law enforcement can work in their communities at events that represent diversity in an effort to recognize and stop the radicalization process. LaFree & Bersani's (2014) work made note of the importance of local law enforcement's ability to impact the prevention of the radicalization process through community engagement and information sharing. Wormeli (2014) suggests that the policy-level implications of LaFree & Bersani's (2014) work should take careful consideration to not apply government resources to highly urbanized cities with a densely populated foreign-born, multi-lingual residency. Instead, Wormeli (2014) suggests building on this research and focusing on the community policing aspect that LaFree & Bersani's (2014) research posits and adds that information sharing regarding suspicious behaviors and incidents is

important. Finally, Wormeli (2014) underlines that this approach can assist in HVE behavior identification also.

Community Policing

The previously mentioned research brings up community policing as a concept that is gaining increasing popularity in both the scholarly and policy research areas in its application to terrorism prevention. Thomas (2016) notes that as local law enforcement officers are heavily involved in their community through community policing, information is shared with them due to two-way trust that is developed. Learning about a community, including its culture, languages, pockets of crime, and what is normal and abnormal for the community can also be obtained from community policing and can also be labeled community intelligence (Thomas, 2016). Chermak et al.'s (2013) study emphasized the importance of the flow of information between a community and a local law enforcement agency and the significance it has on the application of intelligence collection on radicalizing individuals.

Local Law Enforcement

Local law enforcement agencies are in a unique position to obtain threat and warning indicators about potential HVE attacks, which can assist in the prevention of those attacks (Cohen, 2016; Hewitt, 2014; The Heritage Foundation, 2015; Pelfrey, 2014; Randol, 2013). When it comes to domestic terrorism and obtaining HVE indicators, Davis (2016) suggests that local law enforcement information sharing and partnerships are the most important strategies. The use of fusion centers as a tool for terrorism related information sharing was also found to be helpful for law enforcement in identifying

threats (Chermak et al., 2013). Cohen (2016) indicates that in the detection of radicalization behavior, local law enforcement is best suited to use a community policing approach. However, Cohen (2106) notes that local law enforcement should rely more heavily on community leaders (i.e., religious, mental health and educators) to be more hands-on prior to any law enforcement interventions.

In his study of law enforcement tactics and their effectiveness with 20 incidents of domestic terrorism and 38 incidents of terrorism prevention, Hewitt (2014) identified the following:

Table 1

Law Enforcement Tactics Used in Domestic Terrorism Incidents

Tactic	Terrorism Attacks	Lone Wolves	Terrorist Cells	Terrorism Prevention
Surveillance			*X*	*X*
Informants	*X*	*X*	*X*	*X*
Routine Policing	*X*			
Information from Public	*X*			
Witness Identification		*X*		

Recent Domestic Attacks: Information Sharing Gaps

A brief account of three recent domestic HVE attacks are provided in the following section with information derived from scholarly and government reports regarding the law enforcement information sharing gaps that occurred leading up to the events.

Pulse Nightclub Attack

In June 2016, Omar Mateen open fired at the patrons of the Pulse Nightclub in Orlando, Florida, resulting in the death of 49 people and the injury of approximately 50 additional more (Beydoun, 2018; Crawford, 2017). Omar Mateen was born into an Afghan-American family, was a practicing Muslim, but was also known through his social media postings to have views that were closely associated with foreign terrorist organizations (Beydoun, 2018; Wilber, 2016). It was revealed that the FBI investigated him between 2013 and 2014, and after surveilling him and interviewing him twice, they closed his case (Wilber, 2016). After the Pulse Nightclub attack, an FBI gap analysis of their investigation identified that Omar Mateen's social media records were not reviewed, which they assessed would have allowed them to determine that he had espoused ideology or actual ties with the Islamic State (Beydoun, 2018; Wilber, 2016).

Fort Hood Attack

In 2009, a U.S. Army soldier, Nidal Malik Hasan, attacked the front entrance at a U.S. Army base in Fort Hood, Texas where he injured approximately 30 and killed 13 people (Peled, 2016). This example of an HVE was difficult to detect prior to the event because he was self-radicalized on the Internet, and although he made some comments

about not agreeing with the war in Afghanistan to his colleagues, he did not exhibit extremist behavior to his fellow soldiers before his attack (Weimann, 2012). However, his online behavior illustrated his extremist views, as Weimann (2012) notes, he communicated with a known terrorist and created extremist propaganda material. In 2010, Hasan's Fort Hood attack was found on a jihadist website as an example for inspiration for other HVE attackers to commit terrorist attacks (Weimann, 2012).

San Bernardino Attack

In 2015, 14 people were killed and over 20 others were injured at the Inland Regional Center (IRC) in San Bernardino, California by an HVE attack carried out by U.S. citizen Syed Farook and his wife Tashfeen Malik (Lee, et al., 2016; Nowrasteh, 2016). The TTPs used included arriving in a rented vehicle, parking outside of the (IRC), where Farook worked, and quickly firing more than 100 .233 caliber rounds around the front room of the office building, before they exited and left in the vehicle (Braziel et al., 2016). Three secondary homemade bombs were also found, that were left by Farook, and later removed by a local bomb squad (Braziel et al., 2016). After Farook and Malik were killed by local law enforcement officers, the detonators to the homemade bombs, hundreds more .233 caliber rounds, first aid supplies and handguns were found in the rented vehicle (Braziel et al., 2016).

Contingency Theory Overview

Contingency theory is used in this study as a basis for understanding and explaining the way law enforcement agencies adapt and respond. "The theory's logic is evident in a number of 'thought' or prescriptive pieces arguing for the need for change in

law enforcement organizations in order to address homeland security matters," (Burruss, et al., 2010). Contingency theory is the basis for this study because it seeks to explain the complex relationship of the external environment of government organizations (law enforcement organizations at each level) and how it impacts the success of the organization (Donaldson, 2001).

Contingency theory is rooted in leadership research and seeks to explain how leaders are motivated to make decisions for an organization (Hoffman-Miller, 2013). Fiedler (1964) developed the contingency model in response to his research surrounding group behavior in the workplace in response to leadership styles. In his work, Fielder (1964) found that work groups had similar goals to achieve a collective outcome and the success of that group's leader was contingent on the group's performance. Further, Fielder (1964) postulated that certain traits (i.e. personality, background, perception of the group, etc.) of the leader impacted his/her success with the organizational group.

Donaldson (2001) is renowned as the researcher that added to Fiedler's (1964) contingency theory of leadership and applied it more heavily to the organization. In his research, Donaldson (2001) put forward that there are many ways an organization can become structurally successful, and there is not one model that is best for all organizations. Donaldson (2001, 2006) added to his work and created the structural contingency theory, which argues that organizations will adjust themselves to succeed as new contingencies arise to arrange for the best structural fit. The new contingencies, in the structural contingency theory, can be changes in organizational size, policies, budgets, personnel, technology, and others. Donaldson's (2001, 2006) theory posits that

the organization will adjust to fit with the new contingencies but delineates the difference in organizational performance based on whether the contingencies originated inside or outside of the organization. Further, Donaldson labeled his research, structural adaptation to regain fit (SARFIT) model when an organization adjusts to external environmental changes to increase performance (Donaldson, 2001, 2006; Haynes and Giblin 2014).

Zhao et al. (2010) used contingency theory in their empirical research to study local police department organizational structures from 1990-2000. In their research, they analyzed the impact that differences in technology, organizational size, and environmental complexities had on police departments as an organization. One such environmental complexity analyzed was the impact community oriented policing (COP) activities had on municipalities, as a result of the 1994 Crime Control Act (Zhao et al., 2010, p. 222). The initial additional intent of COP was to modify the control and administration portion of a police department, replace the police department's staff with civilians in areas that are in the office and do not require police work, and also compress the hierarchy system in the organization (Zhao et al., 2010). Their study, using contingency theory, found that police department's organizational structure remained mostly unchanged, even after the principles of COP had been implemented.

Roberts et al. (2012) used contingency theory in their local law enforcement terrorism preparedness study, where they sought to explain how large local enforcement agencies adjusted to contingency factors like terrorism vulnerability, organizational elements and activities to explain relationship aspects of terrorism preparedness. In this study, Roberts et al. (2012), divided the elements of terrorism preparedness into

prevention, response, and recovery. Roberts et al. (2012) noted that contingency theory is an appropriate method to analyze police agencies because of their organizational design, multiple policy changes that occur, and external environmental factors (p. 722). Contingency theory illustrates the importance of the contingencies external to the organizational design and the reaction it creates internal to the agency (Donaldson, 2001; Donaldson, 2006).

In this study, contingency theory was used as the basis to explore how law enforcement agencies adapt to the changing terrorism prevention policy of information sharing in an environment where HVEs are also adapting their TTPs. To further breakdown the concept of contingency theory, as it relates to this study, the notion includes: when HVE threat information is not shared between law enforcement agencies (i.e. the counterterrorism prevention policy is not implemented properly), then the country is not safe from terrorism. As for contingency theory, when a contingent is not followed (information sharing), the organization is not "fit" and successful (Donaldson, 2001, 2006).

Summary

There is a significant gap in current academic literature surrounding law enforcement HVE prevention information sharing. Counterterrorism policies have been implemented and revised to address the issue of terrorism prevention information sharing since 09/11, but the challenge remains for law enforcement agencies at the federal, state and local levels. This research seeks to fill the gap in literature by using a local law enforcement agency and the Boston Marathon Bombing as a case study and explores

contingency theory to explain how the terrorism prevention policy of information sharing was implemented prior to the Boston Marathon Bombing in 2013. The following chapter three discusses the qualitative methodology in greater detail, including the case study research design.

Chapter 3: Research Method

Introduction

The purpose of this qualitative study is to develop an understanding of the information sharing gap that takes place among law enforcement agencies in HVE cases, as identified in the literature review. In this chapter, I provide a detailed overview of the case study research design, the data collection and analysis procedures and how they are addressed with this particular case, and how trustworthiness is accomplished. This chapter outlines the methodology for the qualitative case study of the Boston Marathon Bombing in Boston, Massachusetts in April 2013 and the procedures taken to accomplish the study.

Research Design and Rationale

Research Questions

The research questions that are examined in this study include the following:

RQ1: What level of HVE information is shared by federal agencies with local law enforcement agencies?

RQ2: What level of HVE information is shared by state agencies with local law enforcement agencies?

RQ3: What level of HVE information is shared between local law enforcement agencies and other law enforcement agencies?

