2010-12

The internet and homegrown jihadist terrorism assessing U.S. detection techniques

Banez, Justin D.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE INTERNET AND HOMEGROWN JIHADIST TERRORISM: ASSESSING U.S. DETECTION TECHNIQUES

by

Justin D. Bañez

December 2010

Thesis Advisor:	Erik J. Dahl
Second Reader:	Sean F. Everton

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE The Internet and Homegrown Jihadist Terrorism: Assessing U.S. Detection Techniques		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Justin D. Bañez			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The idea of homegrown terrorism is not a new concept, especially considering the history of challenges faced by the United States and other Western countries. However, the current violent jihadist problem has overshadowed those past misfortunes in terms of its objective and volatility. What is emergent is the means by which the individuals involved in this movement reinforce or possibly operationalize their radicalized behavior. The Internet is often that vehicle.

Efforts to reform U.S. intelligence have placed increasing value on open source information for threat assessments. Consequently, the open Internet has been targeted in search of radical actors, both foreign and homegrown. Some analysts contend that the availability of radical discourse on the Internet presents an opportunity for early identification by authorities. This thesis analyzes the value of open source exploitation of the Internet in the domestic counterterrorism role in relation to other detection techniques in order to extract best practices and lessons learned for improved intelligence and law enforcement activities.

14. SUBJECT TERMS Homegrown Terrorism; Jihad; Internet; Open Source			**15. NUMBER OF PAGES** 141
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE INTERNET AND HOMEGROWN JIHADIST TERRORISM: ASSESSING U.S. DETECTION TECHNIQUES

Justin D. Bañez
Captain, United States Air Force
B.S., United States Air Force Academy, 2004

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2010**

Author: Justin D. Bañez

Approved by: Erik J. Dahl
Thesis Advisor

Sean F. Everton
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The idea of homegrown terrorism is not a new concept, especially considering the history of challenges faced by the United States and other Western countries. However, the current violent jihadist problem has overshadowed those past misfortunes in terms of its objective and volatility. What is emergent is the means by which the individuals involved in this movement reinforce or possibly operationalize their radicalized behavior. The Internet is often that vehicle.

Efforts to reform U.S. intelligence have placed increasing value on open source information for threat assessments. Consequently, the open Internet has been targeted in search of radical actors, both foreign and homegrown. Some analysts contend that the availability of radical discourse on the Internet presents an opportunity for early identification by authorities. This thesis analyzes the value of open source exploitation of the Internet in the domestic counterterrorism role in relation to other detection techniques in order to extract best practices and lessons learned for improved intelligence and law enforcement activities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ALF	Animal Liberation Front
BOLO	Be on the Lookout
CA	California
CO	Colorado
CIA	Central Intelligence Agency
CSIS	Canadian Security Intelligence Service
DHS	Department of Homeland Security
ELF	Earth Liberation Front
ERRI	Emergency Response and Research Institute
FBI	Federal Bureau of Investigation
FIPP	Fair Information Practice Principle
GA	Georgia
I&A	Office of Intelligence and Analysis
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
IL	Illinois
INTERPOL	International Criminal Police Organization
IPB	Intelligence Preparation of the Battlefield
IRA	Irish Republican Army
ISP	Internet Service Provider
JIS	Jam‘iyyat Ul-Islam Is-Saheeh
JTTF	Joint Terrorism Task Force
LET	Lashkar-e-Tayyiba
NATO	North Atlantic Treaty Organization
NCTC	National Counterterrorism Center
NIE	National Intelligence Estimate
NOSC	National Open Source Center
NSA	National Security Agency

NYPD	New York Police Department
ODNI	Office of the Director of National Intelligence
OH	Ohio
OR	Oregon
OSINT	Open Source Intelligence
PA	Pennsylvania
PII	Personally Identifiable Information
SITE	Search for International Terrorist Entities
SNMC	Social Networking Monitoring Center
TX	Texas
USA PATRIOT	United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
USG	United States Government

ACKNOWLEDGMENTS

I first and foremost want to extend my sincere gratitude to Professors Eric Dahl and Sean Everton for their patience, guidance, and expertise. I truly enjoyed their respective classes, both of which first inspired me to pursue the subject of my thesis.

Finally, I would like to thank my family and the many new friends who supported me and truly made this experience fulfilling.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

> *We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect with one another, justify and intensify their anger, and mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.*[1]
>
> -National Intelligence Estimate, July 2007

When the Office of the Director of National Intelligence (ODNI) published the U.S. Intelligence Community's assessment of the terrorist threat to the Homeland, it solidified what many scholars and intelligence professionals had long speculated. The spread of jihadist websites and related Internet media were contributing to the growth of self-radicalized actors in Western societies, to include the United States.[2] Dennis Blair's more recent Annual Threat Assessment to the Senate stressed that though successful attempts at domestic attacks would be sparse, extremist reinforcement through the Internet would continue to play a critical role in the "homegrown" jihadist threat.[3] In each appraisal, intelligence officials made clear that this contemporary threat poses challenges for intelligence and law enforcement efforts.

Prominent among these challenges is the question of how to best detect, collect, and assess homegrown radical activity on the Internet. The Intelligence Community has a history of scouring the cyber realm in search of nefarious activity, sometimes by

---

1 Office of the Director of National Intelligence, *National Intelligence Estimate: The Terrorist Threat to the U.S. Homeland* (Washington, DC: ODNI, 2007).

2 Ibid.

3 Dennis C. Blair, Annual Threat Assessment of the Intelligence Community, February 2010, 11.

contentious means of its own.[4] However, measures that potentially threaten civil liberties hold little traction in America as evidenced by society's desire to return to a sense of normalcy in the years following the 9/11 attacks.

Though covert techniques will invariably remain viable tools, the changing nature of threats has called for an evolutions in intelligence methods. Efforts to reform U.S. intelligence have placed increasing value on open source information for threat assessments. Consequently, the open Internet has been targeted in search of radical actors, both foreign and homegrown. This study therefore seeks to answer two questions: Does open source exploitation of the Internet provide an effective means for identifying homegrown jihadist threats? If so, what are the best practices, and what can be improved?

B. PURPOSE AND IMPORTANCE

The idea of homegrown terrorism is not a new concept, especially considering the history of challenges faced by other Western countries. Indeed, even its existence on American soil is not particularly modern when one recalls the chronic blight of "eco-terrorist" events, the Oklahoma City bombing or the wave of bombings carried out by domestic terror groups in the San Francisco Bay Area during the 1970s.[5] However, the current violent jihadist problem has overshadowed those past misfortunes in terms of its

[4] Examples include the Total Information Awareness program which allowed authorities to eavesdrop on Internet communications through wiretaps, and the formerly covert Carnivore system used by the FBI. Carnivore was widely criticized for privacy infringement. See Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges*, (Washington, DC: United States Institute of Peace Press, 2006), 182–185.

[5] Overshadowed by the jihadist threat, often forgotten are the violent radical movements of extreme environmentalist groups like the Earth Liberation Front (ELF) and the Animal Liberation Front (ALF). These two groups alone have accounted for the highest number of domestic terror attacks since 9/11. See START Global Terrorism Database, http://www.start.umd.edu/gtd/search/Results.aspx?expanded=no&casualties_type=&casualties_max=&country=217&ob=GTDID&od=desc&page=1&count=100#results-table (accessed May 29, 2010).

The 1970s experienced a series of politically-driven attacks throughout the Bay Area by groups such as the Weather Underground, New World Liberation Front, and the Red Guerilla Army; see "Radicals: California's Underground," Time.com, http://www.time.com/time/magazine/article/0,9171,913516-1,00.html (accessed May 29, 2010); and Brian Michael Jenkins, "Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States since September 11, 2001," (Santa Monica: RAND, 2010), viii.

objective and volatility. What also is emergent is the means by which the individuals involved in this movement reinforce or possibly operationalize their radicalized behavior. The Internet is often that vehicle.

The Internet's enabling nature is of course a well-researched area of interest, with volumes of laudable publications covering the more operative uses of the Internet by terrorists (e.g., propaganda, fundraising, targeting, and coordination for attacks). Common to many of these works is the call for improved intelligence measures that can successfully identify and preempt terrorist activity. The DNI's statements indicate the call has not fallen on deaf ears and that the Intelligence Community is engaged. Yet the approach with which analysts address homegrown jihadist activity requires evaluation, both for its validity and its effectiveness in assessing the threat. Open source information should not hastily be deemed the "golden bullet," given the overwhelming amount of data, which is often incomplete, and the ever-present potential for false leads. However, the availability of radical discourse on the Internet presents an opportunity for early identification when individual behaviors are viewed as "part of the continuum of the radicalization process."[6] The objective of this research is to analyze the value of open source exploitation of the Internet in the homegrown counterterrorism role, while extracting best practices and lessons learned for improved detection activities. This contribution hopes to expand the body of knowledge in identifying, disrupting, and preventing homegrown jihadist radicalization and attacks, but also has broader implications for the development of the open source intelligence discipline.

C. LITERATURE REVIEW

The increased demand for open source information in the Intelligence Community has sparked debate among policymakers and scholars. This debate by and large focuses on the relative value of open source information. Though intelligence professionals

[6] Mitchell D. Silber and Arvin Bhatt, "Radicalization in the West: The Homegrown Threat," report by the New York City Police Department, 2007, 10.

generally agree that open source information can be useful during collection and analysis, many still consider its use secondary to traditional clandestine activities.[7]

Historically, open sources have taken the back seat due to the conventional mindset of the Intelligence Community. Amy Sands argues that organizations within the Intelligence Community largely have understood their roles as collectors and assessors of secrets, thereby justifying the need for clandestine activities.[8] Directing attention to the collection and assessment of open source information would seem to detract from the organizations' conceptions of their primary purpose.[9] Some policymakers further promote this view, tending to believe that sifting through open source material rarely unveils an adversary's intentions.[10] Sands criticizes this view, arguing that open source information can "complement, supplement, clarify, and frame the 'secrets' uncovered via human and technical means."[11] In some cases, she says open sources may prevail over other methods of collection.

Since the 9/11 terrorist attacks, greater attention has been directed toward the specific role of the Internet in America's counterterrorism strategy. Critics fear that increased government intervention in the cyber realm translates into intrusion on American privacy.[12] The National Security Agency's Terrorist Surveillance Program and the Federal Bureau of Investigations' Digital Collection System (formerly known as "Carnivore") have been harshly criticized. Designed to collect electronic communications, these systems are reportedly capable of tracking e-mail headers, sender and destination identities, financial transactions, and Internet browsing history—

---

[7] Mitchell D. Silber and Arvin Bhatt, "Radicalization in the West: The Homegrown Threat," report by the New York City Police Department, 2007, 64; Richard A. Best, Jr. and Alfred Cumming, "Open Source Intelligence (OSINT): Issues for Congress," Congressional Research Service Report RL34270, December 5, 2007, 2.

[8] Amy Sands, "Integrating Open Sources into Transnational Threat Assessments," in Jennifer E. Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), 64.

[9] Ibid.

[10] Best and Cumming, "Open Source Intelligence (OSINT): Issues for Congress," 2.

[11] Sands, "Integrating Open Sources into Transnational Threat Assessments," 64.

[12] Siobhan Gorman, "NSA's Domestic Spying grows as Agency sweeps up Data," *Wall Street Journal* website, March 10, 2008, http://online.wsj.com/article/SB120511973377523845.html (accessed May 29, 2010); Transcript of Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, "Using Open-Source Information Effectively," June 21, 2005, 3.

unbeknownst to the target individual.[13] Some believe that this capability carries too large of a potential for misuse. Though measures should be taken to guard against the jihadist threat, organizations such as the American Civil Liberties Union and the Center for Democracy and Technology warn that the government's spy programs put American civil liberties at stake.[14] Supporters of open source methods proclaim that open Internet exploitation provides a viable solution to this problem. Open source information is by definition publicly available material that anyone can lawfully obtain by request, purchase, or observation.[15] As such, the use of open sources is regarded as contributing to improved accountability and oversight of the Intelligence Community.[16] Recognition of this feature, some contend, enhances the ability to confront the challenges posed by modern terrorism.

Advocates of open sources argue that exploiting the Internet's permissive nature is vital to understanding the ongoing jihadist threat. Frances Townsend, former Assistant to the President for Homeland Security and Counterterrorism, stresses that open source information drawn from the Internet is indispensible. Intelligence products compiled by the National Open Source Center (NOSC) frequently were included in many of the briefings she gave to the president, and also were made available to federal, state, and local officials.[17] Townsend claims that much of what the Intelligence Community now knows about jihadists is derived from their own "statements, blogs, videos, and chat sessions on the Internet."[18] Terrorism scholar Gabriel Weimann adds to this stance,

---

[13] Siobhan Gorman, "NSA's Domestic Spying grows as Agency sweeps up Data," *Wall Street Journal* website, March 10, 2008, http://online.wsj.com/article/SB120511973377523845.html (accessed May 29, 2010); Transcript of Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, "Using Open-Source Information Effectively," June 21, 2005, 3.

[14] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges*, (Washington, DC: United States Institute of Peace Press, 2006), 218–219.

[15] Best and Cumming, "Open Source Intelligence (OSINT): Issues for Congress," 5–6.

[16] Robert D. Steele, "Open Source Intelligence," in Loch Johnson , ed., *Strategic Intelligence: The Intelligence Cycle* (Westport: Praeger, 2007), 111.

[17] Frances Fragos Townsend, transcript of address given to the ODNI Open Source Conference, July 16, 2007, in Washington, DC, ODNI website, http://www.dni.gov/speeches/20070716_speech_2.pdf (accessed May 30, 2010).

[18] Ibid.

claiming that analysis of online jihadist rhetoric can often reveal radical actors' justifications and motivations for transitioning to violent actions.[19]

Compelling as these statements are, criticisms still remain concerning how the implementation of open source initiatives address more internal problems. Townsend praises the work done by the NOSC to identify and track thousands of jihadist websites from around the world and engage terrorism in the new Internet "battlefield."[20] Richard Best and Alfred Cumming, however, note that the NOSC currently falls under the administrative control of the Central Intelligence Agency (CIA). They highlight that such organizational placement constrains the NOSC's ability to truly "support law enforcement agencies and state, local, and tribal entities."[21] The National Security Act's statutory prohibition of CIA participation in law enforcement activities essentially bars the NOSC from collecting information directly on activities within the United States.[22] This limitation is especially significant for organizations like the Department of Homeland Security (DHS), which have a vested interest in homegrown threats.

Another important area of concern revolves around the use of private firms for open source information and technologies. The establishment of the NOSC was meant to provide the Intelligence Community with its own robust open source capability. Yet the NOSC is meant to analyze a broad range of national security intelligence issues, not just terrorism. In addition, some of its personnel are on temporary assignments in other agencies.[23] In an effort to supplement the deficiency, a number of independent researchers have established private firms specializing in terrorism monitoring on the Internet.

Because analysts in organizations like the Search for International Terrorist Entities (SITE) Institute and the Investigative Project often do not possess security clearances, their daily work relies entirely upon open source exploitation of the

---

[19] Weimann, *Terror on the Internet*, 54–58.

[20] Townsend, transcript of address given to the ODNI Open Source Conference, July 16, 2007, in Washington, DC.

[21] Best and Cumming, "Open Source Intelligence (OSINT): Issues for Congress," 20.

[22] Ibid.

[23] Ibid., 12.

Internet.[24] Rita Katz, head of the SITE institute, argues that she and others like her who zealously pore over open source information on the Internet have been able to effectively supplement the work of other intelligence professionals. She states that the obsession she and her peers share to diligently follow online jihadist discourse has enabled them to produce timely assessments for the people that need them most.[25] Critics, understandably, question the viability of private groups with limited resources in comparison to the larger government agencies. Steven Aftergood from the Federation of American Scientists challenges, "Intelligence analysis is a set of skills that you learn, not just something that anyone can walk in off the street and pick up."[26] Other critics, such as Brian Jenkins, a senior researcher with the RAND Corporation who has studied terrorism for over thirty years, are wary of the motives and credentials of rising private groups.[27] However, prominent terrorism scholars like Gabriel Weimann, Bruce Hoffman, Marc Sageman, and Jarret Brachman are increasingly associated with renowned private firms, which may lend credibility and expert advisory to these currently controversial resources.[28]

In addition to the debate regarding private firms is the concern of the emerging technologies used to carry out the business of Internet sweeping. Not unlike the government's Terrorist Surveillance Program mentioned earlier, private technology initiatives that "sniff" the Internet in search of terrorists are being questioned. Weimann cites the National Institute for Systems Test and Productivity, whose online tools monitor traffic and sweep e-mails for terrorist indicators.[29] The problem here is that these tools go beyond what is considered open source. An alternative that is still in development is

---

[24] Weimann, *Terror on the Internet*, 191-192.

[25] Benjamin Wallace-Wells, "Private Jihad: How Rita Katz got into the spying business," *The New Yorker*, May 29, 2006, 1-2.

[26] Wallace-Wells, "Private Jihad: How Rita Katz got into the spying business," 2.

[27] Weimann, *Terror on the Internet*, 191.

[28] Bruce Hoffman and Gabriel Weimann are both listed as Senior Advisors to the Site Intel Group, Marc Sageman is the founder of Sageman Consulting, LLC, and Jarret Brachman conducts private consulting in addition to his academic work. See, respectively, https://www.siteintelgroup.com; http://www.fpri.org/about/people/sageman.html; http://jarretbrachman.net/?page_id=17 (accessed May 29, 2010).

[29] Weimann, *Terror on the Internet*, 190.

the University of Arizona's *Dark Web* research project. Developed by a team of computer scientists and terrorism researchers, the Dark Web portal relies solely on open source collection for modeling and research. Using a variety of "multilingual data mining, text mining, and Web mining techniques" the team has been able to conduct "link analysis, content analysis, Webmetrics (technical sophistication) analysis, sentiment analysis, authorship analysis, and video analysis" of jihadist content.[30] The project team stresses that their work is not like Total Information Awareness and that their research targets international terrorists and jihadist groups, not "regular citizens."[31] However, the team may soon find itself coming across evidence of homegrown radicals who have reached out to fellow jihadists on the Internet. In this case, the Dark Web project, given its scholarly roots and emphasis on respect for civil liberties, may prove particularly helpful in identifying radical threats in the homeland.

Given the issues just presented, many argue the fundamental challenge that still remains is a lack of widely accepted metrics for the use of the Internet and open sources. Best and Cumming remark that visits to the NOSC's website *opensource.gov* are monitored and counts are taken of how many times open source analyses make it into the President's Daily Brief.[32] Yet, these trivial measures reveal little about effectiveness. Best and Cumming offer that the ultimate metric really is the quality of analysis and the pressure of potentially reflecting ignorance of information that is publicly available.[33]

Focused on homeland issues, Jin Kim and William Allard propose applying the military's Intelligence Preparation of the Battlefield (IPB) framework to assess the utility of Internet-derived information. They argue that the IPB's systematic, layered approach allows analysts to track both terrorist adversary and source by means of event

[30] The University of Arizona, "Dark Web Terrorism Research," University of Arizona website, http://ai.arizona.edu/research/terror/ (accessed April 26, 2010).

[31] Ibid.

[32] Best and Cumming, "Open Source Intelligence (OSINT): Issues for Congress," 17.

[33] Ibid.

templates.[34] Coupled with a radicalization project owned by DHS, Kim and Allard assert that the IPB would focus collection and provide timely feedback to decision makers and planners.[35]

Lucy Resnyansky takes a slightly different approach, arguing that intelligence professionals first need a change in mindset in order to realize the impact of open source information. She maintains that the Internet must be viewed in its social context, rather than as an information repository.[36] Resnyansky states that terrorist data from the Internet is produced in a vague field of opinion (such as blogs), which can be misleading for analysts. To avoid this pitfall, she argues, analysts should approach the data with a social-cultural perspective and conduct meta-analyses of the *context* in which the information was presented.[37] By understanding the social circumstances (institutional discourses, cultural values, actors' interests, etc) of the collected information, analysts are better able to determine the information's relevance to a potential threat.[38] Resnyansky argues that in order to make sense of what is happening on the Internet and to garner tangible results, the Intelligence Community needs to "acquire the epistemological mindset characteristic of qualitative social research."[39] Adopting a sociological mindset and its associated technological tools, she contends, enables analysts to capture the qualitative characteristics of Internet open sources needed to produce meaningful threat analyses authorities can count on.[40]

D. PROBLEMS AND HYPOTHESES

There are two hypotheses that can be generated based upon the literature. The first is that current open source exploitation of the Internet is only marginally effective in

---

[34] Jin Kim and William Allard, "Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Intelligence Analysis," *SAIS Review*, vol. XXVII, no. 1 (Winter-Spring, 2008), 83.

[35] Ibid., 85.

[36] Lucy Resnyansky, "The Internet and the Changing Nature of Intelligence," *IEEE Technology and Society Magazine*, vol. 28, no. 1 (2009), 45.

[37] Resnyansky, "The Internet and the Changing Nature of Intelligence."

[38] Ibid., 46.

[39] Ibid.

[40] Ibid.

identifying homegrown threats. These authors make the case that while there may be an abundance of open source information online, this data may not always promise "an equivalent amount of open source intelligence."[41] Additionally, Abram Shulsky and Gary Schmitt argue that the frequent questionability of quality data drawn from Internet forums, and the credibility of sources, may be a hindrance in providing timely and actionable intelligence.[42] In this case, open source exploitation is better viewed as merely a foundation for effective classified intelligence and covert actions.[43]

On the other hand, the second hypothesis based on other writings is that open source exploitation of the Internet is a considerably effective means for identifying and assessing homegrown radicalization. Advocates such as retired Naval intelligence officer Dr. John Gannon, president of BAE Systems' Intelligence and Security, and John Jardine, president of Open Source Publishing, Inc., argue that the availability of sophisticated search engines, language translation tools, social network analysis programs, geospatial software, and the assistance of motivated private firms allows analysts to evaluate open source data online rapidly while focused on key identifiers of extremist activity.[44] This thesis will investigate documented cases of American homegrown jihadists to see which of the claims hold true.

E. METHODS AND SOURCES

This thesis will apply a qualitative examination of homegrown jihadist incidents in the United States since 9/11 to study the effectiveness of open source exploitation of the Internet in assessing jihadist threats. Ten cases are selected from the population of 46 incidents presented in the 2010 RAND report, "Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States since September 11, 2001." The report defines homegrown jihadists as individuals who lived in the United States and in many

---

[41] Sands, "Integrating Open Sources into Transnational Threat Assessments," 66.

[42] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence* (Washington, DC: Potomac Books, 2002), 142.

[43] Steele, "Open Source Intelligence," 96.

[44] Individual testimonies before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment found in "Using Open-Source Information Effectively," Serial No. 109-22 (Washington, DC: GPO, 2007), 9–15.

cases plotted to conduct attacks against the homeland, provided material support to foreign terrorist organizations, or left the country to join jihadist organizations abroad.[45] For the purpose of this thesis, cases are chosen to represent the span of incidents across the homeland. As such, the locations referenced correspond to the city and state in which the homegrown plot was ultimately foiled and the perpetrators detained. This also affords the opportunity to investigate the measures taken by federal, state, and local entities in each region. For example, though the FBI as a whole embraces the same general mission set, each regional division encounters region-specific circumstances that may influence their approaches.

Drawing from legal documents, scholarly works, and news reports, the selected cases are investigated with the purpose of extracting those sources of information, or indicators, which alerted authorities to the radical threat. Each indicator is then classified under one the following general categories: interpersonal; Inernet-Based; incident reports and watchlist alerts; documents, media, and material; or confidential. These categories are meant to capture a broad range of sources available to authorities. The *interpersonal* category refers to those types of person-to-person interactions that occur in close social environments, such as the workplace or religious establishment, which may provide reports of suspicious behavior. Friendship and kinship ties fall under this category, as relatives and friends may be the first to identify unusual activities of a radicalized individual. *Inernet-Based* sources include, but are not limited to, publicly available material found online in chat rooms, social networking sites, extremist websites, public records, and even commercial online sources that require a fee for access. The *incident reports and watchlist alerts* category captures the automatic reporting that is generated from public safety incidents such as traffic stops, domestic disturbances, or neighborhood watch tip-offs. Included in this category are red flags generated by travel to countries listed as state sponsors of terrorism or as terrorist safe havens. *Documents, media, and Material* refers to commonly available sources such as newspapers, videos, and CDs, and other material items that may be discovered during the course of investigation. Lastly,

[45] Brian Michael Jenkins, "Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States since September 11, 2001," RAND Corporation Occasional Paper 292, 2010, vii.

the *confidential sources* category indicates information gathered from undercover means or recruited contacts. Table 1 illustrates examples of information sources for each category that may be found in the investigated cases.

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
Co-workers	Chat rooms	Legal infractions (traffic stops, domestic violence, etc)	Videos	Undercover agents
Religious venues	Blogs	Neighborhood Watch tip-off	Pictures	Informants
School ties	Social Networks (Facebook, MySpace, etc)	Passport/Visa applications for travel to countries designated as state sponsors or terrorist safe havens	Weapons/bomb components	
Familial ties	Online public records			

Figure 1. Examples of sources that may indicate Jihadist threat

In order to understand the effectiveness of Internet exploitation in each case investigated, all applicable source categories must be measured against a set of metrics. Evaluating the relative value of each factor affords a better understanding of its contribution to the assessment of the homegrown jihadist threat. Therefore, drawing upon valuation metrics offered by Robert David Steele, each category as displayed above is appraised using the following queries:

- Was the information "good enough" at the time of discovery, therefore allowing timely intervention?
- Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?
- Was the information shared in order to attract other useful information?[46]

The goal of this method is to provide a holistic view of the homegrown threat assessments in order to determine if use of the open Internet did indeed contribute

[46] Steele, "Open Source Intelligence," 143.

significantly. Certainly, it may be discovered that in some cases the Internet was not applicable at all. Even so, the absence of its use may be telling of a latent deficiency or highlight the relevance of a more effective tactic. In cases in which the Internet was found to be applicable, the revelations may illuminate practices and techniques that deserve increased application or have potential for improvement.

The roadmap for this thesis is as follows: Chapter II will begin with a historical background, illustrating the increased concerns of terrorism researchers and the Intelligence Community regarding jihadist extremism on the Internet. Tracing the rise of terrorist Internet activity on the transnational scale, this background explores hallmark intelligence assessments from the Intelligence Community that warned of America's new homegrown threat and discusses the reasons governing the increased emphasis on open source exploitation of the Internet. Chapter III provides a comprehensive overview of the current issues surrounding the collection and use of open source Internet information, ranging from information volume management to privacy concerns. Chapter IV presents each of the selected case studies as applied to the model presented above, with the goal of elucidating the success, shortcomings, or non-applicability of open source Internet exploitation. Given the results of the case studies, the concluding chapter will provide an overview of best practices and areas for improvement, leading into an informed and acceptable way ahead for dealing with America's homegrown jihadist threats and open sources.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE GROWING CONCERN OVER JIHAD ON THE NET

A. INTRODUCTION

Globalization trends have changed the dynamics of security and intelligence. Technological breakthroughs continue to sharpen America's offensive and defensive capabilities while providing once unimaginable access to critical information. Conversely, innovative tools like the Internet have given America's terrorist adversaries an opportunity to challenge national security from afar and within the homeland.

