Understanding Law Enforcement Intelligence Processes

Report to the Office of University Programs, Science and Technology Directorate, U.S. Department of Homeland Security

July 2014

National Consortium for the Study of Terrorism and Responses to Terrorism
A Department of Homeland Security Science and Technology Center of Excellence
Based at the University of Maryland

8400 Baltimore Ave., Suite 250 •College Park, MD 20740 • 301.405.6600
www.start.umd.edu

About This Report

The authors of this report are David Carter, Ph.D., Michigan State University; Steve Chermak, Ph.D., Michigan State University; Jeremy Carter, Ph.D., Indiana University-Purdue University Indianapolis; Jack Drew, Michigan State University. Questions about this report should be directed to infostart@start.umd.edu.

This report is part of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) project, "Factors impacting the U.S. Intelligence Process."

This research was supported by the Department of Homeland Science and Technology Directorate's Office of University Programs through Award Number 2012-ST-061-CS0001, Center for the Study of Terrorism and Behavior (CSTAB) 2.13 made to START to investigate the understanding and countering of terrorism within the U.S. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security or START.

About START

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is supported in part by the Science and Technology Directorate of the U.S. Department of Homeland Security through a Center of Excellence program based at the University of Maryland. START uses state-of-the-art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and social and psychological impacts of terrorism. For more information, contact START at infostart@start.umd.edu or visit www.start.umd.edu.

Citations

To cite this report, please use this format:

Carter, David, and Steve Chermak, Jeremy Carter, Jack Drew. "Understanding Law Enforcement Intelligence Processes," Report to the Office of University Programs, Science and Technology Directorate, U.S. Department of Homeland Security. College Park, MD: START, 2014.

Contents

Executive Summary

The September 11th attacks impacted society generally, and law enforcement specifically, in dramatic ways. One of the major trends has been changing expectations regarding criminal intelligence practices among state, local, and tribal (SLT) law enforcement agencies, and the need to coordinate intelligence efforts and share information at all levels of government. Despite clear evidence of significant changes, very little research exists that examines issues related to the intelligence practices of SLT law enforcement agencies. Important questions on the nature of the issues that impact SLT intelligence practices remain.

While there is some uncertainty among SLT law enforcement about current terrorism threats, there is certainty that these threats evolve in a largely unpredictable pattern. As a result there is an ongoing need for consistent and effective information collection, analysis and sharing. Little information is known about perceptions of how information is being shared between agencies and whether technologies have improved or hurt information sharing, and little is known about whether agencies think they are currently prepared for a terrorist attack, and the key factors distinguishing those that think they are compared to those who do not. This study was designed to address these issues, and a better understanding of these issues could significantly enhance intelligence practices and enhance public safety.

To develop a better understanding of perceptions about terrorist threats that SLT agencies face and their efforts to prevent terrorism, the research team distributed questionnaires via a web-designed survey to two separate groups of law enforcement personnel. Development of the survey involved several preliminary drafts. Feedback was sought from SLT intelligence workers about question content and coverage, and specifically whether questions were ambiguous or difficult to answer. After making revisions, the final Institutional Review Board approved instrument had 48 structured, semi-structured, or open-ended questions. The survey, despite its length, enabled respondents to share information about issues such as perceptions of terrorist threats, inter-agency interactions, information sharing, intelligence training, and agency preparedness. Additional questions asked about characteristics of the respondent and the respondent's agency. There are three findings that are quite interesting.

First, law enforcement perceptions about what is a serious threat in their community has changed significantly over time. Law enforcement is much more concerned about sovereign citizens, Islamic extremists, and militia/patriot group members compared to the fringe groups of the far right, including Christian Identity believers, reconstructed traditionalists (i.e., Odinists), idiosyncratic sectarians (i.e., survivalists), and members of doomsday cults. In fact, sovereign citizens were the top concern of law enforcement, but the concern about whether most groups were a serious terrorist threat actually declined for most groups (e.g., the KKK; Christian Identity; Neo-Nazis; Racist Skinheads; Extremist Environmentalists; Extreme Animal Rights Extremists).

Second, when examining whether the respondents thought that various agencies and sources were useful in their counterterrorism efforts, the agencies that appear to be most useful to SLT law enforcement include state/local fusion centers, the FBI's Joint Terrorism Task Force(s), the FBI, and DHS Office of Intelligence and Analysis. Overall, the internet and the use of open source materials, human intelligence sources, and the media were perceived as providing the most useful information. Security clearances, adequate personnel, adequate training, adequate resources, adequate time, or the organizational culture were all perceived as barriers for the sharing of intelligence and information across agencies.

Third, several factors impacted whether an agency was prepared for a terrorist attack. Agencies with satisfied working relationships with state organizations were twice as likely to be prepared, agencies that produce threat assessments and risk assessments more frequently are three-and-a-half times more likely to be prepared than agencies who create them less frequently, and the creation of vulnerability assessments also appears to be a predictor of preparedness as they more than quadruple an agency's preparedness likelihood. In addition, as agencies experience problems related to personnel, training, and resources, the likelihood they will consider themselves prepared is reduced by approximately three-fold. Agencies that felt they were not prepared highlighted problems with resources, training, and quality of working relationships with other organizations.

Particularly for practitioners, the most important aspect of this research may not be the findings on the variable analyses, per se, but on the benchmarks identified in trends found in the data. Some clear trends emerged which indicate programmatic successes for information sharing and intelligence, as well as areas where problems remain. When considering these findings in the context of research on organizational development, it is clear that organizational leadership is an important factor for organizational successes in information sharing as well as for preparedness. If the leadership of a law enforcement agency is willing to expend the effort to train personnel, develop partnerships, and participate in state, regional and national information sharing initiatives, then greater levels of success will be achieved. While one would intuitively assume this, the data empirically supports it.