Qualitative Research Methodology

This study uses a qualitative case study design to examine a relevant, recent HVE case in an immersive setting by using the data set of a local law enforcement agency, that

responded to the Boston Marathon Bombing HVE attack in 2013 (Creswell, 2013). Qualitative research is regarded as a methodology that results in detailed conclusions from primary data analysis that may provide a tool for practitioners and add to the body of scholarly literature (Creswell, 2013; Lewis, 2015; Yin, 2012) in the arena of law enforcement information sharing in HVE cases. The focus of this case study design is from the perspective of participants allowing me, as the researcher, to gain in-depth knowledge of the data by speaking with them as the subject matter experts (i.e., the police officers and administrators; Creswell, 2013; Lewis, 2015; Yin, 2012). With the use of this qualitative methodology, researchers can combine rigorous information exploration and provide personal results, revealing an explanation and a greater knowledge of the occurrence (Creswell, 2013; Lewis, 2015; Yin, 2012). Researchers are regarded as key instruments in data collection in a case study and they use their application of deductive reasoning skills throughout the case study design, data collection, and data analysis process (Lewis, 2015). In this case study, I explored what level of information sharing occurred within the local law enforcement agency with regard to the Boston Marathon Bombing HVE attack in 2013.

Case Study Design

Yin (2012) noted that there are three crucial steps to consider in case study research, including the case definition, selection of case study design, and the application of a theoretical framework in the design. In applying Yin's guidelines, this study addresses law enforcement information sharing gaps in HVE cases. The specific case highlighted for studying this is the Boston Marathon Bombing in Boston, Massachusetts

that occurred on April 15, 2013. The second step in the case study approach is to decide on the design of the case study itself. One may select the case study designs from holistic single case, embedded single case, holistic multiple case, and embedded multiple case (Yin, 2012). This study is an embedded, single case study because it examines the how and why information is shared and the case study includes a single organization (Yin, 2012, pg. 7). The third step in designing a case study is the application of a theoretical framework in the case study design (Yin, 2012). As noted in greater detail previously, in Chapter 3, contingency theory is used as a manner to explain the theoretical framework of this case.

Case study design has an explicit emphasis on a definite event, but the design is open to the investigation of the process (Hancock & Algozzine, 2015). This research can assist in (a) discovering causal relationships, (b) understanding how and why everything has happened in a confident way, and (c) creating robust, interesting, and easily readable descriptions, and rich understanding of occurrences in their typical settings (Yin, 2012). A purposive sampling is the key to this case study design, which regards the participants of this study as individuals and requires active participation by me, as the researcher, in the data collection process (Yin, 2012). In this study, I collected the data by means of interviews directed with open-ended questions (Malhotra, 2012). In addition, I conducted document reviews on information sharing during the data collection phase (Yin, 2012).

Participant Selection and Research Site

One primary local law enforcement agency responsible for responding and follow-on investigation for the Boston Marathon Bombing in 2013 was studied. Because

of this, participants of this case study were representatives from the law enforcement agency. The planned research site was the headquarters office of the agency. However, due to COVID-19 and the impact it had on the department, the interviews were conducted using Zoom. A Letter of Cooperation was obtained stating that I had authorization to interview the participants and gain access to documents, as appropriate, for research purposes.

Role of the Researcher

As the researcher, I was responsible for collecting the data by conducting the interviews, reviewing documents and making observations. I do not have any personal or professional relationships with the law enforcement agency, which was the focus of the case study. While I have professional experience that has given me knowledge of law enforcement counterterrorism policy and the information sharing process, I do not have authority or ability to provide grants to the agency. Additionally, I do not currently work for the federal government. Therefore, there were no ethical concerns with data collection. It should also be noted that I do not have any research bias associated with this particular case, especially as it relates to how the law enforcement agency responded to the Boston Marathon Bombing. I made clear of this fact to all participants prior to and during the interviews so that they did have their guards up when responding to my interview questions. I ensured to delineate to the participants that I was interested in learning about the information sharing procedures and I was not conducting my research to determine errors that occurred in their response to the Boston Marathon Bombing.

Sampling Strategy and Size

Numerous purposeful sampling designs exist. Purposeful sampling is a method that is commonly used as a sampling strategy when a researcher is aiming to obtain the most information saturated cases while also making the best use of time and resources (Patton, 2002). This process identifies those that are the most informed about the case or occurrence that is being studied (Creswell & Plano Clark, 2011). Saturation of the sample size and quality is an important principle within a qualitative sampling strategy (Miles & Huberman, 1994). The design chosen for this study is the interview of a selection of participants involved in the management of the Boston Marathon Bombing case. The sample began by my introduction of this study to a senior level officer at the law enforcement agency who previously provided a counterterrorism briefing about the bombing to a group of my peers. From this introduction, I determined how to obtain the necessary approvals from the agency and also elicited names of officers that 1) responded to the attack, 2) investigated the attack, and/or 3) handled counterterrorism prevention policy for the agency. This was a purposive sampling strategy (Palinkas et al., 2015). During the interviews, I also asked, "Who else do I need to speak to?" This was a snowball effect to the sampling strategy (Palinkas et al., 2015). In the purposive sampling strategy, from the data that I collected, I sought to obtain patterns and themes of information (Yin, 2012). Sampling continued until saturation was achieved. The saturation involved repetition of themes and information (Yin, 2012).

Data Collection

I followed a communication plan for recruitment of study participants. Once I received the initial set of names from the senior officer that I previously mentioned, I began by sending an individual introduction email to each person. This email included the following:

- A descriptive overview of the study;
- An attachment of the consent form;
- Information about the participant's right within the study, including the right to withdraw from the study, and information about confidentiality throughout the entire study;
- An estimated amount of time that the participant will likely spend at the interview and follow-up; and
- A request for a response and some suggested dates for interview availability.

I followed up each email with a phone call for potential participants that did not respond within 1 week or for those respondents with questions. After all interviews were scheduled, I confirmed them by sending an email with a Zoom meeting link that included the date and time of their interview and instructions for the Zoom meeting. I also had a communicating plan in place that had the participant's preferred method of communication (i.e. email, phone call, text message). This ensured that I received a more rapid response when communicating with participants. I made note of their preference in their coded file.

Participants were not offered any stipends. I informed participants that their interview transcripts were available to them within seven days of their interview for their review. They were also provided with a detailed account of the data privacy procedures. This study maintained a low amount of risk to the participants due to the many data protection and privacy measures that were taken. After the data analysis was complete, I provided the participants, via email, with a copy of the conclusions drawn from their interview and collection of interviews as a whole.

Instrumentation

I developed an interview protocol to guide the interviews for this study, as there was not an applicable one that I could replicate. I asked questions that began with "describe how" and "explain" in order to elicit robust responses (Yin, 2012). Additionally, even though I conducted open-ended interviews with potential follow-up questions, my interview protocol formed the basis for each interview in order to guide the interviews appropriately and follow a standard time parameter. The specific questions were designed to gain an understanding of how information is shared in the law enforcement agency and with other law enforcement agencies, specifically related to HVE threats or other counterterrorism information. The interview protocol was specifically developed to answer the research questions pertaining to this study and was guided by a matrix format that outlined each research question and mapped it to interview questions associated with that topic area (Castillo-Montoya, 2016). I ensured that I included introductory questions, main questions, transitional questions, and closing questions within the interview protocol so that the interview flowed like a conversation

(Creswell, 2007). While I did not conduct an official pilot phase of the interview protocol, I practiced asking the questions out loud several times, as well as asking the questions to my peers, so that I had the flow in place prior to conducting the interviews. The procedures of mapping my research questions with interview questions in a matrix, narrowing down the questions, and informally testing the interview protocol are all steps to increase reliability of the interview protocol (Castillo-Montoya, 2016).

Data Collection and Management

Data preservation and participant confidentiality was followed at all times during the data collection phase of this study. While data management began during the literature review phase, it was increasingly important as I began planning the data collection and analysis processes. Both my home and laptop computers are password protected and maintain firewall protection. I have passwords on all of my wireless Internet service connections and also maintain a virtual private network on my computers and cell phones. These security procedures ensure that no unauthorized access to participant records were retrieved at any time or will be in the future. Additionally, my home has a security system and video monitoring system.

I recorded the audio portion of the interviews through Zoom, downloaded the files onto my computer, which was backed up to a cloud network, and transcribed the interview into a Microsoft Word document. I maintained a file folder that locks, and I placed the key in a different secure location. I kept the documents that I needed to store in this locked folder. This type of file folder is one that the U.S. government uses to keep classified documents safe. It is also important to note that I did not keep any files with

participants' names or identifying information. Instead, I created a coding methodology in a separate password-protected file that no one else had access to. These codes provided the manner by which each interview was coded. During the interviews, I took field notes and ensured the notes were coded for each participant and locked and stored properly. The data that I collected will be stored for at least 5 years. In order to organize the data obtained from the interviews, I used NVivo software. NVivo is qualitative data analysis software that was used to transcribe the audio recordings, display data, assisted in developing patterns and themes, and drawing conclusions (Miles et al., 2014).

Data Analysis

The initial stage in the data analysis process was to upload the interviews to NVivo and examine the data for patterns and themes for the purpose of coding (Miles et al., 2014). Data organization was achieved, and manual coding was done for supporting the iteration process (Yin, 2012). As a first step, prior to using the NVivo software, researchers can take a first attempt at coding, categorizing, and editing phase (Miles et al., 2014). I explored the participant's responses and made a first attempt at pattern-recognition with connections of distinctive-wording in explanations of vital attributes of answers (Miles et al., 2014). I then used the NVivo software to analyze the transcripts directly from the interviews. The software conducted a pattern analysis that emphasized key themes corresponding to interview items that synchronized with the research questions (Miles et al., 2014).

A database of the case study was created in NVivo, and included some of my field notes, the organizational documents obtained, and was combined for consolidating. In

this study, triangulation was an important analysis technique (Bekhet & Zauszniewski, 2012). The triangulation of data gained support from more than a single source of evidence such as documents, archival records, and open-ended interviews. A procedure for tactically evaluating the case study may take the form of pattern matching that encompasses correlating all data collected so far to the theoretical framework while dealing with the responses to the research questions. Descriptions were derived from the themes that were developed so that narratives could also be formed (Miles et al., 2014; Yin, 2012).

Research Quality

In qualitative research, research quality is important as it pertains to the trustworthiness of the results of the study (Korstjens and Moser, 2018). Lincoln and Guba (1985) indicate that the main elements of trustworthiness for a qualitative study include credibility, transferability, dependability, conformability, and reflexivity.

Credibility

The issue of trustworthiness is important for many reasons. First, it is important for the internal validity of this study to establish credibility through the dataset (Lincoln & Guba, 1985). This includes ensuring that the sample is saturated (i.e., obtaining more participants will not produce more data). It also means that I have recurring and prolonged contact with the participants. Throughout the data collection and data analysis phase, I was in contact with each participant on a recurring basis. Credibility is also obtained in this study through the use of different methods of data triangulation (Miles et al., 2014).

