Law Enforcement Intelligence: Implications for Self-Radicalized Terrorism

Jeremy G. Carter, Ph.D.[1]
Indiana University – Purdue University Indianapolis

David L. Carter, Ph.D.
Michigan State University

Abstract

A series of tragic events over the last three years has further strengthened the emerging preventative and proactive philosophies adopted by U.S. law enforcement post-September 11, 2001. Law enforcement and the American public now have a heightened awareness of homegrown terrorism. While these terrorist actors operate independent of traditional terrorist networks and groups, they are often influenced by such groups throughout a process where they enter as a non-violent individual and exit as a violent "true believer". Efforts by law enforcement to mitigate or prevent such threats rely on the implementation of intelligence-led policing practices. Central to these practices is the input of raw information into the intelligence cycle. This article will discuss the importance and application of suspicious activity reporting as it impacts law enforcement intelligence practices to prevent threats from self-radicalized terrorism.

Keywords: Self-radicalized terrorism; Suspicious activity reporting; Law enforcement intelligence, Intelligence-Led Policing, Law Enforcement Partnerships

Carter, J. G. & Carter, D. L. (2012). Law enforcement intelligence: Implications for self-radicalized terrorism, *Police Practice and Research*, 13(2), 138-154.

[1] Author Correspondence: 801 W. Michigan Street, Indianapolis, IN 46202, P: (317) 274-4170, carterjg@iupui.edu

Law Enforcement Intelligence: Implications for Self-Radicalized Terrorism

"S*ince the profile of a would-be terrorist is becoming less and less obvious…In that kind of fog, small behaviors necessarily loom large*" – Amanda Ripley, Time Magazine, 2007

Introduction

The terrorist acts of September 11, 2001 demonstrated an evolution[2] of tactics utilized by violent criminal extremists to kill, cause damage and instill fear. Consistent with this evolution of tactics are changes in the practices and policies guiding the prevention of such attacks. The United States is now facing another incarnation[3] of terrorist behavior – the increased prevalence of the "self-radicalized" terrorist who is "home grown" and may be a "lone wolf".

Because of these changes in the threat environment, the practices and policies necessary for prevention must change to reflect the threats. The *Nationwide Suspicious Activity Reporting Initiative* (NSI) emphasizes the input of raw information in the form of observable human behavior into the law enforcement intelligence cycle as critical to law enforcement's counter-terrorism efforts. This raw information is known as "Suspicious Activity Reports (SARs)" and the vehicle by which SARs reach the intelligence cycle is law enforcement's partnerships with the community. This article will briefly discuss law enforcement intelligence practices, SARs, and community partnerships and how they relate to the prevention of homegrown terrorism. The discussion will be supplemented with case studies of the Fort Dix, New Jersey plot and the Fort Hood, Texas attack.

[2] The 9/11 attacks on the World Trade Center and Pentagon demonstrated the detailed and comprehensive planning of modern terrorist groups as well as their patience and willingness to invest in methods of attacks that have not been utilized in the past.

[3] Terrorist methods have evolved consistently with counter-measures. Historically speaking, terrorist groups would often utilize a variety of bombing methods to instill damage and fear. While this approach is still prevalent – especially at the international level - groups and bombings have given way in the U.S. to individual actors who utilize any available means to cause violence and terror.

Self-Radicalization of Terrorists and Criminal Extremists

The National Strategy for Information Sharing posits that “…there is increasing concern regarding the potential threat posed by homegrown terrorists. While lacking formal ties to al-Qaida, these disaffected, radicalized, violent extremists often draw inspiration from al-Qaida and other global terrorist organizations” (WH, 2007:17). The significance of lone-wolf terrorism was felt by the U.S. prior to 9/11. Timothy McVeigh’s 1995 attack on the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma; Eric Rudolph’s bombing at the 1996 Olympic Games in Atlanta, Georgia; and Theodore "Ted" Kaczynski’s – the “Unabomber” – attacks on airlines, universities and other targets across the country from the late 1970s to the mid 1990s serve as prominent examples. Post 9/11, the presence of lone-wolf terrorism has come in various forms. However, in a one-year period in 2009-2010, the pace of lone wolf actions, representing a diverse array of extremist beliefs, increased significantly with several lone wolf attacks or attempts. This significant trend includes,

- May 31, 2009: Right-to-life extremist Scott Roeder, who had a record of right-wing extremist activity and threats against abortion clinics, killed Dr. George Tiller, a Wichita, Kansas physician who performed controversial late-term abortions, for the stated purpose of stopping the physician from performing more abortions.
- June 3, 2009: Self-radicalized Muslim convert Abdulhakim Mujahid Muhammad killed a 23-year-old Army private outside of a Little Rock, Arkansas Army recruiting office, telling investigators he wanted to kill as many members of the U.S. military as he could because he was mad at the military for past actions against Muslims.

- June 9, 2009: Avowed white supremacist and Holocaust-denier James Von Brunn opened fire inside the United States Holocaust Memorial Museum in Washington, killing a security guard who stopped him in the entrance.
- November 5, 2009: Major Nidal Hasan, an Army psychiatrist who had become a self-radicalized Muslim extremist and who had communicated with known terrorist Anwar al-Awlaki, killed twelve people in a shooting attack at Fort Hood, Texas.
- December 25, 2009: Umar Farouk Abdul Mutallab attempted to detonate a bomb on Northwest Airlines flight 253 from Amsterdam, Netherlands as it prepared to land in Detroit, Michigan.
- March 4, 2010: John Patrick Bedell, an anti-government extremist, committed a shooting attack at the Pentagon where he wounded two security guards before being killed.
- May 1, 2010: Faisal Shahzad's attempt to kill hundreds in New York City by leaving a large homemade bomb, that included large amounts of shrapnel, in the back of an SUV parked in the middle of Times Square[4].
- May 20, 2010: Two West Memphis, Arkansas police officers were killed and two Crittenden County, Arkansas Sheriff's Department deputies were wounded by Jerry Kane and his 16-year old son Joseph, both of whom had been involved in anti-government activity.

This list of incidents suggests that self-radicalized lone-wolf attacks are the criminal extremists' methodology of choice.