The concern over homegrown jihadist and other terror-related Internet activity has been gradual. It has only recently become a prominent issue of national concern, as evidenced by John Brennan's May 26, 2010 speech to the Center for Strategic and International Studies:

> Knowing that it is harder to penetrate America's defenses, the likes of al-Qaida's Adam Gadahn and Anwar al-Awlaki in Yemen, American citizens who understand our society, our strengths as well as our vulnerabilities, not only plan attacks, they use the Internet and extremist websites to exhort people already living in the United States to take up arms and launch terrorist attacks from within. Indeed, we have seen an increasing number of individuals here in the United States become captivated by extremist ideologies or causes. Somali Americans from Minnesota traveling to fight in Somalia, the five Virginia men who went to Pakistan seeking terrorist training, David Headley, the Chicago man charged with helping to plan the Mumbai attacks, the Pennsylvania woman, JihadJane, charged with conspiring to murder a Danish cartoonist. The president's national security strategy explicitly recognizes the threat to the United States posed by individuals radicalized here at home.[47]

A relatively small number of researchers, on the other hand, have been tracing this particular Internet trend since before 9/11. Much of their early research, however, focused on fairly well-known international organizations and less on the possible emergence of loose affiliations within the United States. It was not until after the release of the 9/11 Commission Report in July 2004 that greater attention was paid to the latter

[47] John Brennan, Assistant to the President for Homeland Security and Counterterrorism, transcript of speech given to Center for Strategic and International Studies, May 26, 2010, Washington, DC.

by the Intelligence Community (IC). Common discoveries in both scholarly and intelligence arenas illuminated the need for an improved strategy that could deliver warning and opportunities for disruption. This chapter provides a brief historical background illustrating the early warnings by terrorism researchers and the increased concerns of the Intelligence Community regarding jihadist extremism facilitated by the Internet. It traces the evolution of hallmark intelligence assessments from the Intelligence Community that warned of America's new homegrown threat. Furthermore, it discusses reasons behind the increased emphasis on exploiting the open source nature of the Internet.

B. PERSPECTIVES FROM THE TERRORISM RESEARCH COMMUNITY

Terrorists were using the Internet before the attacks on 9/11. Despite its relative newness, the medium was immediately recognized as a powerful tool by established terrorist organizations. By 1999, almost all thirty groups designated as terrorist organizations by the U.S. Department of State were on the Internet.[48] A year prior, Clark Staten of the Emergency Response and Research Institute (ERRI) addressed a U.S. Senate subcommittee, stating that "even small terrorist groups are now using the Internet to broadcast their message and misdirect/misinform the general population in multiple nations simultaneously."[49] Both terrorists and terrorism researchers understood early on the Internet's utility for propaganda and coercion.

Terrorism scholar Gabriel Weimann has followed this development from its early stages and has produced some compelling revelations. In his book *Terror on the Internet: The New Arena, the New Challenges*, Weimann discusses his findings from the systematic investigation of a database of thousands of terrorist websites compiled from 1998–2005.[50] He argues chiefly that it should come as no surprise that terrorists turned to the Internet as it became available. The opportunity to affect mass media was

[48] Weimann, *Terror on the Internet: The New Arena, the New Challenges*, 15.

[49] Clark Staten, Testimony before the Subcommittee on Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee, February 24, 1998; quoted in Dorothy Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999), 68.

[50] Weimann, *Terror on the Internet: The New Arena, the New Challenges*, 4.

attractive and an effective way to voice their goals and concerns. It also was, and still is, "a useful channel of communication, linking terrorists and their followers, spreading propaganda and instructions, launching psychological scare campaigns, and networking terrorist groups and organizations."[51]

The mid-to-late 1990s saw increased growth in society's use of the Internet, as the new means for social interaction, information access, and marketing became ever more appealing.[52] The fruits of globalization, it appeared, were unlocking new doors for peace and prosperity. Weimann notes, however, that those claims were soon challenged as the Internet's unregulated environment was invaded by pornography, violent images, and extremist content of various types.[53] This new communicative space played favorably for violent politically-motivated groups looking to improve their tactics. In 1996 for instance, the Palestinian group Hamas was reported to have used "chat rooms and e-mail to plan and coordinate operations in Gaza, the West Bank, and Lebanon."[54] During this same period, the Lebanese Hezbollah established a number of websites to report successful attacks against Israel, while the Irish Republican Army (IRA) took advantage of the Internet to garner sensitive information about British army bases.[55] Still in its early existence, the Internet provided both communicative and operational advantages to well-known terrorist organizations.

1. Jihad Goes Online

Jihadist terror group Al Qaeda gained instantaneous global infamy after executing the 9/11 attacks. The Internet helped spread its notoriety. Yet prior to those events, the

---

[51] Weimann, *Terror on the Internet: The New Arena, the New Challenges*, 25.

[52] D. Rushkoff, *Coercion: Why We Listen to What 'They' Say* (New York, NY: Riverhead, 1999); cited in Lucy Resnyansky, "The Internet and the Changing Nature of Intelligence," *IEEE Technology and Society Magazine*, vol. 28, no. 1 (2009), 45.

[53] Weimann, *Terror on the Internet: The New Arena, the New Challenges*, 19.

[54] "Israel: U.S. Hamas Activists Use Internet to Send Attack Threats," Tel Aviv IDF Radio, FBIS-TOT-97-001-L, October 13, 1996; cited in Steven A. Hildreth, "Cyberwarfare," Congressional Research Service Report RL30735, June 19, 2001, 15.

[55] Ibid.

group had only maintained one website (www.alneda.com).[56] Edna Reid and Hsinchun Chen, senior researchers at the University of Arizona, note that at the time this one site was primarily a propaganda posting board for "'official statements,' reports, and videos from senior members of the al-Qaeda movement."[57] While counterterrorism officials and Internet service providers (ISP) took the site offline following 9/11, "mirror images" of Alneda frequently reappeared over a two year period on different ISPs or embedded within legitimate sites.[58] It soon became apparent that blocking or removing the site were only temporary fixes. Meanwhile, the jihadist movement, and subsequently its Internet use, was undergoing a dynamic change.

The catastrophic events against the U.S. homeland triggered intense repercussions for Al Qaeda. A U.S.-led coalition was formed to strike at the heart of the jihadist group, which was known to operate terrorist training camps in Afghanistan.[59] This persistent campaign to capture and kill Al Qaeda members significantly degraded the organization as it once was. Some claim however that this weakening was only transitory and that the jihadist movement merely adapted with the help of the Internet.[60]

In his controversial book *Leaderless Jihad*, Marc Sageman argues that the targeting and diffusion of the Al Qaeda core encouraged the adoption of a decentralized structure. Linked by the Internet, modern jihadists and supporters were empowered to act independently or in small cells across a global network.[61] Diffusion, Sageman remarks,

---

[56] Weimann, *Terror on the Internet: The New Arena, the New Challenges*, 67.

[57] Edna Reid and Hsinchun Chen, "Extremist Social Movement Groups and their Online Digital Libraries," *Information Outlook*, vol. 10, no. 6 (June 2006), 58.

[58] Weimann, *Terror on the Internet: The New Arena, the New Challenges*, 67–68.

[59] President George W. Bush, "Bush announces start of a 'War on Terror,'" on GlobalSecurity website, http://www.globalsecurity.org/military/library/news/2001/09/mil-010920-usia01.htm (accessed September 23, 2010).

[60] H. Brinton Milward and Jorg Raab, "Dark Networks as Organizational Problems: Elements of a Theory," *International Public Management Journal*, vol. 9, no. 3 (2006), 13–14.

[61] Marc Sageman, *Leaderless Jihad*, (Philadelphia: University of Pennsylvania, 2008) 126, 143.

served as a means for keeping the terror campaign alive.[62] The present-day idea of Al Qaeda has instead become inspiration rather than a controlling agency.[63]

Sageman believes that direction within this "leaderless" movement comes predominantly from the ongoing discourse on the Internet. Prominent Al Qaeda figureheads, even those who are now dead, still remain as topics of discussion and sources of inspiration for rising jihadists.[64] Scott Atran from the University of Michigan's Institute for Social Research agrees, stating that these types of focal points help individual radicals reach out to a larger jihadist *community*, though these persons may be geographically separated and unrelated.[65] These observations have led some in the West to shift concern from afar to potentially more local threats.

Jarret Brachman, former research director of West Point's Combating Terrorism Center, contends that Al Qaeda's strategic transformation has advanced the jihadist movement onto the global scale. In particular, he finds that the effect on the West has increased substantially. Citing the perpetrators of the 2006 Fort Dix plot and 2009 Fort Hood attack, he argues that the English-speaking jihadist has reached a point where he is indistinguishable from Arabic-speaking counterparts in terms of commitment and knowledge of the movement.[66] The presence of English translations of key literature, media, and frequent discourse on the Internet are largely responsible for this evolution.

Brachman has labeled emerging online Western extremists as "jihobbyists."[67] While the term is intended to be somewhat satirical, he stresses it carries a serious connotation. Self-radicalized individuals, seeking affirmation, turn to the Internet for

---

[62] Marc Sageman, *Leaderless Jihad*, (Philadelphia: University of Pennsylvania, 2008) 126, 143.

[63] Scott Atran, "A Failure of Imagination (Intelligence, WMDs, and 'Virtual Jihad')," *Studies in Conflict and Terrorism*, vol. 29 (2006) 292.

[64] Sageman, *Leaderless Jihad*, 146.

[65] Atran, "A Failure of Imagination (Intelligence, WMDs, and 'Virtual Jihad')," 292.

[66] Jarret Brachman, "Statement of Dr. Jarret M. Brachman before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities on the Topic of Understanding Cyberspace as a Medium for Radicalization and Counter-radicalization," December 16, 2009, 3–4.

[67] Jarret Brachman, 'Jihobbyism' blog forum, found at http://jarretbrachman.net/?cat=3 (accessed September 23, 2010).

support. By continually exposing themselves to ideologically sound propaganda on the Internet, these individuals harden their convictions.[68] These new actors may lack the authoritative direction that typified the traditional Al Qaeda organization. Yet recent events such as the one involving Colleen LaRose (online alias "JihadJane") from Philadelphia warn of the extent the modern jihadist will go to commit violence even from within U.S. borders.[69] Raphael Perl observes that if such trends continue, there can be an expected increase in small, localized attacks carried out by who he labels as "micro actors."[70] The characteristics of these micro actors—homegrown, technologically savvy, diverse in background, and loosely connected to other groups—make detection and disruption of their activities challenging.[71]

Of course, not all agree completely with the claims of Weimann, Sageman, et al. For example, David Tucker of the Defense Analysis Department at the Naval Postgraduate School argues that the Internet has not had a transformative effect on terrorist interaction. While he agrees that the Internet may facilitate communication among 'would-be' radicals, Tucker asserts that it does not replace the value of face-to-face interaction, which more often than not occurs first in potential terrorist relationships.[72] Challenging further, he says "the Internet may make it easier to find accomplices in geographically dispersed places, coordinate with them, and get plans for a bomb, but terrorists did all these things before the Internet existed."[73]

---

[68] Brachman, "Statement of Dr. Jarret M. Brachman before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities on the Topic of Understanding Cyberspace as a Medium for Radicalization and Counter-radicalization," December 16, 2009, 6.

[69] LaRose planned to murder cartoonist Lars Vilks, who had depicted the Prophet Mohammed as a dog. An Islam convert, she used YouTube and other online media to reach out to other jihadists and recruit others into her plot; see The Huffington Press, "Jihad Jane, Colleen LaRose, recruited terrorists and plotted murder, prosecutors say," http://www.huffingtonpost.com/2010/03/09/jihad-jane-colleen-larose_n_492586.html (accessed September 24, 2010).

[70] Raphael Perl, "Trends in Terrorism: 2006," Congressional Research Service Report RL33555, March 12, 2007, 16.

[71] Ibid., 5.

[72] David Tucker, "Jihad Dramatically Transformed? Sageman on Jihad and the Internet," *Homeland Security Affairs*, vol. 4, no. 1 (January 2010), 4.

[73] Ibid.

Bruce Hoffman, a notably preeminent terrorism scholar, fundamentally disagrees with Sageman's assessment about Al Qaeda's present status and relevance to national security. While he too has followed the trend of terrorist Internet use and advocated for increased concern, Hoffman asserts that it is the Internet that "has become something of a virtual sanctuary" for Al Qaeda's continued function.[74] In his scathing retort "The Myth of Grass-Roots Terrorism," he dismisses as folly Sageman's claims that Al Qaeda *the organization* is "dead" and asserts that the terrorist group is more than ever an alive-and-well threat to the U.S. As the title portends, Hoffman's article belittles the concept of homegrown jihadism. Instead, the argument made is that Al Qaeda exists today in the form of sleeper cells, products of a "long-standing campaign of subversion,"[75] that effectively use the Internet for propaganda and sustained recruitment.[76]

A more recent, and thought-provoking, set of observations is offered by Gilbert Ramsay who views the general issue of terrorists on the Internet to be overblown and of little concern. First, he contends, the image of terrorist manipulation of the technology is exaggerated and presented as an abnormal use of the same functionalities afforded to non-terrorists.[77] Addressing Weiman's assertion that the 9/11 hijackers "used the Internet, and used it well," Ramsay questions whether this statement really amounts to anything significant:

> They may indeed have 'used the Internet well' – but did they, in most respects a normal group of Western educated middle class Arabs, use the Internet any better, or any differently than their peers? If not, then the implication is that terrorist use of the Internet is, to this extent, an unremarkable correlate of the age, education and socioeconomic status of the individuals concerned.[78]

---

[74] Bruce Hoffman, "The Use of the Internet by Islamic Extremists," testimony before the House Permanent Select Committee on Intelligence, May 4, 2006, 6.

[75] Bruce Hoffman, "The Myth of Grass-Roots Terrorism," *Foreign Affairs*, vol. 87, no. 3 (May 2008).

[76] Hoffman, "The Use of the Internet by Islamic Extremists," 5–6, 19.

[77] Gilbert Ramsay, "Relocating the Virtual War," *Defense Against Terrorism Review*, vol. 2, no. 1 (Spring 2009) 36.

[78] Ibid.

In other words, it is difficult to claim that terrorists gain an edge by using the Internet for an agenda they would pursue anyway. Second, Ramsay argues that "terrorist use of the Internet…is a *terrorist* problem only when it leads to terrorism in real life."[79] He believes concerns over the presumed threat presented by online chatter ignorantly shifts concern from the real damage that terrorism can cause in physical space.[80] This leads into his principal claim that establishing terrorist use of the Internet as a problem to be directly solved is futile and unnecessarily expensive.[81] Rather, promoting the government's ability to take action in the "real world"—where its power is strongest—is likely to have greater affect on terrorists who try to take advantage of any media.[82] Though he does not address specifically the issue of U.S. homegrown jihadists, Ramsay's arguments imply the same prescription for any shade of terrorism.

Discussion in academic circles over the importance of terrorist Internet use, while in dispute, has in the least illuminated two considerations. The first is that the extensive body of data about jihadist operations and communications, gathered from the Internet by scholars, foretells of a lucrative intelligence capability that could possibly support law enforcement and counterterrorism authorities. Secondly, it highlights a potential avenue for better understanding jihadist operatives within the U.S., regardless of whether or not direct ties to Al Qaeda exist. The fact remains that American citizens with diverse demographics are engaging in jihadist activities—and that is a quandary. For the Intelligence Community and other counterterrorism professionals, these same considerations have progressively grown in significance and beckon new, smart ways to approach them.

C. THE INTELLIGENCE COMMUNITY CATCHES ON

Presently, the concerns over homegrown jihadists and their leveraging of the Internet are on the scope of the IC's upper echelon. As noted in this chapter's

---

[79] Gilbert Ramsay, "Relocating the Virtual War," *Defense Against Terrorism Review*, vol. 2, no. 1 (Spring 2009) 42.

[80] Ramsay, "Relocating the Virtual War," 38.

[81] Ibid.

[82] Ibid., 31, 43.

introduction, the president's "right-hand man" for homeland security and counterterrorism has voiced that part of the nation's latest security strategy is aimed at dealing with the problem. This decision comes as a culmination of over a decade of intelligence reporting and estimates that wrestled with defining the emerging trends. Although the IC had been tracking the issue of international terrorism since the 1980s,[83] the 9/11 attacks brought forth the concern that there were gaps in the understanding of Islamic extremist groups. Similar to the findings from the scholarly field, the intelligence profession observed an increase in small, diffuse groups or single actors engaging in jihadist activity throughout the West following the U.S.-led campaign in Afghanistan. While analysts projected early on that the spread of information technologies like the Internet would likely abet the wide spectrum of potential adversaries (disaffected states, transnational terrorists, proliferators, narcotraffickers, and organized criminals),[84] the tie-in with domestically-formed jihadists was not an immediate assessment. As suggested by a number of authoritative appraisals, this gap may be attributed to a focus on other homeland threats that seemed pressing at the time. The next section will review Federal Bureau of Investigation (FBI) reports on terrorism from the 1996 to 1999 timeframe to help illustrate this claim. In the succeeding section, a number of estimates from throughout the Intelligence Community, culminating in the release of the National Intelligence Estimate from the IC's leading body, reveal the shift in emphasis and a rising consensus on the need to address homegrown radicals who use the Internet.

1. Assessments: 1996 to 1999

The 1996 FBI annual terrorism report briefly mentioned how the Internet and other communications systems were effectively used by right-wing terrorists and the militia movement.[85] Similarly, the 1997 report noted that the means for carrying out attacks by both "domestic right-wing terrorists and extremist religious cults" would

---

[83] Richard A. Best Jr., "Intelligence Issues for Congress," Congressional Research Service Report RL33539, June 11, 2010, 14.

[84] National Intelligence Council, "Global Trends 2015: A Dialogue About the Future With Nongovernment Experts," December 2000, 10.

[85] Federal Bureau of Investigation, "Terrorism in the United States: 1996," Annual Terrorism Report, 1996, 17.

expand as information related to weapons of mass destruction proliferated on the World Wide Web.[86] In 1998, the FBI report observed that "cyber tools and methods…may find their way into the hands of terrorists."[87] The latter statement was primarily a reference to the threat of cyber attacks;[88] however, it was followed thereafter by the statement that "terrorists are known to use information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely." This is important as it suggested that the federal agency was beginning to take greater interest in the darker side of information technology. This assertion was validated the following year in the 1999 report where there were over six references to Internet use by domestic eco-terror groups (namely the extremist animal/environmental rights groups, Animal Liberation Front (ALF) and Earth Liberation Front (ELF)).

Although it was apparent that ALF, ELF, and right-wing extremists were the immediate domestic priorities, the 1999 report, interestingly, provided an assessment that would sound remarkably familiar in the coming decade. The broad message delivered by the following passages bears significance:

> In fact, a growing number of movements…are international in scope and exploit the nearly universal communication opportunities of the Internet to disseminate propaganda, coordinate activities, and issue claims of responsibility for extremist activities.[89]

---

[86] Federal Bureau of Investigation, "Terrorism in the United States: 1997," Annual Terrorism Report, 1997, 21.

[87] Federal Bureau of Investigation, "Terrorism in the United States: 1998," Annual Terrorism Report, 1998, 17.

[88] In this context, cyber attack, or cyberterrorism, refers to the use of computer networked technology to "attack" infrastructures or systems so as to inflict violence, induce fear, or cause severe economic and political disruption. This can be done through denial of service, loss of information integrity or confidentiality, and physical destruction. There has been a growing concern over the threat of cyberterrorism carried out by a variety of actors, to include those of the jihadist vein; however that is beyond the scope of this research. For a more in-depth discussion see: John Rollins and Clay Wilson, "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," Congressional Research Service Report RL33123, January 22, 2007.

[89] Federal Bureau of Investigation, "Terrorism in the United States: 1999," Annual Terrorism Report, 1999, 20.

> The communications opportunities afforded by the World Wide Web can be expected to have a far-reaching impact on the ability of contemporary extremist groups to perpetuate propaganda and attract new members.[90]

> The United States may be experiencing the third major wave of domestic terrorism evident since the 1960s…While these violent special interest movements share similarities with previous extremist movements, they also possess unique features that present new challenges to law enforcement. One of the most potentially troubling of these is the *decentralized* nature of most contemporary special interest extremist movements. In confronting more formalized left- and right-wing groups in the past, law enforcement successfully neutralized many of these organizations by arresting their leaders and dismantling their organizational structures. Such a strategy would have limited impact on less centralized, more broad-based, movements.[91]

These statements marked an important change in perspective. Though the FBI was regarded more for its law enforcement aptitude versus its intelligence capability, these early assessments indicate that the organization was to some degree trying to monitor the shifting character of terrorism within the homeland. Clearly, there was recognition of a decentralized trend among contemporary extremists. The Internet appeared to be a common facilitator. However, an authoritative connection to the jihadist movement was not made at the time; and certainly not to such a movement generating from within U.S. borders. Still, it is interesting to note that in the section titled "Trends in International Terrorism" of the 1999 report, there was a significant discussion about Al Qaeda and its loose affiliations of violent radicals. Specifically, it said that "As the 21st Century dawns, the most direct threat to U.S. interests may stem from Usama Bin Laden, his organization *Al-Qaeda*, and sympathetic groups"[92] and "should either he or *Al-Qaeda* cease to exist this international movement would, in all likelihood, continue."[93]

---

[90] Federal Bureau of Investigation, "Terrorism in the United States: 1999," Annual Terrorism Report, 1999, 32.

[91] Federal Bureau of Investigation, "Terrorism in the United States: 1999," 32.

[92] Ibid., 37.

[93] Ibid., 36.

2. Assessments: 2000 to 2007

Understandably, the 9/11 attacks were of primary focus in the FBI's "Terrorism 2000/2001" report. The Al Qaeda threat was heavily stressed but there were no discussions of either terrorist Internet use or an American jihadist trend.[94] The National Intelligence Council's "Global Trends 2015" publication, released in December 2000, did indicate however that the former was still a broad area of concern for the IC as a whole.[95] How to address that issue was still not defined.

In 2005, the FBI's counterterrorism division released a comprehensive 3-year review (2002 through 2005) of U.S. terrorism incidents and future challenges. Citing a number of foiled jihadist plots involving U.S. citizens and the successful London transit-system bombing, the FBI report posed that "the lack of strong ties between them [the terrorists] and an international terrorist group illustrate the potential threat of 'homegrown' terrorists as perpetrators of future attacks."[96] This was one of the first instances in an official assessment of the term *homegrown*, used to describe jihadist perpetrators of Western origin. Furthermore, it marked a turning point in the scope of future assessments from the greater intelligence and counterterrorism communities.

It should be noted that during this same time period the 9/11 Commission published the findings of its investigation and proposals for reform. Following the Commission's recommendations, the Intelligence Reform and Terrorism Prevention Act of 2004 was instituted, creating an Office of the Director of National Intelligence (ODNI) with the DNI as the head of the Intelligence Community.[97] In October 2005, the ODNI published its first *National Intelligence Strategy of the United States of America*, which

---

[94] The report does provide a brief description of the December 22, 2001 arrest of Richard C. Reid, aka the "Shoe Bomber," who attempted to detonate an improvised explosive device in his shoes while aboard a Paris-to-Miami flight. Reid allegedly received training from Al Qaeda camps. Federal Bureau of Investigation, "Terrorism 2000/2001," Terrorism Report, 2001, 25.

[95] The National Intelligence Council's discussion on 'Asymmetric Warfare' argues that between 2000-2015 an expected increase in the use of information technology by a variety of actors will become a dominant characteristic of threats to the homeland. National Intelligence Council, "Global Trends 2015: A Dialogue About the Future With Nongovernment Experts," December 2000, 14.

[96] Federal Bureau of Investigation, "Terrorism 2002-2005," Terrorism Report, 2005, 1–2, 12, 19, 27.

[97] Intelligence Reform and Terrorism Prevention Act of 2004, Section 1001 and Section 1021, P.L. 108–458.

outlined a series of "mission" and "enterprise" objectives. Notably, Mission Objective 1 emphasized identifying, disrupting, and destroying terrorists abroad and "within U.S. borders" through a variety of means to include communications channels.[98] Mission Objective 4 asserted that new methodologies and better use of open sources would be needed to penetrate some of America's adversaries, like terrorists, who may be of "amorphous groups or networks that may share common goals, training, and methods, but…operate independently."[99] Under Enterprise Objective 1, the existence of "ubiquitous communications technology…and extremists with the resources and intent to harm Americans" demanded U.S. intelligence to "re-think the way we conduct intelligence at home."[100] While not stated explicitly, these strategic objectives set forth by the IC's leading body hinted that, among terrorists, homegrown actors were considered viable threats. The prospect of targeting their use of communications technologies warranted greater attention. These claims were clarified when, in the summer of 2006, a report was submitted by the U.S. House Permanent Select Committee on Intelligence, declaring a linkage between the Internet and homegrown threats in Europe.[101] The committee warned that the United States was not immune from the homegrown models employed elsewhere in the West.[102] Furthermore, it asserted that jihadist use of the Internet posed "new challenges for the Intelligence Community and law enforcement officials."[103]

In 2007, the ODNI released a National Intelligence Estimate (NIE) outlining key judgments of the terrorist threat to the U.S. homeland. Explicitly stated in the first page of the document, "NIEs are the DNI's most authoritative written judgments concerning national security issues. They contain the coordinated judgments of the Intelligence

---

[98] Office of the Director of National Intelligence, *National Intelligence Strategy for the United States of America* (Washington D.C.: ODNI, 2005), 6.

[99] Ibid., 9.

[100] Ibid., 11.

[101] U.S. House Permanent Select Committee on Intelligence, "al-Qaeda: The Many Faces of an Islamist Extremist Threat" (Washington: GPO, 2006), 18.

[102] Ibid.

[103] Ibid., 20.

Community regarding the likely course of future events." One of these key judgments claimed that the number of radical Internet sites and self-generating cells in Western countries, to include the U.S., was expected to increase.[104] The estimate continued on to say that the spread of extremist ideology in both virtual and physical form "points to the possibility that others may become sufficiently radicalized that they will view the use of violence here as legitimate."[105] A report published that same year by the Future of Terrorism Task Force from the Homeland Security Advisory Council echoed the NIE assessment.[106] The task force strongly asserted that countering homegrown radicalization, in all of its forums, must be a top priority for the Department of Homeland Security.[107] Tools, methods, and metrics were needed to develop an early warning system for law enforcement and to produce intelligence that identifies emerging homegrown terrorism trends.[108]

D. NOT A TOOL JUST FOR JIHADISTS

Since the release of the 2007 NIE, statements and publications from the IC and law enforcement have only solidified the resolve to counter homegrown jihadism. Updated from its 2005 predecessor, the *2009 National Intelligence Strategy* explicitly states Mission Objective 1 is to "understand, monitor, and disrupt violent extremist groups…primarily al-Qaida and its regional affiliates, supporters, and the local terrorist cells it inspires…"[109] To do so, it must provide warning, disrupt terrorist plans, prevent acquisition of weapons of mass destruction, and counter radicalization.[110] Achieving such a goal requires both innovation and an appreciation of existing capabilities.

---

[104] Office of the Director National Intelligence, *National Intelligence Estimate: The Terrorist Threat to the U.S. Homeland* (Washington, DC: ODNI, 2007).

[105] Ibid.

[106] Homeland Security Advisory Council, "Report of the Future of Terrorism Task Force," Department of Homeland Security report, January 25, 2007, 8.

[107] Ibid.

[108] Ibid.