Introduction

The September 11th attacks impacted society generally, and law enforcement specifically, in dramatic ways. One of the major trends has been changing expectations regarding criminal intelligence practices among state, local, and tribal (SLT) law enforcement agencies, and the need to coordinate intelligence efforts and share information at all levels of government. The National Commission on Terrorist Attacks Upon the United States' (2004) "9/11 Commission Report" highlighted that despite the United States' sprawling law enforcement community, very few agencies other than the Federal Bureau of Investigation (FBI) engaged in any type of counterterrorism efforts prior to the attacks. The Commission Report also stressed that enhancing intelligence efforts and improving information sharing were critical to the prevention of terrorist acts.

Law enforcement in the United States is decentralized, which poses incredible challenges in terms of effectively sharing information across jurisdictional boundaries, but such decentralization is also an opportunity. An increasing number of SLT law enforcement agencies have expanded their information collection and intelligence analysis practices, and there have been fundamental changes in the national, state, and local information sharing infrastructure. Despite clear evidence of these dramatic changes (U.S. Department of Homeland Security, 2011; U.S. House of Representatives, 2013), law enforcement's expanded role in counterterrorism, and the acknowledgement that local intelligence is critical to the prevention and deterrence of terrorist acts, very little research exists that examines issues related to the intelligence practices of SLT law enforcement agencies.

The growth of intelligence practices in SLT agencies has coincided with an increasing acknowledgement within federal law enforcement, and in some instances the intelligence community, of the importance of state, local, and tribal law enforcement for enhancing the value of intelligence related to terrorism. The importance of SLT's contribution to the intelligence process can be highlighted in several ways. First, although the FBI is the lead agency for the investigation of terrorism, the types of information provided by various sources and the sheer number of cases and leads requiring follow-up, highlights the importance of involving local law enforcement in terrorist investigations (Davis et al., 2004). Second, it is critical to note that terrorism is a local event, and thus SLT law enforcement is in a unique position to contribute important intelligence because of their knowledge about individuals, groups, and organizations operating in local communities (Carter and Carter, 2009a; 2009b).

In addition, the local nature of terrorism clearly highlights that SLT law enforcement agencies must have access to timely and actionable intelligence for the prevention and response to terrorist acts. Third, critical infrastructures and high-value targets are dispersed widely in the United States, and many of these potential targets are located in rural and less-populated areas. Local law enforcement agencies in these communities are in the best position to recognize when suspicious situations occur near these critical targets. Fourth, survey research indicates that the terrorism experiences and expectations regarding intelligence work of state and local agencies increased after September 11th (Davis et al., 2004). Indeed, the FBI as acknowledged the importance of SLT law enforcement in counterterrorism

efforts through the presence of state and local law enforcement officers who are members of every FBI Joint Terrorism Task Force (JTTF).

Important questions on the nature of the issues that impact SLT intelligence practices remain. While there is some uncertainty among SLT law enforcement about current terrorism threats, there is certainty that these threats evolve in a largely unpredictable pattern. As a result there is an ongoing need for consistent and effective information collection, analysis and sharing. Second, little information is known about perceptions of how information is being shared between agencies and whether technologies have improved or hurt information sharing. Finally, little is known about whether agencies think they are currently prepared for a terrorist attack, and the key factors distinguishing those that think they are compared to those who do not. This study was designed to address these issues, and a better understanding of these issues could significantly enhance intelligence practices and enhance public safety.

Data and Methodology

To develop a better understanding of perceptions about terrorist threats that SLT agencies face and their efforts to prevent terrorism, the research team distributed questionnaires via a web-designed survey to two separate groups of law enforcement personnel. The first group included individuals who had attended trainings through the Memorial Institute for the Prevention of Terrorism (MIPT). A non-profit organization, MIPT was created after the Oklahoma City bombings to increase knowledge about terrorism prevention. In line with this goal it offers traditional and online education programs to law enforcement officers, especially with respect to suspicious activity reporting; to date, 19,000 officers have undertaken these trainings.[1] The research team therefore approached representatives of MIPT with a request to conduct survey research within this population and MIPT subsequently agreed to contact individuals who had registered for its training programs with an invitation to participate in the study.

The second group consisted of individuals who had received training from the School of Criminal Justice at Michigan State University. Funded by the Department of Homeland Security, the Law Enforcement Intelligence Toolbox program operated from 2005 until 2011 with over 4,500 officers from 2,100 agencies enrolling during this time (Carter, 2013). Many of these individuals had been selected by their department to learn how to develop an intelligence capacity. This training provided the resources and information to familiarize participants with important issues surrounding intelligence practices. In relation to the study, this sample is appropriate because it comprises personnel with an understanding of intelligence concepts and requirements, who are aware of organizational efforts to utilize knowledge about law enforcement intelligence.

This research used a purposive sample, therefore there is selection bias; however, it was intended. Comparatively few law enforcement officers have worked with the intelligence process. Even fewer have experience with the newest standards and guidelines. Using a random sample of a broad population of

[1] https://www.mipt.org/

law enforcement officers, generally, would provide no valuable results. As a result, use of this sampling frame provided access to a population wherein the research team knew the respondents had been exposed to both law enforcement intelligence and the current standards and practices.
Persons in both the MIPT and MSU samples had received training using the same national standards and programs. Moreover, both training programs were funded by the Department of Homeland Security which had exacting standards for training course content and approval as well as a requirement that training programs had to be delivered in a manner that was consistent. The value of these factors from a research perspective is that it strengthens internal validity of the measures and external validity to the population of law enforcement officers with contemporary experience in law enforcement intelligence.