[4] Shahzad's attempt to detonate the bomb in Times Square was prevented due to a tip from a community member to a local NYPD police officer.

Radicalization is the socialization process of developing political, religious, environmental, economic or other ideological attitudes, values, and beliefs leading to a narrow vision of the ideology that is represented by only a small number of believers who may be characterized as being revolutionary or militant. Hence, the radicalization process develops an individual as an extremist. As an individual is exposed to more of the extremist ideological literature, the process reinforces the beliefs, much like circular logic. It is fundamentally a resocialization process where the individual's attitudes, values and beliefs are eventually transformed to be consistent with the ideology, often leading to violence and/or actions that are traitorous to the individual's previous life. In an ideological context, the person becomes a "true believer". The steps in the radicalization process can vary. Many experts (Silber & Bhatt, 2007; Gartenstein-Ross & Grossman, 2009) believe it involves four primary stages;

> (1) Pre-Radicalization: An individual's lifestyle prior to radicalization (relationships, environment, jobs, social life, etc.).
>
> (2) Self-Identification: An individual is influenced by internal and external factors attributing to the exploration of extreme philosophies, ideologies and values.
>
> (3) Indoctrination: An individual intensifies their beliefs and adopts extreme philosophies, ideologies and values with no exceptions.
>
> (4) Soldier: An individual accepts their duty to participate in the struggle as a warrior fighting those who oppose the ideology in an attempt for the ideology to achieve realization.

Others believe it involves "mentorship" as a key motivator to influence beliefs and actions, referred to as mentorship (Whitelaw, 2009; Sageman, 2004). Under this theory, the individual proactively researches and consumes information that shapes the radicalization process, however, the person's ideological direction is influenced by a mentor who reinforces the belief system. The mentor only provides ideological support, not financial or logistical support. Because the self-radicalized individual typically has no support network, any criminal actions they commit which are intended to support or further the extremist ideology are typically planned and executed solely by that individual – this is characterized as a lone-wolf act.

Regardless of the process by which an individual transforms from a non-risk to a violent risk, opportunities exist that lend themselves to law enforcement collecting information that supports intelligence processes. The progression from stage to stage of self-radicalization requires active exposure to extreme ideologies that are often identifiable in public places – ranging from public statements to extremists blogs. It is these outward behavioral signs of self-radicalization that become important for Suspicious Activity Reporting.

Law Enforcement Intelligence Practices

A Brief Foundation

The emerging law enforcement philosophy for preventing or mitigating transjurisdictional criminal and terrorist risks is intelligence-led policing (ILP). Fundamentally, the intelligence process is designed to identify criminal threats and develop operational responses to eliminate the threats. ILP integrates these processes with other police responsibilities such as handling calls for service and criminal investigations. While there are many dimensions of ILP, due to space considerations only a contextual discussion of the concept will be provided here.[5] ILP can be defined as:

[5] A detailed discussion of ILP can be found in Carter, 2009.

> “The collection and analysis of information related to crime and conditions that contribute to crime, resulting in an actionable intelligence product intended to aid law enforcement in developing tactical responses to threats and/or strategic planning related to emerging or changing threats (Carter & Carter, 2009:317).”

In short, ILP is the business model of policing which relies upon the analysis of raw information to guide decision making that will ultimately influence the actions taken by law enforcement agencies (Ratcliffe, 2008). The process of how ILP is applied varies across law enforcement agencies depending upon geographic responsibility, population, agency size, resources, and other jurisdictional variables. Regardless of the specific model, at the heart of ILP is an information management process that embodies the “intelligence cycle”.

This cycle is comprised of six steps: (1) Planning and Direction, (2) Collection, (3) Processing and Collation, (4) Analysis, (5) Dissemination, and lastly (6) Re-evaluation (Global Intelligence Working Group [GIWG], 2003). These six components depict the methodology by which law enforcement assesses and analyzes raw information that is developed into analytic products. These products inform police leaders on variables related to threats which, in turn, aids them in developing prevention strategies. Interwoven within these steps are a variety of informal and formal partnerships for two-way communication between law enforcement and citizens; policies guiding ethical police behavior and the protection of civil liberties; channels for raw information to be routed to the intelligence cycle; and methods of critical thinking to provide the analysis of raw information. Figure 1 provides a comprehensive diagram of the intelligence cycle illustrating these processes.

_ _ _ _ _ _ _ _ _

Figure 1 about here
_ _ _ _ _ _ _ _ _

Inherent in the intelligence cycle is giving clarity to suspected threats and the discovery of previously unknown threats. Threats may well exist in a community about which law enforcement has no information. Therefore, a method must be in place to solicit, collect, assess, integrate and analyze these diverse data. Having a broad-based, threat-driven information collection protocol is the only way law enforcement may be able to identify and understand threats within a community. The need for this diverse information from citizens is why Suspicious Activity Reporting has become a critical component for threat management.

Suspicious Activity Reporting (SAR)

Law enforcement's utilization of non-traditional sources of information to combat terrorism has been documented as a key resource for successful threat prevention (Riley, *et al*, 2005). Suspicious activity reporting is a formalized process to *document* and *share* observed behaviors which are indicative of criminal activity. Information – including "tips and leads" – may come from law enforcement personnel, private sector partners or citizens. This information is placed in written form and processed through the law enforcement agency, including verifying facts and confirming if the suspicious behavior has a criminal nexus, in order to have the SAR integrated into the analytic process of the intelligence cycle.

There are three types of Suspicious Activity Reports. The first is the *financial SAR*. This was mandated by the Bank Secrecy Act (1970) wherein financial institutions must report certain types of transactions to the Treasury Department. The suspicious activity most commonly associated with financial SARs is money laundering or trafficking in unlawful commodities.[6] The second is the *all crimes SAR*. This is

[6] The financial SAR deals specifically with financial transactions where financial institutions must report large cash transactions as suspicious activity. For more information about the financial SAR see http://www.fincen.gov/reg_sar.html.

simply the documentation and reporting of suspicious activity related to any crime. The activity may be observed by a law enforcement officer or reported to an officer. This is similar to what many law enforcement agencies have used traditionally known by various names such as a Field Intelligence Report, Field Interview Report or Miscellaneous Investigation Report.