[109] Office of the Director of National Intelligence, *National Intelligence Strategy for the United States of America*, 6.

[110] Ibid.

Although it is understood that the Internet is only one of many possible factors contributing to the homegrown jihadist problem, it does appear to be a common enough facilitator. It should be reiterated, of course, that the Internet is not a problem in of itself. What makes it remarkable, on the contrary, is the tremendous utility it can provide all users, regardless of motive and intent. In this vein, scholar Gilbert Ramsay's argument about terrorist use of the Internet may have some salience. However, in line with his assertion of exercising government power in the real world, there must be consideration for exercising available techniques in a world that is increasingly technology-driven.

A number of articles, reports, and indictments within the past two years have drawn attention to the relevance of open source Internet data and dealing with homegrown jihadists. For instance, the FBI and Department of Homeland Security have been following for some time the publicly-available online discourse of Anwar al-Awlaki. The American-born radical cleric, who is suspected to now be hiding in Yemen, is considered by many to be a prominent instigator of U.S. jihad.[111] Awlaki's violent lectures and rants, distributed via his blog site and social networking sites YouTube and Halal Tube, and his connection to Fort Hood shooter Major Nidal Hasan, have made him a high value target for authorities.[112] Similarly, the tracking of Philadelphia-woman Colleen LaRose's social network site activity reportedly played a significant role in the foiling of her jihadist plot. Cases like these reflect a response to the concerns that have grown within the research, intelligence and law enforcement communities. The extent to which this response has contributed to disrupting homegrown jihad since 9/11 will be investigated in a later chapter, but it can be said that the Internet is at the counterterrorists' disposal. Notably, a Congressional Research Service report on the homegrown threat published during the preparation of this thesis also supports this claim.[113] While there are a number of challenging issues surrounding the authorities' use of online information, the Internet's permissive nature keeps it from being a tool just for jihadists; it is also a tool for authorities who track jihadists.

---

[111] Robert Mackey, "Blogging Imam who Counseled Fort Hood Gunman and 9/11 Hijacker goes Silent," *The New York Times*, November 13, 2009.

[112] Evan Perez, "White House Defends Targeted Killing Program," *The Wall Street Journal*, September 25, 2010.

[113] According to the report, "Among the tools employed by law enforcement is the monitoring of Internet and social networking sites." Jerome P. Bjelopera and Mark A. Randol, "American Jihadist: Combating a Complex Threat," Congressional Research Service Report RL41416, September 20, 2010, 39.

THIS PAGE INTENTIONALLY LEFT BLANK

III. COLLECTING AND USING INTERNET INFORMATION: CHALLENGES

A. INTRODUCTION

> *There's no inherent meaning in information; it's what we do with that information that matters.*[114]
>
> -Beau Lotto

The Internet is an essential provider of open source information. Media that was once restricted to print forms, radio, or television is now readily found in digital form that can be accessed from anywhere with a computer and Internet connection. More importantly, information can easily be updated and human interaction facilitated in a permissive, nearly real-time environment. However, the Internet is not to be equated with the "totality of open sources."[115] While it has grown in importance for intelligence operations, "the Internet is in reality a communications medium upon which information flows rather than an information repository in its own right."[116] This distinction is necessary as it is easy to assume, wrongly, that the Internet provides "one-stop shopping" for the most authoritative information a user seeks. Speeches, radio broadcasts, gray literature, and scholarly documents all constitute other forms of open sources that can produce meaningful information for authorities. The advantages gained from Internet information should therefore be realized in terms of relative utility to the whole of an investigative effort.

One key benefit of the Internet worth considering is the potential cost savings for collection activities. Clandestine intelligence and undercover law enforcement operations are risky and expensive. Exploiting Internet sources, such as a suspected jihadist-themed

---

[114] Beau Lotto, "Optical illusions show how we see," video presentation on TED website, http://www.ted.com/talks/beau_lotto_optical_illusions_show_how_we_see.html (accessed October 13, 2010).

[115] North Atlantic Treaty Organization, "Intelligence Exploitation of the Internet," October 2002, 4.

[116] Ibid.

blog or social networking site for example, may produce sufficient contextual information that eliminates the need to place an agent or officer in harm's way. Also, the availability of commercial online geospatial tools like Google™ Maps provides a cost-cutting solution to pricey and controversial imagery technologies.[117] What the Internet may well provide in the counter-homegrown terrorism role is a public gateway into known jihadist operating space, where clues of terrorist activity published by the perpetrators themselves can lead authorities to successful intervention.

Intervention is unlikely to be achieved, however, without careful analysis of Internet-derived information. Analysis determines the information's significance and therefore its applicability to a given user. While the intricacies of the analytical process are beyond the scope of this research, there are related issues that present challenges for the use of the Internet as a feasible and acceptable open source tool. The loftiest is a prevailing view that exploiting Internet information is not worth the time and effort. As observed by CIA veteran Ronald Marks, even a recent Director of Central Intelligence remarked, "I only have money to pay for secrets," when asked about leveraging the Internet's vast array of public sources.[118] Even if such a view dissipates, there remain a number of other obstacles. The rest of this chapter discusses some of the prominent challenges associated with collecting and using Internet information. It first addresses the common problem of information overload and suggests a baseline method for taming it. The second section illuminates the concern over language and cultural skill deficiencies among analysts, which can potentially hinder the ability to evaluate information. The third section discusses the challenge of determining the credibility of Internet information, drawing on the lessons learned from the research community. In the fourth section, a number of organizations closely involved in counterterrorism are presented in order to assess their strengths and suitability in using open source Internet

[117] Chris Pallaris, "Open Source Intelligence: A Strategic Enabler of National Security," Research Institute for European and American Studies website, http://rieas.gr/index.php?option=com_content&task=view&id=633&Itemid=41 (accessed September 27, 2010).

[118] Ronald Marks, "Spying and the Internet," *The Washington Times*, April 25, 2005.

information and to stress the importance of information sharing. Finally, the discussion turns to the controversial topics of protection of American privacy and civil liberty.

B. DEALING WITH INFORMATION VOLUME

Best and Cumming observe that one of the greatest obstacles analysts confront in exploiting open sources is the enormous volume of information. They remark that "identifying and analyzing information from this data stream can be daunting" for analysts.[119] The vastness of the Internet only compounds this dilemma. While queries submitted on standard Internet search engines can produce jihadist-related information, they are likely to turn out "laundry lists of irrelevant results" and create "information overload problems."[120] Some experts argue that such "related but unfocused information" complicates any effort to formulate a complete account of jihadist activity.[121] Therefore the Webmust be filtered to eliminate unrelated or misleading information. Yet the question remains as to what are considered irrelevant results. Certainly, a user will be seeking information that is accurate, complete and timely.

A useful way of addressing the overload problem, as suggested by the NATO OSINT guide *Intelligence Exploitation of the Internet*, is to first establish an Internet Collection Plan.[122] As with any intelligence operation, collection planning helps in keeping collection activities closely tied with the information requirements (in this case, the requirement is information indicative of jihadist activity). The guide outlines four steps for constructing an Internet Collection Plan:

Step 1: Determine Searchable Information Requirements

Step 2: Determine Best Sites or Search Strategy

Step 3: Identify the Details to Access or Find Specific Information

Step 4: Determine Search Time Constraints[123]

---

[119] Best and Cumming, "Open Source Intelligence (OSINT): Issues for Congress," 8.

[120] Hsinchun Chen et al., "Uncovering the Dark Web: A Case Study of Jihad on the Web," *Journal of the American Society for Information Science and Technology*, vol. 59, no. 8 (January 2008), 1348.

[121] Ibid.

[122] North Atlantic Treaty Organization, "Intelligence Exploitation of the Internet," 21.

[123] Ibid., 22.

Step 1 refers to a process of breaking down an information requirement to more specific components that can be reasonably sought after. For example, a requirement that asks for "indications of hostile intent" will likely produce vague results or nothing at all.[124] On the other hand, a searchable information requirement of "indications of recent weapons or explosives training" may yield better, more explicit results. Step 2 attempts to set an analyst on the right path by first starting with known websites that likely contain information related to the search. For instance, a useful starting point may be a visit to the interactive website of the New York-based radical Islamic movement 'Revolution Muslim,' whose goals include establishing Islamic rule in the U.S. and spreading Al Qaeda's word.[125] Step 3 ensures that the analyst identifies the details for website access (e.g., login ID and password) and key words that may lead the analyst to specific information. Step 4 establishes the time parameters for which site information is to be collected. This final step is important to consider as many online servers "only keep information posted for a set amount of time before it is replaced by fresh information."[126] Based on the format provided by the OSINT guide, a simple example of an Internet Collection Plan for homegrown jihad indicators could look like Figure 2:

Information Requirement	Site URL	Access Details or Key Words	Search Time or Frequency
Weapons Training	http://www.revolutionmuslim.com/	Rifles, guns, shooting	Within 48 hours
Jihadist Recruiting	http://www.youtube.com/	Jihad, al Shabab, caliphate	Daily updates
	http://www.jihadspun.com/		

Figure 2. Example Internet Collection Plan[127]

[124] North Atlantic Treaty Organization, "Intelligence Exploitation of the Internet," 22.

[125] Dina Temple-Ralston, "Revolution Muslim a Gateway for Would-be Jihadists," National Public Radio website, http://www.npr.org/templates/story/story.php?storyId=130519592 (accessed October 13, 2010).

[126] North Atlantic Treaty Organization, "Intelligence Exploitation of the Internet," 23.

[127] Ibid., 21.

Formulating a collection framework of this sort, or with more detail, can help with productivity and time efficiency. If anything, it attempts to focus collection efforts and diminish information overload. Still, more can likely be accomplished with the aid of newer, faster technological resources and search engines. Even organizations specialized in information technologies like the Defense Advanced Research Projects Agency found that their Web tools were not tailored for collecting and analyzing terrorist Internet information.[128] Others in counterterrorism are still confined to essentially 'doing it by hand,' using conventional search engines for archival and evaluation of jihadist Web material.[129]

C. LANGUAGE AND CULTURAL OBSTACLES

Another often-cited challenge that is closely tied to the information filtering problem is the deficiency in analyst language and cultural skills. Such skills aid in understanding the context in which information exists and further guide the selection of searchable information requirements. Even if one is able to track down a possible jihadist forum, an inability to interpret dialogue in a foreign language can mask critical leads or may sway the analyst to dismiss the source outright. In the case of homegrown jihadism, this may be of lesser concern considering the presence of more English-based sites. Still, a keen awareness of vulnerable groups within America's multicultural environment and those immigrant communities that may be attracted to these forums can focus collection and prevent analysis turning into broad-based opinion.

Most of the criticism regarding the lack of these important skills points to a greater organizational problem that places minimal emphasis on language proficiencies. Stephen Mercado of the CIA's Directorate of Science and Technology complains that the Intelligence Community "suffers from America's general indifference to foreign

[128] Hsinchun Chen et al., "Uncovering the Dark Web: A Case Study of Jihad on the Web," 1348–1349.

[129] Ibid., 1349; Jin Kim and William Allard also note that 'too frequently, all-source analysts are tasked with performing their own open source research that often results in nothing more than "Google™" searches,' in "Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Intelligence Analysis," 84.

languages and ideas."[130] Because few Americans pursue secondary languages through the undergraduate level, the Intelligence Community finds itself recruiting from a small pool of language and cultural experts.[131] Once hired, these new officers still require extensive training and job exposure before their skills can provide the needed impact.[132] The Foreign Broadcast Information Service, which is now folded under the National Open Source Center, has long been praised as the model for open source translation services, drawing upon foreign national and contract employees; however, it too suffers from the same personnel limitations.[133] Sophisticated translation tools are in development[134] to supplement the deficiency in actual human translators, but it is likely too early to discern whether they can, or should be, deemed effective replacements.

D. ASSESSING CREDIBILITY

If analysts are able to filter the overwhelming volume of information and translate discourse when necessary, they still face the ultimate challenge of determining the credibility of Internet information. Credibility, in essence, means the information's believability.[135] The limitless and generally unregulated nature of the Internet enables almost any person to author content and distribute it online. Miriam Metzger of the University of California's Department of Communication elaborates further:

---

[130] Stephen Mercado, "Sailing the Sea of OSINT in the Information Age," Central Intelligence Agency website, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies (accessed September 24, 2010).

[131] Ibid.

[132] Ellen Laipson, "Foreign Language Requirements in the Intelligence Community," statement to the Senate Government Affairs Committee, September 14, 2000.

[133] Ibid.

[134] For more in-depth discussions of cutting edge translation tools, see Ahmad Abbasi and Hsinchun Chen, "Applying Authorship Analysis to Extremist Group Web Forum Messages," IEEE Distributed Systems Online magazine article, http://ai.arizona.edu/intranet/papers/Abbasi%20Authorship%202005%20IEEEIS%20Final.pdf (accessed September 24, 2010); Mark Last et al., "Multi-lingual Detection of Terrorist Content on the Web," *Lecture Notes in Computer Science*, vol. 3917 (2006), 16; and National Open Source Center, *National Open Source Strategic Action Plan FY09* (Washington D.C.: ODNI, 2009), 8.

[135] C. Nadine Wathen and Jacquelyn Burkell, "Believe it or Not: Factors Influencing Credibility on the Web," *Journal of the American Society for Information Science and Technology*, vol. 53, no. 2 (2002), 134.

> This obviously raises issues of credibility, a problem that is exacerbated by the fact that many websites operate without much oversight or editorial review. Unlike most traditional (i.e., print) publishing, information posted on the Web may not be subject to filtering through professional gatekeepers, and it often lacks traditional authority indicators such as author identity or established reputation.[136]

Reasonably, such freedom increases the possibility that information presented online may be skewed, incomplete, remiss of facts, or manipulated in a manner as to be misleading. It is therefore not difficult to see how an analyst could easily be led astray.

This same difficulty in judging online information has long been a predicament for the academic community. Whereas conventional vetting of print sources like books, magazines and journal articles involve rigorous peer review and a recognized editorial process, little quality control exists for Internet sources scholars may be inclined to use.[137] As a result, efforts have been made to identify and promote the skills needed for evaluating online information.

Not surprisingly, research has shown that the skills best suited for assessing online information are essentially the same as those for assessing information transmitted in other forms of communication.[138] This seems sensible, as people were invariably faced with having to determine information credibility with the advent of print sources, the radio, and then television. Based on the literature, credibility evaluations of Internet information are often recommended to follow five criteria: accuracy, authority, objectivity, currency, and coverage. Metzger explains that *accuracy* measures the extent online information is free from errors and whether the information is both reliable and verifiable offline. *Authority* may be based upon author credentials, qualifications,

---

[136] Miriam J. Metzger, "Making Sense of Credibility on the Web: Models for Evaluating Online Information and Recommendations for Future Research," *Journal of the American Society for Information Science and Technology*, vol. 58, no. 13 (September 2007), 2078.

[137] Tony Doyle and John L. Hammond, "Net Cred: Evaluating the Internet as a Research Source," *Reference Services Review*, vol. 34, no.1 (2006), 59–60.

[138] J.E. Alexander and M.A. Tate, *Web Wisdom: How to evaluate and create information quality on the Web* (Hillsdale: Erlbaum, 1999); D.S. Brandt, "Evaluating information on the Internet. Computers in Libraries," 44-46; and J.W. Fritch and R.L. Cromwell, "Evalating Internet resources: Identity, affiliation, and cognitive authority in a networked world," *Journal of the American Society for Information Science and Technology*, vol. 52, no. 6 (2001) cited in Miriam J. Metzger, "Making Sense of Credibility on the Web: Models for Evaluating Online Information and Recommendations for Future Research," 2079.

affiliations, and external recommendations. *Objectivity* requires discernment of a website's purpose, or slant, which may be represented by the nature of facts and opinions presented and the types of sponsored or recommended links found on the site. *Currency* asks whether or not information is up to date (which may be simply represented by a date-time stamp). Finally, *coverage* assesses comprehensiveness of Internet information.[139]

For academics, meticulously following such criteria can help avoid compromise of their work by untested claims or opinions. For analysts assessing extremist content, however, these rules may not apply so rigidly. Indeed, bold claims and opinions might contain the indicators of violent intent analysts seek. Typographical errors on an open forum bear less consequence in comparison to the consistency and reliability of the information transmitted.

A beneficial characteristic of the Internet is that multiple online sources can be gathered rapidly and compared to help assess credibility. Furthermore, the use of cognitive analytic tools that measure clustering around certain topics of discussion can assist in identifying highly influential, and therefore meaningful, information streams.[140] Nonetheless, effective credibility assessments of online information are contingent upon a synchronous approach that leverages technological analysis with trained human expertise.

E. ORGANIZATIONS

Following the 9/11 Commission, the intelligence and law enforcement communities were charged with paying greater attention to terrorist threats to the

[139] Metzger, "Making Sense of Credibility on the Web: Models for Evaluating Online Information and Recommendations for Future Research," 2079.

[140] In the field of Social Network Analysis, clustering algorithms are applied to identify cohesion among actors with whom there is a shared relationship or tie. The implications for the Internet would be that high clustering around certain suspicious websites or topics within could indicate high levels of support, trust, and influence. For more on clustering, see Sean Everton, "Chapter 7: Cohesion and Clustering," in *Tracking, Destabilizing, and Disrupting Dark Networks with Social Network Analysis*, Naval Postgraduate School (2010), 126. For more on the use of analytical tools for open source information see also John C. Gannon's prepared statement for the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment found in "Using Open-Source Information Effectively," Serial No. 109-22 (Washington, DC: GPO, 2007), 10.

homeland emanating from within or from abroad. This also spurred the creation of new organizations and sub-organizations that were chartered to develop and fully implement advanced techniques to identify and assess terrorist threats. Additionally, these organizations were intended to establish an improved information sharing environment among federal, state, and local entities.[141] Private initiatives, to include federally-supported university projects that specialize in Internet analyses, also joined the counterterrorism effort. Indeed, many of these organizations possess incredible capabilities and resources to address the complicated threat of homegrown jihadist terrorism. Some agency-specific limitations, however, raise the question as to which entities are suited for collecting and assessing open source Internet information that may aid in confronting that threat. This places greater emphasis on integration and the necessity for improved sharing across organizations.

1. National Counterterrorism Center

The National Counterterrorism Center (NCTC) was specifically "established in 2004 to ensure that information from any source about potential terrorist acts against the U.S. could be made available to analysts and that appropriate responses could be planned."[142] More explicitly stated in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), the center's principal mission includes serving as "the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism."[143]

The NCTC is seen as the central organization that breaks down the so-called "wall" between intelligence and law enforcement, serving as an all-source fusion center for both communities. As the hub for intelligence integration and dissemination, NCTC

[141] Intelligence Reform and Terrorism Prevention Act of 2004, Section 1016, P.L. 108–458.

[142] Richard A. Best Jr., "The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns," Congressional Research Service Report R41022, January 15, 2010.

[143] Intelligence Reform and Terrorism Prevention Act of 2004, Section 1021, P.L. 108–458.

is expected to take full advantage of data mining, analytical technologies, and all counterterrorism-related intelligence drawn from the wide range of agencies and private sector entities.[144] Because the specific technical capabilities and practices of NCTC are not publicly available, it is difficult to comment as to what extent the center exploits open source Internet information. While it is understood that NCTC monitors the traffic and other activities of foreign terrorists and their supporters, the exceptions of domestic terrorism and counterterrorism as stated in P.L. 108-458 raise the question as to whether or not the agency can be intimately involved with the issue of homegrown jihad. There is a clause that states the center may receive and disseminate intelligence from any federal, state, local or other source as consistent with applicable law, but details of under what conditions are not specified.[145]

Richard Best points out that the circumstances surrounding the Fort Hood Army Installation attack carried out by Major Nidal Hasan may reflect NCTC's limitations. Because Hasan was a U.S. citizen and a commissioned officer, information regarding his electronic communications and his intentions were likely not to come to the direct attention of NCTC. Details of the center's involvement will perhaps become clearer as the investigation continues.[146] It does seem, however, that NCTC has exhibited more of a role as facilitator among other agencies dealing directly with the homegrown threat. Espousing a "whole of government" approach, director Michael Leiter states that NCTC has worked closely with national security agencies such as DHS and the FBI to counter domestic radicalization in local communities and over the Internet.[147] This could also be due to the fact that NCTC is not a large collection agency nor does it have grasp of a

[144] Best, "The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns," 2.

[145] Intelligence Reform and Terrorism Prevention Act of 2004, Section 1021, P.L. 108–458.

[146] Best, "The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns," 8.

[147] Michael Leiter, "Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland," statement before the Senate Homeland Security and Government Affairs Committee, September 22, 2010, 7–8.

sizable budget in comparison to the rest of the IC.[148] These possible deficiencies and a broadly defined mission challenge the center's full engagement of the homegrown problem.

2. DHS Office of Intelligence and Analysis

In July 2005, also in response to the mandates of P.L. 108-458 and the additional requirements from the Implementing Recommendations of the 9/11 Commission Act of 2007, the Department of Homeland Security established the Office of Intelligence and Analysis (I&A) to serve as the link between the department, the IC, and state, local, and private sector partners.[149] As another intelligence fusion initiative, I&A's mission is to optimize the DHS information collection and analysis capability for distribution of timely and actionable intelligence to a wide range of customers, while respecting American civil liberties and privacy.[150]

Mark Randol discusses that because DHS does not engage in foreign intelligence collection (e.g., imagery intelligence, human intelligence, foreign open source intelligence, etc.), the I&A instead combines that information as provided by other elements in the IC with the information collected by DHS components. For example, information from local law enforcement, the private sector, domestic open sources, and research on violent radicalization may be fused with relevant foreign information to produce intelligence products for a variety of users.[151]

While details of organic collection activities are unclear, it does seem that I&A embraces its role as the sharer of information, producing a number of analytical products,

---

[148] Best, "The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns," 8; Chris Strohm, "Director: NCTC has Analyst Shortage," Government Executive website, http://www.govexec.com/dailyfed/0110/012710cdpm2.htm (accessed October 13, 2010).

[149] Mark A. Randol, "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress," Congressional Research Service Report R40602, March 19, 2010, 2.

[150] Department of Homeland Security, "Office of Intelligence and Analysis," http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm (accessed October 13, 2010).

[151] Randol, "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress," 5.

both classified and unclassified, that cover domestic and foreign terrorist threats.[152] In addressing homegrown jihadism, however, the office focuses on a perspective separate from actual extremist activities. As stated on I&A's webpage:

> Our top priority is radicalized Islam (Sunni and Shia groups), but we also look at radicalized domestic groups. We do not monitor known extremists and their activities; instead, we are interested in the radicalization process—why and how people who are attracted to radical beliefs cross the line into violence.[153]

This statement, at first glance, would seem to make clear that I&A does not engage in monitoring activities, such as Internet monitoring. Yet, as read, one may reasonably offer that the process of understanding the *why* and *how* of homegrown radicalization could invariably lead I&A to evaluate Internet sources that DHS and other agencies have repeatedly recognized as jihadist facilitators. Furthermore, although not widely publicized, other DHS initiatives have specifically involved the monitoring of publicly-viewable sites for more general purposes. Leading up to the January 2009 presidential inauguration of Barack Obama, DHS operated a Social Networking Monitoring Center (SNMC) that collected on "items of interest" from sites like Facebook, Twitter, and YouTube to provide "enhanced situational awareness" to the DHS National Operations Center. The department stressed an adherence to the Fair Information Practice Principles[154] to guard against privacy infringements and the collection of Personally Identifiable Information (PII), which was in line with the DHS mission statement. But it was also made clear that in assessing situational awareness, they were also scanning for indicators of "life or death incidents" and "natural or man-made disasters."[155]

---

[152] Randol, "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress," 9.

[153] Department of Homeland Security, "Office of Intelligence and Analysis," http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm (accessed October 13, 2010).

[154] Department of Homeland Security Privacy Office, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," Department of Homeland Security website, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (accessed October 13, 2010).

[155] Social Networking Monitoring Center, "Concept of Operations for the Presidential Inauguration," slideshow available at Electronic Frontier Foundation website, https://www.eff.org/files/filenode/social_network/DHS_SNMC_Inauguration_monitoring.pdf (accessed October 13, 2010).

Online information collected via centers like the SNMC is likely to pass through the I&A if the office is as integrated as DHS claims it to be. Whether such information is thoroughly analyzed for indications of jihadist activity is still questionable. The I&A's ability to provide quality service to State and local authorities, who are often seen as the "first preventers" of terrorism,[156] will rest upon its capability to receive and evaluate information that is acquired by emerging collection methods as exhibited by the SNMC.

3. National Open Source Center

The National Open Source Center (NOSC) was established by the DNI in November 2005 as the bedrock of what has been labeled the Open Source Enterprise. As identified earlier, increased leverage of open source information was emphasized after the release of the 9/11 Commission Report and the signing of the Intelligence Reform and Terrorism Prevention Act of 2004. The NOSC, which resides at the CIA, builds upon the former Foreign Broadcast Information Service which has long held distinction for its foreign open source exploitation capability. As such, it is uniquely proficient in providing translations and analysis of a wide range of open source information for a number of agencies.

As stated in Intelligence Community Directive 301, "the Center serves to advance the IC's exploitation of open source material and nurtures acquisition, procurement, analysis, dissemination, and sharing of open source information, products, and services throughout the USG."[157] Although the NOSC would appear to be the principal organization for collecting and assessing open source Internet information to counter the homegrown threat, it does have limitation. Because it currently falls under the administrative control of the CIA, the NOSC is constrained in providing adequate support to law enforcement agencies and state, local, and tribal entities."[158] The National Security Act's statutory prohibition of CIA participation in law enforcement activities

---

[156] Randol, "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress," 6.

[157] Office of the Director of National Intelligence, *Intelligence Directive 301: National Open Source Enterprise*, July 11, 2006, 5.

[158] Best and Cumming, "Open Source Intelligence (OSINT): Issues for Congress," 20.

essentially bars the NOSC from collecting information directly on activities within the United States.[159] As a result, organizations like the DHS Office of Intelligence and Analysis have in the interim relied on the NOSC more for technical support and training.

4. Federal Bureau of Investigation

The FBI has both been praised and harshly criticized for its broad range of activities with the Internet. Recognized for its successes in countering cyber fraud, cyber crime, and online predators, the FBI's counterterrorism efforts using the Internet have generally not been well received. This is predominantly due to the revelation in 2000 of the bureau's software program known as *Carnivore* that could be installed in Internet Service Provider equipment to intercept private e-mails and track user Web activity. Consequently, this raised the heated issue of possible privacy infringement of innocent Internet users.[160] A key distinction to be made here is that Carnivore enabled the FBI to essentially conduct electronic eavesdropping (versus open source collection), which is prohibited under Title III of the Electronic Communications Privacy Act.[161]

Legislative reform has provided improved governance and oversight of wiretapping and electronic surveillance while still allowing the FBI to confront a host of cyber-related threats. The bureau's Cyber Division, for example, claims to be tailored to address domestic cyber threats and the pursuance of the perpetrators.[162] However, according to the division's director Gordon Snow the primary thrust of the Cyber Division is to track down criminals or terrorists who attempt to conduct computer network penetrations and attacks.[163] Snow remarks that "the first cyber threat is terrorist groups and organizations using cyber as a means for recruitment, radicalization and

---

[159] Best and Cumming, "Open Source Intelligence (OSINT): Issues for Congress," 20.