Dependability

As mentioned previously, to ensure reliability or dependability, I provided participants with a copy of the interview transcripts so that they were able to validate the transcripts and ensure accuracy (Creswell, 2007). Additionally, without causing any confidentiality concerns, I provided a draft aggregate of the theme analysis results for a peer review (Miles et al., 2014) to each participant, individually, via email. They had the ability to comment through a simple Word document form and state if they had any feedback with the preliminary results. This process of documenting and describing the records keeping of this study is considered an audit trail (Lincoln & Guba, 1985) and increases dependability of the data.

Confirmability and Reflexivity

I maintained a research diary during the data collection and analysis phase that included a review of my own potential biases that may arise and self-reflection (Korstjens & Moser, 2018, p. 121; Lincoln & Guba, 1985). While conducting my research, I did not foresee any biases. However, the use of a diary to explore the research thought process while collecting data assists in reducing bias and allows a researcher to be critical of oneself (Korstjens & Moser, 2018). Finally, the use of the NVivo software assisted with confirmability, as it explored patterns and themes within the interviews and field notes, and removed the potential for researcher's preconceived notions (Lincoln & Guba, 1985).

Ethical Considerations

Prior to speaking and interviewing anyone in the law enforcement agency, I let each potential participant know that all aspects of the study would be aggregated and the

answers to their interview questions are completely confidential. Additionally, I informed them that no other person within the law enforcement agency or outside of this study would be able to obtain their identifying information. This step is important due to the potential political or career concerns that participants may have had prior to participating.

Once a person tentatively agreed to participate in this study, I provided them with a Consent Form and requested them to review it, sign it and provide it back to me. I let participants know that they could withdraw from the study at any time. No participants chose to withdraw from this study prior to completion.

It was especially important for me, as the researcher and data collector, to inform all participants of the data storage procedures also. I let them know that their information was password protected and that all notes would be stored as identified in the data management section. The participants were informed that once their interviews were transcribed and reviewed by them, the original audio recordings were then deleted to add an additional layer of confidentiality. The only people that had access to the data within the study were my dissertation committee and myself; however, my committee would only have access to the data without participant's personal identifying information. Additionally, it is important to note that Institution Review Board approval was obtained prior to reaching out any potential participant.

Summary

A case study design applies to the analysis of the problem statement (Yin, 2012). This chapter highlights the case study research design and explores how with the use of an interview guide protocol I cultivated a narrative through the analysis of the responses

to the questions and development of themes. In this chapter, elements of participant recruitment and communication are discussed. A detailed discussion on instrumentation, data analysis, trustworthiness, and ethical procedures was also established. In the following chapter, I discuss the results of this case study research.

Chapter 4: Results

Introduction

In this chapter, I provide a background of the baseline investigative details of the Boston Marathon Bombing. I also include the results of my case study where I used open-ended questions to gain an understanding of law enforcement information sharing in a homegrown violent extremism case. The participants were law enforcement professionals who had a role in the response of the Boston Marathon Bombing and who have knowledge of interagency counterterrorism law enforcement information sharing. The case study design allowed qualitative data collection through open-ended interviews using Zoom as a method for communication. In this chapter, I will explore the setting that was used for the study, the demographics of the study participants, the data collection procedures, a representation of the data analysis, an overview of the evidence of trustworthiness, the research findings, and a summary of the study.

Boston Marathon Bombing Background

The Russian-born and Boston residents Tamerlan and Dzhokhar Tsarnaev used simple, yet destructive TTPs by making improvised explosive devises that caused approximately 260 injuries and three deaths at the Boston Marathon finish line in 2013 (Cohen, 2016; Peled, 2016). Prior to the bombing, in 2011, the FBI received information from the Russian Federal Security Service regarding the possibility that Tamerlan Tsarnaev was planning to travel to Russia for purposes of radicalization (House of Representatives, 2014). At the time, both Tsarnaev brothers were living in the Boston area and were questioned by the FBI, but local law enforcement was not notified of any

potential threat (House of Representatives, 2014; Peled, 2016). The FBI questioned Tamerlan Tsarnaev and his parents but found them to have no terrorism connection (House of Representatives, 2014; Peled, 2016). Tamerlan Tsarnaev eventually traveled to Russia in 2012, despite being on a terrorism travel watch list (Peled, 2016). It is unknown if Tamerlan Tsarnaev was radicalized through a friend that he met in the United States and inspired him to travel to overseas for training or if he was radicalized while he was in Russia (House of Representatives, 2014). In their investigative findings, the House of Representatives (2014) determined that the FBI should have shared the potential threat information with local law enforcement and Joint Terrorism Task Force personnel when it was received from the Russian government.

Setting

Based on the Institutional Review Board (IRB) recommendation, due to the COVID-19 pandemic, the participant interviews were completed using Zoom. This method worked well for the participants due to their varied schedules in law enforcement. Upon receiving IRB approval, I sent an email to a senior level representative in the law enforcement agency, who then approved me to begin the study by providing a signed Letter of Cooperation Form and Consent Form. All interviews were conducted in the August 2021 – September 2021 timeframe. I requested in advance that all participants hold their Zoom interview in a private location, and I verified at the beginning of their interviews that they were alone where no one else were able to listen to their responses. The purpose of the request for privacy was to ensure that there was no outside influence or any extenuating factors that could have impacted how they provided their response.

Demographics

The eight study participants had direct knowledge of the Boston Marathon Bombing based on their participation in planning for the event, participating in the Boston Marathon in a law enforcement capacity, and responding to the aftermath. I coded each of the participants by numbering them one through eight, which I also ensured that I coded their interview transcript and field notes with their participant code. Three of the participants have a master's degree in homeland security studies, which they explained provided them with a knowledge and understanding of counterterrorism issues as it pertains to law enforcement. Two of the participants relayed that their spouse works in law enforcement intelligence; one of them felt that gave him some additional benefit if threat related information was needed because he could ask his spouse for assistance. Participant demographics are included in the following Table 2.

Table 2

Participant Demographics

Participant ID	Gender	Rank during Boston Marathon Bombing	Education	Military or operational counterterrorism training
1	Male	Lieutenant detective	Master's degree	Yes
2	Female	Officer	Bachelor's degree	Yes
3	Male	Lieutenant	Master's degree	No
4	Male	Lieutenant detective	Master's degree	Yes
5	Male	Deputy chief	Bachelor's degree	No

6	Male	Lieutenant detective	Bachelor's Degree	No
7	Male	Lieutenant	High school	Yes
8	Male	Civilian	Bachelor's degree	Yes

While the rank of the participants is currently different because they had been promoted, they provided what their rank was at the timeframe of the Boston Marathon Bombing. One participant was in a senior administrative supervisory position, two were supervisory detectives, one was a mid-level supervisor, one was a mid-level non-supervisor, one was a patrol officer, one was a public safety officer, and one was a civilian in a supervisory logistics position. One participant held a security clearance. Several years prior to the bombing, one of the supervisory detectives was detailed to the NCTC in Washington, D.C., and while there, he created a law enforcement intelligence product that was and is currently disseminated to fusion centers across the country.

Data Collection

This qualitative case study uses eight participants to examine their understanding of law enforcement counterterrorism information sharing in homegrown violent extremism cases using the Boston Marathon Bombing as the case study. The participants all had direct knowledge of the case. One face-to-face interview using Zoom was conducted with seven participants, and one participant interview was conducted through a Zoom voice only call. It should be noted that the Zoom voice only interview yielded just as rich responses as the face-to-face interviews. The interviews lasted between 33 and 55

minutes. At the beginning of each interview, I requested permission to record the interviews with audio only, and I received verbal permission to record the audio interview from all participants. The audio was recorded using the Zoom feature, and the data file was stored in an encrypted folder on my computer. Upon completion of each interview, I transcribed it into a Word file and then deleted the audio file from my computer. Additionally, I ensured that there were no audio files maintained in Zoom. I kept the coded Word file transcripts of each interview in an encrypted folder on my computer. There was no identifying participant information stored at any time either electronically or in hand-written notes associated with my interviews.

An interview protocol with 14 open-ended questions was used for each participant interview. Additionally, I asked follow-up questions to elicit more detailed responses. For example, when participants provided a short response to a question or appeared like they had additional information related to a specific question, I asked the following:

- "Can you explain that in more detail?"
- "Do you have an example of that?"

Furthermore, if there was a response to a question that required clarification or that needed additional explanation (Creswell & Creswell, 2018), I asked the following:

- "Let me repeat this to you to ensure I understand correctly."
- When you say _____, are you referring to _____?"

During each interview, field notes were also taken. The field notes documented the additional background information that the participants provided, such as their

experiences during the bombing itself, their educational background, and other information that I observed while they were talking.

Evidence of Trustworthiness

Throughout the data collection and analysis process, I maintained contact with the participants through their preferred methods of communication. I also maintained trustworthiness through credibility, transferability, dependability, and confirmability.

Credibility

As mentioned in Chapter 3, the data set was determined to be complete when saturation was reached (Creswell, 2013). After the sixth interview, it was noted that the participants were providing rich data, and by the eighth participant interview, nothing new was being revealed. Therefore, after the eighth participant interview, it was clear that this study had reached its saturation point (Creswell & Creswell, 2018). After each interview, the audio transcripts were transcribed into Word documents, using only the participant codes with no identifying information. Each participant was provided the opportunity to review and edit their transcript to ensure accuracy.

Transferability

The data analysis included in this chapter includes rich descriptions which allows the applicability of this study to be used by other researchers in future studies (Creswell, 2013). The participant responses were analyzed, coded, and developed into themes in an effort to provide detailed findings that are applicable for future research. Additionally, the participants' demographics are provided and illustrate similar demographics of other local law enforcement jurisdictions.

Dependability

I had no changes to the strategies in Chapter 3 regarding dependability. Additionally, as mentioned in the previous data collection section, I ensured that during the interviews, if the participants provided a response to a question that I had difficulty interpreting, I repeated it back to them until I gained a full understanding. Dependability was also achieved by reviewing and analyzing the audio interview transcripts with handwritten field notes, and cross-checking those with the final transcripts.

Confirmability

I had no changes to the strategies that I included in Chapter 3 with regard to confirmability. For example, I took field notes as a manner of self-auditing and reflection of the study to ensure that I reduced the possibility of bias as I proceeded through the study (Korstjens & Moser, 2018). Additionally, I maintained a research diary whereby I analyzed the interviews and made a series of draft codes prior to entering the interview transcripts into NVivo.