The third type is the Information Sharing Environment-Suspicious Activity Report (ISE-SAR). This is the documentation of suspicious behavior specifically related to terrorism or crimes that support or facilitate terrorist planning and acts. The reason for having a distinct SAR for terrorism is based on statutory provisions emanating from the *Intelligence Reform and Terrorism Prevention Act of 2004*. At a law enforcement agency, the form and processes for line officers are typically the same for both the "all crimes" SARs and ISE-SARs. However, when the SAR is processed through the intelligence unit or fusion center[7], the ISE-SAR is processed differently and shared much more widely. The reason for the different processing is based on the responsibility of the ISE to deal only with terrorism and crimes supporting terrorism. It is this type of SAR that holds most important promise for identifying self-radicalized terrorists.

An important caveat for the fundamental implementation of SAR processes is the commitment to protect citizen's privacy, civil rights, and civil liberties. The Program Manager's Office for the-Information Sharing Environment (PM-ISE) and its federal partners examined potential privacy and civil liberties risks associated with SARs and consulted privacy and civil liberties advocacy groups to identify effective mitigation strategies. As a result, explicit types of suspicious activities have been identified which are based on past cases that reasonably indicate the planning of a terrorism incident. These actions are documented in the *ISE-SAR Functional Standard* (Program Manager's Information Sharing Environment [ISE], 2008). By focusing on observed behavior, this standard mitigates the risk of profiling based on race, ethnicity, national

[7] For more information on law enforcement fusion centers, refer to Chapter 8 of the Carter, D. L. 2009 reference.

origin, or religion. It also improves mission effectiveness by enabling agencies to focus on and address potential threats in a more efficient and standardized manner (ISE, 2008).

Partnerships for Law Enforcement Intelligence

While important knowledge that may forewarn of a future attack may be derived from information reported by patrol officers in the course of routine law enforcement and other activities (White House [WH], 2007), the current discussion focuses on the importance of developing community and private sector partnerships to increase the awareness of suspicious behavior within communities. Moreover, based on lessons learned from community policing, that agencies engaged in a SAR program must educate their partners and community members on the purpose of the program, the types of information that is needed and why they should participate in the program (ISE, 2010b). Simply stated, law enforcement seeks the assistance of community members and the private sector to report suspicious behavior because this significantly increases the probability of criminally-related suspicious actively being observed. To be effective, however, community members and private partners must be informed about identifying suspicious behavior that has a criminal nexus.

The promise ILP has demonstrated, especially the heavily emphasized analytic component (McGarrell *et al*., 2007), to combat terrorism is not complete without access to raw information to be input into the intelligence cycle. Partnerships forged between law enforcement agencies and their communities serve as the vehicle by which critical raw information enters this cycle. The value of developing partnerships for two-way information flow has been reaffirmed continuously within federal reports and recommendations (International Association of Chiefs of

Police [IACP], 2004; GIWG, 2005; GIWG, 2008; ISE, 2010a). This approach has been recognized by both the Department of Justice and the Department of Homeland Security as an effective counter-terrorism strategy. In response to the 2005 London bombings, the United Kingdom developed an initiative referred to as "neighborhood policing" where police officers gained the trust of community members in order to establish an information exchange dialogue (Innes, 2006). Furthermore, in efforts to combat terrorism, Australia has adopted this partnership approach with private sector entities at airports (Wheeler, 2005) and within community businesses – referred to as "networked policing" (Palmer & Whelan, 2006). Similarly, both the Israeli Police and the Turkish National Police have developed "community partnership" programs to gain information from community members about terrorism-related suspicious activity (Carter, 2009). Despite the diverse environments of those initiatives, they have all been met with demonstrable successes.

In a February 2010 Homeland Security Advisory Council (HSAC) meeting, Department of Homeland Security Secretary Janet Napolitano tasked the HSAC to "…work with state and local law enforcement as well as relevant community groups to develop…and provide recommendations regarding how the Department can better support community-based efforts to combat violent extremism domestically" (Homeland Security Advisory Council [HSAC], 2010:2). In response, the HSAC identified multiple such partnerships where law enforcement and the community were successfully engaging in counter-terrorism/extremist information:

- *Los Angeles, California*
  Law enforcement joins communities and government agencies to improve quality of life issues and reduce violent crime.

- *Austin, Texas*

Law enforcement works with community on rapid response teams to mitigate tough issues and work in partnership to reduce violent crime.

- *Las Vegas, Nevada*
  Grassroots community effort led by faith based organizations that assist in reducing violent crimes and gangs.

- *Dearborn, Michigan*
  Collaborative effort to engage the community in the identification and resolution of community issues to include combating violent crime.

- *State of Maryland*
  Established an executive level coordinating office within the Governor's Office to work with community groups, ethnic groups, and-faith based organizations to address quality of life and other issues of concern.

- *State of Ohio*
  Established a community engagement office which built a collaborative and cooperative relationship with the communities based on trust and mutual respect.

- *Minneapolis, Minnesota*
  Designated crime professional specialists who are liaisons between the community and local law enforcement and have safety centers that are funded by the neighborhoods (HSAC, 2010:7).

Moreover, in July 2010 DHS Secretary Napolitano announced the launch of “See Something, Say Something” program to anchor a new national information-sharing partnership with Amtrak as part of the *Nationwide Suspicious Activity Reporting (SAR)* initiative. This national program utilizes public education materials, advertisements and other outreach tools to engage and educate travelers, businesses, community organizations, and public and private sector employees to identify suspicious behavior on railway systems (Department of Homeland Security [DHS], 2010). These examples of partnerships forged with the community serve as illustrations of the unique approach law enforcement is taking with community members and organizations in efforts to promote two-way communication flow. As mentioned, these partnerships are the essential foundation needed to channel raw information related to suspicious behavior to law enforcement agencies.

Law enforcement Intelligence: Determination and Prevention

The mission of law enforcement intelligence is to prevent or mitigate crimes/threats/attacks from reaching fruition. This mission requires, or assumes, certain knowledge to be available to law enforcement – such as information on the criminal actors along with their motives, methods and targets. Without this information the probability of law enforcement successfully preventing crimes and terrorism diminishes. This is the importance of gaining raw information in the form of SARs to serve as the "bridge" between intelligence gaps.[8] These vital pieces of information, that may seem irrelevant at the time of the report, may be the missing piece necessary to "complete the puzzle" about the presence and nature of a terrorism threat.