[160] Marcia S. Smith et al., "Internet: An Overview of Key Technology Policy Issues affecting its Use and Growth," Congressional Research Service Report 98-67, December 29, 2004, 5.

[161] 18 U.S.C 2511.

[162] Federal Bureau of Investigation, "National Cyber Investigative Joint Task Force," FBI website, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (accessed September 29, 2010).

[163] Ben Bain, "Meet the FBI's new top cyber cop," Federal Computer Week website, http://fcw.com/Articles/2010/06/28/FEAT-QandA-gordon-snow-FBI.aspx?Page=1 (accessed October 13, 2010).

communication," but "the threat we mine down on here in the Cyber Division is them using their capabilities and tools as a point or vector to do damage to critical infrastructure or systems within the United States."[164] While the division seeks to identify domestic terrorists, it seems that this program within the FBI places less emphasis on what Snow identifies as the first threat. Another FBI initiative, however, may be filling that void.

An advanced electronic surveillance program known as the "Going Dark" program was budgeted $233.9 million for 2010.[165] The FBI has stated that the program's purpose is to exploit changing technology and Inernet-Based capabilities and to conduct automated analysis of surveillance subjects.[166] Whether this program specifically involves open source monitoring is not yet known. Since the public release of the program, however, there have been recent reports of suspected homegrown jihadist incidents that involved the FBI monitoring public websites and blogs prior to advancing investigations.[167]

5. University of Arizona Dark Web Project

In 2002, a team of terrorism researchers and computer scientists came together at the University of Arizona's Artificial Intelligence Laboratory to devise a new way of obtaining and analyzing terrorism on the Internet. They defined their research environment as the "Dark Web," referencing "the portion of the World Wide Web used to help achieve the sinister objectives of terrorists and extremists."[168]

---

[164] Bain, "Meet the FBI's new top cyber cop."

[165] Department of Justice, "FBI FY2010 Budget Report," http://www.justice.gov/jmd/2010summary/pdf/fbi-bud-summary.pdf (accessed October 10, 2010).

[166] Jason Ryan, "DOJ Budget Details High-Tech Crime Fighting Tools," ABC News website, http://abcnews.go.com/TheLaw/story?id=7532199&page=1 (accessed October 10, 2010).

[167] See for example Carol Cratty, "Terror suspect pleads guilty in threat against 'South Park' creators," CNN website, http://www.cnn.com/2010/CRIME/10/20/us.south.park.terror.threat/index.html?eref=mrss_igoogle_cnn (accessed October 20, 2010); and Kim Zetter, "FBI allegedly caught using GPS to spy on student," CNN website, http://www.cnn.com/2010/TECH/gaming.gadgets/10/08/fbi.tracks.student.wired/index.html?eref=mrss_igoogle_cnn (accessed October 8, 2010).

[168] Hsinchun Chen et al., "Uncovering the Dark Web: A Case Study of Jihad on the Web," 1347.

The team had observed that advanced Web data mining technologies had been widely used in business and scientific research. Yet to their knowledge no such approach had been applied to collect and analyze terrorist information on the Internet.[169] As a result, they devised a semi-automated system that methodically collects jihadist-related information, filters it, and then analyzes it. Using a collection technique called "spidering," the system is able to harvest extremist websites, forum threads, and multimedia files such as images, audio, and video clips.[170] More impressively, the system collects and processes forum contents in Arabic, English, Spanish, French and Chinese.[171]

The Dark Web system is designed to reduce the challenges faced by researchers and information managers in collecting and analyzing multilingual information generated by terrorists and their sympathizers.[172] Furthermore, the system relies totally on open source information. Unlike some of the controversial NSA and FBI programs, the Dark Web project is not supposed to be a secretive interception tool. Rather, it is a targeted retrieval system that searches for specific terrorist indicators posted on the public web. Because America now faces a homegrown jihadist threat that also makes use of the Internet, open source systems like the Dark Web project may be particularly useful in early identification. This capability may provide a feasible solution to the current statutory prohibition limiting the NOSC and serve as a model for ongoing efforts within the FBI and DHS in focusing scope and protecting individual privacy.

F. PRIVACY AND CIVIL LIBERTIES

As alluded to throughout this research, the protection of American privacy and civil liberties is a highly contentious issue and arguably presents one of the more daunting challenges of those discussed thus far. In the wake of 9/11, Congress passed the United and Strengthening America by Providing Appropriate Tools Required to Intercept

169 Chen et al., "Uncovering the Dark Web: A Case Study of Jihad on the Web," 1349.

170 The University of Arizona, "Dark Web Terrorism Research."

171 Ibid.

172 Edna Reid and Hsinchun Chen, "Extremist Social Movement Groups and their Online Digital Libraries," 61.

and Obstruct Terrorism (USA PATRIOT) Act, P.L. 107-56, thereby increasing the ability for law enforcement and other government entities to intercept computer communications. In particular, e-mail sender and addressee information (not message content) and website visits could be captured by way of trap and trace devices attached to Internet service equipment.[173] According to Marcia Smith et al., the debate about law enforcement monitoring Internet activity was not a highly visible issue leading up to the September 11, 2001 attacks.[174] This was due in part to the congressional mandate that a court order must first be issued before surveillance could take place. Furthermore, many citizens were more concerned at the time on consumer privacy issues; that is to say, "the collection, use, and dissemination of personally identifiable information by commercial website operators" without the consent of the owners.[175] The authorization of the USA PATRIOT Act, however, quickly shifted concerns about commercial misuse to the more unnerving possibility of government abuse of personal information.

Section 212 of the USA PATRIOT Act stirred some of the greatest controversy, as it authorized ISPs to act without customer consent prior to disclosing personal information.

> Section 212 *allows* ISPs to divulge records or other information (but not the contents of communications) pertaining to a subscriber if they believe there is immediate danger of death or serious physical injury or as otherwise authorized, and *requires* them to divulge such records or information (excluding contents of communications) to a governmental entity under certain conditions. It also allows an ISP to divulge the *contents* of communications to a law enforcement agency if it reasonably believes that an emergency involving immediate danger of death or serious physical injury requires disclosure of the information without delay.[176]

---

[173] Gina Marie Stevens and Charles Doyle, "Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping," Congressional Research Service Report 98-326, December 3, 2009, 31.

[174] Marcia S. Smith et al., "The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government," Congressional Research Service Report RL31289, March 4, 2002, 16–17.

[175] Ibid.

[176] Ibid., 17.

Although Section 212 was subject to sunset, Congress was able to subsume and further expand the section's authorizations in Section 225 of the Homeland Security Act (P.L. 107-296). Congress amended the original clause to lower the threshold in which ISPs could disclose information and to whom they could divulge in. Instead of requiring a "reasonable belief," ISPs only needed a "good faith" belief of a life-threatening danger. Nor did the danger need to be "immediate."[177] Section 225 also allowed ISPs to voluntarily divulge private communications to federal, state, or local government agencies instead of just a "law enforcement agency" as originally stated in Section 212 of the USA PATRIOT Act.[178]

The perception of privacy infringement predictably weighs heavily on any future developments in technology-based surveillance. Even the use of open source information that is drawn from online public forums carries the risk of inadvertent collection of personally identifiable information. Such risk can result in significant backlash by the American public if not handled with care. While any range of measures still may not appease the most ardent of privacy advocates, there have been policies put forth by Congress and government agencies to uphold the right to privacy yet still allow sufficient leeway, in their view, to protect the public from harm. DHS, for example, published in December 2008 a Privacy Policy Guidance Memorandum that explicitly states the department's adherence to the Fair Information Practice Principles (FIPPs), a set of principles that form the framework of the Privacy Act of 1974. The FIPPs govern the department's use of personally identifiable information, requiring transparency, purpose specificity, and data minimization to ensure individual privacy is maintained.[179] More recently, DHS disseminated a Privacy Impact Assessment statement in June 2010 that describes the department's new publicly available social media monitoring initiative and

[177] Electronic Frontier Foundation, "Let the Sun Set on Patriot: Section 212 and Homeland Security Act Section 225," Electronic Frontier Foundation website, http://w2.eff.org/patriot/sunset/212.php (accessed October 13, 2010).

[178] Smith et al., "Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth," 5.

[179] Department of Homeland Security Privacy Office, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security."

outlines the measures in place to safeguard personal information.[180] These types of policies help to improve the transparency of government activities on the Internet. Greater secrecy on the other hand, especially in relation to domestic affairs, is likely only to result in greater recoil.

Transparency through public announcements is only half of the solution, however. The other half rests on the government's ability to prove that the methods it employs are also not an infringement on First Amendment rights. Public opinion, to include dissent, is protected, and Internet venues arguably support that constitutional right. Consequently, the challenge for authorities in using publicly available Internet discourse is "successfully proving criminal intent to incite" or carry out violent jihadist attacks.[181] According to Siobhan O'Neil, authorities have had some success in this arena when dealing with other domestic extremist groups that operate online.[182] A recent case involving a self-proclaimed jihadist from Virginia, who reportedly posted violent threats online and provided material support to known terrorists, also displays the capacity for success against homegrown jihad.[183]

The implication for policymakers therefore is one that has been stressed time and again. Policymakers, and the policy enforcers, must strive for a balance in protecting American society through as many means as available while still upholding the fundamental rights of its citizenry. Increasing awareness of government activities over the open Internet (and the governing laws and regulations of those activities) is essential, as is spreading the knowledge that such methods can potentially aid in countering homegrown terrorist activity.

---

[180] Department of Homeland Security Office of Operations Coordination and Planning, "Privacy Impact Assessment: Publicly Available Social Media Monitoring and Situational Awareness Initiative," Department of Homeland Security website, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia.pdf (accessed October 20, 2010).

[181] Siobhan O'Neill, "Terrorist Precursor Crimes: Issues and Options for Congress," Congressional Research Service Report RL34014, May 24, 2007, 15.

[182] Ibid., 16.

[183] Carol Cratty, "Terror suspect pleads guilty in threat against 'South Park' creators," CNN website, http://www.cnn.com/2010/CRIME/10/20/us.south.park.terror.threat/index.html?eref=mrss_igoogle_cnn (accessed October 20, 2010).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDIES

A. OVERVIEW

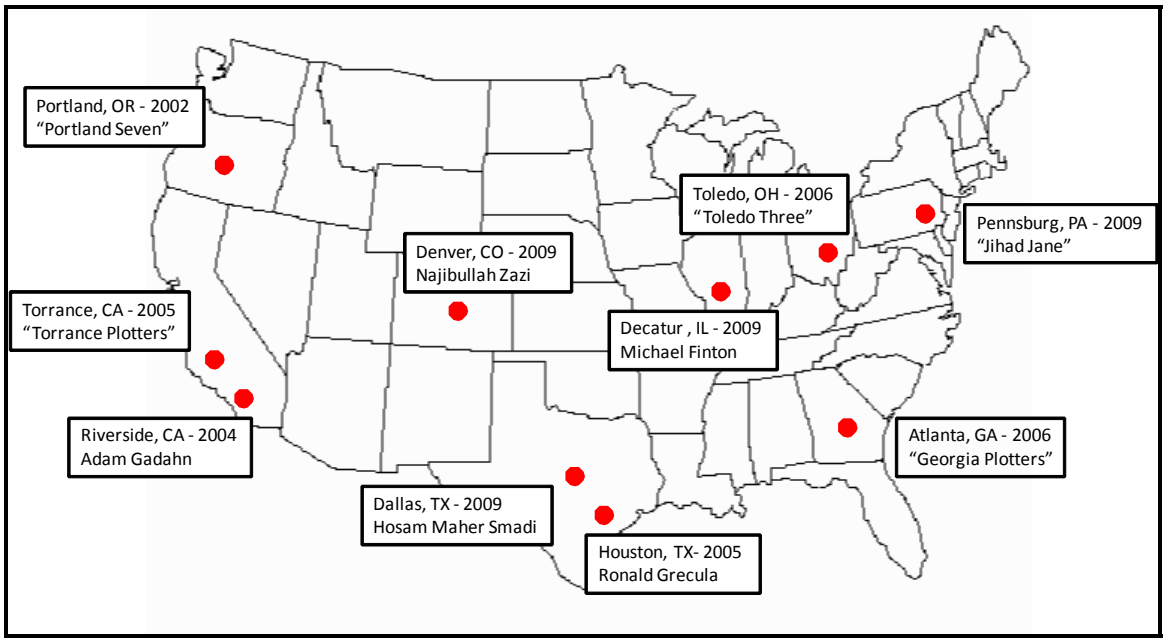

Figure 3. Case Study Map

This chapter presents a series of case studies of homegrown jihadist incidents that occurred across the nation since 9/11, providing a description of the plotters involved, a synopsis of each incident, and detailed evaluations of the investigations. Figure 3 above provides a snapshot of those cases. The analysis of each incident followed the construct that was discussed in Chapter I, with the purpose of providing a qualitative understanding of detection techniques and the contribution by open source Internet exploitation. Using available legal documents and media reports, potential indicators were classified under these general categories: interpersonal; Inernet-Based; incident reports and watchlist alerts; documents, media, and material; or confidential. Each category was then appraised at length using the following queries:

- Was the information "good enough" at the time of discovery, therefore allowing timely intervention?
- Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?
- Was the information shared in order to attract other useful information?

The first question sought to determine if reported or discovered indicators were immediately telling of a possible jihadist plot and allowed for authorities to intervene or initiate the investigative process. The second question, though seemingly redundant, sought to answer whether certain indicators provided contextual knowledge of jihadist activity that assisted in furthering the investigation or intervention. The third question attempted to capture instances of information sharing not only among government agencies, but also from the private and community sectors. An assessment was then provided for each case to elucidate the success, shortcomings, or non-applicability of open source Internet exploitation. Figure 4 is an overview of the profile for each case that was evaluated. This chapter concludes with a summary discussion of key findings.

Plot	Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
Portland Seven		X	X	X	X
Torrance Plotters		X	X	X	X
Adam Gadahn	X	X	X	X	
Ronald Grecula			X	X	X
Najibullah Zazi	X	X	X	X	X
Michael Finton	X	X	X	X	X
Hosam Smadi	X	X	X	X	X
Georgia Plotters	X	X	X	X	X
Toledo Three	X	X	X	X	X
Colleen LaRose	X	X	X	X	

Figure 4. Overview of Indicators for Selected Studies

B. PORTLAND SEVEN—PORTLAND, OR (2002)

Habis Abdulla al Saoub. A Jordanian native, Al Saoub had served as a former mujahedeen during the Soviet-Afghanistan conflict. He was considered the de facto leader of the Portland cell, providing the political justification for the group's endeavors.

Jeffrey Leon Battle. A U.S. national originally from Houston, Texas, Battle moved to Portland after washing out of U.S. Army boot camp.

October Martinique Lewis. Lewis, a convert to Islam and Battle's ex-wife, joined the cell when she too moved to Portland from Houston.

Patrice Lumumba Ford. An Islamic convert raised in Portland, Ford was once held in high esteem at the Portland City Hall where he served twice as an intern. He was introduced to the cell through the Masjid as-Saber mosque.

Maher Hawash. A naturalized citizen originally from Palestine, Hawash was a respected software engineer for Intel. He returned to the Islamic faith after the death of his father in 2000, but subsequently joined the extremist cell while attending the Masjid as-Saber mosque.

Ahmed Ibrahim Bilal and Muhammad Ibrahim Bilal. Little background information is available, but the two U.S.-born brothers were also reportedly recruited through mosque affiliations.[184]

Summary. In October 2002, five members of the Portland-based group were arrested by the FBI for attempting to travel to Afghanistan and join the Taliban in fighting the U.S. military. Maher Hawash, was arrested a year later in connection to the conspiracy, and the seventh member, al Saoub, was reportedly killed in Afghanistan by Pakistani forces.[185] During the course of their plot, members conducted firearms training, provided

[184] Bjelopera and Randol, "American Jihadist Terrorism: Combating a Complex Threat," 115; Silber and Bhatt, "Radicalization in the West: The Homegrown Threat," 57–58, 59, 61.

[185] Bjelopera and Randol, "American Jihadist Terrorism: Combating a Complex Threat," 115–116.

funding, conspired to attack Jewish establishments, and attempted to enter Afghanistan multiple times by way of China and Pakistan.[186]

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
N/A	Surveillance of email and bank transfers	Police report for firearms incident	Discarded Jordanian passport and "Martyr's Will"	Informant/Taped Conversations Wiretaps

Figure 5. Portland Seven Indicators

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Inernet-Based

Yes. By the time the FBI had chosen to conduct surveillance of e-mails under the USA PATRIOT Act, authorities already had suspicion that there were a number of individuals involved in a conspiracy to enter Afghanistan.[187] Authorities scrutinized hundreds of e-mail exchanges between Battle and his partners and confirmed identities of the other six cell members.[188]

Incident Reports

No. On September, 29, 2001, a Sheriff's Deputy from Skamania County, Washington was dispatched to a gravel pit after receiving a report of men shooting firearms. The deputy made no arrests after talking with the group but he did write a

[186] *United States v. Jeffrey Leon Battle et al.*, Criminal No. 02-399HA, in the U.S. District Court for the District of Oregon, October 3, 2002, www.justice.gov/ag/100402indictment.pdf (accessed August 21, 2010), 4–6.

[187] Department of Justice, "Report from the Field: The USA PATRIOT Act at Work," July 2004, 6.

[188] Ibid., Bjelopera and Randol, "American Jihadist Terrorism: Combating a Complex Threat," 116.

police incident report, identifying the names of all involved. The deputy was unaware that the conspirators were training to fight American forces abroad and sent them on their way without further dispute.[189]

Documents

Unknown. According to the October 2002 indictment, al Saoub discarded a bag containing a cancelled Jordanian passport and a 'Martyr's will' addressed to the Mujahideen leader Mohammad Ibin Abdallah.[190] The bag was reportedly fished out of the recycling bin at his apartment by a neighbor who then turned it into the FBI.[191] Although the information would prove useful in the case later on, it is not clear if it was a sufficient indicator at the time to allow intervention of the plot.

Confidential Sources

Yes. The FBI placed a confidential informant in the mosque attended by the group. He in turn befriended Battle, allowing him to secretly record a number of conversations revealing the group's intentions to attack local Jewish synagogues and the plan to go to Afghanistan. While investigators could have moved on Battle at that time, they chose to continue monitoring with the intent of capturing the rest of the cell.[192]

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Inernet-Based

Yes. According to Assistant U.S. Attorney Charles Gorder, a prosecutor in the case, the information gathered from intercepted e-mails helped corroborate the evidence

[189] William McCormack, "State and Local Law Enforcement Contributions to Terrorism Prevention," http://www2.fbi.gov/publications/leb/2009/march2009/terrorism.htm (accessed August 21, 2010).

[190] *United States v. Jeffrey Leon Battle et al.*, Criminal No. 02-399HA, 7.

[191] Terence P. Jeffrey, "Terrorist Blamed his Failure on Bush," Human Events website, http://www.humanevents.com/article.php?id=12329&keywords=gorder (accessed August 21, 2010).

[192] U.S. Department of Justice, "Report from the Field: The USA PATRIOT Act at Work," 5–6.

investigators had gathered on the cell members. The FBI was able to track instructions and money transfers, thereby enabling the bureau to build the case for conspiracy to provide material support to terrorists.[193]

Incident Reports

Yes. The Sheriff's Deputy may not have picked up on a jihadist conspiracy at the time, but his report did catch the attention of his boss who recognized the name of a wanted individual he saw on the news. The deputy's report later served as evidence of the jihadist cell's training.[194]

Documents

Yes. Though the discarded passport and will did not enable early intervention, the documents did later support the investigation. As found in the indictment, they were considered as part of a number of specific overt acts in furtherance of the conspiracy to wage jihad.[195]

Confidential Sources

Yes. The information from the informant did indeed provide "good enough" understanding of jihadist plotting to move forward with investigation. As noted earlier, Battle openly admitted to the informant that the group considered attacking Jewish establishments. According to the Department of Justice, "this gave prosecutors the confidence not to arrest Battle prematurely while they continued to gather evidence on the other members of the cell."[196] The FBI was then able to attain clearance to conduct wiretaps of the other members. The information gained by these undercover sources, supported by e-mail exchanges, allowed authorities to arrest the entire group (instead of just Battle) prior to executing any sort of domestic attack.[197]

---

193 Jeffrey, "Terrorist Blamed his Failure on Bush."

194 McCormack, "State and Local Law Enforcement Contributions to Terrorism Prevention."

195 *United States v. Jeffrey Leon Battle et al.*, October 3, 2002, 7.

196 Department of Justice, "Report from the Field: The USA PATRIOT Act at Work," 6.

197 Ibid.

3. Was the information shared in order to attract other useful information?

Inernet-Based

Unknown. Available reporting does not indicate whether or not intercepted e-mail information was shared outside of the FBI.

Incident Reports

Yes. Upon processing the police report, the Skamania County Sheriff's Office identified one of the shooters as a convicted felon in Oregon, and in turn passed the report to the Portland FBI office.[198] The report helped open the investigation that would lead to the discovery of the jihadist cell.

Documents

Yes. An alert and apparently suspicious neighbor turned over the documents to the FBI.

Confidential Sources

Yes. It was an Oregon state trooper, who learned of the investigation through the Portland Joint Terrorism Task Force (JTTF) who first developed the confidential informant within the local Muslim community.[199]

Assessment. In the case of the Portland Seven, open source Internet information did not contribute to the investigation. Rather, a combination of other indicators helped discover this case of homegrown jihadism. While the firearms incident report may be seen as the most important catalyst, it may have yielded nothing at all had not the Skamania County Sheriff's Office passed along the information. Successful maneuvering of a confidential informant and interceptions of communications under the USA PATRIOT Act contributed the most in directly uncovering the conspiracy. The reporting of the suspicious documents by a wary neighbor helped confirm the group's intent. In this instance, overall success was achieved through proactive information sharing by local law enforcement and coordination between partner agencies.

---

[198] McCormack, "State and Local Law Enforcement Contributions to Terrorism Prevention."

[199] Ibid.

C. TORRANCE PLOTTERS—TORRANCE, CA (2005)

Kevin James. Considered the leader of the cell, James founded the Jam'iyyat Ul-Islam Is-Saheeh group while in prison.

Levar Washington. Washington was recruited by James while also serving as an inmate. Upon release, he took guidance from James who orchestrated the group's plot from prison.

Gregory Patterson. An employee at the Los Angeles Airport, Patterson was recruited by Washington while attending the Jamaat-E-Masijudal mosque.

Hammad Samana. Samana was a U.S. resident originally from Pakistan and a student at Santa Monica College. He too was recruited by Washington while at the Jamaat-E-Masijudal mosque.

Summary. In August 2005, the members of the homegrown group known as Jam'iyyat Ul-Islam Is-Saheeh (JIS) were charged with conspiracy to levy war against the U.S. through terrorism. They plotted to attack Los Angeles-area military facilities, Jewish establishments, and the Los Angeles International Airport. James, who was incarcerated, directed from prison the other members of the cell to conduct training, reconnoiter targets, and finance their jihadist operation through armed robberies.[200]

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
N/A	Search of Internet browsing history	Criminal Investigation following a number of armed robberies of gas stations	Target lists & Jihadist manifestos Bin Laden poster	Trace of lost cell phone Surveillance

Figure 6. Torrance Plotters Indicators

[200] *United States v. James et al.*, Criminal No. 05-CR-214, In the U.S. District Court for the Central District of California, August 31, 2005, http://nefafoundation.org/file/FeaturedDocs/U.S._v_James_Indictment.pdf (accessed July 23, 2010); NEFA Foundation, "The LA Plot to Attack U.S. Military, Israeli Government, & Jewish Targets," Report No. 1, January 2008, http://www.nefafoundation.org/miscellaneous/LA_Plot.pdf (accessed July 23, 2010), 1–2.

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Inernet-Based

No. After their arrest, Patterson and Samana admitted to using the Internet on home computers to research U.S. military, Israeli government, and Jewish targets that were listed on the cell's handwritten "Modes of Attack" document. Validation of these claims was subsequently conducted after the computers had been seized and exploited by authorities.[201] The information was certainly good enough to support the case. However, because it was not discovered until after the suspects had been apprehended, the information contributed little to an early intervention of the plot.

Incident Reports

No. The cell conducted a string of gas station robberies throughout southern California to fund their terrorist plans.[202] However, police response was criminally-focused, and reasonably so—nothing from any of the robberies roused suspicion of potential terrorism.

Documents, Media, Material

Yes. The subsequent search of the residence shared by Washington and Patterson revealed the JIS "Modes of Attack" document, which identified the group's proposed targets. In addition to this document were found military-style equipment and a Usama Bin Laden poster.[203] One of the police officers, who had been trained to identify potential signs of radicalism, deemed the discovery significant enough to report it to the Los Angeles JTTF. The task force went to work immediately.[204]

---

[201]NEFA Foundation, "The LA Plot to Attack U.S. Military, Israeli Government, & Jewish Targets," 5–6.

[202] McCormack, "State and Local Law Enforcement Contributions to Terrorism Prevention."

[203] The NEFA Foundation, "The LA Plot to Attack U.S. Military, Israeli Government, & Jewish Targets," 4, 7, 9.

[204] Shane Harris, "L.A.'s anti-terrorism hub serves as a model," Government Executive website, http://www.govexec.com/dailyfed/0507/050207nj1.htm (accessed August 21, 2010).

Confidential Sources

No. Police discovered a cell phone that had been dropped at one of the robbed gas stations and were able to trace it back to Patterson. There were no indications of jihadist activity, but the evidence as related to the criminal incident was significant enough for the authorities to locate Patterson's residence and place him under surveillance in the hope of catching him in a criminal act.[205]

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Inernet-Based

Yes. The Internet history information, though discovered after the apprehension of the suspects, was good enough to support the existence of a jihadist conspiracy. Authorities were able to use this information to demonstrate the JIS intent to attack the targets listed on the "Modes of Attack" document.[206]

Incident Reports

No. Given the string of robberies and limited information available, Southern California police believed they had strictly a criminal case on their hands. Police remained unaware even after the discovery of Patterson's cell phone at a crime scene.

Documents, Media, Material

Yes. The "Modes of Attack" document seized during the apartment search clearly stated "Military Targets" and listed known military offices in the Los Angeles area. The Los Angeles airport and the Israeli Consulate were also listed.[207] Given the types of

[205] Shane Harris, "L.A.'s anti-terrorism hub serves as a model;" McCormack, William, "State and Local Law Enforcement: Contributions to Terrorism Prevention."

[206] *United States v. James et al.*, Criminal No. 05-CR-214.

[207] NEFA Foundation, "The LA Plot to Attack U.S. Military, Israeli Government, & Jewish Targets," Report #1, 4–9.

targets identified, the confiscation of military-style equipment, and the presence of jihadist propaganda at the household, the JTTF was more than compelled to move forward with investigation.[208]

Confidential Sources

No. In context, the cell phone trace and surveillance were not sufficient indicators of jihadist activity. The police were after gas station robbers. By actively observing Patterson, the police were able to capture him and his associates during a criminal act, and subsequently conduct a search of their residence.[209]

3. Was the information shared in order to attract other useful information?

Inernet-Based

Unknown. The indictments against the suspects indicate that the information found on their computer Internet history was useful to the prosecution.[210] However, it is not explicitly clear as to what extent the information was shared among partner agencies of the JTTF.

Incident Reports

Unknown. Available sources do not indicate that the reports of the robberies were proactively shared among Los Angeles area police departments or other agencies. However, this is not to say that the information was not made available.