Data Analysis

In order to analyze the data, I first input the transcribed interviews into NVivo 12 for Mac. Creswell and Creswell (2018) suggested that qualitative data analysis is best completed using computer software because it stores and sorts the data into patterns and themes. It is noted that while the researcher is still required to review, code, and develop themes, qualitative analysis software assists with the process. Because of this, even after I transcribed the interviews, each transcribed interview was reviewed three times. I created a word cloud using NVivo that illustrated the words that were repeated more than six

times by each participant, which contained four letters or more. Figure 1 illustrates the word cloud.

Figure 1

Word Cloud: Top 6 Most Repeated Words From Participant Interviews

I then developed first and second cycle codes (Saldana, 2016). The first cycle codes were developed as a result of the interview questions. Second cycle coding (Saldana, 2016) allowed me to reorganize the codes and provided a more descriptive picture of the data by merging it into smaller groups.

Moving From Codes to Categories to Themes

The next step in the data analysis process was developing themes using NVivo. The coded interviews were reviewed and re-coded (Saldana, 2016) using a "splitter coding" method, which analyzed the social action within the data (pg. 24). I then reviewed the codes for a third time and revised any codes that should be grouped together (Saldana, 2016). I then moved to the process of inductive coding in order to develop categories from the codes, which were identified utilizing NVivo (Saldana, 2016). From the categories that were identified, I originally developed four themes. I eventually divided one of the themes into two separate themes, as detailed in the narrative about Theme 1. The following Table 3 illustrates the progression from Codes to Categories to Themes.

Table 3

Codes, Categories, and Themes

Code	Category	Theme
▪ Community policing ▪ Preparation meetings ▪ Reports disseminated from BRIC ▪ Emails from BRIC ▪ Interagency working group ▪ Threat briefing specific to event	▪ Type of information sharing	Methods of information sharing leading to Boston Marathon bombing
▪ Police Radio ▪ Command Center ▪ Cell phone ▪ Email ▪ Printed Photo ▪ Word of mouth	▪ Interagency response to bombing ▪ Understanding of bombers	Methods of information sharing during and after Boston Marathon bombing

▪ Lack of security clearance ▪ Some do not check their email ▪ State and federal agencies do not share with local agencies ▪ Territorial with case information ▪ Power struggle	▪ Examples of lack of info sharing ▪ Limited state information sharing ▪ Limited federal information sharing	Barriers to information sharing
▪ BRIC will send information ▪ Federal agencies will share if there is a threat ▪ FBI will share threats with fusions centers if necessary ▪ BRIC obtains information and sends it when there is a threat	▪ Lack of communication post 9/11	Trust/Reliance (that information is or will be shared)
▪ Not aware of any policy changes ▪ Social media policy changes ▪ Interagency exercises implemented and funded ▪ Intelligence Bulletins sent weekly instead of monthly ▪ HVE education and awareness across department since bombing ▪ Desired written decision-making policy for incident response	▪ Increased local info sharing ▪ Policy changes desired for improved interagency info sharing	Changes to information sharing policy (incorporated or desired)

Creswell, J.W. and Creswell, J.D. (2018) suggests that five to seven themes are the appropriate number to develop “major findings” for a qualitative study (pg. 194). The

codes holistically fit clearly within five themes. As Saldana (2016) illustrates, the themes emerged from the coding into greater "concepts" due to their repetitive references or the participants mentioning the same type of phrases. The themes with their definitions are included in the following Table 4.

Table 4

Themes, Mentions/Participants, Definitions

Theme	Mentions/Participants	Definition
Methods Leading Up to Bombing	11/P1-P7	This theme refers to the various methods that information was shared within the agency, from outside agencies, and between other agencies leading to the bombing.
Methods During and After	16/P1-P8	This theme refers to the various methods of information sharing within the agency, from outside agencies, and between other agencies during the bombing and during the response to the bombing.
Barriers	16/P1, P2, P6, P7	This theme refers to real or perceived barriers to HVE and/or counterterrorism information sharing.
Trust/Reliance	18, P1-P8	This theme refers to the trust and reliance that the participants have that HVE/counterterrorism information is shared.
Changes	18, P1-P4, P6-P8	This theme refers to changes made or changes desired as a result of the bombing.

Research Findings

This section provides a narrative of the results, exemplified by the themes that were identified. The analysis includes the linkage to my research questions. The participants' responses, including direct quotes, are included as an explanation of how the

themes were developed. Chapter 5 will add to this notion and provide a linkage of how the themes are associated with the theoretical framework of this study.

Overview of Research Questions

Each of the three research questions include a request to delineate the "level" of information shared. The below quantifies the level of information sharing that occurred from the participants based on their experience with local, state, and federal law enforcement agencies, specifically related to this case. For purposes of this study, the following is provided, which explain the levels of information sharing:

- 1) As much as possible,
- 2) Some, and
- 3) None or unknown.

RQ1: What level of HVE information is shared by federal agencies to local law enforcement agencies?

RQ2: What level of HVE information is shared by state agencies to local law enforcement agencies?

RQ 3: What level of HVE information is shared with other local law enforcement agencies and law enforcement agencies?

Theme 1: Methods of Information Sharing Leading up the Boston Marathon

As exemplified in Table 2, the first theme that emerged is related to the methods of information sharing leading up to the Boston Marathon Bombing, were used as a method to prepare for the potential threats related to the Boston Marathon, or to the potential threats to the Boston area prior to the bombing. This theme was first coded and

grouped with theme 2, but it appeared obvious after further review that it should be separated. In regards to how they received threat, HVE, or counterterrorism related information prior to the bombing, Participant 2 said:

> We have like an Intel unit that pushes out information to us whether it's local, regional, nationwide, you know, other trends and throughout the world. You know, if it has potential to affect around here you know like they'd come out and say, you know, this is what's going on and, you know, so let's pay attention to, you know, the consulate and things of that nature and here's where they're located and stuff like that so I mean I think we're always kind of aware and if as long as you're reading the materials that they're putting out there for us.

Participant 3 relayed, "We receive emails from the BRIC. I believe that DHS and FBI also provide input at the BRIC when they send finished products to us through email." Participant 4 identified that prior to the bombing,

> No, we did not have anyone provide any information about that. Prior to the bombing, we had some items that if it was important that will be disseminated to us. No, there was no alert, there was no one bring it to our attention that possibly could happen, nothing, nothing like that.

A suggestion by Participant 5 about HVE or counterterrorism threat information prior to the bombing was:

> At that time, I think if there was threat information coming out, it would find its way through the department, either through bulletins or through, you know, from

> the FBI or through Homeland Security bulletins, or even through maybe our intelligence unit.

Participant 6 shared that he believed the threat information was disseminated through a "daily email." Similarly, Participant 7 relayed that "we did get threat reports from the BRIC. We got intelligence briefings beginning two weeks prior to the marathon."

Participants 2, 3, and 5 relayed that they interacted with their community to share information, which is also called community policing. This is a method where they had casual conversations with neighborhood representatives, religious centers, and any large groups within their jurisdictions to request that they remain vigilant. Participant 2 shared:

> Casual conversations here and there with people in the community, whether it was at calls or just passing people out and about. Do you think like a person in the community would have approached an officer with a concern? I think so, yeah, I think if it was serious enough. I went on two calls for people thinking, you know, that we should investigat[e] persons for, you know, taking pictures…of a Jewish school in the neighborhood. There was a guy taking pictures of the kids in the schoolyard. So, you know, that type of stuff was happened prior to the marathon. People [were] definitely vigilant.

Participant 3 participated in community policing in the following way prior to the Boston Marathon: "Informally. To interact with the neighborhood as a whole in my jurisdiction for public safety purposes. The specific goal was for crime reduction, but it helps for many reasons."

Additionally, Participant 5 explained that leading up to the Boston Marathon, he participated in "Constant Meetings"; whereby he continually received crime data for those neighborhood areas so that when he went on their community policing campaigns, he knew who to talk to and what to look out for in advance of the Boston Marathon. Participant 5 explained:

> Everyone attended what they call Constant Meetings, and at the constant meeting they use computer statistics to measure the crime using data that is taking place in the neighborhood so everyone across the big part of the police command would take part in "camp meetings." And this comes out of Stanford University community statistics. It's, I think, it's crime statistics, which was started in New York back in the 1990s. This helped police officers kind of use intelligence led policing.

Participant 1 shared that those in supervisory positions received reports called Roll Call Releases, which he described as finished law enforcement products that were disseminated through the Boston Regional Intelligence Center (BRIC). Participant 3 echoed that sentiment by indicating that "key people receive emails from the BRIC." Participant 4 said, "The BRIC is a positive story. That is where we [would] get our intelligence. We would get it by email every day leading up to the marathon."

Participant 6 relayed that he was a member of a working group which planned for the Boston Marathon. He highlighted that the working group consisted of key members of law enforcement agencies, universities, private organizations, federal agencies, and

security personnel that were involved in the operations during the marathon. Furthermore, Participant 6 shared:

> We had an unclassified briefing that included possible threats to the marathon and the general area. The whole working group received the brief from different agency participants, including federal agencies that were traveling from out of town. Threat information was verbally shared with the group if it was applicable. The threat brief was given about two weeks before the marathon. No one talked about the possibility that there could be a bombing.

None of the study participants stated that they had knowledge of the bombers prior to the bombing from any method of information sharing. In fact, Participant 6 stated, "I did not hear the Tsarneav brothers' names until after the bombing. Even then, I heard their names from word of mouth."

Theme 2: Methods of Information Sharing During and After the Bombing

The second theme that emerged from the participant interviews includes the methods of information sharing during the Boston Marathon Bombing and throughout the response to the bombing. These methods of information sharing include those between the department, from outside agencies, and between other agencies. Most participants had a vivid description of the methods of information sharing used in the response to the bombing, but most of them did not have a clear understanding of the interagency information sharing that occurred.

Participants 1, 2, 5, 7, and 8 each shared that they initially heard the bombing from their police radio transmission. Participant 1 mentioned that he heard the following

radio transmission: “I'm getting on a radio - stop the marathon there's been an explosion, you know, stop the marathon there have been two explosions.” Additionally, during the investigative phase after the bombing, he shared that:

> The information was disseminated through press releases and that was how we found out. All of the investigative work from the various agencies was how they had the two pictures of the two brothers. The best way to get it out to the Department was through the press release.

Participant 2 recalled:

> It's hard to hear at a big event - to hear your radio even. Though, you know, we have shoulder mics, and I just remember one of the Sergeant Detectives that was at the finish line just yelling about secondary devices like any trash cans and things. I thought it was like a generator or one of those blue electric boxes or something like that…You don't ever think you're going to be in a situation like that, but you can revert back to like the things that you're told when you're in training and the police academy…It was eerie, but I just remember hearing the Sergeant Detective on the radio yelling about secondary devices and then, you know…I remember one of the bosses came down and was, you know, screaming at everybody because it's a crime scene so as we're trying to still help people and get people loaded up still trying to preserve a crime scene at the same time so it was just very chaotic. And then they started using a bike unit to secure the crime scene.