Fundamental to this discussion is that the prevention of crime and terrorism is a process based upon a set of operational assumptions. This process requires a commitment to a philosophy of practice that emphasizes proactive operations even though most law enforcement activities are reactive in nature. Ratcliffe (In Press) sums up the operational assumptions – illustrated in Figure 2 – which law enforcement must recognize when determining threats and identifying ways to mitigate or prevent threats from reaching fruition. Simply put, in order to prevent crime or terrorism it is operationally assumed that law enforcement must be proactive – such as training community members on the types of suspicious activity to look for and report. Moreover, in order for law enforcement to be proactive they must rely on a certain degree of

[8] As a matter of nomenclature, an "intelligence gap" is information law enforcement does not possess about the existence, nature and/or viability of a threat. An "intelligence requirement" is information that is identified and proactively collected to "fill the gaps".

predictability of criminal and terrorist actions. In the case of SARs, we rely on the predictability of known criminal “indicators” that law enforcement, in turn, informs community members to be aware of. Lastly, for actions to be predictable, a *pattern* of these actions must be identifiable (Ratcliffe, In Press). In the SARs example, law enforcement looks for the series of indicators representing a pattern of behavior that can be compared with other reported suspicious activity not only within the jurisdiction but also regionally and nationally.

– – – – – – – – –

Figure 2 about here

– – – – – – – – –

Coupled with these operational assumptions is a scale of opportunity and time that has implications for risk identification and thus prevention. Opportunity and time play different roles in street crimes than in complex (or enterprise[9]) crimes and pertains differently to terrorism as well. Street crimes, such as robbery and sexual assault, rely upon little planning and time to carry out the criminal act. Offenders of street crimes rely more heavily on an opportunistic target, hence there is little preparation time and few criminal instruments needed to commit the crime. Complex criminality, such as terrorism or white-collar crime, require more planning before the criminal act occurs. For example, identifying channels through which money can be laundered and the processes of laundering the money through these channels is time consuming. Moreover, the targets available for complex criminality are far more limited than those of street crimes – it is more difficult to skim money from a brokerage house than to rob a liquor store.

[9] The FBI defines a criminal enterprise as a group of individuals with an identified hierarchy, or comparable structure, engaged in significant criminal activity that often engage in multiple criminal activities and have extensive supporting networks (Federal Bureau of Investigation [FBI], 2010).

Terrorism, both acts by lone wolfs and networks alike, require significant planning prior to an attack. Examples abound, such as the sophistication and logistics of the 9/11 attacks on the United States, the complexity of four significant and deadly attacks in Istanbul, Turkey in November 2003 by the Turkish al-Qaida, and the detailed planning of the July 7, 2005 coordinated bombings in London, England. All three of these incidents had multiple coordinated attacks which required significant logistics, preparation and people to make the attacks a reality. The time and planning required for these attacks was significant because "suitable" targets had to be identified and reconnoitered in consideration of the targets' accessibility, security, and physical and emotional impact. Just as terrorism requires preparation time and logistical planning, street crimes are just the opposite – often little planning and the victim is frequently only a target of opportunity. In consideration of these factors, when balanced against the ability of law enforcement to intervene and stop the incident, considerations for crime and terrorism threat control have two intervening factors: As the time and complexity required to plan a criminal act increases, 1) there will be more information (and indicators) that will likely be observed and reported to law enforcement and 2) the greater the likelihood that law enforcement will be able to intervene in the incident's planning and execution. Figure 3 illustrates the prevention relationship between terrorism/crime opportunity and time.

Perspective

The discussion thus far has identified both an emerging threat paradigm – self-radicalized, home-grown criminal extremists – and a process to manage the threat. The process is Intelligence Led Policing that relies on the use of Suspicious Activity Reporting from the community and private sector to provide law enforcement with raw information about behaviors that likely have a criminal nexus. The application of these factors will be illustrated in two brief case studies: The attempted attack on Fort Dix, New Jersey and the Fort Hood, Texas attack.

– – – – – – – – –

Figure 3 about here

– – – – – – – – –

Case Study: Fort Dix, New Jersey

On the evening of May 7, 2007, six men described as homegrown “Islamic militants” (DHS, 2007; New York Police Department [NYPD], 2007) with no apparent connection to international terrorist networks were arrested for conspiring to attack U.S. armed forces personnel at Fort Dix, NJ. These men had planned to attack the base armed with a variety of firearms in an attempt to kill as many soldiers as possible (NYPD, 2007). Of the six individuals involved in the Fort Dix terrorist plot, three were brothers. Dritan "Anthony" or "Tony" Duka; Shain Duka; and Eljvir "Elvis" Duka, undocumented aliens from the former Yugoslavia, had been living illegally in the U.S. for more than 23 years and were accepted as Americans by neighbors and friends who had no idea they would scheme to attack a military base (Anastasia, 2007). The Duka brothers entered the United States near Brownsville, Texas, in 1984 when they crossed the border from Mexico (FOX News, 2009). The brothers had no criminal record, however reports indicate the three accumulated 19 traffic citations, but because they operated in "sanctuary cities," where law enforcement does not routinely report undocumented immigrants to homeland security, none of the tickets raised red flags (DHS, 2007). The three brothers operated a roofing business together.

The brothers conspired with three other suspects in the plot - Mohamad Ibrahim Shnewer from Jordan; Serdar Tatar from Turkey; and, Agron Abdullahu from the former Yugoslavia. Shnewer was a legal U.S. citizen and worked as a taxi cab driver, a construction laborer, and also at his family's supermarket. Tatar was in the U.S. legally with a green card and worked as an assistant manager at a 7-11 store in Philadelphia and delivered pizzas for his family's pizzeria (Stansbury, 2007). Abdullahu was also in the U.S. legally with a green card and worked as a baker in a supermarket (USA Today, 2008). Five were charged with conspiracy to kill U.S. military personnel while Abdullahu was charged with aiding and abetting illegal immigrants in obtaining weapons. The weapons were reportedly Abdullahu's personnel weapons and included a SKS Semi-Automatic Rifle, a Beretta Storm Semi-Automatic Rifle, a Mossberg 12-gauge Pump Shotgun and a Beretta 9 millimeter handgun (Stansbury, 2007).