Documents, Media, Material

Yes. Attorney Thomas P. O'Brien of the Central District of California, the office that prosecuted the Torrance case, stated that after the initial notification of the jihadist material the JTTF was "up within hours with a command post, and we had at least 25 agencies and over 500 investigators, analysts and prosecutors at the local, state and

[208] Andrew Murr, "Thwarting Terror: A U.S. Attorney on the guilty pleas of two men in a homegrown jihadist cell, and the difficulty of deciding when to move in for an arrest," Newsweek, December 15 2007, http://www.newsweek.com/2007/12/14/thwarting-terror.html (accessed July 23, 2010).

[209] Ibid.

[210] Department of Justice, "Four Men Indicted on Terrorism Charges related to Conspiracy," Press Release, August 31, 2005, http://www.justice.gov/opa/pr/2005/August/05_crm_453.html (accessed July 23, 2010).

military levels. We seized and analyzed thousands of documents."[211] John J. Neu, Chief of Police for the Torrance Police Department, further confirmed that the information relating to the seized evidence was widely disseminated among partner agencies in order to advance the investigation. "The vertical sharing of intelligence information, coupled with communication and coordination throughout the investigation, proved to be invaluable to all of the agencies involved."[212]

Confidential Sources

No. Sources indicate that information related to the lost cell phone was confined to the robbery investigation by the Torrance Police.[213]

Assessment. Of the possible indicators, it was the discovery of the jihadist manifesto and related propaganda that alerted authorities to the extremist threat. Up to that point, law enforcement admittedly believed they were dealing with money-driven criminals. Neither the police reports nor the subsequent undercover work were in response to a jihadist plot; the latter did, however, prove lucky for the authorities. While Internet information did prove useful later in the investigation, it was not discovered in such a manner as to prompt an early intervention of the plot. Furthermore, the information on its own would have meant very little without the existence of the other documents or the admission by the suspects. Finally, information sharing played a key role. The extent of sharing is not well known, but the coordinated responses by the Torrance police and the JTTF (which is comprised of multiple agencies) after the household search indicate that sharing among agencies did occur.

D. ADAM GADAHN—RIVERSIDE, CA (2004)

Adam Yahiye Gadahn. Also known as "Azzam the American" and Abu Suhayb Al-Amriki, Gadahn is an American citizen who was raised in Riverside, California. He converted to Islam as a teenager and moved to Pakistan in 1998. He resurfaced in 2004

211 Murr, "Thwarting Terror: A U.S. Attorney on the guilty pleas of two men in a homegrown jihadist cell, and the difficulty of deciding when to move in for an arrest."

212 John Neu, testimony before the House Committee on Homeland Security's Subcommittee on Intelligence, Information Sharing and Risk Assessment, April 5, 2007.

213 Harris, "L.A.'s anti-terrorism hub serves as a model."

when he appeared in a video broadcast declaring he had joined Al Qaeda, "a movement waging war on America and killing large numbers of Americans," and that "the streets of America shall run red with blood."[214] He is considered to be a leading propagandist, translator, and planner of terrorist attacks for Al Qaeda.

Summary. In 2006, Gadahn was indicted in the Central District of California for treason and material support to Al Qaeda and subsequently added to the FBI's *Most Wanted Terrorists List*.[215] According to the indictment, Gadahn "gave al-Qaeda aid and comfort, within the United States and elsewhere, with intent to betray the United States" and "did knowingly provide, and aid and abet the provision of, material support and resources…including personnel and services, to a foreign terrorist organization, al-Qaeda."[216] Two years prior to his indictment, Gadahn was listed as a suspected Al Qaeda associate who had attended training camps in Afghanistan.[217] The first American to be charged with treason since World War II, he is still considered a fugitive at large.[218]

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
Former mosque affiliations	Internet broadcasts and postings	CIA interrogations of Abu Zubyadah and Khalid Sheik Mohammed	Videotapes	N/A

Figure 7. Adam Gadahn Indicators

214 Department of Justice, "U.S. Citizen Indicted on Treason, Material Support Charges for Providing Aid and Comfort to Al Qaeda," DOJ Press Release, October 11, 2006, http://www.usdoj.gov/usao/cac/news/pr2006/138.html (accessed August 30, 2010).

215 Ibid.

216 *United States v. Adam Gadahn*, Criminal No. CR 05-254A, in the U.S. District Court for the Central District of California, October 11, 2006, http://nefafoundation.org/file/FeaturedDocs/U.S._v_Gadahn_Indictment.pdf (accessed August 30, 2010).

217 David Anthony Denny, "Al-Qaeda Expected to Strike U.S. Soon, Attorney

General Says; Seven suspects identified by FBI director," May 26, 2004, http://nefafoundation.org/file/FeaturedDocs/FBI_GadahnZubaydah.pdf (accessed August 30, 2010).

218 Maddy Sauer, "The Hunt for American Al Qaeda," ABC News website, June 2, 2008, http://abcnews.go.com/Blotter/story?id=5026716 (accessed October 28, 2010).

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Interpersonal Interaction

No. Between 1996 and 1997, several of Gadahn's mosque affiliates from the Islamic Society of Orange County noticed a distinct change in his behavior. In short order, he began wearing traditional Muslim garb and joined a small discussion group of men who were known to be militant in their religious and political beliefs. Haitham "Danny" Bundakji, a prominent leader from the mosque who served as a witness at Gadahn's conversion to Islam, had a number of confrontations with him and was even assaulted by Gadahn after admonishing him.[219] Muzammil Siddiqi, the society's religious director, recollected that "'He was becoming very extreme in his ideas and views…he must have disliked something."[220] Despite the behavioral change, assault, and radical affiliations, no indications were relayed to authorities that Gadahn was considering jihad.

Inernet-Based

Yes. The California native's online vitriol sufficiently alerted authorities to a homegrown jihadist threat. Following the release of his first videotape in 2004, Gadahn appeared numerous times in Internet broadcasts posted on jihadist websites. In many of his early postings, Gadahn wore a scarf and sunglasses to cover his face, but openly identified himself under his alias Azzam the American. On July 7, 2006, he again appeared online, this time unmasked, advocating violence against the homeland. The FBI conducted voice analysis of the clips and confirmed that the individual was indeed Gadahn.[221]

---

[219] Raffi Khatchadourian, "Azzam the American: The Making of an Al Qaeda Homegrown," the New Yorker website, January 22, 2007, http://www.newyorker.com/reporting/2007/01/22/070122fa_fact_khatchadourian?currentPage=all (accessed August 30, 2010).

[220] FOX News, "American Sought Had '97 Arrest, 'Extreme' Ideas," FOX News website, May 27, 2004, http://www.foxnews.com/story/0,2933,121040,00.html (accessed August 30, 2010).

[221] WorldNetDaily, "Al-Qaida American was poster boy for USC Muslim Student Association," WorldNetDaily website, July 14, 2006, http://www.wnd.com/?pageId=37011 (accessed August 31, 2010).

Incident Reports

Yes. Few details are known, but the CIA was reportedly alerted to some of Gadahn's peripheral involvement with Al Qaeda during the interrogations of apprehended jihadists, Abu Zubaydah and Khalid Sheikh Mohammed.[222] Though the agency did not know Gadahn's whereabouts, the information was "good enough" at the time of discovery to begin tracking of his jihadist activity.

Media

Yes. Gadahn first reached a worldwide audience in 2004 when both ABC News and FOX News aired a videotape featuring "Azzam the American." ABC News had attained the tape from a source in Waziristan. In the video, Gadahn claimed that he joined Al Qaeda and promised that the United States would face continued attack. Authorities said they could not verify the authenticity of the tape after a "preliminary technical analysis" by the CIA, but intelligence officials did confirm the signature markings of Al Qaeda's media arm, Al Sahab, and that the video content was "classic Al Qaeda propaganda, in terms of anti-U.S. ideology and denunciation of the U.S."[223]

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Interpersonal Interaction

Yes. Although Gadahn's personal relationships did not trigger early intervention, they did later contribute to advancing investigation after his first videotape was released. Bundakji reported that he believed it was Gadahn from the gestures and voice (Gadahn's face was covered in his first video). Gadahn's aunt also told the FBI that she thought the individual was possibly her nephew.[224] After Gadahn's identity was confirmed, Saraah Olson, who also attended the same mosque, passed on her recollection of Gadahn's

---

[222] Khatchadourian, "Azzam the American: The Making of an Al Qaeda Homegrown;" and George Michael, "Adam Gadahn and Al-Qaeda's Internet Strategy," *Middle East Policy Council* 16, no. 3 (Fall 2009).

[223] William LaJeunesse et al., "Official believe 'Azzam' is Gadahn," FOX News website, October 29, 2004, http://www.foxnews.com/story/0,2933,137087,00.html (accessed August 30, 2010); and Brian Ross, "Alleged American Warns of U.S. Attacks," ABC News website, October 28, 2004, http://abcnews.go.com/WNT/story?id=206661 (accessed August 30, 2010).

[224] William LaJeunesse et al., "Official believe 'Azzam' is Gadahn."

radicalization and association with other radicals: "Adam turned very, very quickly…they would be every day in our living room—Khalil and Hisham—saying, 'You have to kill the kufar, the nonbeliever.'"[225]

Inernet-Based

Yes. Gadahn's online postings, which appeared on obscure or extremist websites, were good enough for authorities to pursue the case fervently. His 2006 releases showed him umasked with Osama bin Laden's top lieutenant, Ayman al-Zawahiri, who endorsed Gadahn and introduced him as a "brother." Gadahn then proceeded to claim the United States as "enemy soil."[226] This information was important "because al-Qaeda's leadership had never before given one of its members such a direct and intimate endorsement." It also earned Gadahn the count of treason on his indictment.

Incident Reports

Yes. Specific mention of Gadahn during interrogations convinced authorities to seek further information about his activities. Khalid Sheikh Mohammed told interrogators in 2003 that he had personally asked Gadahn to join him in a plot to blow up gas stations in Maryland.[227] Soon thereafter, the FBI issued 'Seeking Information' and 'Be on the lookout' (BOLO) notices for Gadahn.[228]

Media

Yes. Though authorities were not able to ascertain the authenticity of the videotape immediately, the nature of the content was clear enough. Authorities were able to use the video in their inquiries with Gadahn's former personal contacts.

---

225 Khatchadourian, "Azzam the American: The Making of an Al Qaeda Homegrown."

226 Adam Gadahn's "An Invitation to Islam," Internet video found at http://www.foxnews.com/story/0,2933,211886,00.html# (accessed August 30, 2010).

227 Khatchadourian, "Azzam the American: The Making of an Al Qaeda Homegrown."

228 Federal Bureau of Investigation, "Seeking Information: Adam Yahiye Gadahn," found at NEFA website, http://nefafoundation.org/file/FeaturedDocs/FBI_SeekingInfo_Gadahn.pdf (accessed August 30, 2010); and FBI BOLO for May 26, 2004, found at NEFA website, http://nefafoundation.org/file/FeaturedDocs/FBI_BOLOSummer04.pdf (accessed August 30, 2010).

3. Was the information shared in order to attract other useful information?

Interpersonal Interaction

Yes. After the widespread reporting of Gadahn's videotape, a number of relatives, friends, and former mosque affiliates contributed their stories both to the authorities and media. This enabled the FBI and CIA to understand Gadahn's early connections to Al Qaeda.

Inernet-Based

Yes. Gadahn's Internet postings were made available for all to view. According to available reporting, Gadahn's first release was analyzed and shared among a number of agencies and it is reasonable to say the same occurred for the online videos. In 2008, for example, rumors had spread that Gadahn had been killed in an airstrike.[229] Information from a newly discovered Internet post, transcribed and disseminated by private open source centers, quickly facilitated the FBI and intelligence officials in confirming that the claim was false.[230]

Incident Reports

Yes. The information obtained by CIA officials was passed to other agencies. For example, in May 2004, Attorney General John Ashcroft and FBI Director Robert Mueller announced during a press conference confirmed that they had obtained the "credible intelligence."[231]

---

[229] Nick Meo, "Al-Qa'eda's American-born propaganda chief may have died in predator attack," *Telegraph*, September 6, 2008, http://www.telegraph.co.uk/news/newstopics/onthefrontline/2695294/Al-Qaedas-American-born-propaganda-chief-may-have-died-in-predator-attack.html (accessed October 28, 2010).

[230] Bill Roggio, "Adam Gadahn resurfaces in new al Qaeda tape," Long War Journal website, October 4, 2008, http://www.longwarjournal.org/archives/2008/10/adam_gadahn_resurfac.php (accessed October 28, 2010); and NEFA Foundation, "Video from Al-Qaida Spokesman Adam Gadahn," NEFA website, October 4, 2008, http://www.nefafoundation.org/newsite/file/nefagadahn1008.pdf (accessed October 28, 2010).

[231] David Anthony Denny, "Al-Qaeda Expected to Strike U.S. Soon, Attorney General Says; Seven suspects identified by FBI director."

Media

Yes. ABC News shared the videotape with the CIA, NSA, and FBI for analysis prior to airing it to the public.

Assessment. All of the indicators, with the exception of interpersonal interactions, were "good enough" at the time of discovery to alert law enforcement and intelligence officials to a homegrown jihadist threat. Though none led to Gadahn's capture, each were critical to building a credible case against him and subsequently indicting him for treason and material support to terrorists. Furthermore, open source Internet information played an extensive role in this case. Because the majority of evidence of Gadahn's allegiance to Al Qaeda was substantiated by his public Internet postings, both government analysts and private monitors were able to collect and analyze the information free from more confidential means. This also allowed a more permissive setting for the sharing of information among all investigators. While there is little question that it was Gadahn's intent to use the Internet to broadcast his violent intentions widely, this case demonstrates that authorities are tracking the material and that it can be used against homegrown jihadists in the court of law.

E. RONALD GRECULA—HOUSTON, TX (2005)

Ronald Allen Grecula. A 68-year old engineer and resident of Bangor, Pennsylvania at the time of his arrest, Grecula already had criminal history with the FBI. In November 2000, he abducted his own children without the knowledge of his wife and fled to Malta. The FBI issued a warrant for "Unlawful Flight to Avoid Prosecution."[232] Grecula was arrested and subsequently spent time in a Malta prison while awaiting extradition to the United States. His grievances toward the U.S. government apparently began after ultimately losing custody of the children to his wife.[233]

---

[232] MaltaMedia News, "Court awards custody to French-born mother," Dr. Mifsud Bonnici website, March 6, 2002, http://www.mifsudbonnici.com/press/PressMaltamedia060302.html (accessed October 29, 2010).

[233] FOX News, "Pa. Man Arrested on Terror Charges," FOX News website, May 24, 2005, http://www.foxnews.com/story/0,2933,157394,00.html (accessed October 29, 2010).

Summary. In May 2005, Grecula was arrested in Houston, Texas and charged with "attempting to provide material support and resources to a designated foreign terrorist organization, namely Al Qaeda."[234] According to case reports, Grecula negotiated over a one-month period with a confidential source and undercover agents a plan to build and sell an explosive device to terrorists targeting the United States.[235] In exchange for the bomb, Grecula requested custody of his children and the assassination of his estranged wife in Houston.[236]

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
N/A	N/A	Prior FBI Conviction	Written Bomb Information Device Triggers	Confidential Informant Undercover Agents Wiretaps

Figure 8. Ronald Grecula Indicators

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Incident Reports

No. Grecula's prior FBI conviction was for parental kidnapping. There were no signals of terrorist affiliations or motivations at that time.

Documents and Material

Yes. According to a detailed FBI criminal complaint, Grecula presented documents to an undercover agent (whom he thought was an Al Qaeda associate)

234 Department of Justice Southern District of Texas, "Ronald Grecula Sentenced To Prison in Plot to Sell Bomb to Terrorists," News Release, February 9, 2007, http://www.justice.gov/usao/txs/releases/February%202007/070209-Grecula.htm (accessed October 29, 2010).

235 Ibid.

236 FOX News, "Pa. Man Arrested on Terror Charges."

describing how he would construct a bomb using hydrogen chloride. Immediately following that meeting, FBI officials executed a search warrant of Grecula's residence and discovered "Lithium Nitrate and a Mercury Switch that could be used to trigger an explosive device."[237] The evidence made Grecula's intentions clear at the time of discovery and allowed the FBI to act.

Confidential Sources

Yes. Information provided by a combination of confidential sources was good enough to prompt the authorities. While Grecula was in prison in Malta, he befriended an individual whom he did not know was a confidential informant for the FBI. He later contacted the informant to ask for assistance in connecting him with Al Qaeda or any other terrorist group targeting the U.S. The informant relayed Grecula's plans to the Houston Division of the FBI in late April 2005, prompting an investigation that relied on undercover agents and telephone wiretaps.[238]

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Incident Reports

Yes. Although Grecula's prior arrest had little connection with his attempt to aid Al Qaeda, some information from a past FBI interview was referenced and proved useful to the new investigation. Grecula told the confidential informant that all of the components for his proposed bomb could be purchased at a welding supply store and explained that bottles of hydrogen or oxygen could be used for the explosive device.[239] The FBI went back and reviewed a 2002 interview FBI officials had with Grecula and saw he stated that he was educated as a mechanical engineer, experimented with alternative fuels and energy, and knew how to weld.

---

[237] *United States v. Ronald Allen Grecula*, Criminal Complaint No. H-05-453M, in the U.S. District Court for the Southern District of Texas, May 21, 2005, http://nefafoundation.org/file/FeaturedDocs/US_v_Grecula_Complaint.pdf (accessed October 29, 2010).

[238] Ibid.

[239] Ibid.

Documents and Material

Yes. Grecula brought with him to Houston a suitcase full of information relating to his background and his bomb. As mentioned earlier, he produced this information and gave it to an undercover agent during their meeting. With key evidence in hand, the agent was able to press the meeting further, bringing in another undercover agent to finalize negotiations with Grecula.[240]

Confidential Sources

Yes. After the confidential informant first alerted the FBI, the agency had the informant engage in a number of monitored telephone conversations with Grecula. The FBI was able to collect information on Grecula's initial bomb design and his plot to fly anywhere to meet with an Al Qaeda representative. An undercover agent posing as an Al Qaeda member then contacted Grecula to set up the meeting in Houston, where the FBI hoped they would gather sufficient proof to arrest him for attempting to provide material support.

3. Was the information shared in order to attract other useful information?

Incident Reports

Yes. The information from the 2002 FBI interview pertaining to his kidnapping charge was shared with the Houston office. According to Special Agent Lisa Baldwin, this allowed Houston officials to corroborate the claims Grecula made to the confidential informant about his technical capacity to actually construct a bomb.[241]

Documents and Material

Yes. While it is not clear if the bomb information from Grecula's meeting in Houston was immediately shared with other offices, it is clear that the Pennsylvania FBI office did pass on the results of the search of his residence. Special Agent Baldwin confirmed that there was correspondence between the Houston and Pennsylvania divisions after the discovery of the lithium nitrate and mercury switch.[242]

---

240 *United States v. Ronald Allen Grecula*, Criminal Complaint No. H-05-453M.

241 Ibid.

242 Ibid.

Confidential Sources

Yes. Again, according to the official FBI complaint, there were several instances in which undercover agents from the Pennsylvania division shared information with the Houston office. They conducted surveillance of Grecula, collecting information on his daily activities, vehicle location, telephone protocol, and eventual departure for Houston. Information from the recorded telephone conversations was also passed between the two offices to support the investigation.[243]

Assessment. Though Grecula did not exhibit any sort of ideological connection to jihad, his overt willingness to support Al Qaeda was still of serious concern. Confidential sources contributed overwhelmingly to the foiling of his plot. A chance relationship with an FBI informant exposed the initial plan and the use of undercover agents and techniques helped to confirm it. The Internet, however, was not applicable in this case. As evidenced by the FBI criminal complaint, Grecula was quite open (and detailed) with his intentions over the phone and in meetings with the undercover agents. The success of the investigation was also contingent on the cooperation between two geographically separated FBI offices, which conducted different activities yet maintained open lines of communication to facilitate each other's efforts.

F. NAJIBULLAH ZAZI—DENVER, CO (2009)

Najibullah Zazi. Born in Afghanistan, Zazi moved to Pakistan at age 7. He and his family emigrated to the U.S. in 1999 and settled in New York, where he worked as a coffee vendor for several years. Zazi moved to Aurora, Colorado in 2009 where he found a job as a shuttle driver at the Denver International Airport. He admitted to having received weapons and explosives training from Al Qaeda during a trip to Pakistan in 2008.[244]

Summary. In September 2009, Colorado FBI agents arrested Zazi and his father, Mohammed Wali Zazi, in Aurora for "knowingly and willfully making false statements

---

[243] *United States v. Ronald Allen Grecula*, Criminal Complaint No. H-05-453M.

[244] Dan Fletcher, "Terrorism Suspect Najibullah Zazi," Time.com website, September 22, 2009, http://www.time.com/time/nation/article/0,8599,1925270,00.html (accessed September 12, 2010).

to the FBI in a matter involving international and domestic terrorism."[245] A few weeks later, a grand jury returned an indictment charging Najibullah Zazi with conspiracy to use weapons of mass destruction, namely improvised explosive devices, against the New York subway system. Zazi later pled guilty to that charge in addition to charges of "conspiracy to commit murder in a foreign country and providing material support to al-Qaeda."[246] He originally flew to Pakistan to join the Taliban but was instead recruited and trained by Al Qaeda and asked to carry out suicide operations in the U.S.[247] He possessed detailed notes which he used in attempts to construct explosive devices.

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
Relatives	Review of Emails/Internet searches	Travel to Pakistan	Bomb-making notes	Confidential Informants
Mosque affiliations		Police stops	Chemicals/Components	Wiretaps
Customers		False Statement (FBI Interview)	Store video footage	

Figure 9. Najibullah Zazi Indicators

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Interpersonal Interaction

No. Sometime after 2006, Zazi flew to Pakistan where he took a wife. Each following year, he would go back, claiming to visit her. Some of his relatives, friends

[245] Federal Bureau of Investigation, "Three Arrested in Ongoing Terror Investigation," Press Release, September 20, 2009, http://www.fbi.gov/pressrel/pressrel09/zazi_092009.htm (accessed September 12, 2010).

[246] Department of Justice, "Najibullah Zazi Pleads Guilty to Conspiracy to Use Explosives Against Persons or Property in U.S., Conspiracy to Murder Abroad and Providing Material Support to Al-Qaeda," Press Release, February 22, 2010, http://www.justice.gov/opa/pr/2010/February/10-ag-174.html (accessed September 12, 2010).

[247] Ibid.

from the mosque, and customers who often bought coffee from him, began to notice a change in Zazi. According to friends, he was never really religious when he was younger. However, after visiting Pakistan a few times, he shifted from wearing Western clothing to a more traditional Muslim appearance. He also took great interest in online videos of an Indian scholar who advocated Islamic fundamentalism. Some said Zazi also became less friendly and sometimes argumentative.[248] While signs of radicalization may have been picked up by these personal interactions, none were concrete enough to alert authorities to a possible homegrown jihadist plot.

Inernet-Based

Yes. After the FBI discovered bomb-making notes on Zazi's computer in New York, officials were able to find supporting proof that Zazi did not accidentally download them like he claimed. The FBI conducted a review of Zazi's e-mail accounts and found that he had e-mailed himself the notes while he was in Pakistan. Furthermore, the FBI discovered Zazi had conducted online research of baseball and football stadiums and the Grand Central Terminal in New York.[249]

Incident Reports

Yes. A number of documented incidents were key indicators of suspicious and possible jihadist activity. The first, which initially tipped off the authorities to Zazi, was his travel to Peshawar, Pakistan in 2008. Because Peshawar is considered a hotbed for Al Qaeda training and refuge, the CIA quickly took notice and reported the news of Zazi's travel to the FBI.[250] After Zazi's return to the U.S. and sudden relocation to Colorado, the FBI initiated surveillance of his activities. During the later stage of his plot, Zazi was stopped several times by police for speeding while driving cross-country overnight to

[248] Michael Wilson et al., "From Smiling Coffee Vendor to Terror Suspect," New York Times, September 25, 2009, http://www.nytimes.com/2009/09/26/nyregion/26profile.html (accessed August 30, 2010).

[249] Richard Esposito and Brian Ross, "Officials Worry NY Terror Plot 'Still Alive' as Case Broadens," ABC News website, September 22, 2009, http://abcnews.go.com/Blotter/ny-terror-plot-officials-worried-attack-plan-lurking/story?id=8642956 (accessed August 30, 2010).

[250] Brian Ross et al., "FBI Arrests Three Men in Terror Plot that Targeted New York," ABC News website, September 20, 2009, http://abcnews.go.com/Blotter/men-arrested-fbi-nyc-terror-plot/story?id=8618732&page=1 (accessed, August 30, 2010).

New York. The FBI was reportedly made aware of each incident.[251] Finally, the FBI took a statement from Zazi after he returned to Colorado, in which he lied about the bomb-making notes. According to the criminal complaint, the FBI requested a warrant for Zazi's arrest after he made the false statement.[252]

Documents, Media, Material

Yes. The authorities discovered documents, media, and material that strongly indicated Zazi was plotting a jihadist attack. It was while Zazi was in New York that the authorities discovered his bomb-making notes on his computer. The jpeg image of Zazi's handwritten notes contained "formulations and instructions regarding the manufacture and handling of initiating explosives, main explosive charges, explosives detonators and components of a fuzing system."[253] FBI agents also found bomb components with Zazi's fingerprints and traces of residue where Zazi attempted to heat chemicals. Additionally, surveillance cameras in a number of beauty supply stores captured Zazi purchasing large quantities of hydrogen peroxide and acetone, key ingredients for his bomb.[254]

Confidential Sources

Yes. A confidential informant and numerous wiretaps provided authorities with telling information of a possible plot. According to the criminal complaint, the NYPD lawfully intercepted phone conversations between Zazi and the informant in which the latter warned Zazi that the authorities were asking questions about him. Numerous other

---

251 Dina Temple-Ralston, "Terrorism Case Shows Range of Investigators' Tools," NPR website, October 3, 2009, http://www.npr.org/templates/story/story.php?storyId=113453193 (accessed August 30, 2010).

252 *United States v. Najibullah Zazi*, Criminal Complaint No. 09-MJ-03001, in the U.S. District of Court for the District of Colorado, September 19, 2009, http://nefafoundation.org/file/FeaturedDocs/US_v_NajibullahZazi_complaint.pdf (accessed August 30, 2010).

253 *United States v. Najibullah Zazi*, Criminal Complaint No. 09-MJ-03001.