Participant 7 explained that there was a Command Operations Center, which held a representative from local, state, and federal agencies that managed the security for the

Boston Marathon. He further elaborated that he was the command center leader and oversaw the Command Operations Center. He relayed that the operations center "shows cameras [and] everything that's happening so I organized all the bureaus in the department and a representative from other agencies that were needed." Participant 7 shared:

> I was the commander of the command center and I saw the explosion on the screens in my command center. Luckily there was no sound. I remember someone saying that there was an explosion, and I said, "No, that was a detonation." I then put out a call for all ambulances to come as quickly as possible. I also requested that there was radio silence so that we can communicate with all officers. It was my job to get my boss's orders out to all officers in the department. My boss was the Superintendent-In-Charge.

Participant 8 relayed:

> I had an earpiece in my ear with the radio, and I was two blocks away from the finish line. So, when I hear crazy talk on the radio, they were talking about the finish line. And I knew that gentlemen personally. I knew he was calling up a help on the radio, and that was how I heard. There was a real problem.

Participants 1, 3, 4, 6, and 8 explained that when they moved to a response role after the bombing, they shared information through email. Participant 4 elaborated: "Well, everyone has access to cell phones…The email would pop into your phone." He explained that all shift assignments were provided by email, and the information about the Tsarneav brothers was also distributed by email. Participant 3 reiterated that during

the response to the bombing, law enforcement issued phones were used to share emails about instructions and assignments.

Participant 7 stated that he learned about the Tsarnaev brothers by seeing a picture of them "distributed by the FBI" on television the morning after the bombing. Participant 2 shared:

> I remember they passed out pictures of the younger brother that I have. It was a license picture, and I actually still have it on my phone to this day…So we could see what it looked like and that's who you're looking for. And they just briefed us on, you know, in a giant Roll Call of, you know, hundreds of officers.

Participant 1 explained:

> The information was disseminated through press releases and that was how we found out [about the bombers]. All of the investigative work from the various agencies was how they had the two pictures of the two brothers. The best way to get it out to the Department was through the press release… It turned into a joint investigation. We had all of our detectives taking the leads, helping the FBI with all the leads that will come in. All people had their phones, right, although we didn't know if they captured anything. So anyone that said, hey, I was on Boylston Street that date filming with my phone - that was a lead. And our detectives would go out and capture that video and give it to the FBI.

Participants 2 and 6 explained similar experiences as each other, when they responded to their squad leader's request to arrive at Watertown to do a grid search along residential streets for Dzhokhar Tsarnaev. Participant 2 shared: "There were two transit

guys in a car [and] I was on foot. And there was like a bomb squad nearby on like every grid pattern that we did in Watertown to find them." Participant 6 described:

> In that situation I think it was, you know, word of mouth, like, you know, walking and talking. So, I mean, at that point we're divided up into blocks, right. It's like walking down to the next block and the information - it was like that old game of telephone used to play when you're a kid. Walking down to the next block and getting it for me. What did you hear? What people thought. So and so went to the hospital, you know, that kind of thing.

Both Participants 2 and 6 stated that they did not use any technology when they searched in Watertown for Dzhokhar Tsarnaev.

Theme 3: Barriers to Information Sharing Between Law Enforcement Agencies

Real or perceived barriers to information sharing in HVE or counterterrorism cases between law enforcement agencies at the local, state, and federal level were identified by Participants 1, 2, 6, and 7. The reason that the terminology "real or perceived" is used is due to some of the barriers that were identified can potentially be rectified by the participants. For instance, one of the barriers that Participant 6 identified is the fact that the BRIC sends law enforcement bulletins and other noteworthy information through email. However, he also said that "many people don't check their email or read the bulletins."

Participants 1 and 6 both mentioned that they felt state and federal agencies do not "play well with others" and "share information." Participant 1 shared that he felt federal

agencies, in particular, do not share information with local and state law enforcement agencies because they worry about the misuse of the information. Participant 1 stated:

> Federal agencies don't want to share with state and local because they're afraid it's going to end up in the media on stuff that they could do more with because there are not developed relationships. So, it's all about developing relationships and developing trust. They want to know it's okay that once you get the information that you're not going to mismanage it.

Participant 6 mentioned that he felt law enforcement agencies are "territorial" and prefer to handle the case information themselves without including other agencies.

Participant 2 shared that during emergencies the radio frequencies between local, state, and federal law enforcement agencies do not sync; therefore, they are not able to adequately communicate. She explained that during the bombing response:

> We use different radios, so we didn't know what they were doing at Watertown. They didn't know what we're doing. And the state and like the feds and, you know, the National Guard guys that where with us, like, we're not all on the same wavelength. So that was like interesting to deal with, you know, patching up radio frequencies and things like that… I don't remember how that worked, but usually like we'll have where I am, there's a command center, and for major events (like the marathon) the command center will have different agencies like Boston police, State police, National Guard, and somebody from the fire department. But with the bombing - no one could communicate.

Participant 6 highlighted that a limited number of officers within his department hold a security clearance. Because of this, they do not have access to the classified HVE and counterterrorism threat reporting that is located at the BRIC. He explained that there is one or a few department representatives that remain detailed at the BRIC who hold a security clearance and are responsible for coordinating with all other law enforcement agencies, obtaining the correct HVE and counterterrorism threat information, and ensuring that it is disseminated to the correct person at the department.

Finally, Participant 6 explained that the detailed officer would then send it to a limited number of people at the department, and those people are responsible for determining who else needs to see it. Participant 1 added that an information sharing barrier related to others in his department not having a security clearance is that they "did not know about the information unless they were assigned to the unit or they did not have a perceived reason to know.

Participant 7 explained that 24-36 hours after the bombing, federal agencies were not sharing information with his department. He explained:

> However, after that, Washington, D.C. eventually started forcing them to share information through the Command Center. They provided a representative from the FBI, the CIA, the ATF, and some other federal agencies at the command center and at the BRIC. I guess it was because the case was moving fast, and there was so much info to move through related to the bombers and the crime scene data. In general, I think they don't want to share information with local law enforcement and other agencies. Other times, it may be the type of case.

Theme 4: Trust and Reliance that Information is Shared

Each participant reflected that they trusted that the HVE and counterterrorism threat information was shared with them from their department, state law enforcement agencies, and federal agencies. In fact, they learned to rely on their means of receiving their information that they trusted.

Participant 1 reflected: "The BRIC tells me what I need to know and I trust that, you know, that information is coming from a plethora of different agencies so that's kind of how I view it."

Participant 3 added:

> Our command provided the intelligence information or threat information that we needed for our area. I think that they received State and Federal agency input with regard to threats. The BRIC also sent this information. If there were any barriers, it would be known to senior level and command level folks.

Participant 4 echoed that "if there was any homegrown terrorist activity or a suspicion that we should be aware of that the information would be disseminated through the BRIC."

Participant 5 explained his opinion:

> I think if there was threat information coming out, it would find its way through the department, either through bulletins or through, you know, from the FBI or through Homeland Security bulletins, or even through maybe our intelligence unit… And, if something happened across the country, say, if you had something that took place in Oakland. There would normally be a quick study of whatever

> that crime or that event that took place was. There would then be a briefing put out, which one could read on different things and then if there was more specific information, it would filter its way through the federal government, to [the] FBI, and Homeland Security. These agencies would make us aware of specific threats. But there's always concerning events, you know, there's always going to be events that take place, which are always going to be in highly concerning areas.

Participant 1 shared: **"**I'm sure the Fed don't share as much with us. But I would assume, you know, if it was a threat that we needed to be aware of, you know, I would hope that we would be made aware." Even as Participant 6 hesitated and assumed that the federal government does not share as much information, he continued to "trust" that the information would arrive if it was a threat. Participant 8 further stated that he did not feel that the FBI shares as much information as other agencies do, but he thinks they would share important threat information with the fusion center if it was "necessary." Participant 8 also stated:

> When I need something in my everyday operations in logistics, I pick up the phone and make calls to the right people. When everyone at the BRIC creates their reports, they must be getting their information from the right people. They must have the same type of system.

Theme 5: Changes to Information Sharing Policy as a Result of the Boston Marathon Bombing

All of the participants except for one of them discussed some information sharing policy changes or a desire for information sharing policy changes as a result of the

Boston Marathon Bombing. Participant 5 stated that he was “not aware of any” policy changes. Participants 1 and 2 highlighted the use of social media. Participant 1 shared:

> Social media use and social media policy changed. I know the commission wanted high level ranking officers to have social media accounts, Twitter accounts, and stuff like that to get stuff out. We developed a policy for media relations afterwards because we have some examples of fake news getting out about incidents, arrests, or threats that were not true.

Participant 2 shared that social media currently is used by intelligence officers at the BRIC prior to large events to determine if there are any HVE or counterterrorism threats being discussed. Participant 2 referred to it as an informal policy change. Participant 2 elaborated:

> There is someone who does strictly social media information “snooping” so, you know, sometimes we'll hear of an event going on, it could be a potential for violence and we'll ask her to snoop around on social media. Whether it's informal, or, you know, just to be made aware of the numbers [of attendees], you know, at the rallies, and protests, and marches and all that stuff. They're not sanctioned with permits, you know, so it's, how do we find out on my end -- how do we find out like how many officers we need for any given event? That's what I do for work, and so in order to figure that out, it's like, go to social media where you know everything's posted and that's how people are getting together. So, I don't want to call it informal, it's funny that, that's how we're gaining information these days.

Participants 1 and 3 explained that since the bombing, interagency planning exercises have been implemented. Participant 3 said, "We participate in interagency exercises for active shooter events, and other operational scenarios." This policy change includes an interagency agreement and funding with a federal agency, and incorporates a scenario, such as a shooting, bombing, or a large-scale explosion.

Participant 3 highlighted that he felt that there has been "more community outreach with the private sector, universities, [and] local government in the Boston area" since the bombing. Participants 3 and 6 indicated that they received increased intelligence bulletins from the BRIC since the bombing, noting that Special Bulletins are received before special events. One reason that may have occurred is that since the bombing, Participants 3 and 7 explained that the BRIC received additional funding and personnel and the BRIC became its own Bureau within the department.