During November 2006, the six suspects began planning the attack in more detail. Tatar's parents owned a pizzeria near Fort Dix where Tatar stated he had made deliveries to the base multiple times. Beyond the normal deliveries, Tatar mentioned that he noticed an increase in business during times when large numbers of troop were stationed on the base on temporary duty or prior to going overseas. Due to the number of deliveries Tatar's family pizzeria made to Fort Dix, the pizzeria possessed a detailed map of Fort Dix labeled "Cantonment Area Fort Dix, NJ" – a map that Tatar took from the pizzeria and provided to the group for planning.

The plot to attack Fort Dix was prevented through a citizen tip. Specifically, in January 2006 the Duka brothers went to a local Circuit City store in Cherry Hill, NJ to get an 8-mm video converted into a DVD (Stansbury, 2007). They were greeted by store clerk Brian Morgenstern who later called the police after becoming troubled by what he saw on the video - 10 long-bearded men of Middle Eastern descent shooting weapons at a firing range and calling for jihad

(Inskeep, 2008). The police arrived at Circuit City, watched the video with Morgenstern and determined the video was suspicious enough to call the County Counter Terrorism Coordinator who then contacted the local FBI field office. That same afternoon the Duka brothers returned to pick up their copied video without incident – the FBI received their copy of the video a week later. Despite this video, authorities maintain there was no direct evidence connecting the men to any international terror organizations such as al-Qaeda (Russakoff & Eggen, 2007).

The tip from Morgenstern led to an investigation that included infiltration by a cooperating witness - Mahmoud Omar, a legal immigrant from Egypt. Omar's history included a 2001 conviction for bank fraud and a 2004 arrest for a fight with a neighbor. In 2006 the FBI recruited him to infiltrate this group. The group often watched terror training videos, clips featuring Usama bin Laden, a tape containing the last will and testament of some of the Sept. 11 hijackers, and tapes of armed attacks on U.S. military personnel (DHS, 2007). The men trained by playing paintball in the woods in New Jersey and taking target practice at a firing range in Pennsylvania's Pocono Mountains where they had rented a house (Mulvihill, 2008).

In addition to plotting the attack on Fort Dix, the defendants spoke of assaulting a Navy installation in Philadelphia during the annual Army-Navy football game and conducted surveillance at other military installations in the region. The group also considered targeting Dover Air Base in Delaware, Fort Monmouth in NJ, the Coast Guard Building in Philadelphia as well as the Philadelphia Federal Building (NEFA, 2010). The individuals involved in the terror plot were arrested when attempting to purchase AK-47 assault weapons, M-16s and other weapons from an FBI informant. It remains unclear when the attack was to take place.

Fort Dix Implications for Law Enforcement Intelligence and Risk Prevention

The Fort Dix case provides an excellent illustration of law enforcement intelligence practices in the prevention of self-radicalized terrorism. The initial awareness of the attack came from an alert citizen working at Circuit City (Morgenstern) who witnessed suspicious behavior on the videotape. The existence of this al-Qaeda training video and other terrorism literature in the suspects' possession demonstrate the "Self-Identification" stage of the radicalization process wherein the individuals began exploring and learning this extreme philosophy and applied it in the form of training and planning for an attack on a U.S. military base. This step in radicalization of the six Fort Dix suspects, which has been specifically endorsed by terrorist experts (Emerson, 2010), serves as a point of opportunity for law enforcement to learn of potential attacks through successful partnerships with non-law enforcement entities. This SAR from Circuit City's Morgenstern is one that came as a result of community partnerships in which community members were educated and aware of such suspicious activity and to inform the police if such suspicious activity was observed. The importance of such partnerships for raw information collection to combat terrorism has been well documented (Jenkins, 2010; ISE, 2010a; IACP, 2004).

This information was then relayed to a local police department and then was turned over to the County Counter Terrorism Coordinator who forwarded it to the FBI. The local field office then initiated the intelligence-led investigation that ultimately connected the information and prevented the attack. Not only was the initial suspicious activity report from Morgenstern critical, but the local police department did not stall on the information but rather forwarded it appropriately as envisioned by the ISE SAR processes. Local, state and federal agencies then shared information and follow-up investigation, intelligence collection, and analysis. The case also illustrates what the FBI describes as “pre-emptive prosecution.” This relied on an informant to infiltrate and provide information and then a pre-emptive arrest. Despite the success of this approach, it can result in a weaker case from a prosecution standpoint – an issue that has risen on several accounts as many reports argue the suspects had no intention of actually attacking Fort Dix (Piette, 2009).

As aforementioned, terrorism relies on long-term planning and the right opportunity. As a result of the time it took for the six suspects to review maps of the Fort Dix military base, collect numerous weapons, train with these weapons, and do strategic training with paintball guns, law enforcement agencies had time to gather information and develop strategic and tactical intelligence to prevent the attack on Fort Dix. Moreover, the suspects had multiple targets in mind at the outset of the planning stages. Based upon a variety of factors – mainly accessibility and potential casualties – the six suspects chose Fort Dix as the target for the attack since it provided the most ideal opportunity for their desired outcome.

Case Study: Fort Hood, Texas

On November 5, 2009, Nidal Malik Hasan concealed his FN Herstal 5.7x28mm pistol along with 13 extra ammunition magazines and went to the Soldier Readiness Center at Ft. Hood, Texas where hundreds of deploying soldiers were being given shots and eye examinations. Hasan jumped on a table and yelled “Alla Akbar!” (God is Great) in Arabic and began firing (CNN, 2009b). The result was 13 people dead and 31 injured. Hasan's attack ended when two base police officers shot and seriously wounded him. Born in the United States to Palestinian parents, Hasan graduated from Virginia Tech and joined the U.S. Army against his family's wishes (Sherwell & Spillius, 2009). The military paid for him to go to medical school and he became one of the few psychiatrists in the military when he was assigned to Ft. Hood (*Washington Post*, 2010). Hasan had asked about resigning his commission and began to doubt his military commitment, a situation thought to have worsened after he received orders to deploy to Afghanistan.