254 *United States v. Najibullah Zazi*, No. 09-CR663 (RJD), Memorandum of Law in Support of Government's Motion for a Permanent Order of Detention, in the U.S. District Court for the Eastern District of New York, September 24, 2009, http://nefafoundation.org/file/FeaturedDocs/US_v_NajibullahZazi_detentionmemo.pdf (accessed August 30, 2010).

phone conversations were intercepted in which Zazi frantically sought from another individual the "correct mixtures of ingredients to make explosives."[255]

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Interpersonal Interaction

Unknown. Although Zazi's personal relationships were not "good enough" to trigger early intervention, it is also unclear as to what extent they may have facilitated investigation after Zazi was suspected of a terrorist conspiracy. As shown earlier, some of his personal contacts shared their observations of Zazi's changing behavior, but it is difficult to determine if they provided information to authorities that was useful in advancing the investigation or in thwarting the plot. Naiz Khan, a friend whom Zazi stayed with while in New York, was interviewed by the FBI after they discovered probable bomb components with Zazi's fingerprints in his apartment. Yet Khan claimed he knew nothing of the items nor that Zazi might have been involved in a plot.[256]

Inernet-Based

Yes. Both the e-mail history and the discovery of online searches of possible targets led the authorities to dig deeper into Zazi's Internet use. They subsequently found that Zazi had also conducted extensive searches on types of muriatic acid and hydrochloric acid to facilitate the construction of his bomb, per his written instructions.[257]

Incident Reports

Yes. The CIA's report to the FBI of Zazi's Peshawar, Pakistan visit appears to have been taken seriously even though there were little details. After a number of FBI interviews in Colorado, Zazi finally admitted that he had received weapons and explosives training from Al Qaeda and that the bomb-making notes were actually his.[258]

---

[255] *United States v. Najibullah Zazi*, No. 09-CR663 (RJD).

[256] Brian Ross et al., "Man On 24-Hr Surveillance in Terror Case Denies Terrorist Connections," ABC News website, September 30, 2009, http://abcnews.go.com/Blotter/terror-plot-case-man-surveillance-denies-terrorist-connection/story?id=8711539&page=1 (accessed August 30, 2010).

[257] *United States v. Najibullah Zazi*, No. 09-CR663 (RJD).

[258] Ross et al., "FBI Arrests Three Men in Terror Plot that Targeted New York."

Documents, Media, Material

Yes. Zazi's handwritten bomb-making notes were so explicit that authorities knew they had a possible plot on their hands. The notes, which outlined critical ingredients for an explosive device, helped authorities focus subsequent searches. As a result, they discovered bomb components, chemical residue, and video footage of Zazi purchasing abnormal quantities of chemical products that were found on his list.

Confidential Sources

Yes. While the informant's phone call may not have been overly revealing, it was suspicious enough for authorities to pursue further surveillance of Zazi's phone conversations. Information drawn from the wiretaps allowed them to corroborate Zazi's intentions with the chemicals and components that were discovered.[259]

3. Was the information shared in order to attract other useful information?

Interpersonal Interaction

Yes. Shortly after Zazi was arrested, a number of relatives, mosque affiliates, and former customers shared their stories with the authorities and media. Though the information may not have been consequential to thwarting the plot, it did help authorities begin to piece together Zazi's path to radicalization.

Inernet-Based

Yes. According to FBI reports, the e-mail and Internet information that agents obtained in New York was passed to the FBI division in Denver. Agents were able to question Zazi about the information shortly after he returned to Colorado.[260]

Incident Reports

Yes. Interagency sharing is what set off the domestic investigation. The CIA first become aware of Zazi's presence in known Al Qaeda territory and promptly informed the

[259] *United States v. Najibullah Zazi*, No. 09-CR663 (RJD).

[260] Federal Bureau of Investigation, "Three Arrested in Ongoing Terror Investigation."

FBI. Once the investigation was underway, the NYPD and New York and Denver FBI offices were in frequent contact, relaying information from Zazi's police stops and official statements.[261]

Documents, Media, Material

Yes. As with the Internet information and incident reports, FBI and NYPD officials shared with each other the discoveries of the bomb-making notes and components. Even though materials were found in two separate states at various establishments, the open lines of communication enabled the agencies to piece them together.

Confidential Sources

Yes. Several court documents indicate that the information obtained from the confidential informant wiretaps were shared among the FBI offices and NYPD throughout the extent of the investigation.[262]

Assessment. Some consider the Zazi case to be the most serious homegrown jihadist terrorism investigation since 9/11.[263] In comparison to other homegrown attempts, Zazi actually had connections to Al Qaeda and technical training in improvised explosive devices. Yet, as demonstrated above, there were a significant number of plot indicators picked up by a comprehensive array of detection measures. Open source Internet exploitation, however, was not one of them. As stated by a former analyst with the NYPD intelligence unit, "I think what's striking about the Zazi case is not so much that new tools were being used, but that old tools were being used in a comprehensive fashion… and that they were being stitched together in a thoughtful, strategic way, so that one tool naturally gave way to another."[264] This is an accurate statement, as almost every indicator provided authorities with "good enough" information to intervene. Still, what is most illuminating from this case is the level of cooperation, sharing, and expediency

261 *United States v. Najibullah Zazi*, Criminal Complaint No. 09-MJ-03001.

262 Ibid.; *United States v. Najibullah Zazi*, No. 09-CR663 (RJD).

263 Neal Conan, "Facts and Fiction about Alleged Zazi Plot," transcript from National Public Radio show 'Talk of the Nation,' September 28, 2009, http://www.npr.org/templates/story/story.php?storyId=113279071&ps=rs (accessed August 28, 2010).

264 Temple-Ralston, "Terrorism Case Shows Range of Investigators' Tools."

among numerous agencies. The willingness to pass information across traditional boundaries helped the authorities stay a step ahead of Zazi and his plan to attack the New York subway.

G. MICHAEL FINTON—DECATUR, IL (2009)

Michael Finton. Finton, 29, had converted to Islam while he was in prison for aggravated battery and aggravated robbery charges.[265] After release, he moved to Decatur, Illinois, in violation of his parole, to attend a mosque there. He was arrested for his parole violation in August 2007. A search of Finton's vehicle yielded several personal writings, including a martyrdom letter and a note indicating that Finton had written a letter to John Walker Lindh, an American citizen who was captured while fighting for the Taliban in Afghanistan. The FBI maintained those documents while Finton served another 4 months in prison.[266]

Summary. The Springfield Division of the FBI Joint Terrorism Task Force arrested Finton in September 2009 on charges of "attempted murder of federal employees and attempted use of a weapon of mass destruction (explosives) in connection with a plot to detonate a vehicle bomb at the federal building in Springfield, Ill."[267] Finton unknowingly worked with a confidential informant and undercover FBI agent to develop his plot and attempt to carry it out until the time of his arrest. He willingly parked a truck that he thought was filled with explosives near the federal building and attempted to detonate it remotely.

---

[265] Bernard Schoenburg and Bruce Rushton, "Downtown Springfield bombing plot foiled," State Journal-Register website, September 25, 2009, http://www.sj-r.com/news/x1128380368/Decatur-man-arrested-for-attempting-to-bomb-Springfield-federal-building (accessed October 27, 2010).

[266] Federal Bureau of Investigation, "Illinois Man Arrested in Plot to Bomb Courthouse and Murder Federal Employees," Press Release, September 24, 2009, http://springfield.fbi.gov/dojpressrel/2009/si092409.htm (accessed October 27, 2010).

[267] Federal Bureau of Investigation, "Illinois Man Arrested in Plot to Bomb Courthouse and Murder Federal Employees."

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
Mosque affiliations	MySpace posts	Parole Violation	Martyr letter	Confidential Informant
College affiliations	Muslim blogs	Speeding violation	Letter to John Walker Lindh	Undercover Agents
			"Bomb" components	
			Propaganda video	

Figure 10. Michael Finton Indicators

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Interpersonal Interaction

No. Accounts of personal relationships did not come forward until after Finton was arrested. While some of his former colleagues from the Richland Community College in Decatur described Finton as always wanting "to talk about Islam," none reported suspicious behavior to authorities.[268] Members of the Masjid Wali Hasan Islamic Society, where Finton often prayed, also stated that they saw no signs of radical behavior. Shamshad Syed Ahmed, the vice president of the society's board, described Finton as "very humble and very polite."[269]

Inernet-Based

No. News reporting shows that Finton often posted about Islam-related issues on his MySpace page and Muslim-themed websites like *muxlim.com*.[270] However, neither the detailed criminal complaint nor the indictment discusses his online rants as critical to

[268] Schoenburg and Rushton, "Downtown Springfield bombing plot foiled."

[269] Ibid.

[270] Ibid.

the investigation, suggesting that authorities may not have discovered them. Of interest though is an independent inquiry conducted by the NEFA Foundation, which found that Finton expressed admiration online for known jihadist ideologues like Anwar al-Awlaki and Ibn Taymiyyah.[271]

Incident Reports

No. Available reporting indicates that Finton's parole officer was more concerned about the parole violation and less about the underlying reasons. The infraction simply was not enough to warn of homegrown jihadism. It appears that no red flags went up either when Finton was stopped for speeding outside of Springfield after working all day on his bombing plot.

Documents, Media, Material

Yes. While the parole violation itself was not a warning, the results of Finton's arrest and search were. Parole officers found and turned over jihadist-themed letters to the FBI who later questioned Finton about them. Finton admitted that he idolized John Walker Lindh, the "American Taliban," and indeed attempted to correspond with him.[272] That signaled the FBI to promptly open an investigation into Finton's activities. Later during the investigation, Finton handed over to an undercover agent what he thought to be bomb components and his homemade jihadist propaganda video, providing further information in support of a jihadist conspiracy.[273]

Confidential Sources

Yes. According to the criminal complaint, significant information about Finton's plot was provided by a confidential informant and undercover FBI agent. Numerous conversations held between each source reveal Finton's candor about joining the jihad

---

[271] Madeleine Gruen, "Attempt to Attack the Paul Findley Federal Building in Springfield, Illinois," Report no. 23 in the 'Target: America' Series, December 2009, http://www.nefafoundation.org/miscellaneous/FeaturedDocs/nefa_fintontargetamerica.pdf (accessed October 27, 2010).

[272] Federal Bureau of Investigation, "Illinois Man Arrested in Plot to Bomb Courthouse and Murder Federal Employees."

[273] *United States v. Michael C. Finton*, Criminal Complaint No. 09-3048-M, in the U.S. District Court for the Central District of Illinois, http://www.investigativeproject.org/documents/case_docs/1073.pdf, 18-21.

and damaging the U.S. government. On more than one occasion, Finton expressed his willingness to wage jihad and the progress of his plot (e.g., potential targets and reconnaissance he had conducted). This enabled the FBI to plan their intervention accordingly.[274]

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Interpersonal Interaction

No. Statements from colleagues and mosque associates indicate that, at best, Finton was passionate about Islam and was always willing to discuss the topic. However, it appears that Finton did not communicate his attraction to jihad openly in those forums, thereby providing little reason for alarm. Furthermore, the statements came after Finton was arrested and when the authorities already had sufficient information to foil his plot.

Inernet-Based

No. Though Finton's publicly-available Internet posts may have provided some insight into his leanings, it does not appear that authorities came across them or found them useful to the investigation.

Incident Reports

No. Neither Finton's parole violation nor his traffic violation provided suspicion of jihadist activity. It was the subsequent search following his arrest for violating parole that tipped off authorities.

Documents, Media, Material

Yes. Finton's jihadist-themed letters did indeed provide enough understanding to move forward with investigation. Numerous references to death, martyrdom, and another American jihadist were important signals that compelled the FBI to question Finton and facilitate a relationship with a confidential informant. The video and components Finton later produced gave authorities proof of his intent to carry out an attack.

[274] *United States v. Michael C. Finton*, Criminal Complaint No. 09-3048-M, 6–24.

Confidential Sources

Yes. The criminal complaint reveals that information obtained by persistent use of the informant and agent advanced the investigation to a successful, well-timed intervention. Finton divulged every detail of his plot to both individuals. The FBI was able to manipulate the information to set up a scenario in which they could effectively catch Finton in the act. The result was an attempted vehicle-borne explosive attack against a federal building, which Finton wholeheartedly agreed to carry out to the end.

3. Was the information shared in order to attract other useful information?

Interpersonal Interaction

Unknown. Those who knew Finton from school or the mosque provided their accounts of his character to the media after his arrest. It is not clear, though, that the information was shared with the authorities or if it attracted other useful information.

Inernet-Based

No. According to court records, the Internet information was not even considered in the case.

Incident Reports

Yes. News of Finton's parole violation was shared with the FBI after parole officers discovered the documents in his truck. Also, details of Finton's speeding ticket from a Springfield Deputy Sheriff indicate that the information was obtained by the FBI.[275]

Documents, Media, Material

Yes. While it is not clear if information of the video or components was shared widely, it is clear that the parole office promptly shared the seized jihadist documents with the FBI. The sharing of that information was critical to the opening of this investigation.

[275] *United States v. Michael C. Finton*, Criminal Complaint No. 09-3048-M, 22.

Confidential Sources

Yes. Records show that the Springfield FBI division handled both the informant and undercover agent. However, the indictment also states that the investigation was supported by other law enforcement agencies as part of the Joint Terrorism Task Force, which according to the Springfield FBI website is comprised of 30 partner agencies.[276] Information from the confidential sources was likely shared in order to coordinate the extensive surveillance and artificial vehicle attack.

Assessment. Finton's written and spoken statements pointed authorities to a clear, well-defined homegrown jihadist threat. Persistent use of confidential sources resulted in critical information about capability and intent, allowing the FBI and its partners to stay steps ahead. Certainly, part of the success can be attributed to Finton's own negligence and candor, exhibited by his willingness to profess his jihadist leanings in person, on paper and video, and online. Although his Internet postings were not indicators for authorities during the investigation, the nature of those posts suggests they could have been supportive of information collected from those other sources. Products like the NEFA report could have provided a contextual analysis. Nevertheless, interagency cooperation and effective use of a small number of tools detected the threat and enabled successful intervention.

H. HOSAM SMADI—DALLAS, TX (2009)

Hosam Maher Husein Smadi. Smadi, a Jordanian native, came to the United States in 2007 on a visitor visa. He lived south of Dallas, Texas, where he held a job at a roadside barbecue restaurant. After his visa expired, Smadi remained in the U.S. illegally, spending most of his time away from work online.[277]

Summary. Smadi, 19 at the time, was arrested September 24, 2009 by FBI agents when he attempted to detonate a truck bomb outside a Dallas skyscraper. He unknowingly

---

[276] Federal Bureau of Investigation, Springfield, "Partnerships," Springfield FBI website, http://springfield.fbi.gov/partners.htm (accessed October 27, 2010).

[277] Jason Trahan, "Man who confessed to Dallas terror plot may face questions about letter at sentencing today," *Dallas Morning News*, October 18, 2010, http://www.txcn.com/sharedcontent/dws/news/localnews/stories/101810dnmetsmadi.26f34cd.html (accessed October 20, 2010).

worked with undercover FBI agents, who were posing as members of an Al Qaeda sleeper cell, to further his plot until the time of his arrest. The FBI claims that Smadi first came to their attention when agents monitoring jihadist Internet sites came across a number of his posts calling for terrorist attacks within the U.S.[278]

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
Relatives Friends	Posts on jihadist websites Email correspondence	Expired Visa	Propaganda video	Undercover Agents

Figure 11. Hosam Smadi Indicators

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Interpersonal Interaction

No. According to reports from family members and friends, Smadi's character never gave way to suspicion that he was interested in jihad. Those who knew him growing up said that he was far from being a strict Muslim and often attended chapel with his Christian friends. Smadi's friends in the U.S. said that he exhibited some teenage angst but nothing extremist.[279] He "loved techno music, wore earrings, drank and smoked cigarettes—behavior frowned upon by strict adherents of Islam."[280]

[278] Federal Bureau of Investigation, "Terror Plot Foiled: Inside the Smadi Case," FBI website, November 5, 2010, http://www.fbi.gov/news/stories/2010/november/terror-plot-foiled/terror-plot-foiled (accessed November 5, 2010).

[279] Taylor Luck, "Dallas terror plot: Troubled Jordanian teen or jihadist?," *Christian Science Monitor*, September 30, 2009, http://www.csmonitor.com/World/Middle-East/2009/0930/p06s01-wome.html (accessed October 20, 2010).

[280] Trahan, "Man who confessed to Dallas terror plot may face questions about letter at sentencing today."

Inernet-Based

Yes. FBI reports and court documents claim that Smadi's violent rhetoric on a radical Islamic website alerted them to a possible jihadist threat. Special Agent Tom Petrowski, who led the investigation, said "he [Smadi] was on a very extreme website, where people were saying a lot of unspeakable things, endorsing and celebrating acts of violence against U.S. citizens and our allies." Petrowski said further, "what made Smadi's postings stand out from the other rhetoric was that he was saying, 'I want to act.' That's what really got our attention."[281]

Incident Reports

Yes. Authorities discovered that Smadi overstayed his visa after they had suspected him of contemplating a jihadist attack. Special Agent Petrowski noted that law enforcement knew they could have immediately arrested and deported Smadi, but chose not to because they felt they would only be displacing the threat.[282]

Media

Yes. Authorities obtained from Smadi a homemade propaganda video that he made for Osama bin Laden, signaling that he was about to carry out an attack on U.S. soil. In it he proclaims, "The date of the blessed strikes, September 11, was a celebration for us, so let us make another date become a celebration for us that history will mark for us."[283]

Confidential Sources

Yes. The criminal complaint shows that after Smadi was found online, significant information about his terror plot was obtained by two undercover FBI agents, both native Arabic speakers. Several conversations held between each source illuminate Smadi's enthusiasm for jihad and perseverance to conduct an attack against the U.S. On more

---

[281] Federal Bureau of Investigation, "Terror Plot Foiled: Inside the Smadi Case."

[282] Ibid.

[283] Jason Trahan, "Would-be Dallas bomber Hosam Smadi appears enthusiastic in video made for bin Laden," *Dallas Morning News*, October 21, 2010, http://www.dallasnews.com/sharedcontent/dws/dn/latestnews/stories/DN-smadi_21met.ART.Central.Edition1.3368bd4.html (accessed October 21, 2010).

than one occasion, Smadi discussed potential targets, reconnaissance he had conducted, and the possible damage he could incur. This information allowed the FBI to plan an intervention that would catch Smadi in the act.[284]

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Interpersonal Interaction

No. The few character references from family and friends did not provide "good enough" information to assist the investigation. As in many other cases, the observations came forward after the individual was detained. Even still, when it did come forward, the information did not reveal insight into Smadi's jihadist leanings.

Inernet-Based

Yes. An FBI agent who was specifically monitoring jihadist websites came across a message Smadi had posted online under the screen name, "Aba Al-Ayyubi." In response to a long thread of increasingly violent discussion, Smadi posted in Arabic, "Brothers…I am currently in America and I am able to strike their interests in their own home however I only need help with the tools…Allah willing we will strike them on their heads…"[285] The agent came across several other messages by Smadi repeating that he was in prime position to wage jihad but only needed the tools. According to Petrowski, an FBI Behavioral Analysis team evaluated the online vitriol and determined that "Smadi was not making empty threats."[286] They chose to then make direct e-mail contact with Smadi to find out who he was and what he was conspiring.

---

[284] *United States v. Hosam Maher Husein Smadi*, Criminal Complaint No. 3-09-MJ-286, in the U.S. District Court for the Northern District of Texas, September 24, 2009, http://nefafoundation.org/file/FeaturedDocs/US_v_Smadi_complaint.pdf (accessed October 20, 2010).

[285] *United States v. Hosam Maher Husein Smadi*, Case No. 3-09-MJ-286, Government Exhibit 2, in the U.S. District Court for the Northern District of Texas, http://www.txnd.uscourts.gov/judges/smadi/002.pdf (accessed October 20, 2010).

[286] Federal Bureau of Investigation, "Terror Plot Foiled: Inside the Smadi Case."

Incident Reports

Yes. In context, the knowledge that Smadi overstayed his visa appeared to support his desire to infiltrate and attack America. The authorities pressed forward with the investigation, armed with the knowledge that they could at least deport Smadi if he fell short of trying to conduct an attack.

Media

Yes. Smadi's propaganda video was made with the help of undercover agents shortly before he attempted to detonate the truck bomb. This video gave authorities further evidence of Smadi's intent to act and therefore prompted measures to detain him in the process.[287]

Confidential Sources

Yes. According to the criminal complaint, the information an undercover agent received from Smadi provided sufficient understanding to continue investigation of a jihadist conspiracy. Smadi told the agent numerous times "his intention to serve as a soldier for Usama bin Laden and al-Qa'ida, and to conduct violent jihad."[288] The complaint states that undercover agents communicated with Smadi over 60 times after the initial contact via e-mail, phone, and in person.[289] Smadi provided the agents with elaborate details and timelines of his plot. Authorities used this information to maneuver Smadi into a situation in which they could intervene.

---

[287] *United States v. Hosam Maher Husein Smadi*, Case No. 3-09-MJ-286, Government Exhibit 277, in the U.S. District Court for the Northern District of Texas, http://www.txnd.uscourts.gov/judges/smadi/277.pdf (accessed October 20, 2010); and Rebecca Lopez and Gary Reaves, "Dallas bomber's message to 'beloved' bin Laden," KHOU News Web video, October 21, 2010, http://www.khou.com/news/texas-news/Dallas-bombers-message-to-beloved-bin-Laden--105445843.html (accessed October 21, 2010).

[288] *United States v. Hosam Maher Husein Smadi*, Criminal Complaint No. 3-09-MJ-286.

[289] Ibid.

3. Was the information shared in order to attract other useful information?

Interpersonal Interaction

Unknown. Smadi's family and friends recounted their relationships to the teenager with the media after his arrest. It is not clear, though, that the information was shared with the authorities or if it attracted other useful information.

Inernet-Based

Yes. Several sources indicate that there was significant cooperation and information sharing throughout this case.[290] While all the details are not known, some of these sources assert that Smadi's public Web postings were shared among behavioral specialists, language analysts, agencies of the Dallas JTTF, and the Counterterrorism Division in Washington, DC.[291] These specialists were able to evaluate the credibility of Smadi's postings and validate the FBI's reason for concern.

Incident Reports

Yes. According to Special Agent Petrowski, law enforcement agencies other than the FBI were made aware of both Smadi's expired visa and the decision to not deport him until further investigation could be conducted.[292]

Media

Yes. As suggested previously, language analysts played a key role in translating Smadi's communications. An English transcript of Smadi's videotaped speech, which was recorded in Arabic, suggests that these analysts were called upon.[293] The videotape was likely shared with the JTTF partners investigating the case.

---

[290] *United States v. Hosam Maher Husein Smadi*, Criminal Complaint No. 3-09-MJ-286; Federal Bureau of Investigation, "Terror Plot Foiled: Inside the Smadi Case;" and Department of Justice, "Federal grand Jury in Dallas Indicts Man for Attempting to Bomb Dallas Skyscraper," Press Release, October 8, 2009, http://www.usdoj.gov/usao/txn/PressRel09/smadi_indict_pr.html (accessed October 20, 2010).

[291] *United States v. Hosam Maher Husein Smadi*, Criminal Complaint No. 3-09-MJ-286; and Federal Bureau of Investigation, "Terror Plot Foiled: Inside the Smadi Case."

[292] Federal Bureau of Investigation, "Terror Plot Foiled: Inside the Smadi Case."

[293] *United States v. Hosam Maher Husein Smadi*, Case No. 3-09-MJ-286, Government Exhibit 240, in the U.S. District Court for the Northern District of Texas, http://www.txnd.uscourts.gov/judges/smadi/240.pdf (accessed October 20, 2010).

Confidential Sources

Yes. Similar to the Internet information, the information from the undercover agents was shared with other task force partners to assess Smadi's capability and commitment. It also was shared to ensure that Smadi believed he was going to carry out a real attack. For example, a month before the attempted attack, Smadi disclosed to an agent the size and expectations of the bomb to be used. Bomb experts were able to use this information to craft a phony yet convincing bomb made to Smadi's specifications.[294]

Assessment. The above review shows that a number of sources provided critical indications of a jihadist plot. Once discovered, the information was analyzed by partner agencies and used to guide further investigation. As in other cases, skilled undercover agents were able to get in close with Smadi to confirm his intentions and ultimately drive him to his demise. But before that could be done, a gateway was required. This case revealed that the FBI was actively monitoring jihadist-themed Internet sites, searching for that gateway. When they discovered online rhetoric that was abnormally explicit, they conducted language and credibility analysis to steer follow-on actions, thereby setting a precedent for the technique. Special Agent Petrowski voiced, "one big takeaway from this case is the question of how many other potential violent extremists are out there, being exposed to terrorist ideologies online and contemplating an attack."[295] This case suggests the FBI and the multi-agency task forces are going online to answer that question.

I. TOLEDO THREE—TOLEDO, OH (2006)

Mohammed Zaki Amawi. A resident of Toledo, Ohio with both Jordanian and U.S. citizenship, Amawi was considered the de facto leader of the homegrown cell. He worked at a local travel agency and met the other cell members through the Masjid Saad

[294] *United States v. Hosam Maher Husein Smadi*, Criminal Complaint No. 3-09-MJ-286.

[295] Federal Bureau of Investigation, "Terror Plot Foiled: Inside the Smadi Case."

and Masid At-Tawfeeq mosques. Amawi reportedly attempted to enter Iraq through Jordan to join the insurgency in 2003, prior to meeting the other two men.[296]

Marwan Othman El-Hindi. A naturalized U.S. citizen born in Jordan, El-Hindi had apparently received early FBI attention in 2002 when he was cited at an Islamic fundamentalist meeting as "'one of the brothers from Toledo' who was adept at coming up with money-making schemes."[297] In fact, he used past lessons learned to create a fraudulent charity organization in support of the group's conspiracy.[298]

Wassim I. Mazloum. Mazloum was born in Lebanon but was a legal permanent resident of the U.S. He owned and operated two car dealerships in Toledo, which he offered to provide as cover during the group's conspiracy to join the Iraq insurgency.[299]

Summary. In February 2006, the three men from Toledo were arrested and subsequently indicted for "conspiring to kill or maim persons outside the United States, including U.S. military personnel serving in Iraq, and conspiring to provide material support to terrorists."[300] According to reports, the authorities uncovered the conspiracy when the cell unknowingly worked with an FBI informant to conduct planning and training in preparation to join the Iraq insurgency. The informant, a former Special Forces soldier, had assumed the identity of an "Islamic extremist" in order to penetrate the cell.[301]

---

296 Institute for Preventive Strategies, "Preventing Jihad in Toledo," IPS website, June 22, 2006, https://www.preventivestrategies.net/public/library_file_proxy.cfm?lid=37 (accessed October 12, 2010), 4-5.

297 Christopher Evans et al., "Nickel-and-dime hustler, or something worse?" The Plain Dealer, May 21, 2006, http://www.cleveland.com/search/index.ssf?/base/news/1148200314107070.xml?nohio&coll=2 cited in Institute for Preventive Strategies, "Preventing Jihad in Toledo," 3.

298 *United States v. Mohammed Zaki Amawi et al.*, Case No. 3:06CR719, Sentencing Memorandum, in the U.S. District Court for the Northern District of Ohio Western Division, October 5, 2009, http://www.investigativeproject.org/documents/case_docs/1100.pdf (accessed October 12, 2010).

299 Mike Wilkinson and Christina Hall, "3 charged in terror plot; local suspects planned attacks in Iraq, U.S. says," The Blade website, February 22, 2006, http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20060222/NEWS03/60222005 (accessed October 12, 2010).

300 Department of Justice, "Three Sentenced for Conspiring to Commit Terrorist

Acts Against Americans Overseas," Press Release, October 22, 2009, http://www.usdoj.gov/opa/pr/2009/October/09-nsd-1136.html (accessed October 12, 2010).

301 Tim Andrassy, "Informant: Terror Suspects Sought Him," Fox Toledo, May 10, 2008, http://www.foxtoledo.com/dpp/news/Informant_Terror_Suspects_Sought_Him (accessed October 12, 2010).