Development of the survey involved several preliminary drafts. Feedback was sought from SLT intelligence workers about question content and coverage, and specifically whether questions were ambiguous or difficult to answer. After making revisions, the final Institutional Review Board approved instrument had 48 structured, semi-structured, or open-ended questions. The survey, despite its length, enabled respondents to share information about issues such as perceptions of terrorist threats, inter-agency interactions, information sharing, intelligence training, and agency preparedness. Additional questions asked about characteristics of the respondent and the respondent's agency.

Data collection involved the preparation of a web-based survey and then the transmission of emails to individuals in both samples. In order to preserve the confidentiality of study participants, MIPT distributed emails to the first sample while the research team sent emails to the Toolbox sample. Collection began with an invitation email that outlined the purpose of the research and asked the addressee to complete a self-administered, online questionnaire. It also included a URL that study participants could use to access the online survey. As the study progressed, two sets of follow up emails at monthly intervals were sent.

The number of responses by intelligence workers was 327 for the MIPT sample and 190 responses for the Toolbox sample. However, as the study's unit of analysis is at the agency level, we recorded counts for distinct organizations represented by individuals in both sampling frames. Thus, the research team determined the MIPT sample consisted of 597 target and 179 responding agencies, while the Toolbox sample consisted of 302 target and 124 responding agencies. The response rate was therefore 30.0 percent for the MIPT sample and 40.6 percent for the Toolbox sample. These response rates are promising given response rates to cross sectional surveys have declined (Brick and Williams, 2013) and that police personnel working in intelligence are highly sensitive to responding to questions regarding information sharing practices (Chermak *et al*., 2013). Prior to analysis, submissions were removed where the law enforcement agency name could not be identified. This left 364 responses from individuals who worked at 175 agencies, of which responses for seven agencies were included in both samples.

Demographics

Table 1 shows categorical counts for the sworn status, role, and tenure of the study participants. Most of the MIPT respondents indicated they were sworn officers (66.2%). Many were investigators (39.7%) or analysts (32.4%), and very few held administrative positions (6.9%). Approximately 18 percent of the respondents represented state agencies, 54 percent municipal agencies, and 28 percent represented county agencies. Roughly half of the respondents also reported serving for more than 15 years with their current agency. Conversely, the vast majority of Toolbox respondents were also sworn officers (80%) and most had served for 15 years or more (58.5%). However, most held roles as supervisors (31.3%), investigators (27.3%), or administrators (25.8%).

Table 1: Sworn Status, Role and Tenure within their Agency

	MIPT		Toolbox Training	
	n	Percent[a]	*n*	Percent[a]
Sworn status				
Sworn	151	66.2	108	80.0
Non-sworn	77	33.8	27	20.0
Role				
Administrator	15	6.9	33	25.8
Supervisor	47	21.5	40	31.3
Investigator	86	39.7	35	27.3
Analyst	71	32.4	20	15.6
Tenure				
Less than a year	3	1.3	0	0
1-3 years	16	7.0	2	1.5
4-9 years	57	25.0	20	14.8
10-15 years	52	22.8	34	25.2
More than 15 years	100	43.9	79	58.5

[a] Percentages may not equal 100.0 due to rounding.

Data Measures

Efforts to combat terrorism among state and local law enforcement agencies have been a difficult area to empirically assess. Concerns over security and the sensitivity of information coupled with high fidelity of such practices across agencies has hampered researchers' ability to provide insights on such practices as compared to more traditional aspects of policing. With this in mind, there is value in presenting both descriptive and inferential insights from the data gathered. First, descriptive data is presented about state and local law enforcements' perceptions of threats, information sharing relationships and networked systems. Second, critical factors are identified that lead to the belief that an agency was either "Prepared" or "Not Prepared" for a terrorist attack.

Results

Perceptions of Terrorist Threats

In 2009, Freilich, Chermak, and Simone published results from a Department of Homeland Security (DHS) study that examined several issues, including law enforcement perceptions of terrorist threats in the United States. Data were collected for this research in 2006-2007. One of the goals of the current project was to again ask law enforcement officers about their concerns about several potential terrorist threats by type of group and type of incident. The results from both studies are presented in Tables 2 and 3 for comparative purposes. In Table 2, respondents were asked if they agreed that any of the seventeen extremist groups listed were a serious terrorist threat. In this table, the mean scores are presented on a 4-point scale (1=strongly disagree to 4=strongly agree) and the (rank order) of officer concerns. There are several interesting findings. First, there is wide variation about what groups are perceived to be a serious terrorist threat. Law enforcement is much more concerned about sovereign citizens, Islamic extremists, and militia/patriot group members compared to the fringe groups of the far right, including Christian Identity believers, reconstructed traditionalists (i.e., Odinists), idiosyncratic sectarians (i.e., survivalists), and members of doomsday cults. Second, the major concerns of law enforcement have changed considerably over time. For example, when examining the 2006-07 survey results, law enforcement's top concern was Islamic extremists.