Hasan had met Anwar al-Awlaki, a radical Yemeni-American, while living in the Washington, DC area and later communicated with him via Internet[10]. Al-Awlaki had left the United States for Yemen after being investigated in connection with the 9/11 attacks[11]. On July 15, 2009, al-Awlaki had posted a message on his website urging the deaths of U.S. army personnel (Hsu, 2009). Three weeks later, Hasan purchased the weapon used on the November 5th attack at a Killeen, Texas gun store for $1,140 (Allen, 2009). Hasan criticized the wars in Iraq and Afghanistan. He called himself a Muslim first and an American second. He spoke at a seminar at Walter Reed Military Hospital in Washington in June 2007, making a presentation entitled "Why the War on Terror is a War on Islam." During his presentation he said, "It's getting harder…for Muslims…to morally justify being in a military that seems constantly engaged against fellow Muslims" (Friedman, 2009). He was reported to have "applauded the killing of a US soldier at an Arkansas recruiting center". Hasan is also believed to have had business cards

[10] Hasan's relationship with Al-Awlaki serves as an example of the "mentorship" role within the process of self-radicalization.

[11] al-Aulaqi has also been tied to Faisal Shahzad, the man who attempted to detonate a bomb in New York City's Times Square on May 1, 2010 (Huffington Post, 2010; Shane & Mekhennet, 2010).

which contained the abbreviation “SoA (SWT)” which means “Soldier of Allah,” and “Subhanahu Wa Ta’all,” - or Glory to God (Gibbs, 2009).

In December 2008 Hasan’s emails to al Aulaqi were discovered by the Joint Terrorist Task Force (JTTF) in San Diego. A report stated that the “content of those communications was consistent with research being conducted by Major Hasan in his position as a psychiatrist at… Walter Reed….and nothing else derogatory was found…. the JTTF concluded Hasan was not involved in terrorist activities or planning” (Marquise, 2010:22). This information was shared with members of the Washington JTTF. As a result of the consistencies between Hasan’s research at Walter Reed and the content of the email exchanges with al Aulaqi, the investigation was dismissed even despite allegations that his emails to al Aulaqi contained cryptic or coded communications explaining how to transfer money overseas so as to not attract the attention of law enforcement (Marquise, 2010). Based on all that is known, many have concluded that the Fort Hood attack was a terrorist attack against the U.S. military. Despite this, the FBI has said its investigation indicates that the alleged gunman acted alone and was not part of a broader terrorist plot (CNN, 2009a).

Fort Hood Implications for Law Enforcement Intelligence and Risk Prevention

The attack on Fort Hood is a tragic and frustrating reminder to the law enforcement community as to the “nature of the beast” when attempting to combat terrorism in the United States. As a harsh reality reminds us, despite the best efforts of dedicated law enforcement personnel, preventing every threat is simply beyond reach. As discussed previously, terrorism requires long-term planning and thus instances for law enforcement to identify suspicious behavior.

However, terrorism also has limited opportunities. When compared to other complex criminality, such as organized crime, terrorism does not provide law enforcement the ability to pattern certain behavior and methods as a result of a “one chance to strike” approach taken by terrorists. Terrorist methods may be similar; however they are not consistent enough for law enforcement to identify specific patterns of behaviors to implement prevention methods. Law enforcement must then rely upon lessons learned from incidents that do reach fruition in an effort to identify precursors to such events and develop mechanisms to get this information into the intelligence cycle.

Even from tragic events such as the Fort Hood shootings, there are lessons to be learned. In this case, future application of intelligence practices – specifically the identification of an individual’s behavior that may illicit further investigation as it challenges the boundaries of reasonable suspicion. Hasan’s behavior certainly warranted further investigation. His views on the U.S. military, his speech at Walter Reed hospital and his business cards identifying him as a “Soldier of Allah” were enough to meet the threshold of reasonable suspicion for an investigation. Further compounding the risk he posed were his access to Fort Hood and access to weapons.

Just as hindsight is 20/20, these facts seem obvious and yet the attack came to fruition. However, the information simply was not there to guide law enforcement decision making. Without the mechanisms in place to identify Hasan’s behavior as suspicious, there was no way for this raw information to be passed along to the necessary actors. Throughout the course of events leading to the attack, if the mechanisms had been in place to identify and report his behavior, these suspicious activities would have been reported at different times and each within its own context. Moreover, as each suspicious behavior makes its way into the intelligence cycle, the “pieces of the puzzle” begin to paint a picture of what may occur. As intelligence analysts continue to input files on Hasan, his behaviors begin to shed light on a series of events leading up to what could possibly be a lethal attack. Thus, if the events had been reported through partnerships with personnel at the hospital, personnel on Fort Hood’s military base and an conscious awareness among citizens of what behaviors are suspicious law enforcement would have had the information necessary to act and prevent the threat.

Conclusions

The Fort Dix and Fort Hood case examples provide real-world context to the application of law enforcement intelligence practices and, more specifically, suspicious activity reporting, as applied to the self-radicalized criminal extremist threat. Law enforcement’s ability to prevent criminal and terrorist risks relies on the availability of raw information that is often times outside the law enforcement purview. Preventing crimes and terrorism relies not so much on the highly sophisticated and technological tools available, but the simple, informal passing of information related to observed behavior that when taken in context of the totality of circumstances “simply doesn’t seem right”. State, local and tribal law enforcement agencies must continue their efforts to establish relationships with their communities, businesses and infrastructure entities to develop channels for raw information to get into the intelligence cycle.

The principles discussed here are not new to law enforcement. The foundation to develop communication channels with the community were instilled, by most US agencies, through community policing efforts (Carter & Carter, 2009). Once again it is importance to reiterate that even though SARs are a formal method of documenting behavior, the exchange of this information is highly informal and is seeded in trust and familiarity between law enforcement personnel and the communities they serve. Without raw information, there cannot be analysis. Without analysis, there cannot be pattern identification. Without pattern identification, there cannot be predictability. Without predictability, there cannot be prevention.