Participant 8 shared that he desired a "structured" decision-making policy change to enact for use during incidence response. For instance, he explained that due to the level of hierarchy in the department during the response phase after the Boston Marathon Bombing, he still had several levels of seniority over him which he felt "got in the way" to how he was able to do his job. He noted that the information sharing between his role and other agencies was cut-off because he was not receiving information about the decision-making process and how to go forward. Because his role was related to crime scene preservation, he said the FBI "took control quickly" and he did not know who to listen to. He offered that an internal policy change was needed prior to another incident occurring. Further, he said:

> I guess I've learned to be more interactive with the commands, with the higher up command in the department as opposed to the lower level. Like, getting information from them or giving information to them. Getting front information from them has been more effective for me and has been something that I have personally implemented since the marathon. This has helped me in operational times for the whole department because I can directly implement what is instructed instead of waiting around. I think this should be changed officially in writing for emergency scenarios.

Participant 7 shared that as a result of the changes made since the bombing, more threat information is shared within the department, weekly intelligence bulletins are received "instead of monthly bulletins" and many in the department have an "awareness" of what HVEs are now that did not know prior to the bombing.

Summary

The purpose of this qualitative study was to gain an understanding of the level of law enforcement information sharing in homegrown violent extremism cases using the Boston Marathon Bombing as a case study. Eight study participants were interviewed one-on-one using Zoom as a platform. An interview protocol with open ended questions was used to guide each interview and addressed the three research questions. Five themes resulted from the analysis of the data.

This study illustrates how contingency theory explains the counterterrorism law enforcement information sharing process for HVE cases. Donaldson's (2001) concepts of examining the organization and environment through the lens of contingency theory with

this case study was applied. As aligned with the literature review, (Bersani 2014; Pelfrey, 2014; Thomas, 2016) study participants identified several information sharing methods that were used while planning for the Boston Marathon within Theme 1. Within Theme 2, additional information sharing methods were identified that the participants used during or after the Boston Marathon Bombing. Themes 1 and 2 exemplify the environmental factors of contingency theory as they illustrate how counterrorism information is shared between law enforcement agencies (Roberts, et al., 2012).

The study participants identified contingencies, or barriers, to the information sharing process within Theme 3. The barriers that participants recognized were clearly aligned with previous literature (Carney; 2015; Dawes; 1996; Peled, 2016; Roberts, et al., 2012) and are an integral part of contingency theory. Donaldson (2001, 2006) indicates that the contingencies (or barriers) to information sharing will reduce the level of success of the law enforcement agency. To apply this premise of contingency theory, the barriers that the participants identified can be seen as reducing the level of counterterrorism law enforcement information sharing (Donaldson 2001, 2006).

Theme 4 relates to the fact that all of the participants trusted and relied that the right threat information would be shared with them because resources, such as the BRIC, were put in place. The notion identified within Theme 4 is considered a contingent (Donaldson 2001, 2006) because it can be seen as reducing the law enforcement agency's success if information sharing is not actively being implemented to reduce HVEs. Instead, the participants expressed that they were relying on the threat information to be shared with them. As Donaldson (2001, 2006) identified, and which aligned with the

findings that were evident in this study within Theme 5, the participants explained that after the bombing, organizational changes and information sharing changes were implemented. Theme 5 specifically aligns with contingency theory as it shows how the law enforcement agency sought to increase its terrorism and/or HVE prevention success by implementing policy changes, adding education and training programs, and other desired changes for the future (Donaldson 2001, 2006; Roberts, et al., 2012; Zhao et al., 2010).

In Chapter 4, the study's setting, research questions, demographics of the participants, data collection and analysis procedures, evidence of trustworthiness, the results, and a summary was provided. In Chapter 5, I will interpret these findings and incorporate them into my conceptual framework. I will also include the limitations of my study, describe recommendations for future research, the potential impact for social change, and a conclusion.

Chapter 5: Discussion, Conclusions, and Recommendations

Summary

The purpose of this qualitative study was to gain an understanding of law enforcement counterterrorism information sharing in HVE cases. The Boston Marathon Bombing was used as a case study in order to examine how information was shared between local, state, and federal law enforcement agencies. HVEs are difficult to detect and predict; therefore, understanding the information sharing process among law enforcement agencies with these cases is of the utmost importance. This study yielded five major themes related to information sharing in this HVE case at the local, state, and federal law enforcement levels. The first theme includes the methods of information sharing used prior the Boston Marathon Bombing. Theme 2 includes the methods of information sharing both during and after the bombing. The third theme encompasses the real and perceived barriers to information sharing in HVE cases. Within the fourth theme, participants identified that there is a trust or reliance that information is or will be shared if there is a HVE or counterterrorism related threat within their jurisdiction. The fifth theme incorporates the information sharing policy changes or desired policy changes as a result of the Boston Marathon Bombing.

In this chapter, I review the theoretical framework of contingency theory and how it relates to the themes identified in my study. An overview of one additional potential limitation to the study is provided that was not already identified in Chapter 1. A discussion on recommendations for future research is offered as well as a discussion on how they relate to the current literature on the topic of HVE information sharing in law

enforcement agencies. Implications for positive social change are described in an effort for actionable takeaways to be a result of this study. Finally, a conclusion is provided.

Interpretation of Findings

This study offers insight into the procedures that law enforcement agencies take to share information related to counterterrorism and HVE related threats with each other at the same agency and with outside agencies at the local, state, and federal levels. The literature review highlighted that methods of detecting violent extremist behavior in HVEs can likely be done through policing activities like community policing, the use of information sharing among agencies in fusion centers, and though use of various forms of technology (Cohen 2016; Davies, 2016; LaFree & Bersani, 2014) within Themes 1 and 2. This study identified that community policing was utilized prior to the bombing by some participants. As Thomas (2016) presented in his research, local law enforcement agency's relationships with their community, which includes academia, local businesses, religious groups, and private citizens, can have tremendous importance in obtaining terrorist threat information from suspicious behaviors that may not otherwise be achieved (Chermak et al., 2013).

The use of fusion centers, such as the BRIC, was used as an information sharing mechanism before, during, and after the bombing by most study participants and was identified as a "unique" information sharing tool in the literature (Peled, 2016). In fact, prior to the bombing several participants highlighted that the BRIC disseminated reports and sent emails in preparation for the Boston Marathon, after the bombing, and it is continually used as a method of reliance for threat information dissemination. It is

notable that if the participants were relying on their information from the BRIC prior to the Boston Marathon and continue to rely on information too heavily from one source, but state and federal agencies are not adequately sharing terrorism or HVE information than an information sharing gap will remain (Bjelopera, 2014; Foley, 2016; Inspectors General, 2017). Based on the participants' reported understanding, they identified that federal, state, and other local law enforcement agencies shared HVE information through the BRIC.

While Theme 2 highlighted methods of information sharing during and after the Boston Marathon Bombing, it illustrated another finding. A noteworthy finding in Theme 2 was that communications equipment, specifically police radios, used for information sharing among federal, state, and local law enforcement agencies had a lack of interoperability. This notion was not addressed within the literature review but is highlighted in Dawes's (1996) study as "incompatible technologies" (pg. 378) and is explained as a barrier to interagency information sharing. In Dawes's study, this information sharing barrier referenced computer hardware and software, but it presents the same type of implication.

As illustrated within Theme 3, barriers to information sharing, participants identified four barriers to information sharing that align with the literature review. These include lack of a security clearance that makes classified threat information unable to access by those at the agencies without a security clearance. Additionally, participants relayed that they felt state and federal law enforcement agencies were less likely to share HVE threat information with local law enforcement agencies. This belief was aligned

with findings that were highlighted in the literature review. Carney (2015) suggested that strengthening trust among federal, state, and law enforcement agencies may bridge the gap in information sharing (Peled, 2016). Another barrier found was that agencies are territorial with any case related information and do not like to share specific details of cases with each other. Furthermore, it was determined that a "power struggle" exist between federal law enforcement agencies about sharing their information with local law enforcement agencies. A resistance to share case related information and a bureaucratic power struggle were determined to be counterterrorism information sharing gaps in the Inspector General's (2017) study. The resistance to change organizational procedures of information sharing (Peled, 2016) by sharing counterterrorism or HVE information on an interagency level will only continue to increase the risk of future attacks (DHS, 2015b).

One barrier found in this case study that was not highlighted in the literature review was that police officers in the participating agency may not be opening their emails that contain the threat information from the BRIC, even though it is sent to them. This barrier provides an opportunity for further exploration given that the participants shared that they rely on the information disseminated by the BRIC as their threat information shared by federal and state law enforcement agencies.

Contingency Theory Applied

An additional purpose of this study was to build upon previous literature which identified that there was a gap in information sharing with HVE cases and provide recommendations on how to reduce the barriers to share information among law enforcement agencies at the local, state, and federal levels. As identified in contingency

theory, when an agency is faced with an external contingent such as a terrorist attack, it will adapt and determine a resolution to increase its performance (Donaldson, 2001, 2006). Based on the theoretical principals of contingency theory, this law enforcement agency reacted and adapted to the barriers that they identified and implemented policy changes (Roberts, 2012).

The local law enforcement agency realized gaps based on the HVE attack, the Boston Marathon Bombing, whereby there was no previous knowledge inside the local law enforcement agency of the bombers themselves. Within Theme 5, the participants indicated that they presently conduct interagency training exercises whereby they simulate a terrorism event and respond to it using their equipment, communication technology, and other means to practice their capabilities to respond to an event with interagency law enforcement partners. They also said that additional funding was provided to the BRIC. Additionally, the participants relayed that they receive department wide HVE specific education and training. It was noteworthy that several of the participants had never heard the term homegrown violent extremist or HVE prior this study, even though they specialized in counterterrorism law enforcement, and they were involved in the response to the Boston Marathon Bombing.

An additional recommendation was made by a participant to implement a formal policy for a decision-making protocol in the event that a future HVE or terrorism related incident occurs. This participant highlighted that during the Boston Marathon Bombing, there was a breakdown in interagency communication and a lack of understanding of which agency had the right to the make the decisions and give the orders. This

recommendation aligns with Horgan's (2014) suggestions regarding creating HVE law enforcement information sharing policies that can be implemented in an operational capacity. However, it is highlighted that because the issue of HVE and counterterrorism is an operational issue with multiple law enforcement agencies that have similar missions that the best approach is to share information using relationships (Inspectors General, 2017). Finally, it was noted that social media policy changes were implemented as a result of the bombing. For instance, this policy was made such that only those in a leadership position are authorized to make social media posts related to agency business.

Limitations of the Study

A limitation of the study can be seen as the lack of gender diversity of study participants. Specifically, there was one female participant that responded. Hill et al. (2022) illustrated that since 1980, even though police departments across the country have maintained a goal to increase the number of female police officers, there is a gender gap in policing as a whole, promotion rates, and those that represent specialized units. Within their study on wage and gender in law enforcement agencies, Lou et al. (2019) found that even in those agencies where women are represented at a more statistically equal level as men, there remains a pay disparity among women. These two reasons highlight that because there is a gender gap in the law enforcement profession that having one female study participant is a meaningful addition to the study.