Table 2. Perceived Threat of Extremist Groups by Type of Group

Type of Group	Potential Threat (2013-14)	Potential Threat (2006-07)
Sovereign Citizens	3.20 (1)	2.49 (7)
Islamic Extremists/Jihadists	2.89 (2)	3.13 (1)
Militia/Patriot	2.67 (3)	2.61 (6)
Racist Skinheads	2.58 (4)	2.82 (3)
Neo-Nazis	2.56 (5)	2.94 (2)
Extreme Animal Rightists	2.54 (6)	2.79 (4)
Extreme Environmentalists	2.51 (7)	2.74 (5)
Klux Klux Klan	2.38 (8)	2.47 (8)
Left-Wing Revolutionaries	2.36 (9)	2.04 (13)
Extreme Anti-Abortion	2.36 (9)	2.30 (11)
Black Nationalists	2.34 (11)	2.35 (10)
Extreme Anti-Tax	2.33 (12)	2.47 (8)
Extreme Anti-Immigration	2.33 (12)	2.41 (9)
Christian Identity	2.19 (13)	2.59 (8)
Idiosyncratic Sectarians	2.19 (13)	2.13 (12)
Millennial/Doomsday Cults	2.17 (15)	1.93 (14)
Reconstructed Traditions	2.13 (16)	2.04 (13)

The 2013-14 study results show that law enforcement's top concern is sovereign citizens. Although Islamic extremists remain a major concern for law enforcement, they are no longer their top concern. Approximately 39 percent of respondents agreed and 28 percent strongly agreed that Islamic extremists were a serious terrorist threat. In comparison, 52 percent of respondents agreed and 34 percent strongly agreed that sovereign citizens were a serious terrorist threat. This is interesting because sovereign citizens were ranked as the eighth highest group of concern among the 2006-07 sample. Third, although estimates about some groups were a serious terrorist threat increased comparing the two time periods, (e.g., Left-Wing Revolutionaries; Extreme Anti-Abortion Extremists), the concern about whether most groups were a serious terrorist threat actually declined for most groups (e.g., the KKK; Christian Identity; Neo-Nazis; Racist Skinheads; Extremist Environmentalists; Extreme Animal Rights Extremists).

The change is interesting as there was significant concern about the resurgence of the radical far right (as evidenced by the 2006-07 survey, as well as additional concerns raised after the 2008 election of President Barack Obama), but it appears as though law enforcement is, at present, less concerned about these groups. Such changing perceptions about what is a serious terrorist threat is an important finding because identifying and prioritizing a threat is akin to hitting a moving target and evolves as new intelligence, data, and events develop. Law enforcement must be steadfast in identifying major concerns, substantiating the concerns, providing products and resources to better understand the nature of the threat, and supporting efforts to respond to such concerns.

Table 3 presents findings of the perceived likelihood of various types of terrorist incidents comparing the 2006-07 and 2013-14 survey results. In general, law enforcement perceptions on the likelihood of various types of terrorist incident are similar when comparing the two periods, although their top concerns changed. In the 2006-07 survey, law enforcement officers rated an attack with conventional explosive devices and cyberterrorism as the two most likely events in that order. Although the mean average for cyberterrorism was identical in the 2013-14 survey results, concern about the use of conventional explosive devices declined somewhat. Similarly, the results from the 2013-14 survey show that law enforcement was somewhat less likely to think that most other types of incident were going to occur, compared to the 2006-07 results.

Table 3. Perceptions of Likelihood of Terrorism-Related Crimes by Type of Incident

Type of Incident	Likelihood of Incident (2013-14)	Likelihood of Incident (2006-07)
Cyberterrorism	3.09 (1)	3.09 (2)
Conventional Explosive Devices	2.85 (2)	3.18 (1)
Military Weapons Incident	2.60 (3)	2.50 (5)
Biological	2.37 (4)	2.47 (7)
Agroterrorism (food)	2.35 (5)	2.56 (3)
Agroterrorism (disease)	2.26 (6)	2.56 (3)
Chemical	2.25 (7)	2.50 (5)
Radiological	2.13 (8)	2.13 (8)

Information Sharing Issues

Table 4 presents the findings on whether the respondents thought that the agencies and sources listed were useful to them in their counterterrorism efforts. Respondents were asked their opinions about both specific agencies as well as sources of information. Mean values on a 4-item Likert scale are provided with 4 meaning that the information provided by a type of source or agency was very useful. Overall, the law enforcement respondents thought that the agencies listed were useful or very useful sources of information on counterterrorism issues. There was some variation of usefulness comparing across agency. The agencies that appear to be most useful to SLT law enforcement include state/local fusion centers, the FBI's Joint Terrorism Task Force(s), the FBI, and DHS Office of Intelligence and Analysis. The other sources asked about were considered to be somewhat less useful compared to agency information. Overall, the internet and the use of open source materials, human intelligence sources, and the media were perceived as providing the most useful information.

Table 4. Usefulness of Information from Agencies and Sources

Agency	Score	Source	Score
State/Local Fusion Centers	3.53	Internet	3.40
FBI's Joint Terrorism Task Force	3.42	Media	3.14
Federal Bureau of Investigation	3.34	Sources on the Street	3.12
Department of Homeland Security Office of Intelligence and Analysis	3.27	Pro. LE Publications	3.06
Bureau of Alcohol, Tobacco, and Firearms	3.18	LEO	2.95
Drug Enforcement Administration	3.15	Non-Law Enforcement Books	2.78
Immigration and Customs Enforcement	3.13	RISS.net	2.76
Law Enforcement Prosecutors	3.06	Alternative Literature	2.70
State Office of Homeland Security	3.01	Risk Assessments	2.67
Customs and Border Protection	2.69	HSIN.Intell	2.66
State Attorney General Anti-terrorism Task Force	2.62		

The research team asked whether the respondent was satisfied with the relationship they had with various law enforcement and government agencies. Table 5 presents these results on a 5-point scale with 5 meaning very satisfied. The results show that respondents overall where very satisfied with the working relationship with most of the law enforcement, government, and even private sector agencies that were asked about. In fact, the scores were over four for most agencies. Some of the highest averages were for state and local law enforcement agencies, state/local fusion centers, and the Department of Homeland Security.