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
Muslim community	Jihadist websites Email correspondence	Fraudulent charity organization Travel to Jordan	Training and bomb-making videos Handwritten note Laptop computers	Informant

Figure 12. Toledo Three Indicators

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Interpersonal Interaction

Yes. Details are not clear, but several reports claim that the Toledo Muslim community had alerted both local and federal authorities about extremist attitudes of some of the men 18 months prior to their arrest.[302] FBI Special Agent Ted Wasky later told the press that "individuals within Toledo's Muslim community contacted the FBI about what he termed the 'violent and radical views' the suspects were articulating."[303] The authorities acted on this information with the assistance of a confidential informant.

Inernet-Based

Yes. While it does not appear that authorities were conducting active Internet monitoring, court records show that the cell's Internet activities were a significant indicator of their intent to commit violent jihad. The men frequented jihadist websites,

[302] Institute for Preventive Strategies, "Preventing Jihad in Toledo," 5; Wilkinson and Hall, "3 charged in terror plot; local suspects planned attacks in Iraq, U.S. says."

[303] WTOL News, "Toledo's Arab Community Called 'Crucial' to Terrorism Investigation," WTOL website, February 21, 2006, http://www.wtol.com/global/Story.asp?s=4533250 (accessed October 12, 2010).

downloading violent videos and instructional manuals, all of which they shared with the confidential informant. El-Hindi also frequently sent incriminating e-mails to the informant.[304]

Incident Reports

Yes. Two important incidents signaled the scale of the cell's operation and need for intervention. The first was the discovery of a fraudulent charity organization that El-Hindi created to acquire federal grant money. While he and a co-conspirator were indicted separately for the fraud, the scheme caused the FBI to suspect that it might be tied to funding terrorist operations, given El-Hindi's previous connections.[305] The second incident was a report of Amawi's travel to Jordan in August 2005. Accompanied by the informant, Amawi flew to Jordan, carrying with him five computers he stated he intended to give to the mujahideen "brothers."[306]

Documents, Media, Material

Yes. During one meeting, Amawi handed over a CD to the informant that had a video entitled "Martyrdom Operation Vest Preparation," which detailed the construction of a suicide bomb vest. Amawi told the informant that he wanted him to download the video to his own computer for use in the cell's jihadist training.[307] On a separate occasion, Amawi passed the informant a note with a code word representing a chemical explosive the cell was trying to acquire.[308] And, as noted previously, Amawi procured laptop computers that were meant for Iraq insurgents. All of these items provided authorities with concrete proof of a jihadist conspiracy.

Confidential Sources

Yes. Court records indicate that the majority of information of the cell's activities came from the confidential informant. Notably, the informant was not originally aware

---

304 *United States v. Mohammed Zaki Amawi et al.*, Case No. 3:06CR719, Indictment, February 16, 2006, http://www.investigativeproject.org/documents/case_docs/93.pdf (accessed October 12, 2010), 3–6.

305 *United States v. Mohammed Zaki Amawi et al.*, Case No. 3:06CR719, Sentencing Memorandum, 42-46.

306 *United States v. Mohammed Zaki Amawi et al.*, Case No. 3:06CR719, Indictment, 8.

307 Ibid., 4–5.

308 Ibid., 7.

of this particular cell, as he was tasked by the FBI to observe other undisclosed individuals at the mosque. According to the informant, Amawi and El-Hindi actually sought him out, convinced by the guise that he was a former soldier turned jihadist. They approached him, asking specifically for violent jihad training, and thereby triggering an in-depth investigation.[309]

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Interpersonal Interaction

Yes. Media reports contend that the tipoffs from the Toledo Muslim community were "good enough" for the FBI to begin targeting suspicious individuals. While the nature of the tips remained confidential, the information led to the targeting of nearly 20 people from the local mosques. The informant was inserted in an effort to collect further information on possible homegrown extremists.[310]

Inernet-Based

Yes. Once authorities were made aware of the extensive Internet use by the cell, the prosecution was able to later then trace and attribute the multitude of violence-related posts the men had communicated on online forums. For example, Amawi made contact with a supposed Syrian jihadist in which they discussed attempts to acquire an explosive substance called astrolite.[311] El-Hindi posted repeatedly "I am a terrorist" and "kill Jews and Americans" on the jihadist website *Ekhlass*.[312] It was posts like these that helped the prosecution demonstrate the cell's commitment to carrying out jihad against Americans.

Incident Reports

Yes. Suspicious of El-Hindi's charity organization, the FBI, with the assistance of the IRS, discovered that El-Hindi was in fact pocketing the organization's funds for

309 *United States v. Mohammed Zaki Amawi et al.*, Case No. 3:06CR719, Indictment, 4; Michael Isikoff, "The Secret Agent," *Newsweek* website, July 3, 2008, http://www.newsweek.com/2008/07/02/the-secret-agent.html (accessed October 12, 2010).

310 Isikoff, "The Secret Agent."

311 *United States v. Mohammed Zaki Amawi et al.*, Case No. 3:06CR719, Sentencing Memorandum, 20.

312 Ibid., 46–47.

himself and the cell's plot. Authorities determined he had defrauded the government of over $40,000.[313] Following up on Amawi's intentions to travel to Jordan, the FBI worked with Jordanian authorities to track the conspirator when he arrived and ultimately arrested him in February 2006.[314]

Documents, Media, Material

Yes. The contents of Amawi's CD (and several others later seized) were heavily analyzed during investigation. Court records state that authorities were able to establish that Amawi's "'world class' collection of violent jihadist propaganda, terrorist training materials, extremist doctrine and videos… constitutes convincing evidence of his commitment…"[315] Furthermore, the laptops he carried with him to Jordan gave proof of his attempt to provide material support to terrorists. The Department of Justice confirmed that Amawi was prevented from delivering the computers.[316]

Confidential Sources

Yes. Because the informant was the sole material witness, the information he collected effectively steered the investigation. From the moment he was approached by the cell until the final arrest, the informant documented many of the key activities for which the men were indicted to include weapons training, distribution of bomb-making information, material support, and explicit verbal threats to kill the President of the United States.[317]

3. Was the information shared in order to attract other useful information?

Interpersonal Interaction

Yes. While the Toledo Muslim community was generally unaware of the specifics

313 *United States v. Mohammed Zaki Amawi et al.*, Case No. 3:06CR719, Sentencing Memorandum, 43–46.

314 Institute for Preventive Strategies, "Preventing Jihad in Toledo," 7.

315 *United States v. Mohammed Zaki Amawi et al.*, Case No. 3:06CR719, Sentencing Memorandum, 31-32.

316 Wilkinson and Hall, "3 charged in terror plot; local suspects planned attacks in Iraq, U.S. says."

317 Ibid.; *United States v. Mohammed Zaki Amawi et al.*, Case No. 3:06CR719, Indictment.

of the cell's conspiracy, it did have a sense that there were radicals among them. By sharing that information with local and federal authorities they were able to effectively help remove the threat.

Inernet-Based

Yes. In addition to the FBI's analysis of the Web postings, the U.S. Attorney's Office for the Northern District of Ohio requested an analyst from the NEFA Foundation to review the evidence and provide expert witness testimony. He concluded to the court that the "material is very likely to be useful to a person or persons conspiring to join a terrorist organization or preparing an act of terrorism."[318]

Incident Reports

Yes. The FBI worked with the IRS to establish that El-Hindi's fraudulent organization was indeed a cover for jihadist funding. Furthermore, the FBI worked with Jordanian officials and presumably U.S. Immigration and Customs Enforcement to secure Amawi and return him to the U.S for trial.[319]

Documents, Media, Material

Yes. In addition to the Internet information, the NEFA analyst was asked to assess the CDs containing the jihadist videos and training documents. He concluded that the information was also representative of Al Qaeda's ideology and encouraging for aspiring jihadists.[320]

Confidential Sources

Yes. Department of Justice records indicate that several members of the Toledo JTTF and other law enforcement agencies assisted in the case.[321] Because the confidential informant was the key node for all information regarding the cell's activities, it is reasonable to imply that his findings were shared with the partner agencies.

---

318 Evan F. Kohlmann, "Expert Report II: U.S. v. Amawi et al.," January 2008, http://nefafoundation.org/file/FeaturedDocs/amawiexpertreport0608.pdf (accessed October 12, 2010), 30.

319 Institute for Preventive Strategies, "Preventing Jihad in Toledo," 7.

320 Kohlmann, "Expert Report II: U.S. v. Amawi et al.," 2.

321 Department of Justice, "Three Sentenced for Conspiring to Commit Terrorist Acts Against Americans Overseas."

Assessment. The "Toledo Three" conspiracy was thwarted by community awareness, inside help, and effective information sharing. It is evident, however, that much of the success rests upon the confidential informant who was actually solicited by the plotters. Without his alert, many of the other indicators may have been overlooked and the men could have slipped away to Iraq. That point aside, this case does show the significant contribution that open source Internet information offered. While it was not actively monitored, it was later collected and analyzed by both authorities and private partners to demonstrate that the homegrown cell had capability and intent to wage violent jihad. This is important as the cell was not caught actually conducting an attack or joining the insurgency. Authorities were able to lawfully preempt the plot by identifying critical information that, when synthesized, showed a logical progression toward actual violence.

J. GEORGIA PLOTTERS—ATLANTA, GA (2006)

Syed Haris Ahmed. A naturalized citizen originally from Pakistan, Ahmed was a mechanical engineering student at Georgia Tech University and worked part time at a perfume shop.[322] He frequently attended the Al-Farooq Masjid mosque near the Georgia Tech campus.[323] In July 2005, he traveled to Pakistan in an attempt to receive terrorist training and to join in fighting.[324]

Ehsanul Islam Sadequee. Sadequee was a U.S. citizen born in Fairfax, Virginia and lived with his family in Roswell, Georgia. He reportedly worked for the Atlanta-based non-profit group Raksha, which addresses South Asian community issues in the Atlanta area.[325] He befriended Ahmed through the Al-Farooq Masjid mosque.[326] While his

---

322 Bill Rankin, "Ruling boosts terror case," Atlanta Journal-Constitution website, August 20, 2008, http://www.ajc.com/services/content/printedition/2008/08/20/ahmed.html (accessed September 19, 2010).

323 Bill Rankin, "Homegrown terrorists sent to prison," Atlanta Journal-Constitution website, December 14, 2009, http://www.ajc.com/news/north-fulton/homegrown-terrorists-sent-to-240912.html (accessed September 19, 2010).

324 Ibid.

325 CNN, "Atlanta college student faces terror charge," CNN website, April 21, 2006, http://articles.cnn.com/2006-04-20/us/bangladesh.arrests_1_terror-charge-ehsanul-islam-sadequee-fbi?_s=PM:US (accessed September 19, 2010).

326 Bill Rankin, "Homegrown terrorists sent to prison."

partner was in Pakistan, Sadequee traveled to Bangladesh to work more closely with members of a group called "Al Qaeda in Northern Europe."[327]

Summary. In 2006, following the investigation by the Atlanta JTTF, Ahmed and Sadequee were charged with conspiracy to provide material support to terrorists and the designated foreign terrorist organization, Lashkar-e-Tayyiba (LET).[328] Ahmed and Sadequee were first arrested for making false statements to the FBI concerning their foreign travel as related to an ongoing terrorism investigation. The men were alleged to have begun their quest for jihad on extremist websites, engaging with other would-be terrorists in Canada and Great Britain. Through these connections, they joined in a conspiracy that crossed international boundaries yet included targets within the U.S. Spokesmen for the case said that the two men did not present immediate danger, however, they asserted that "in the post-9/11 world we will not wait to disrupt terrorism-related activity until a bomb is built and ready to explode."[329]

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
Relatives	Posts on jihadist websites	International travel (Pakistan, Bangladesh, Canada) False statements (FBI Interviews)	Videos of targets	Informant

Figure 13. Georgia Plotters Indicators

[327] Department of Justice, "Atlanta Defendant Found Guilty of Supporting Terrorists," Press Release, August 12, 2009, http://www.usdoj.gov/opa/pr/2009/August/09-nsd-790.html (accessed September 19, 2010).

[328] *United States v. Syed Haris Ahmed*, Criminal Indictment No. 1:06-CR-147-CC, in the U.S. District Court for the Northern District of Georgia, December 9, 2008, http://nefafoundation.org/file/FeaturedDocs/US_v_SyedHarisAhmed_2ndSpcInd.pdf (accessed September 19, 2010).

[329] David Nahmias, U.S. Attorney for the Northern District of Georgia, cited in Department of Justice, "Defendant Found Guilty of Conspiracy to Support Terrorists," Press Release, June 10, 2009, http://www.usdoj.gov/opa/pr/2009/June/09-nsd-572.html (accessed September 19, 2010).

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Interpersonal Interaction

No. After the men's arrest, the families were interviewed several times by state and federal authorities and the media. According to reports from family members, none knew how devoted the young men were to carrying out jihad and therefore provided no indications to authorities. Dr. Tameema Ahmed, a college professor and Syed Ahmed's father, thought his son had always just been emotional and concerned about worldly affairs. Ahmed's sister said that her brother was always trying to get the family to be more religious, but she did not see the violent leanings.[330] Likewise, Sadequee's family said they were "very shocked and startled and hurt" by the news that he was arrested for involvement with jihadist terrorism.[331]

Inernet-Based

Yes. Several reports and court documents claim that overly suspicious posts by Canadian nationals and others on jihadist Web forums were discovered by the Canadian Security Intelligence Service (CSIS) and the private U.S.-based Internet monitoring group, SITE. These discoveries apparently set off an investigation of the "Toronto 18" jihadist cell, which authorities would later find had conspired with Ahmed and Sadequee.[332]

Incident Reports

Yes. After the investigation into the Toronto cell had begun, the FBI found out from Canadian authorities that Ahmed and Sadequee possibly had met with the cell in

330 Public Broadcasting Service, "Canada: The Cell Next Door," transcript from *Frontline* broadcast, January 30, 2007, http://www.pbs.org/frontlineworld/about/episodes/602_transcript.html (accessed September 19, 2010).

331 CNN, "Atlanta college student faces terror charge."

332 *United States v. Syed Haris Ahmed*, Criminal Indictment No. 1:06-CR-147-CC; CBC News, "Among the Believers: Cracking the Toronto Terror Cell," CBC News website under 'Timeline,' http://www.cbc.ca/fifth/torontoterror/timeline.html (accessed September 19, 2010); and Stewart Bell, "Web forum linked cells," National Post website, June 15, 2006, http://www.canada.com/nationalpost/news/story.html?id=84d54ba3-0a74-4462-8f36-2b4dbd47025f&k=86609 (accessed September 19, 2010).

March 2005. Because the cell was under investigation for jihadist conspiracy, the authorities had good enough reasoning to question the two Americans about the purpose of their travel.[333]

Media

Yes. Canadian authorities discovered that the central coordinating figure among the extremist websites was Younis Tsouli, a propagandist and recruiter for Al Qaeda in Iraq. In October 2005, British officials arrested Tsouli and found in his residence video clips of Washington monuments. Tsouli revealed that the clips were sent by Sadequee, therefore sending another flag to U.S. authorities that the Georgia pair was involved in a conspiracy.[334]

Confidential Sources

Yes. Mubin Shaikh, an informant who had penetrated the Canadian cell, reported that he overheard that the two Americans were looking to seek safe haven in Canada if they were to plan and carry out attacks in the U.S.: "The chatter was that an attack of some sort was going to be planned. And the setup was that the attack would be planned and the attack would be carried out and they [the Americans] would fall back over to the border in Canada... and we would give them logistical support on this end."[335]

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Interpersonal Interaction

No. The men's families claimed to know nothing of their jihadist activities and appeared to provide little useful information to the investigation.

---

[333] *United States v. Ehsanul Islam Sadequee*, No. M-06-335, Affidavit in Support of Arrest Warrant, in the U.S. District Court of the Eastern District of New York, May 28, 2006, http://nefafoundation.org/file/FeaturedDocs/U.S._v_Sadequee_FBIAffidavit.pdf (accessed September 19, 2010).

[334] CBC News, "Among the Believers: Cracking the Toronto Terror Cell," and Bell, "Web forum linked cells."

[335] Public Broadcasting Service, "Canada: The Cell Next Door."

Inernet-Based

Yes. The jihadist Web forums were in fact good enough sources of information for further inquiry. Authorities monitoring the sites soon found out that the users were not limited to the Canadian cell. In fact, they came across terror suspects originating in the United Kingdom, Australia, Sweden and elsewhere, setting off multiple investigations that would lead to their eventual arrest.[336] Ahmed and Sadequee were also found to be frequent contributors to the forums, which they used to coordinate trips to Canada, Pakistan, and Bangladesh in support of their plot.[337] Because the Internet seemed to be a critical node in the case, an analyst from a private monitoring group was brought in to demonstrate the very real linkages to terrorist groups like Al Qaeda and LET that existed. The analyst synthesized voluminous open source information from the websites, showing the communications structure of the jihadist network of which the two Americans and others were members.[338]

Incident Reports

Yes. Ahmed was interviewed several times about his Canada trip by the FBI over a period of eight days. "Amid efforts to deny his illegal activities and mislead the agents, Ahmed made increasingly incriminating statements," according to a Department of Justice report.[339] The FBI was trying to compare information they obtained from Sadequee about the pair's international travel. When the information did not match up, the FBI conducted a travel records investigation, confirming the men had lied. They were then arrested for providing false statements.[340]

Media

Yes. The authorities were interested to find out further the purpose of the videos that were found in Tsouli's possession abroad. The FBI subsequently determined that the

---

336 Bell, "Web forum linked cells."

337 Department of Justice, "Atlanta Defendant Found Guilty of Supporting Terrorists."

338 *United States v. Syed Haris Ahmed and Ehsanul Islam Sadequee*, No. 1:06-cv-0147-WSD, in the U.S. District Court for the Northern District of Georgia, June 1, 2009, http://nefafoundation.org/file/US_v_HarisAhmed_ekdaubert.pdf (accessed September 19, 2010).

339 Department of Justice, "Atlanta Defendant Found Guilty of Supporting Terrorists."

340 *United States v. Ehsanul Islam Sadequee*, No. M-06-335.

videos were, in fact, casing videos of potential targets. In April 2005, Ahmed and Sadequee traveled to Washington, D.C. and recorded images of the Capitol, World Bank, Masonic temple, and a fuel tank farm. The videos were then sent out to establish the men's credibility and to aid in jihadist planning.[341]

Confidential Sources

Yes. The authorities understood clearly the informant's report of a Canadian and American connection. Armed with that knowledge, the FBI was able pursue a series of interviews of Ahmed and Sadequee, as discussed earlier, to determine the extent of that connection.

3. Was the information shared in order to attract other useful information?

Interpersonal Interaction

Yes. Reports indicate that the families of both men spoke to several state and federal authorities as part of the investigation.[342] This at least gave the authorities a sense of the relationships and levels of communication with the men. As noted earlier, however, the families did not appear to offer indication of jihadist activity.

Inernet-Based

Yes. The Internet information was shared across several organizations in a number of countries. The Canadian intelligence service and SITE both uncovered information critical to the Royal Canadian Mounted Police, who arrested the Toronto cell. The information pertaining to Younis Tsouli was also shared with British authorities. Likewise, U.S. authorities were led to Ahmed and Sadequee's Web posts with the assistance of foreign agencies and private Internet monitors and analysts.[343]

Incident Reports

Yes. When the official statements by Ahmed and Sadequee did not agree, the FBI contacted Immigration and Customs Enforcement (ICE). ICE records showed the men

---

[341] Department of Justice, "Atlanta Defendant Found Guilty of Supporting Terrorists."

[342] CNN, "Atlanta college student faces terror charge."

[343] Bell, "Web forum linked cells;" Stewart Bell, "Probe had global dimension," National Post website, June 5, 2006, http://www.canada.com/nationalpost/news/story.html?id=7db46260-ee0e-455d-8c06-3b92e571b050 (accessed September 19, 2010).

crossing the border from Canada back into the U.S. on March 12, 2005. The FBI also obtained from Greyhound confirmation that the men had indeed traveled together on a bus from Atlanta to Toronto.[344] Additionally, the warrant for the men's arrest, which detailed then-known activities and the contents of their false statements, was made available to other U.S. and foreign law enforcement and the International Criminal Police Organization (INTERPOL).[345]

Media

Yes. The videos discovered in Tsouli's residence were shared with U.S. authorities as part of what clearly had become an international investigation. The FBI was then able to trace the videos back to the April 2005 trip Ahmed and Sadequee had made to Washington, D.C.

Confidential Sources

Yes. While it is not known if Shaikh ever had direct contact with U.S. authorities, it is clear that significant cross-border and interagency cooperation ensured that the informant's knowledge of the Americans and their co-conspirators was communicated.[346]

Assessment. The successful intervention of the "Georgia Plotters" case clearly was a multilateral effort that relied upon sources of information from all categories. The analysis of this case reveals several important take-aways. The first is that open source exploitation of the Internet not only "sensed" a possible jihadist plot, it also helped identify the network of actors and determined the credibility of the threat they posed. This allowed authorities to focus their investigative efforts. Furthermore, they relied upon analyses from both government agencies and private specialists. Second, this case once again highlights the indispensability of confidential informants. An "inside man" often is able to thread together the abundance of information that is collected from other sources. The concern that remains, however, is that the job is risky and there are no guarantees that a viable informant can be found in every situation. Finally, this case

344 *United States v. Ehsanul Islam Sadequee*, No. M-06-335.

345 Ibid.

346 Public Broadcasting Service, "Canada: The Cell Next Door," under 'Interview: Neil Docherty.'

illuminates the extent to which information sharing across agencies (and borders) can effectively disrupt the plots of homegrown jihadists, whose networks may extend beyond local boundaries.

K. COLLEEN LAROSE—PENNSBURG, PA (2009)

Colleen R. LaRose. A U.S. citizen and Pennsylvania resident, LaRose commonly referred to herself as "JihadJane" or "Fatima Larose," her online aliases. She moved from Texas to Pennsburg, near Philadelphia, sometime in 2004 where she was unemployed and had a live-in boyfriend. LaRose, who was never considered religious and apparently never attended a mosque, declared herself a "desperate" Muslim supporter on a 2008 YouTube video.[347]

Summary. LaRose was arrested in October 2009 immediately after returning from a trip she took to Europe in an attempt to track down and kill Swedish cartoonist Lars Vilks. She was charged with "conspiracy to provide material support to terrorists, conspiracy to kill in a foreign country, making false statements to a government official and attempted identity theft."[348] Her indictment states that LaRose used the Internet to recruit men to conduct violent jihad in South Asia and Europe, and to recruit women with passports to travel in support of the jihad.[349] LaRose was apparently brought to the authorities' attention by civilian web-monitoring groups who had been tracking her online posts for three years.[350]

---

347 Maryclaire Dale, "Colleen LaRose: Accused 'Jihad Jane' Pleads Not Guilty," *Huffington Post*, March 18, 2010, http://www.huffingtonpost.com/2010/03/18/colleen-larose-accused-ji_n_504401.html (accessed November 1, 2010).

348 Department of Justice, "Pennsylvania Woman Indicted in Plot to Recruit Violent Jihadist Fighters and to Commit Murder Overseas," Press Release, March 9, 2010, http://www.justice.gov/opa/pr/2010/March/10-ag-238.html (accessed November 1, 2010).

349 Ibid.

350 Eamon McNiff, "Net Posse Tracked Jihad Jane for Three Years," ABC News website, March 11, 2010, http://abcnews.go.com/TheLaw/Technology/internet-monitors-tracked-jihad-jane-years/story?id=10069484 (accessed November 1, 2010); Ian Urbina, "Views of 'JihadJane' Were Unknown to Neighbors," *New York Times*, March 10, 2010, http://www.nytimes.com/2010/03/11/us/11pennsylvania.html (accessed November 1, 2010).

Interpersonal Interaction	Internet-based	Incident Reports/Watchlist Alerts	Documents, Media, Material	Confidential Sources
Boyfriend Neighbors	Posts on jihadist websites YouTube posts Email correspondence	Overseas travel False statement (FBI interview)	Stolen passport	N/A

Figure 14. Colleen LaRose Indicators

1. Was the information "good enough" at the time of discovery, therefore allowing timely intervention?

Interpersonal Interaction

No. According to media reports, neither LaRose's live-in boyfriend, Kurt Gorman, nor their apartment neighbors suspected her involvement in a jihadist conspiracy. Gorman claimed that he was not even aware of LaRose's interest in Islam and that she spent most of her time on the computer and taking care of Gorman's elderly father.[351] He told reporters "she seemed normal to me" and "she wasn't no rocket scientist."[352] Kristy Newell, who lived across the hall from the couple, stated that LaRose never exhibited indications of being Muslim and was often "seen staggering, drunk, up and down the street before her companion came to get her."[353]

Inernet-Based

Yes. Court records and several media reports show that authorities first became aware of LaRose's extremist leanings through her online posts on popular websites like YouTube and on jihadist websites. According to the indictment, her first overt act in connection with the conspiracy to provide material support was a comment she posted in

351 Dale, "Colleen LaRose: Accused 'Jihad Jane' Pleads Not Guilty."

352 Christina Lamb, "Jihad Janes spread fear in suburban US," The Sunday Times, March 14, 2010, http://www.timesonline.co.uk/tol/news/world/us_and_americas/article7060959.ece (accessed November 1, 2010).

353 Urbina, "Views of 'JihadJane' Were Unknown to Neighbors."

June 2008 under the alias "JihadJane," stating that she was "desperate to do something somehow to help the suffering Muslim people."[354] In June 2009, LaRose reportedly created a public account in which she openly solicited online for funds to support terrorism. An alert member of the volunteer Web group YouTube Smackdown, which identifies jihadist videos and tries to have them removed, had long been monitoring LaRose's online activity and discovered the solicitation scheme. The Web monitor claimed, "I knew she had become a real threat for our safety and had officially violated U.S. Federal Law…I formally called the FBI in Philadelphia to report her."[355]

Incident Reports

Yes. Aware that LaRose was trying to petition jihadist support online, the FBI formally questioned her in July 2009 about soliciting funds for terrorism, posting on jihadist websites, and using the online alias "JihadJane." LaRose provided a false statement, denying knowledge of each claim.[356] Her false statement gave authorities reason to believe she was covering something up. When a month later LaRose unexpectedly left the U.S. for Europe without her boyfriend's knowledge, the FBI was convinced that she was furthering her conspiracy.[357]

Documents

Yes. The FBI found out that LaRose stole her boyfriend Gorman's passport without his knowledge when she left for Europe. This discovery was significant to authorities as LaRose had been posting online about using passports to support her jihadist "brothers."[358]

---

354 *United States v. Colleen R. LaRose*, Criminal No. 10-Cr-123, in the U.S. District Court for the Eastern District of Pennsylvania, March 4, 2010, http://www.investigativeproject.org/documents/case_docs/1196.pdf (accessed November 1, 2010), 2–3.

355 McNiff, "Net Posse Tracked Jihad Jane for Three Years."

356 *United States v. Colleen R. LaRose*, Criminal No. 10-Cr-123, 6.

357 Ibid., 7; Lamb, "Jihad Janes spread fear in suburban US."

358 *United States v. Colleen R. LaRose*, Criminal No. 10-Cr-123, 7; Department of Justice, "Pennsylvania Woman Indicted in Plot to Recruit Violent Jihadist Fighters and to Commit Murder Overseas."