Figures

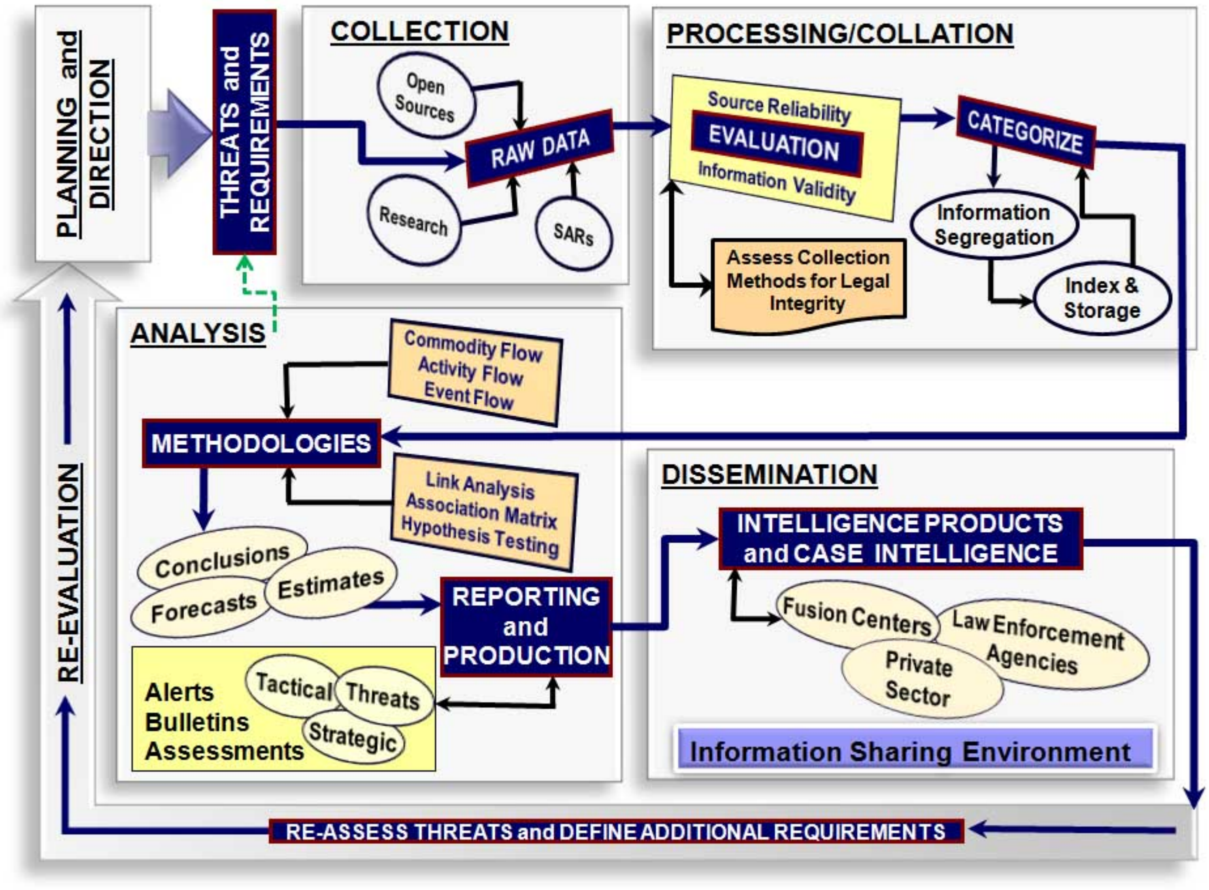

Figure 1. Detailed Law Enforcement Intelligence Cycle
Source: Taken from Carter (2009) with permission

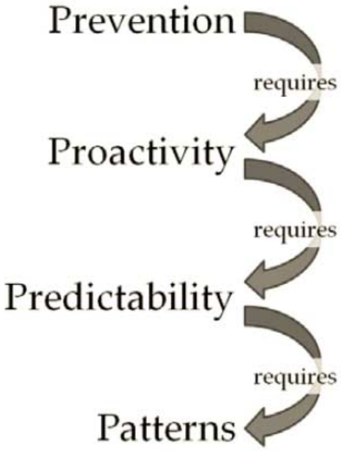

Figure 2. Operational Assumptions for Risk Prevention
Source: Taken from Ratcliffe (In Press) with permission