Respondents were asked about several issues and whether they posed significant problems to the sharing of information. These issues included security clearances, adequate personnel, adequate training, adequate resources, adequate time, or the organizational culture caused a problem to the sharing of intelligence and information across agencies. A three item scale was used, with not a problem

(0), somewhat of a problem (1), and significant problem (2) as the response options. The results indicate that most of these issues remain a significant challenge to effectively sharing information and intelligence. The mean averages for the items were as follows: security clearance (.82); adequate personnel (1.31); adequate training (1.19); adequate resources (1.22); adequate time (1.32); and organizational culture (1.17).

Table 5. Satisfied with the Working Relationship

Agency	Score	Agency	Score
Local Law Enforcement	4.47	National Guard	4.12
State/Local Fusion Center	4.45	State Office of Homeland Security	4.10
State Law Enforcement	4.37	Homeland Security Investigation	4.10
Department of Homeland Security	4.22	Hospitals	4.08
Federal Bureau of Investigation	4.15	Public Transportation	4.03
Emergency Management	4.18	Public Works	3.99
Fire Marshals	4.18	Private Sector Agencies	3.97
Department of Corrections	4.14	Public Health	3.93
Critical Infrastructure Security	4.01	Internal Revenue Service	3.74
Tribal Law Enforcement	3.99		

Finally, various information systems and networks were examined that are used to share intelligence and information and whether the respondents were satisfied with their use. Table 6 presents these results.[2] In Column 2, the results report the percentage of respondents who do not use a respective system. Approximately one-third of the respondents have not used ATIX, FBINET, or LLIS. Approximately 15

[2] A brief description of each system follows:
ATIX – Automated Trusted Information Exchange. A secure, but unclassified, information and messaging system, managed by RISS, to provide users with access to homeland security, disaster, and terrorist threat information.
FBINET – The Federal Bureau of Investigation Network which is a global-wide area network used for communicating classified information at the Secret level, including investigative case files and intelligence pertaining to national security; it also runs administrative applications. Most predominantly used by state and local law enforcement officers in fusion centers and HIDTA intelligence centers.
LLIS – Lessons Learned Information Sharing, operated by the Department of Homeland Security, is accessible by law enforcement and emergency response personnel and contains a wide variety of information on best practices, after action reports, relevant alerts and news and a secure communications system. LLIS includes an area specifically for law enforcement intelligence fusion centers.
RISS – Regional Information Sharing System operates a secure intranet, known as RISS.NET, to facilitate law enforcement communications and information sharing nationwide. RISS local, state, federal, and tribal law enforcement member agency personnel have online access to share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines.
HSIN – Homeland Security Information Network is a secure internet-based system of integrated communication networks designed to facilitate information sharing between DHS and other Federal, state, county, local, tribal, private sector commercial, and other non-governmental organizations involved in identifying and preventing terrorism as well as in undertaking incident management activities.
LEO – Law Enforcement Online, operated by the FBI, is a secure, Internet-based information sharing system for agencies around the world that are involved in law enforcement, first response, criminal justice, anti-terrorism, and intelligence. With LEO, members can access or share sensitive but unclassified information anytime and anywhere.
OSC – Open Source Center the focal point for the intelligence community's exploitation of open source material. It also aims to promote the acquisition, procurement, analysis, and dissemination of open source information, products and services throughout the U.S. Government.

percent of the respondents have never used RISS, HSIN, or the Open Source Center. Only 9 percent of the respondents have never used LEO. When a respondent stated that they used a particular network or system, they were generally very satisfied with it. The response options were a four item Likert scale from "Not at All Satisfied (1)" to "Very Satisfied (4)." The respondents were at least satisfied with all of the network and systems, but were generally more satisfied with LEO and the Open Source Center.

Table 6. Does Networked Systems Meet Information Sharing Needs?

Networked System	System Not Used	Level of Satisfaction
LEO	8.8%	3.33
RISS	14.6%	3.28
Open Source Center	14.8%	3.31
HSIN	15.7%	3.23
FBINET	28.3%	3.11
ATIX	35.7%	3.04
LLIS	32.4%	2.94

Indicators of Preparedness

Survey respondents were asked "In your opinion, how prepared is your organization for terrorist or criminal extremist threats in your region?" Response options ranged from "not at all prepared" to "very prepared" along a five-point scale. Two dichotomous dependent variables were created using the responses to this question. Only agencies indicating they were "very prepared" were coded as being "Prepared," and only the agencies indicating they were "not at all prepared" were coded as "Not Prepared." The research team then explored what characteristics increased the likelihood that an agency was prepared or not prepared for the threats in their region.

The analysis explored whether threats, relationships, or organizational factors affect these two dependent measures. Threats are representative of serious and likely threats to the responding agency's jurisdiction (see Table 1). This threat variable was recoded into four categories. Respondents were asked if a number of terrorist/extremist groups posed a serious threat to their jurisdiction with response options ranging from "strongly disagree" to "strongly agree" along a four-point scale. "Right-wing" is an additive index of an agency's response to Militia, Sovereign Citizens,[3] Klu Klux Klan, Christian Identity, Idiosyncratic Sectarians, Neo-Nazi, Reconstructed Traditions, and Racist Skinheads threats ($\alpha = .917$; single factor eigenvalue = 5.156). "Left-wing" is an additive index of an agency's response to Left-Wing Revolutionary, Black Nationalist, Extreme Environmental, and Extreme Animal Rights threats ($\alpha = .910$; single factor eigenvalue = 3.150). Single-Issue is an additive index of an agency's response to Extreme Anti-Tax, Extreme Anti-Abortion, Extreme Anti-Immigration, and Doomsday Cults threats ($\alpha = .913$;

[3] Although most organizations group Sovereign Citizens with other right wing groups, they are quite unique. Sovereigns do not specifically share the "supremacist" views of the Klan, etc. Their focus is not on individuals (e.g., minorities, Jews, etc.) rather their focus is on government dysfunction and abuse of authority. Their anti-government ideology is arguably more akin to left wing anarchists than right wing Klansmen.

single factor eigenvalue = 3.717). Jihad is an agency's response to a single item of an Islamic Extremists/Jihad threat.