2. Did the information provide, in context, "good enough" understanding to move forward with investigation or intervention?

Interpersonal Interaction

Unknown. Available sources do not specify if Gorman went to authorities after discovering that LaRose had fled. It is therefore difficult to determine whether he provided information supportive of the ongoing investigation.

Inernet-Based

Yes. The FBI appears to have paid considerable attention to LaRose's subsequent Web posts following the initial alert to her Internet activity. Many of her comments and the responses they received were rather incriminating. For example, an unidentified co-conspirator confirmed on LaRose's online forum that funds LaRose had solicited for her jihad would be transferred.[359] While in Europe she openly declared, "only death will stop me now I am so close to the target," referring to the Swedish cartoonist she conspired to kill.[360] Though not specifically stated in the indictment, it is also apparent that the authorities later gained access to some of LaRose's personal e-mails, which provided further proof of her intent. In a series of e-mail exchanges with a foreign co-conspirator, LaRose agreed to fly to Sweden and kill the cartoonist, stating in one instance "I will make this my goal till I achieve it or die trying."[361]

Incident Reports

Yes. LaRose's false statement did give authorities enough understanding to continue investigation and to later indict her for lying. The FBI continued to track LaRose's movements and communications even while she was in Europe, finding further proof of illegal activity. Knowing that her overseas travel was in connection with a conspiracy to kill in a foreign country, the authorities finally moved in to stop her.[362]

---

359 *United States v. Colleen R. LaRose*, Criminal No. 10-Cr-123, 5.

360 Lamb, "Jihad Janes spread fear in suburban US."

361 *United States v. Colleen R. LaRose*, Criminal No. 10-Cr-123, 5.

362 Lamb, "Jihad Janes spread fear in suburban US."

Documents

Yes. Because the FBI already knew that LaRose sought to use passports in support of her conspiracy, the knowledge of her possession of a stolen passport was good enough to earn LaRose a charge of attempted identity theft to facilitate terrorism.[363]

3. Was the information shared in order to attract other useful information?

Interpersonal Interaction

Unknown. It is not clear if the personal accounts from Gorman or the neighbors were shared beyond the media to aid in investigation.

Inernet-Based

Yes. While FBI spokesmen have not formally confirmed it, several sources indicate that information sharing occurred between the volunteer Web monitoring group and the FBI.[364] Philadelphia U.S. Attorney Patrick Meehan stated: "I'm aware and know that there certainly was a role in this case served by such a group in alerting the federal authorities."[365]

Incident Reports

Yes. The FBI reportedly tracked LaRose's European travels to Ireland. Working with Irish counterterrorism officials there, the FBI was able to identify LaRose's co-conspirators who may have been involved in a larger plot than just killing the Swedish cartoonist.[366]

Documents

Unknown. Available sources do not indicate to what extent knowledge of the stolen passport was shared with partner agencies.

---

363 Lamb, "Jihad Janes spread fear in suburban U.S."

364 Ibid; McNiff, "Net Posse Tracked Jihad Jane for Three Years;" Jane Podesta, "'Jihad Jane' Case 'Tip of Iceberg,' Net Posse Warns," *Huffington Post*, March 23, 2010, http://www.huffingtonpost.com/jane-podesta/jihad-jane-case-tip-of-ic_b_509797.html (accessed November 1, 2010).

365 Larry King, "Web-monitoring groups didn't take 'JihadJane' seriously at first," *Philadelphia Inquirer*, March 11, 2010, http://www.allbusiness.com/crime-law/criminal-offenses-crimes-against/14094753-1.html (accessed November 1, 2010).

366 John F. Burns, "Irish Town Puzzled by Role in Investigation," *New York Times*, March 19, 2010, http://www.nytimes.com/2010/03/20/world/europe/20ireland.html (accessed November 1, 2010).

Assessment. While much has been gathered from LaRose's indictment and press releases, more details of her activities and those of the investigators are likely to surface once prosecution is complete. This case clearly demonstrates, however, the broader nature of Internet exploitation. In fact, it was open source monitoring in its purest sense that tipped off the authorities. A civilian activist group that flags jihadist Internet videos and posts on open forums with nothing more than a standard Web browser keyed in on "JihadJane" long before the FBI and subsequently reported her escalating activity. Though such groups may be controversial, U.S. Attorney Meehan did offer an interesting perspective, saying that "online tipsters are natural descendants of the 'eyes and ears' community contacts who tipped off police to crime rackets, drug deals, and other impending crimes."[367] In this case, online tips of information enabled the authorities to track LaRose, reveal other important indicators, and discontinue her jihadist conspiracy.

L. FINDINGS

The analysis of these 10 cases has revealed several insights into the factors that have contributed to the successful disruption of homegrown jihadist plots. As evidenced, all were thwarted through a combination of indicators that gave authorities sufficient understanding of a credible threat and the legal justification to intervene. Because the circumstances in each case were so varied, it is difficult to claim any one indicator or technique as preeminent. This analysis did, however, achieve the goal of illuminating the contributions made by open source exploitation of the Internet. In many cases the information collected from jihadist Web forums or social networking sites was assessed to be proof of intent to carry out or incite violence. While many of the details of the collection and analytical processes remain unclear, the value of the detection technique is validated. What follows now are a number of key findings drawn from the analysis.

Confidential informants and undercover agents remain invaluable sources of information. A majority of the cases reflected the overwhelming contribution made by confidential sources. Indeed, the classic tactic that has served law enforcement so well in criminal investigations has proven viable in confronting homegrown jihad. Yet as noted

[367] Larry King, "Web-monitoring groups didn't take 'JihadJane' seriously at first."

in some of the analyses, the risks still remain high and the chances of successfully inserting an "inside man" are unpredictable. The track record and expected payoff, however, are likely to serve as reasonable justifications to continue the tactic.

Personal relationships and public awareness are still important in understanding radicalization. Of the cases evaluated, none had their investigations initiated by tips from family, friends, or other close civil ties. However, the character and behavior accounts that were reported to the media (and to the authorities in some known cases) in the aftermath provided a glimpse into the lives of those American citizens and residents who aspired to conduct acts of terrorism. Though such accounts may not be enough to establish a concrete profile of those on the path to radicalization, they do contribute to a growing body of research that seeks to increase awareness at the interpersonal level.

Open source exploitation of the Internet has become a viable means for identifying homegrown threats and evaluating terrorist intent. The data shows that agencies like the FBI have adopted Internet monitoring as a gateway into jihadist operating space. Because they recognize that the Internet serves as an important vehicle for would-be jihadists, authorities have countered by using the same tool to identify networks of actors, evidence of communication, and violent intent. With the help of behavioral analysts and linguists, authorities are able to evaluate credibility and synthesize into intelligence what may on the surface appear to be nothing more than online chatter.

Private Web monitoring organizations have played a significant role in identifying homegrown threats and assisting prosecution. Specialists from private organizations have on more than one occasion infiltrated and monitored hard-to-find jihadist Web forums and tracked serious actors. Because these specialty organizations focus solely on jihadist Internet activity, they have built an indispensable base of knowledge that has provided law enforcement and prosecution with important contextual analyses, cultural background and actionable intelligence.

Community-based Web monitoring groups supplement the search for homegrown jihadists. The recent case of "JihadJane" demonstrates the power of civilian all-volunteer

groups intent on doing their part to counter radical activity and violence. Though they may not be technically trained or equipped, they represent a sort of 'neighborhood watch' that may provide authorities with context clues. While Internet vigilantes are likely not the final answer in detecting homegrown jihadists, there is value in listening to community members who are attune to the Internet environment.

Future plot disruptions will be contingent on information sharing and interagency cooperation. Regardless of how information is collected, embracing a multilateral approach that fosters information sharing among federal, state, and local agencies and the communities they serve will increase the chances of thwarting an attack or conspiracy in a timely manner. The case study analysis has shown that FBI-led Joint Terrorism Task Forces across the nation have met success due to cooperation with partner agencies, private firms, the American public, and in some cases international partners. This suggests that there has been progress among the intelligence and law enforcement communities since 9/11 to cooperatively develop an effective domestic counterterrorism apparatus.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. SUMMARY

Global response to the aftermath of 9/11 set about a change in the threat of jihadist terrorism. Al Qaeda's ideological influence was no longer confined to a location oceans away. Though the danger of Al Qaeda persists, the rise of homegrown jihadist actors—American citizens and residents—has prompted the need for effective domestic counterterrorism measures. As introduced in Chapter I, terror within the homeland is not a new phenomenon. Authorities have long battled violent left and right-wing organizations and extreme environmentalist groups, and continue to do so. What sets those groups apart from the homegrown jihadist, however, is that the latter is indiscriminate and seeks to inflict mass casualties. Furthermore, the Internet has become a prominent means by which jihadists operationalize their radical behavior, using the technology to spread violent propaganda, transfer funds, conduct targeting, and coordinate their attacks. Consequently, more attention has been paid to the Internet environment.

Chapter II discussed in detail the evolution of concern regarding jihadist use of the Internet. Notably, the tracking of terrorist Internet activity began before 9/11, predominantly by the terrorism research community. While early studies focused on established international organizations, researchers soon discovered an evolution in the jihadist movement. The Internet appeared to be an empowering tool that promoted decentralization as a means of maintaining the terror campaign. Though it was not immediate, the U.S. Intelligence Community, including the FBI, caught on to the growing trend. Several assessments beginning in the mid-1990s and continuing to the present demonstrate that the IC has traced the shifting character of terrorism within the homeland. Key intelligence judgments have suggested that those in counterterrorism turn to the very forums where homegrown radicalization thrives.

Chapter III described the prominent challenges of collecting and using Internet information as a means to identify homegrown jihadist threats. Because it is largely

ungoverned, the Internet environment can often lead to the problem of information overload. Language and cultural skill deficiencies can hinder the ability to evaluate online information, and if those obstacles are overcome, there remains the difficult task of determining the information's credibility. There are also a number of organizations charged with counterterrorism that may or may not be well-suited for exploiting open source Internet information, therefore stressing the importance of effective information sharing. Finally, there are concerns about how this technique affects American privacy and civil liberty.

Chapter IV addressed the primary question this thesis sought to answer: Does open source exploitation of the Internet provide an effective means for identifying homegrown jihadist threats? Two hypotheses were posed, one stating that the detection technique is merely a foundation for the more effective classified approaches, and the other stating that the technique is in fact a considerably effective means for assessing homegrown threats. Indeed, the analysis has demonstrated that the answer to the question lies somewhere in the middle. Internet exploitation, as a stand-alone capability, can detect signs of homegrown jihadist activity and, in a supporting role, provide significant contextual information that supplements that which is derived from riskier confidential measures, such as the use of informants and undercover agents.

B. RECOMMENDATIONS

Based on the findings of this study, there are several recommendations for increasing the effectiveness of open source Internet exploitation as a viable technique to detect home grown jihadist threats:

- Provide increased funding to support the growth of the FBI's cyber investigative technology and the number of analysts.
- Invest in and integrate innovative open source technologies like the Dark Web research project and social network analytical tools.
- Develop sustainable partnerships with private open source centers and educate state and local authorities of those organizations' utility.

- Renew emphasis on recruiting and/or developing both analysts and law enforcement specialists with foreign language skills and cultural expertise.
- Train analysts to identify linguistic patterns and phraseology consistent with jihadist rhetoric.
- View community-based Web monitoring groups as another extension of 'neighborhood watch' and provide recognition when their alerts prove helpful.
- Conduct frequent congressionally-mandated checks on Internet exploitation measures to ensure infringement on America privacy and civil liberty is minimized.
- Establish detailed measures of effectiveness and promote regular reviews of *all* detection techniques to ensure the United States is appropriately resourcing those tools and techniques that best keep its citizens safe from jihadist terrorist attacks.

By smartly embracing Internet exploitation as a valuable detection technique, intelligence and law enforcement officials can continue to adopt a proactive, intelligence-driven approach that seeks to preempt violent attacks and conspiracies perpetrated by American homegrown jihadists.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Atran, Scott. “A Failure of Imagination (Intelligence, WMDs, and ‘Virtual Jihad’).” *Studies in Conflict and Terrorism*, vol. 29 (2006).

Best, Richard A. Jr. “Intelligence Issues for Congress.” Congressional Research Service Report RL33539, June 11, 2010.

_____. “The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns.” Congressional Research Service Report R41022, January 15, 2010.

Best, Richard A., Jr. and Alfred Cumming. “Open Source Intelligence (OSINT): Issues for Congress.” Congressional Research Service Report RL34270, December 5, 2007.

Bjelopera, Jerome P. and Mark A. Randol. “American Jihadist: Combating a Complex Threat.” Congressional Research Service Report RL41416, September 20, 2010.

Blair, Dennis C. “Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence.” February 2, 2010.

Brachman, Jarret. “Statement of Dr. Jarret M. Brachman before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities on the Topic of Understanding Cyberspace as a Medium for Radicalization and Counter-radicalization.” December 16, 2009.

Brennan, John. Transcript of speech given to Center for Strategic and International Studies, Washington, DC, May 26, 2010.

Chen, Hsinchun, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, and GabrielWeimann. “Uncovering the Dark Web: A Case Study of Jihad on the Web.” *Journal of the American Society for Information Science and Technology*, vol. 59, no. 8 (January 2008).

Department of Homeland Security. “Office of Intelligence and Analysis.” Accessed October 13, 2010. http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm.

_____. “The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security.” DHS Privacy Office. Accessed October 13, 2010. http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

_____. “Privacy Impact Assessment: Publicly Available Social Media Monitoring and Situational Awareness Initiative.” DHS Office of Operations Coordination and Planning. Accessed October 20, 2010. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia.pdf.

Department of Justice. “FBI FY2010 Budget Report.” Accessed October 10, 2010. http://www.justice.gov/jmd/2010summary/pdf/fbi-bud-summary.pdf.

_____. “Report from the Field: The USA PATRIOT Act at Work.” July 2004.

Doyle, Tony and John L. Hammond. “Net Cred: Evaluating the Internet as a Research Source.” *Reference Services Review*, vol. 34, no.1 (2006).

Everton, Sean. “Chapter 7: Cohesion and Clustering.” In *Tracking, Destabilizing, and Disrupting Dark Networks with Social Network Analysis*. Monterey, CA: Naval Postgraduate School, 2010.

Federal Bureau of Investigation. “Terrorism in the United States: 1996.” Annual Terrorism Report, 1996.

_____. “Terrorism in the United States: 1997.” Annual Terrorism Report, 1997.

_____. “Terrorism in the United States: 1998.” Annual Terrorism Report, 1998.

_____. “Terrorism in the United States: 1999.” Annual Terrorism Report, 1999.

_____. “Terrorism 2000/2001.” Terrorism Report, 2001.

_____. “Terrorism 2002-2005.” Terrorism Report, 2005.

_____. “National Cyber Investigative Joint Task Force.” Accessed September 29, 2010. http://www.fbi.gov/about-us/investigate/cyber/ncijtf.

Gruen, Madeleine. “Attempt to Attack the Paul Findley Federal Building in Springfield, Illinois.” Report no. 23 in the ‘Target: America’ Series, December 2009. Accessed October 27, 2010. http://www.nefafoundation.org/miscellaneous/FeaturedDocs/nefa_fintontargetamerica.pdf.

Hoffman, Bruce. “The Use of the Internet by Islamic Extremists.” Testimony before the House Permanent Select Committee on Intelligence, May 4, 2006.

_____. “The Myth of Grass-Roots Terrorism,” *Foreign Affairs*, vol. 87, no. 3 (May 2008)

Homeland Security Advisory Council. “Report of the Future of Terrorism Task Force.” Department of Homeland Security Report, January 25, 2007.

Intelligence Reform and Terrorism Prevention Act of 2004, Section 1001 and Section 1021, P.L. 108–458.

“Israel: U.S. Hamas Activists Use Internet to Send Attack Threats.” Tel Aviv IDF Radio, FBIS-TOT-97-001-L, October 13, 1996. Cited in Steven A. Hildreth, “Cyberwarfare,” Congressional Research Service Report RL30735, June 19, 2001.

Jenkins, Brian Michael. “Would-Be Warriors: Incidents of Jihadist Radicalization in the United States since September 11, 2001.” RAND report, 2010.

Kim, Jin and William Allard. “Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Intelligence Analysis.” *SAIS Review*, vol. 28, no. 1 (2008).

Kohlmann, Evan F. “Expert Report II: U.S. v. Amawi et al.” January 2008. Accessed October 12, 2010. http://nefafoundation.org/file/FeaturedDocs/amawiexpertreport0608.pdf.

Laipson, Ellen. “Foreign Language Requirements in the Intelligence Community.” Statement to the Senate Government Affairs Committee, September 14, 2000.

Leiter, Michael. “Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.” Statement before the Senate Homeland Security and Government Affairs Committee, September 22, 2010.

McCormack, William. “State and Local Law Enforcement Contributions to Terrorism Prevention.” Accessed August 21, 2010. http://www2.fbi.gov/publications/leb/2009/march2009/terrorism.htm.

Mercado, Stephen. “Sailing the Sea of OSINT in the Information Age.” Central Intelligence Agency website. Accessed September 24, 2010. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies.

Metzger, Miriam J. “Making Sense of Credibility on the Web: Models for Evaluating Online Information and Recommendations for Future Research.” *Journal of the American Society for Information Science and Technology*, vol. 58, no. 13 (September 2007).

Milward, H. Brinton and Jorg Raab. “Dark Networks as Organizational Problems: Elements of a Theory.” *International Public Management Journal*, vol. 9, no. 3 (2006).

National Intelligence Council. “Global Trends 2015: A Dialogue About the Future With Nongovernment Experts.” December 2000.

NEFA Foundation. “The LA Plot to Attack U.S. Military, Israeli Government, & Jewish Targets.” Report No. 1, January 2008. Accessed July 23, 2010. http://www.nefafoundation.org/miscellaneous/LA_Plot.pdf.

Neu, John. Testimony before the House Committee on Homeland Security‘s Subcommittee on Intelligence, Information Sharing and Risk Assessment, April 5, 2007.

North Atlantic Treaty Organization. “Intelligence Exploitation of the Internet.” October 2002.

Office of the Director of National Intelligence. *National Intelligence Estimate: The Terrorist Threat to the U.S. Homeland*. Washington DC: ODNI, 2007.

_____. *National Intelligence Strategy for the United States of America*. Washington DC: ODNI, 2005.

_____. *Intelligence Directive 301: National Open Source Enterprise*. Washington DC: ODNI, 2006.

O‘Neill, Siobhan. “Terrorist Precursor Crimes: Issues and Options for Congress.” Congressional Research Service Report RL34014, May 24, 2007.

Pallaris, Chris. “Open Source Intelligence: A Strategic Enabler of National Security.” Research Institute for European and American Studies website. Accessed September 27, 2010. http://rieas.gr/index.php?option=com_content&task=view&id=633&Itemid=41.

Perl, Raphael. “Trends in Terrorism: 2006.” Congressional Research Service Report RL33555, March 12, 2007.

Ramsay, Gilbert. “Relocating the Virtual War.” *Defense Against Terrorism Review*, vol. 2, no. 1 (Spring 2009).

Randol, Mark A. “The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress.” Congressional Research Service Report R40602, March 19, 2010.

Reid, Edna and Hsinchun Chen. “Extremist Social Movement Groups and their Online Digital Libraries,” *Information Outlook*, vol. 10, no. 6 (June 2006).

Resnyansky, Lucy. “The Internet and the Changing Nature of Intelligence.” *IEEE Technology and Society Magazine*, vol. 28, no. 1 (2009).

Ressler, Steve, "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research," *Homeland Security Affairs*, vol. 2, no. 2 (2006).

Rollins, John and Clay Wilson, "Terrorist Capabilities for Cyberattack: Overview and Policy Issues." Congressional Research Service Report RL33123, January 22, 2007.

Rushkoff, D. *Coercion: Why We Listen to What 'They' Say*. New York, NY: Riverhead, 1999. Cited in Lucy Resnyansky, "The Internet and the Changing Nature of Intelligence," *IEEE Technology and Society Magazine*, vol. 28, no. 1 (2009).

Sageman, Marc, *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2008.

Sands, Amy. "Integrating Open Sources into Transnational Threat Assessments." In *Transforming U.S. Intelligence*, ed. Jennifer Sims and Burton Gerber. Washington DC: Georgetown University Press, 2005.

Silber, Mitchell D. and Arvin Bhatt. "Radicalization in the West: The Homegrown Threat." Report by the New York City Police Department, 2007.

Shulsky, Abram N. and Gary J. Schmitt. *Silent Warfare: Understanding the World of Intelligence*. Washington, DC: Potomac Books, 2002.

Smith, Marcia S., John D. Moteff, Lennard G. Kruger, Glenn J. McLoughlin, Jeffrey W. Seifert, and Patricia Moloney Figliola. "Internet: An Overview of Key Technology Policy Issues affecting its Use and Growth." Congressional Research Service Report 98-67, December 29, 2004.

Smith, Marcia S., Jeffrey W. Seifert, Glenn J. McLoughlin, and John Dimitri Moteff. "The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government." Congressional Research Service Report RL31289, March 4, 2002

Social Networking Monitoring Center. "Concept of Operations for the Presidential Inauguration." Accessed October 13, 2010. Slideshow available at Electronic Frontier Foundation website, https://www.eff.org/files/filenode/social_network/DHS_SNMC_Inauguration_monitoring.pdf.

Staten, Clark. Testimony before the Subcommittee on Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee, February 24, 1998. Quoted in Dorothy Denning, *Information Warfare and Security*, Reading, MA: Addison-Wesley, 1999.

Steele, Robert D. "Open Source Intelligence." In *Strategic Intelligence: The Intelligence Cycle*, ed. Loch Johnson. Westport: Praeger, 2007.

Stevens, Gina Marie and Charles Doyle, "Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping." Congressional Research Service Report 98-326, December 3, 2009.

Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. "Using Open-Source Information Effectively." Serial No. 109-22. Washington, DC: GPO, 2007.

Townsend, Frances Fragos. Transcript of address given to the ODNI Open Source Conference, Washington, DC, July 16, 2007. Accessed May 30, 2010. http://www.dni.gov/speeches/20070716_speech_2.pdf.

Tsfati, Yariv and Gabriel Weimann, "www.terrorism.com: Terror on the Internet," *Studies in Conflict & Terrorism* 25 (2002).

Tucker, David. "Jihad Dramatically Transformed? Sageman on Jihad and the Internet." *Homeland Security Affairs*, vol. 6, no. 1 (January 2010).

United States v. Jeffrey Leon Battle, Patrice Lumumba Ford, Ahmed Ibrahim Bilal, Habis Abdullah al Saoub, and October Martinique Lewis. Criminal No. 02-399HA, in the U.S. District Court for the District of Oregon, October 3, 2002. Accessed August 21, 2010. www.justice.gov/ag/100402indictment.pdf.

United States v. Kevin James, Levar Washington, Gregory Patterson, and Hammad Samana. Criminal No. 05-CR-214, in the U.S. District Court for the Central District of California, August 31, 2005. Accessed July 23, 2010. http://nefafoundation.org/file/FeaturedDocs/U.S._v_James_Indictment.pdf.

United States v. Adam Gadahn. Criminal No. CR 05-254A, in the U.S. District Court for the Central District of California, October 11, 2006. Accessed August 30, 2010. http://nefafoundation.org/file/FeaturedDocs/U.S._v_Gadahn_Indictment.pdf.

United States v. Ronald Allen Grecula. Criminal Complaint No. H-05-453M, in the U.S. District Court for the Southern District of Texas, May 21, 2005. Accessed October 29, 2010. http://nefafoundation.org/file/FeaturedDocs/US_v_Grecula_Complaint.pdf.

United States v. Najibullah Zazi. Criminal Complaint No. 09-MJ-03001, in the U.S. District of Court for the District of Colorado, September 19, 2009. Accessed August 30, 2010. http://nefafoundation.org/file/FeaturedDocs/US_v_NajibullahZazi_complaint.pdf

United States v. Najibullah Zazi. No. 09-CR663 (RJD), Memorandum of Law in Support of Government's Motion for a Permanent Order of Detention, in the U.S. District Court for the Eastern District of New York, September 24, 2009. Accessed August 30, 2010. http://nefafoundation.org/file/FeaturedDocs/US_v_NajibullahZazi_detentionmemo.pdf.

United States v. Hosam Maher Husein Smadi. Criminal Complaint No. 3-09-MJ-286, in the U.S. District Court for the Northern District of Texas, September 24, 2009. Accessed October 20, 2010. http://nefafoundation.org/file/FeaturedDocs/US_v_Smadi_complaint.pdf.

_____. Case No. 3-09-MJ-286, Government Exhibit 277, in the U.S. District Court for the Northern District of Texas. Accessed October 20, 2010. http://www.txnd.uscourts.gov/judges/smadi/277.pdf.

_____. Case No. 3-09-MJ-286, Government Exhibit 240, in the U.S. District Court for the Northern District of Texas. Accessed October 20, 2010. http://www.txnd.uscourts.gov/judges/smadi/240.pdf.

United States v. Mohammed Zaki Amawi, Marwan Othman El-Hindi, and Wassim I. Mazloum. Case No. 3:06CR719, Sentencing Memorandum, in the U.S. District Court for the Northern District of Ohio Western Division, October 5, 2009. Accessed October 12, 2010. http://www.investigativeproject.org/documents/case_docs/1100.pdf.

_____. Case No. 3:06CR719, Indictment, February 16, 2006. Accessed October 12, 2010. http://www.investigativeproject.org/documents/case_docs/93.pdf.

United States v. Syed Haris Ahmed. Criminal Indictment No. 1:06-CR-147-CC, in the U.S. District Court for the Northern District of Georgia, December 9, 2008. Accessed September 19, 2010. http://nefafoundation.org/file/FeaturedDocs/US_v_SyedHarisAhmed_2ndSpcInd.pdf.

United States v. Ehsanul Islam Sadequee. No. M-06-335, Affidavit in Support of Arrest Warrant, in the U.S. District Court of the Eastern District of New York, May 28, 2006. Accessed September 19, 2010. http://nefafoundation.org/file/FeaturedDocs/U.S._v_Sadequee_FBIAffidavit.pdf.

United States v. Syed Haris Ahmed and Ehsanul Islam Sadequee. No. 1:06-cv-0147-WSD, in the U.S. District Court for the Northern District of Georgia, June 1, 2009. Accessed September 19, 2010. http://nefafoundation.org/file/US_v_HarisAhmed_ekdaubert.pdf.

United States v. Colleen R. LaRose. Criminal No. 10-Cr-123, in the U.S. District Court for the Eastern District of Pennsylvania, March 4, 2010. Accessed November 1, 2010. http://www.investigativeproject.org/documents/case_docs/1196.pdf.

University of Arizona. "Dark Web Terrorism Research." Accessed April 26, 2010. http://ai.arizona.edu/research/terror/.

U.S. House Permanent Select Committee on Intelligence. "al-Qaeda: The Many Faces of an Islamist Extremist Threat." Washington DC: GPO, 2006.

Wathen, C. Nadine and Jacquelyn Burkell. "Believe it or Not: Factors Influencing Credibility on the Web." *Journal of the American Society for Information Science and Technology*, vol. 53, no. 2 (2002).

Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges* Washington DC: United States Institute of Peace, 2006.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Erik J. Dahl
   Naval Postgraduate School
   Monterey, California

4. Sean F. Everton
   Naval Postgraduate School
   Monterey, California