Another potential limitation to the study is that it was focused on one specific case, which was the Boston Marathon Bombing and included participants who prepared for the Boston Marathon and responded to the Boston Marathon Bombing. However, it

should be noted that this type of limitation is inherently common in qualitative studies. This study offers a deep understanding of the knowledge of the information sharing process as it pertains to HVE cases, which can be applied to the understanding of those processes in other law enforcement jurisdictions. Finally, a potential limitation to the study can be seen as the number of study participants. While there were eight study participants, as noted in Chapter 1, saturation was reached when no new data elements were being identified (Miles & Huberman, 1994). In their discussion on qualitative study sample size saturation, Fusch and Ness (2015) indicated that it is not the number of study participants, but when there is enough information collected to "replicate the study" that saturation is complete.

Recommendations

Three recommendations were identified as a result of this case study. The first is to replicate this study by completing a similar case study to confirm the themes and determine if additional themes would be identified. As continually highlighted by Wray (2020), HVEs are difficult to detect prior to an attack, and without information coordination among law enforcement agencies at the local, state, and federal levels, they will remain undetected. A future study designed to replicate the themes and determine if additional themes are identified, will assist in improving the coordination efforts among law enforcement agencies. It is vital to continue this research, and in doing so, it can help detect and prevent future HVE attacks.

A second recommendation is to build upon the fourth theme of trust and reliance that was identified by the study participants for future research. Examining the theme of

trust and reliance that counterterrorism and HVE threat information is shared among law enforcement agencies as identified in this case study can be a topic for future research. While HVE information sharing was previously identified as a gap among law enforcement agencies in the literature review (Carney, 2015; Foley, 2016; Peled, 2016), if those agencies are trusting and relying that the information will be shared with them when the threat becomes realized, without any action taken on their part, that is an additional gap identified in the information sharing process.

A third recommendation is to conduct a case study using participants at a fusion center. According to the DHS, a fusion center is owned and operated by states for the purpose of "the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTT), federal and private sector partners" (DHS, 2022). This study illustrated that the participants used the bulletins and read the emails before the Boston Marathon Bombing that they received from the BRIC. They recurrently mentioned the BRIC as where they received their threat information, and that is also where the information sharing occurs from interagency law enforcement personnel with or without a security clearance. Finally, the participants indicated that they trusted that if there was a threat, that they would receive it from someone at the BRIC. Therefore, a study using participants from a fusion center similar to the BRIC would be extremely useful in determining how information is shared and disseminated to various law enforcement agencies as it pertains to HVE cases.

Implications

Preventing domestic terrorism remains the highest domestic priority for the FBI (Wray, 2020). It is because of this that the identification of HVEs and sharing the information with the correct law enforcement jurisdiction is vital to ensuring the homeland security of the United States. Peled (2016) identified that one of the tools that was created by legislators as a result of interagency information sharing gaps post 09/11 was fusions centers. Chermak et al. (2013) explained that the purpose of fusion centers, such as the BRIC, is to share information among federal, state, and local law enforcement agencies in order for those agencies to disseminate the information to their respective personnel. The participants in this study repeatedly mentioned their reliance on the BRIC to provide them with HVE and terrorism threat information. In their review of the "lessons learned" from the Boston Marathon Bombing, the House of Representatives (2014) found that there were information sharing gaps between the FBI and the local police department. They further explained that when the Russian government provided the FBI with potential information about a U.S. citizen radicalizing overseas and traveling back to the United States, specifically in Boston, the FBI did not share that information with the local law enforcement agency (House of Representatives, 2014).

This study illustrated that information sharing gaps remain that were identified in the literature review, specifically related to the participants that did not feel that information was shared with them from federal law enforcement agencies because of a lack of trust (Carney, 2015) and a power struggle (Dawes, 1996; Peled, 2016). The participants shared that what continued to be information sharing gaps for the study

participants occurred both during the 2013 timeframe at the Boston Marathon Bombing and during their interviews in 2021. Establishing an increased community policing program at the federal, state, and local level without a targeted population in mind is a method to build trust in the community (Thomas, 2016) and can build a positive social change in the jurisdiction (Davies, 2016). Because HVEs are difficult to detect, implementing a community driven approach to learn what behaviors stand out from typical behaviors is both an academic field of study and a federal level plan to reduce violent extremism (Davies, 2016; *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*, 2016). This community policing process can also lead to working group discussions with academia and private organizations and provide access to build relationships with the community in an effort to ensure that if a threat was identified that one of these partners would report it to the appropriate law enforcement agency. Building on community policing and extending the approach to educating the community (Combs, 2017) to report back to the law enforcement agency if they see suspicious behaviors, builds on the literature and the DHS campaign, *If You See Something, Say Something* (Davies, 2016).

Information sharing recommendations like this at its most basic level can be provided to decision makers at local and state law enforcement jurisdictions. Working toward approaches that offer trust between agencies will build communities that may rely on their networks to share information if violent extremist views are identified (Davies, 2016; Heydemann, 2014). The participants indicated that after the Boston Marathon Bombing, their local law enforcement agency implemented HVE education and exercise

scenarios geared toward the response of an attack. As Foley (2016) notes, agencies that have a counterrorism response role experience challenges when they are confronted with new contingencies. As contingency theory explains, in order to be successful at information sharing, agency behavior and policy also needs to change related to information sharing (Davison, 2001). The FBI identified that HVEs are the "single greatest threat to the homeland," (Wray, 2020) and it is because of that threat that each level of law enforcement maintains a continued mission of sharing potential threats with each other.

Conclusion

This study provided a further inquiry into public policy issue of law enforcement interagency sharing post 09/11. It confirmed the previous academic research on law enforcement information sharing in HVE cases. It also illustrated how contingency theory is relevant and how the law enforcement agency adapted when the external factor of the Boston Marathon Bombing caused it to adapt through implementing changes (Donaldson, 2006). This study also provides an addition to the body of research by illustrating that the participants may not be actively engaging in information sharing or seeking threat information from outside law enforcement agencies because they trust or rely that it will be shared with them.

References

Berkley, G. (1970). Centralization, democracy and the police. *Journal of Criminal Law and Criminology, 61*(2), 309-312. https://doi.org/10.2307/1142225

Beydoun, K. (2018). Lone wolf terrorism: Types, stripes, and double standards. *Northwestern University Law Review Online,* 112, 187-215. https://doi.org/10.5937/bezbednost1801112k

Bjelopera, J. (2014). *Countering violent extremism in the United States* (CRS Report No R42553). https://doi.org/10.4135/9781452287508.n93

Brand, M., Kerby, D., Elledge, B., Johnson, D., Magas, O. (2006). A model for assessing public health emergency preparedness competencies and evaluating training based on local preparedness plan. *Journal of Homeland Security and Emergency Management, 3*(2), 1-19. https://doi.org/10.2202/1547-7355.1182

Burruss, G., Giblin, M. & Schafer, J. (2010). Threatened globally, acting locally: Modeling law enforcement homeland security practices. *Justice Quarterly, 27*(1), 77-101. https://doi.org/10.1080/07418820902763053

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report, 21*(5), 811-830. https://doi.org/10.46743/2160-3715/2016.

Chan, J., Logan, S., & Bennett Moses, L. (2022). Rules in information sharing for security. *Criminology & Criminal Justice, 22*(2), 304322. https://doi.org/10.1177/1748895820960199

Chermak, S., Carter, J., Carter, D., McGarrell, E., & Drew, J. (2013). Law enforcement's information sharing infrastructure: A national assessment. *Police Quarterly 16*(2), 211-244. https://doi.org/10.1177/1098611113477645

Cohen, J. D. (2016). The next generation of government CVE strategies at home: Expanding opportunities for intervention. *The American Academy of Political and Social Science, 668*(1), 118-128. https://doi.org/10.1177/0001726669933

Combs, C. (2017). *Terrorism in the twenty-first century*. Routledge. https://doi.org/10.4324/9781315617053

Comey, J. W. (2014). Statement before the House Homeland Security Committee. Worldwide threats to the Homeland. https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland

Creswell, J. W. (2009). *Qualitative, quantitative and mixed methods approaches.* (3rd ed.). Sage. https://doi.org/10.4324/9781003103141-33

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches*. (3rd ed.). Sage. https://doi.org/10.1086/317417

Creswell, J. W., & Creswell, J. D. (2018). *Research design: qualitative, quantitative, and mixed* methods *approaches.* (5th ed). Sage. https://doi.org/10.1002/nha3.20258

Creswell, J. W., Vicki, L., & Clark, P. (2011). *Designing and conducting mixed method research*. (2nd ed.). Sage. https://doi.org/10.1111/j.1753-6405.2007.00096.x

Davies, L. (2016). Wicked problems: How complexity science helps direct education responses to preventing violent extremism. *Journal of Strategic Security, 9*(4), 32-52. https://doi.org/10.5038/1944-0472.9.4.1551

Davis, L., Helmus, T., Hunt, P., Payne, L., Jahedi, S., & Tsang, S. (2016). Assessment of state and local anti-terrorism training (slatt) program. RAND Corporation. https://doi.org/10.7249/rr1276

Dawes, S. (1996). Interagency information sharing: Expected benefits, manageable risks. *Journal of Public Analysis and Management, 15*(3), 377-395. https://doi.org/10.1002/(sici)1520-6688(199622)15:3%3C377::aid-pam3%3E3.0.co;2-f

Department of Homeland Security. (n.d.). *Homeland Security Information Network*. https://www.dhs.gov/homeland-security-information-network-hsin

Department of Homeland Security. (n.d.) *If You See Something, Say Something*. https://www.dhs.gov/see-something-say-something/about-campaign

Department of Homeland Security. (2015a). *National preparedness goal*. Washington, D.C.