Respondents were also asked if a number of types of attacks were likely to occur in their jurisdiction within the next five years. Chemical, Biological, Radiological/Nuclear, and Explosive – CBRNE – is an additive index of an agency's response to these four types of attacks (α = .856; single factor eigenvalue = 2.839).

Relationship variables are representative of the extent to which an agency has satisfied working relationships with organizations across sectors and levels of government. While relationships between individual agencies are important, preparedness is likely reliant on relationships with a range of organizations across different levels and sectors. Respondents were asked to indicate how satisfied they were with their working relationship with a variety of organizations. Responses ranged from "we have no relationship" to "very satisfied" along a five-point scale. Federal relationships is an additive index of an agency's response to relationships with the Federal Bureau of Investigation, Department of Homeland Security, Homeland Security Investigations, Internal Revenue Service, and National Guard (α = .790; single factor eigenvalue = 2.768). State relationships is an additive index of an agency's response to relationships with State Law Enforcement, State Fusion Center, State Government Officials, Critical Infrastructure, Department of Corrections, Emergency Management, and State Office of Homeland Security (α = .869; single factor eigenvalue = 3.981). Public relationships is an additive index of an agency's response to relationships with Hospitals, Public Health Agencies, Public Works, and Public Transportation (α = .852; single factor eigenvalue = 2.791). Private sector relationship is a single item of agency responses to their relationships with the private sector.

Organizational factors represent a variety of agency characteristics likely to influence preparedness. Training is an additive scale representative of the total number of training programs attended by personnel from the responding agency. These training programs included Fundamentals of Intelligence Training, Federal Law Enforcement Training Center Analyst Course, Department of Homeland Security Critical Thinking as well as Report Writing, Drug Enforcement Administration Federal Law Enforcement Analyst Training, Federal Bureau of Investigation National Academy as well as Center for Intelligence Training, National White-Collar Crime Center Intelligence Analyst Course, State and Local Anti-Terrorism Training, Bureau of Justice Assistance 28 CFR 23, and the Regional Counterdrug Training Academy (α = .778; single factor eigenvalue = 3.560).

Threat assessments, threat warnings, vulnerability assessments, and risk assessments are analytic products created by the responding agency on a five-point frequency range of "never" to "daily." Responding agencies were asked to indicate the extent to which a number of issues were serious problems in their agency, ranging from "not a problem at all" to "significant problem." These organizational problems included personnel, training, resources, and agency culture. Responding agencies also indicated whether or not they had received external funding from federal, state, or local organizations in support of training, personnel, or equipment. Lastly, responding agencies indicated the

number of total personnel employed by their organization as one of six total employee brackets. The modal agency size response was 501 to 3,000 total personnel. The table that presents the descriptive for these variables is provided as an appendix.

Analytic Strategy

Bivariate analyses were conducted to explore the relationship between agency preparedness and jurisdictional threats, relationships, and organizational factors. Given the limited empirical work in this area, only bivariate logistic regressions were employed to test whether individual threats, relationships, and organizational factors predicted an agency's perception of being prepared or not prepared. Results of these bivariate relationships are presented in Table 7. Descriptive information for the variables included is provided in the Appendix in Table A.

The results are insightful and support intuitive suppositions. With respect to factors predicting preparedness, agencies with satisfied working relationships with state organizations (O.R. = 2.67) were twice as likely to be prepared. It appears that, at the bivariate level, as agencies produce threat assessments (O.R. = 3.59) and risk assessments (O.R. = 3.61) more frequently, they are three-and-a-half times more likely to be prepared than agencies who create them less frequently. The creation of vulnerability assessments also appears to be a predictor of preparedness as they more than quadruple an agency's preparedness likelihood (O.R. = 4.60). Lastly, as agencies experience problems related to personnel (O.R. = -3.42), training (O.R. = -2.71), and resources (O.R. = -2.45) the likelihood they will consider themselves prepared is reduced by approximately three-fold.

A number of factors appear to contribute to an agency being not prepared. Clarification of the interpretation of these findings is needed. First, when interpreting odds ratios for logistic regression, the percent above 1.0 indicates a more likely effect while the percent below 1.0 indicates a less-likely effect. If an odds ratio is negative, it simply means the predicting likelihood is increased in the negative, or opposite, direction. Second, there is a difference between predicting an agency that is prepared and negatively predicting an agency that is not prepared. While the presence of a certain factor may not statistically drive the prediction of being prepared, its presence may be strong enough to deter agencies from being not prepared.

For example in Table 7, perceptions of the satisfaction of relationships with federal organizations do not predict an agency being prepared. However, this same perception does predict that agencies are more than six times (O.R. = -6.48) as likely to be not prepared. Thus it could be assumed that the perception of federal relationships among prepared agencies was not strong enough to indicate why they were prepared, while agencies that did perceive federal relationships as satisfactory were six-times as likely to indicate they were not well prepared. This is a dramatic difference in perception and also applies to state (O.R. = -5.84), public (O.R. = -.490), and private sector (O.R. = -5.10) relationships. It appears that as agencies perceive to be working satisfactorily with organizations across levels of government and

sectors, they will not perceive the agency as not being prepared. Such findings lend support to the importance of working relationships with external organizations.

Table 7. Bivariate Relationships of Factors Influencing Agency Preparedness

	Prepared[a]		Not Prepared[b]	
Threats	Coef	Odds Ratio	Coef	Odds Ratio
Right-Wing	.092	1.39	-.097	-1.84
Left-Wing	.104	1.19	-.124	-1.87
Single-Issue	.131	1.31	-.125	-1.26
Jihad	.233	.76	-.272	-1.36
CBRNE	.246	1.91	-.156	-1.84
Relationships				
Federal	.223	1.84	-.262	-6.48***
State	.236	2.67**	-.234	-5.84***
Public	.203	1.67	-.227	-4.90***
Private	.835	1.80	-.807	-5.10***
Organizational				
Training	.043	.47	-.304	-3.85***
Threat Assessments	.847	3.59***	-.829	*2.65**
Threat Warnings	.347	1.65	-.525	-4.01***
Vulnerability Assessments	.964	4.60**	-1.287	-2.75**
Risk Assessments	.678	3.61***	-1.501	-2.87**
Personnel Problem	-1.169	-3.42***	.414	2.25*
Training Problem	-1.122	-2.71**	.733	4.03***
Resources Problem	-.886	-2.45*	.446	2.83**
Agency Culture Problem	-.394	-1.28	.706	3.81***
Received Federal Funding	.834	1.33	.105	.21
Received State Funding	1.231	1.36	-.088	-.15
Received Local Funding	-.094	-.09	-.014	-.02
Agency Size	.242	1.50	-.131	-.82

[a] The reference group for the "Prepared" dichotomous dependent variable is representative of an agency indicating their agency is "very prepared" to a preparedness question.

[b] The reference group for the "Not Prepared" dichotomous dependent variable is representative of an agency indicating their agency is "not at all prepared" or "not prepared" to a preparedness question.

***p>.001, **p>.01, *p>.05

Attendance at training programs also has a dramatic impact on the perception of being not prepared. As attendance at training programs increases, the perception of being not prepared is reduced by almost four-times. Moreover, analytic products also reduce the likelihood that an agency perceives to be not prepared. As threat assessments, threat warnings, vulnerability assessments, and risk assessments are produced more frequently, there is approximately a three-fold reduction in an agency's perception of being not prepared.

Lastly, problems within the agency that inhibit information sharing appear to increase the perception of being not prepared. Problems related to personnel (O.R. = 2.25) and resources (O.R. = 2.83) double the likelihood of an agency indicating they are not prepared. Training problems (O.R. = 4.03) has a quadrupling effect on being not prepared while problems related to the agency's culture (O.R. = 3.81) leads to a more than three-fold increase in being not prepared.

Discussion

Particularly for practitioners, the most important aspect of this research is not the findings on the variable analyses, per se, but on the benchmarks identified in trends found in the data. Some clear trends emerged which indicate programmatic successes for information sharing and intelligence as well as indicators of areas where problems remain. When considering these findings in the context of research on organizational development, it is clear that organizational leadership is an important factor for organizational successes in information sharing as well as for preparedness. If the leadership of a law enforcement agency is willing to expend the effort to train personnel, develop partnerships, and participate in state, regional and national information sharing initiatives, then greater levels of success will be achieved. While one would intuitively assume this, the data empirically supports it.
The findings provide indicators of progress that has been made in the domestic intelligence enterprise as well as obstacles that remain to be overcome. The reader is cautioned to not exclusively judge one's own agency based upon the findings of one or two variables in this study. The findings collectively reflect a point in time on a continuum of development. Rather than judge how one's agency rates on a specific variable – for example, the nature of public-private partnerships in the jurisdiction – the reader should view all preparedness variables and make a judgment of progress and use the findings as a roadmap to increase preparedness and functionality of the intelligence process.

A core responsibility of strategic intelligence is to identify changes in the threat picture, whether that is the emergence of new threats, changes in the methodology of current threats, or a diminished threat from some group or ideology. The findings indicate that respondents believe that the changing nature of threats is of continued concern to law enforcement. Respondents also indicated the nature of the changing threats have been effectively identified in the strategic intelligence process and shared with officers through bulletins and intelligence products. Thus, it appears the intelligence process is producing actionable strategic results.

A key issue for law enforcement in the post-9/11 environment has been "information sharing" – there had long been a chorus that information sharing among state and local law enforcement was limited, but it was virtually non-existent with federal law enforcement. In this study, SLT law enforcement respondents clearly indicate that the counterterrorism information sharing infrastructure and processes put in place post-9/11 (often referred to the Domestic Intelligence Enterprise) have been working to provide information among law enforcement agencies at all levels of government. Anecdotally, the current concern is not about information sharing processes, but often about the quality of the information. For example, an FBI or DHS intelligence product will be widely disseminated to state and local law enforcement, but it is often of the nature that officers should be "on alert" for certain types of threats, without more specific details. Conversely, federal law enforcement often does not have any more detail about threats to provide.

Respondents indicated they were highly satisfied with their relationships with other law enforcement agencies, government agencies and selected private sector partners in their counterterrorism activities. State and local law enforcement agencies, state/local fusion centers, and the Department of Homeland Security received the highest levels of satisfaction in mutual relationships.

Despite these notable successes, there are still barriers to effective information sharing that need to be addressed in the eyes of SLT law enforcement. The most prominent are: security clearances for SLT personnel, adequate staffing of the intelligence function, the need for adequate pre-assignment training and in-service training, adequate resources to effectively perform the intelligence process and changing the organizational culture to utilize the intelligence process. Interestingly, with the exception of security clearances, the major barriers as viewed by the respondents were factors within the law enforcement agencies. Hence, these are barriers that can be more easily overcome than systemic barriers. Perhaps the greatest challenge is changing the organizational culture, which is true for virtually any type of organizational change.