Department of Homeland Security. (2015b). Preventing terrorism overview. https://www.dhs.gov/topic/preventing-terrorism-overview

Department of Homeland Security. (2016). History. https://www.dhs.gov/history

Donaldson, L. (2001). The contingency theory of organizations. Sage. https://doi.org/10.4135/9781452229249

Donaldson, L. (2006). The contingency theory of organizational design: challenges and opportunities. In: Burton R.M., Håkonsson D.D., Eriksen B., Snow C.C. *Organizational design: The evolving state-of-the-art*, (19-40). Springer. https://doi.org/10.1007/0-387-34173-0_2

Drake, D. B., Steckler, N. A., & Koch, M. J. (2004). Information sharing in and across government agencies: The role and influence of scientist, politician, and bureaucrat subcultures. *Social Science Computer Review*, *22*(1), 67–84. https://doi.org/10.1177/0894439303259889

Executive Office of the President. (2011). *National Strategy for Counterterrorism*. Washington, DC: Office of the Press Secretary. https://obamawhitehouse.archives.gov/sites/default/files/counterterrorism_strategy.pdf

Fiedler, F. E. (1964). A theory of leadership effectiveness. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology, 1*, 149-190. https://doi.org/10.1126/science.147.3654.140

Flinn, C. (2016). As support materializes: An examination of contemporary policy in the prosecution under the material support statutes during the current wave of terrorism. *Homeland Security Review, 5*, 79-82. https://www.govinfo.gov/content/pkg/CHRG-108shrg95100/html/CHRG-108shrg95100.htm

Foley, F. (2016). Why inter-agency operations break down: US counterterrorism in comparative perspective. *European Journal of International Security, 1*(2), 150-175. https://doi.org/10.1017/eis.2016.10

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The qualitative report, 20*(9), 1408-1416. https://doi.org/10.46743/2160-3715/2015.2281

Fusion Centers. (2022, October 17). Department of Homeland Security. https://www.dhs.gov/fusion-centers

Giblin, M., Burrus, G., & Schafer, J. (2014). A stone's throw from the metropolis: Re-examining small-agency homeland security practices. *Justice Quarterly, 31*(2), 368-393. https://doi.org/10.1080/07418825.2012.662993

Gunaratna, R. & Haynal, C. (2013). Current and emerging threats of homegrown terrorism: The Case of the Boston bombings. *Perspectives on Terrorism, (7),* 3-6. https://doi.org/10.4324/9781315039626-12

Hancock, D., & Algozzine, B. (2015). *Doing case study research: A practical guide for beginning researchers*. Teachers College Press. http://dx.doi.org/10.1353/csd.2007.0003

Haynes, M. & Giblin, M. (2014). Homeland security risk and preparedness in police agencies: the insignificance of actual risk factors. *Police Quarterly, 17*(1), 30-53. https://doi.org/10.1177/1098611114526017

Hewitt, C. (2014). Law enforcement tactics and their effectiveness in dealing with American terrorism: organizations, autonomous cells, and lone wolves. *Terrorism and Political Violence, 26*(1), 58-68. https://doi.org/10.1080/09546553.2014.849913

Heydemenn, S. (2014). Countering violent extremism as a field of practice. *United States Institute of Peace Insights, Spring(1),* 1-11. https://www.usip.org/sites/default/files/Insights-Spring-2014.pdf

Hill, L., Theriault, J., Cherry, T., & Stiver, W. (2022). Is a seat at the table sufficient? Specialized unit participation and perspectives of female law enforcement officers, *Police Practice and Research, 23*(5), 569-583. https://doi.org/10.1080/15614263.2021.2022481

Hoffman-Miller, P. M. (2014). Contingency theory. *Encyclopedia of Theory*. Sage. https://doi.org/10.4135/9781446273050145341 79

Homeland Security Act of 2002. (Public Law 107-296). https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf

Horgan, J. (2014). Countering violent extremism field vs. practice. *United States Institute of Peace Insights, (1),* 2-3. https://www.usip.org/sites/default/files/Insights-Spring-2014.pdf

House of Representatives. (2014). The road to Boston: Counterterrorism challenges and lessons from the marathon bombings. House Homeland Security Report. https://homeland.house.gov/files/documents/Boston-Bombings-Report.pdf

Information sharing environment – functional standard – suspicious activity reporting, version 1.5.5. https://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf

Inspectors General of the Intelligence Community, Department of Homeland Security and Department of Justice. (2017). Review of domestic sharing of counterterrorism information. https://oig.justice.gov/reports/2017/a1721.pdf

Inserra, D. (2015). 68th terrorist plot calls for major counterterrorism reforms. *The Heritage Foundation, 4408*. http://www.heritage.org/terrorism/report/68th-terrorist-plot-calls-major-counterterrorism-reforms

Intelligence Reform and Terrorism Prevention Act of 2004. (Public Law 108-458). https://www.congress.gov/bill/108th-congress/senate-bill/2845

Jackson, B., Burgette, L., Stevens, C., Setodji, C., Herberman, E., Kovalchik, S., Mugg, K, Cahill M., & Traub, J. (2017). Knowing more, but accomplishing what? Developing approaches to measure the effects of information-sharing on criminal justice outcomes. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/corporate_pubs/CPA600/CPA614-4/RAND_CPA614-4.pdf

Kassap, N. (2013). Rivals for influence on counterterrorism policy: White House political staff versus executive branch legal advisors. *Presidential Studies Quarterly, (43)*2, 252-273. https://doi.org/10.1111/psq.12023

Korstjens, I. & Moser, A. (2018) Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing, *European Journal of General Practice, 24*(1),120-124. https://doi.org/10.1080/13814788.2017.1375092

LaFree, G. & Bersani, B. (2014). County-level correlates of terrorist attacks in the United States, *Criminology & Public Policy, 13*, 455 - 481. https://doi.org/10.1111/1745-9133.12092

Lewis, A. R. (2014). *The American culture of war: A history of US military force from World War II to Operation Enduring Freedom*. Routledge. https://doi.org/10.4324/9781315544021-15

Lincoln, Y.S. & Guba, E.G. (1985). Naturalistic inquiry. Sage. https://doi.org/10.1016/0147-1767(85)90062-8

Luo, X. I., Schleifer, C., & Hill, C. M. (2019). Police income and occupational gender inequality. *European Journal of International Relations*, *22*(4), 638–661. https://doi.org/10.1177/1098611119862654

Malhotra, N. K. (2012). Basic marketing research: Integration of social media. Pearson. https://doi.org/10.2139/ssrn.2655449

Miles, M.B., & Huberman, A.M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Sage. https://doi.org/10.1016/s1098-2140(99)80125-8

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Sage. https://doi.org/10.1080/10572252.2015.975966

Miller, G. (2013). Terrorist decision making and the deterrence problem. *Studies in Conflict & Terrorism*, *36*(2), 132-151. https://doi.org/10.1080/1057610x.2013.747075

Nowrasteh, A. (2016). Terrorism and immigration: A risk analysis. *Cato Institute Policy Analysis*, *798*, 1-26. https://doi.org/10.1163/2210-7975_hrd-9985-2016007

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed

method implementation research. *Administration and policy in mental health*, *42*(5), 533-44. https://doi.org/10.1007/s10488-013-0528-y

Patton, M. Q. (2002). *Qualitative research & evaluation methods* (3rd ed.). Sage. https://doi.org/10.1177/10928102005003006

Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Sage. https://doi.org/10.4324/9781315664972-14

Peled, A. (2016). Coerce, consent, and coax: A review of U.S. Congressional efforts to improve Federal counterterrorism information sharing. *Terrorism and Political Violence, 28*(4), 674-691. https://doi.org/10.1080/09546553.2014.924410

Parker, T. (2014). Countering violent extremism field vs. practice. *United States Institute of Peace Insights, (1),* 2-3. https://www.usip.org/sites/default/files/Insights-Spring-2014.pdf

Pelfrey, W. (2014). Policing in an omnicultural environment: Population heterogeneity and terrorism prevention. *Criminology & Public Policy, 13*(3), 483-491. https://doi.org/10.1111/1745-9133.12103

Perliger, A., Koehler-Derrick, G., & Pedahzur, A. (2016). The gap between participation and violence: Why we need to disaggregate terrorist profiles. *International Studies Quarterly, 60*(2), 220-229. https://doi.org/10.1093/isq/sqv010

Randol, B. (2013). An exploratory analysis of terrorism prevention and response

preparedness efforts in municipal police departments in the United States: which agencies participate in terrorism prevention and why? *The Police Journal*, 86, 158-181. https://doi.org/10.1350/pojo.2013.86.2.618

Randol, B. (2012). The organizational correlates of terrorism response preparedness in local police departments. *Criminal Justice Policy Review*, *23*(3), 304-326. https://doi.org/10.1177/0887403411400729

Roberts, A., Roberts, J. & Leidka, R. (2012). Elements of terrorism preparedness in local police agencies, 2003-2007: An impact of vulnerability, organizational characteristics, and contagion in the post-9/11 era. *Crime & Delinquency*, *85*(5), 720-747. https://doi.org/10.1177/0011128712452960

Saldana, J. M. (2016). *The coding manual for qualitative researchers* (4th ed.). Sage, 569-583. https://doi.org/10.46743/2160-3715/2009.2856

Senate Committee on Homeland Security and Governmental Affairs. (2013, November, (14). Threats to the homeland. Senate Hearing, 113-426. Washington, Government Printing Office.

Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States (2016, October 17). https://www.dhs.gov/sites/default/files/publications/2016_strategic_implementation_plan_empowering_local_partners_prev.pdf

Sullivan, J. & Bauer, A. (2008). Terrorism early warning: 10 Years of achievement in fighting terrorism and crime. LA, CA: Los Angeles Sheriff's Department.

Testimony before the Senate Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations, ISIL online: Countering terrorist radicalization and recruitment on the internet and social media. (2016, July 6). (testimony of Michael Steinback, Executive Assistant Director, National Security Branch, Federal Bureau of Investigation). https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-

Thomas, G. (2016). A case for local neighborhood policing and community intelligence in counter terrorism. *The Police Journal: Theory, Practice and Principles, 89*(1), 31- 54. https://doi.org/10.1177/0032258x16630489

Waxman, M. (2012). National security federalism in the age of terror. Stanford Law Review, 64(2), 289-350. https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1883&context=faculty_scholarship

Weiman, G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research, 3*(2), 75-90. https://doi.org/10.15664/jtr.405

Wilber, D. (2016, July 14). The FBI investigated the Orlando mass shooter for 10 months — and found nothing. Here's why. The LA Times. https://www.latimes.com/nation/la-na-fbi-investigation-mateen-20160712-snap-story.html

Woodward, J. (1965). *Industrial organization: theory and practice*. Oxford University Press. https://doi.org/10.2307/2520605

Wormeli, P. (2014). Developing policies for countering terrorism. *Criminology & Public Policy*, *13*(3), 493-497. https://doi.org/10.1111/1745-9133.12098

Yin, R. (2012). A (very) brief refresher on the case study method. Applications of case study research, pp. 3-20. Sage. https://doi.org/10.3138/cjpe.26.008

Wray, C. (2020). Statement before the House Homeland Security Committee. Worldwide threats to the Homeland. https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-091720

Zhao, J., Ren, L., & Lovrich, N. (2010). Police organizational structures during the 1990s: An application of contingency theory. *Police Quarterly*, *13*, 209-232. https://doi.org/10.1177/1098611110365691