A core investment by the federal government to increase information sharing has been developing or enhancing electronic information sharing systems and networks. In the unclassified environment this includes, most notably, RISSnet,[4] Law Enforcement Online (LEO)[5] and the Homeland Security Information Network (HSIN).[6] The findings indicate that many of the information sharing networks and systems appear to be somewhat underutilized. Anecdotally, analysts and investigators, while having access to all of these systems, typically rely predominantly on one of the systems for simplicity, despite the fact that each system will have somewhat different information.[7] However, those who use those networks and systems are highly satisfied with their operations and value.

[4] http://www.riss.net
[5] http://www.fbi.gov/about-us/cjis/leo
[6] http://www.dhs.gov/homeland-security-information-network
[7] A common complaint of users of these systems is the inconvenience of the logon processes as well as auto-logoff if the system has been idle. Efforts of developing a Single Sign On have been unsuccessful.

The research team measured several factors on the general variable of "preparedness" to assess the kinds of knowledge, relationships, and tactical plans that were in place for attacks by various groups and methods. Overall, respondents stated their agencies were generally well prepared, although there is always room for improvement. It is probable that preparedness is also correlated with agency size and resources; however, this conclusion cannot be validated by the current data. Nonetheless, it is clear that the information sharing structures and processes as well as other training and technical assistance provided to law enforcement agencies post-9/11 has increased both awareness and preparedness in response to threats by criminal extremists. In particular, the findings show that those agencies which produce regular threat assessments and risk assessments are the most prepared. A conclusion that might be drawn from this finding is that not only do the assessments identify threats and risks, but leaders of agencies that require such assessments are more attuned to preparedness.

Respondents had attended a number of training programs related to intelligence and counterterrorism. Interestingly, as attendance at training programs increases, the perception of being not prepared is reduced by almost four-times. While training is certainly a component of preparedness, there are many other policy and resource factors that contribute to overall agency preparedness. However, consistently the respondents to this study viewed understanding the threat and responses to threats via training as an important component in overall agency preparedness.

Similarly, respondents indicated that analytic products also support the perception that the agency is prepared for threats. Ideally, this means threats were being recognized and tactical responses to threats being developed. However, pragmatically one must also consider the fact that mere knowledge of threats contributed to the respondents' perception of preparedness. Interestingly, as threat assessments, threat warnings, vulnerability assessments, and risk assessments are produced more frequently, there is approximately a three-fold reduction in an agency's perception of being not prepared. This suggests that an agency which devotes time and expertise to analysis and information sharing with respect to its threat environment sees value in this type of intelligence and, consequently, would presumably act on that information to prevent or mitigate threats.

The findings presented here are consistent with previous examinations of law enforcement's progress in improving information sharing and intelligence practices at a more macro-level (see U.S. Department of Homeland Security (2011) and the U.S. House of Representatives Committee on Homeland Security (2013)). Collectively the findings show significant progress among law enforcement agencies for developing and sharing intelligence and information related threats by criminal extremists. Not surprisingly, barriers still remain, yet the progress is significant in several fronts.

References

Brick, J. M. and Williams, D. (2013). Explaining rising nonresponse rates in cross-sectional surveys. *The ANNALS of the American Academy of Political and Social Science*, 645(1), 36-59.

Carter, D. L. and Carter, J. G. (2009a). Intelligence-led policing: Conceptual considerations for public policy. *Criminal Justice Policy Review*, 20(3), 310-325.

Carter, D. L. and Carter, J. G. (2009b). The intelligence fusion process for state, local and tribal law enforcement. *Criminal Justice and Behavior*, 36(12), 1323-1339

Carter, J. G. (2013). *Intelligence-Led Policing: A Policing Innovation*. El Paso, TX: LFB Scholarly.

Chermak, S, Carter, J. G., Carter, D. L., McGarrell, E. F. and Drew, J. (2013). Law enforcement's information sharing infrastructure: A national assessment. *Police Quarterly*, 16(2), 211-244.

Davis, L. M., Riley, J. K., Ridgeway, G., Pace, J., Cotton, S. K., Steinberg, P. S., Damphousse, K. and Smith. B. L. (2004). *When terrorism hits home: How prepared are state and local law enforcement?* Santa Monica, California: RAND Corporation.

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report*. Washington, DC: Government Printing Office.

U.S. Department of Homeland Security. (2011). *Implementing 9/11 Commission Recommendations*. Progress Report. Washington, DC. U.S. Department of Homeland Security.

U.S. House of Representatives. (2013). *Majority Staff Report on the National Network of Fusion Centers*. Washington, DC: Committee on Homeland Security.

Appendix

Table A. Descriptives

Variable	Mean	S.D.	Min	Max
Prepared	0.08	0.27	0	1
Not Prepared	0.15	0.36	0	1
Threats				
Right-Wing	19.76	4.91	8	32
Left-Wing	9.74	2.84	4	16
Single-Issue	11.27	3.18	5	20
Jihad	2.89	0.90	1	4
CBRNE	9.56	2.36	4	16
Relationships				
Federal	17.79	4.89	5	25
State	27.55	5.85	7	35
Public	15.01	3.89	4	20
Private	3.65	1.20	1	5
Organizational				
Training	3.20	2.65	0	11
Threat Assessments	2.52	1.23	1	5
Threat Warnings	3.16	1.43	1	5
Vulnerability Assessments	2.25	1.10	1	5
Risk Assessments	2.33	1.14	1	5
Personnel Problem	1.47	0.85	0	3
Training Problem	1.36	0.86	0	3
Resources Problem	1.39	0.87	0	3
Agency Culture Problem	1.36	0.91	0	3
Received Federal Funding	0.41	0.49	0	1
Received State Funding	0.08	0.27	0	1
Received Local Funding	0.11	0.31	0	1

Note: Modal agency category is 501-3000.