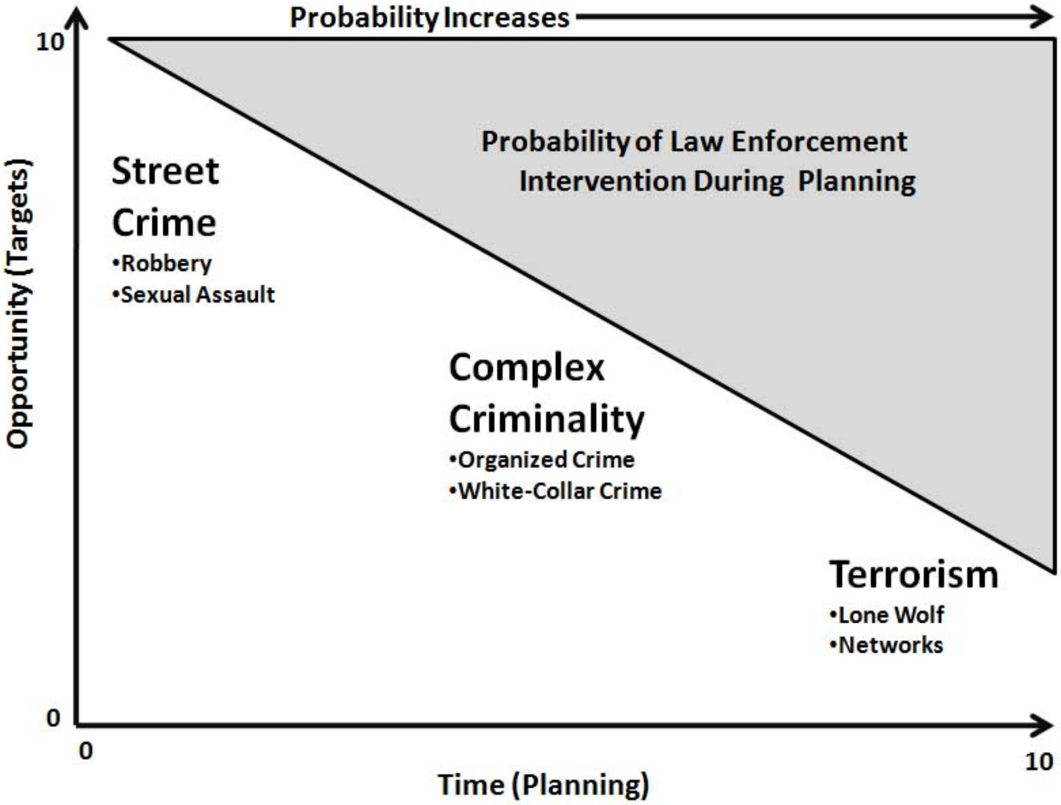

Figure 3. Planning and Opportunity for Crime and Terrorism

References

Allen, N. (2009). Fort Hood massacre: Barack Obama would have to sign death warrant. *Telegraph*. November 9. Retrieved from http://www.telegraph.co.uk/news/worldnews/northamerica/usa/barackobama/6531599/Fort-Hood-massacre-Barack-Obama-would-have-to-sign-death-warrant.html

Anastasia, G. (2007, May 13). Fort Dix 6: “good boys” or terrorists?. *The Seattle Times*. Retrieved from http://seattletimes.nwsource.com/html/nationworld/2003704914_dixprofiles13.html

Carter, D.L. (2009). *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies*. Second Edition. Washington, DC: Office of Community Oriented Policing Services.

Carter, D. L. & Carter, J. G. (2009). Intelligence Led Policing: Conceptual Considerations for Public Policy. *Criminal Justice Policy Review*, 20(3), 310-325.

CNN. (2009a, November 10). *Investigators look for missed signals in Fort Hood probe*. Retrieved from http://www.cnn.com/2009/CRIME/11/09/fort.hood.shootings/

CNN. (2009b, November 9). *Fort Hood soldier: I 'started doing what I was trained to do’*. Retrieved from http://www.cnn.com/2009/CRIME/11/09/fort.hood.foster/index.html

Department of Homeland Security [DHS]. (2010, July 1). *Secretary Napolitano Announces Rail Security Enhancements, Launches Expansion of “See Something, Say Something” Campaign*. Press Release. Retrieved from http://www.dhs.gov/ynews/releases/pr_1278023105905.shtm

Department of Homeland Security [DHS]. (2007). *Fort Dix Plot Illustrates Continuing Threat Posed by Homegrown Islamic Extremists*. Joint Homeland Security Assessment. Washington, DC.

Emerson, S. (2010). *Fort Dix Terror Plot*. Investigative Project on Terrorism. Retrieved from http://www.investigativeproject.org/379/fort-dix-islamist-terrorist-plot

Federal Bureau of Investigation [FBI]. (2010). *Organized Crime*. Retrieved from http://www.fbi.gov/hq/cid/orgcrime/glossary.htm

FOX News. (2009, April 29). *Fifth Man Convicted in Fort Dix Terror Plot Sentenced to 33 Years in Prison*. Associated Press. Retrieved from http://www.foxnews.com/story/0,2933,518337,00.html

Friedman, T. L. (2009, November 28). American v.s. The Narrative. *The New York Times*. Retrieved from http://www.nytimes.com/2009/11/29/opinion/29friedman.html

Gartsenstein-Ross, D. & Grossman, L. (2009). *Homegrown Terrorists in the U.S. and U.K. An Empirical Examination of the Radicalization Process*. Foundation for Defense of Democracies Press. Washington, DC.

Gibbs, N. (2009, November 11). The Fort Hood Killer: Terrified ... or Terrorist?. *History News Network*. Retrieved from http://hnn.us/roundup/entries/119883.html

Global Intelligence Working Group. (2003). *National Criminal Intelligence Sharing Plan*. Washington, DC: Global Justice Information Sharing Initiative. Retrieved from http://it.ojp.gov/documents/NCISP_Plan.pdf

Global Intelligence Working Group [GIWG]. (2005). *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: U.S. Department of Homeland Security. Retrieved from http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

Global Intelligence Working Group [GIWG]. (2008). *Baseline capabilities for state and major urban area fusion centers*. Washington, DC: U.S. Department of Homeland Security. Retrieved from http://it.ojp.gov/default.aspx?area=home&page=1224#cat_Intell

Homeland Security Advisory Council. (2010). *Countering Violent Extremist Working Group*. Spring.

Huffington Post. (2010, May 13). *Faisal Shahzad Had Contact with Anwar al Awlaki, Key Figure in Fort Hood, Christmas Day Attacks*. Retrieved from http://www.huffingtonpost.com/2010/05/06/faisal-shahzad-had-contac_n_566666.html

Hsu, S. S. (2009, November 18). Hasan's ties to radical cleric raise issues for law enforcement. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2009/11/17/AR2009111703830.html

Innes, M. (2006). Policing uncertainty: Countering terror through community intelligence and democratic policing. *The ANNALS of the American Academy of Political and Social Science*, 605, 222-241.

International Association of Chiefs of Police [IACP]. (2004). *National Policy Summit: Building Private Security / Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder*. Community Oriented Policing Services. Retrieved from http://www.theiacp.org/Portals/0/pdfs/Publications/ACFAB5D.pdf

Inskeep, S. (2008, October 20). *Opening Statements to Start in Fort Dix Plot*. National Public Radio. Retrieved from http://www.npr.org/templates/story/story.php?storyId=95891389

Jenkins, B. M. (2010). *Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001*. RAND Corporation.

Marquise, R. (2010). Fort Hood attack. *The Counterterrorist, Official Journal of the Homeland Security Professional*, 3(1), 20-28.

McGarrell, E. F., Freilich, J. D., & Chermak, S. (2007). Intelligence-led policing as a framework for responding to terrorism. *Journal of Contemporary Criminal Justice,* 23(2), 142-158.

Mulvihill, G. (2008, March 31). Man sentenced in Fort Dix plot case. *USA Today*. Retrieved from http://www.usatoday.com/news/nation/2008-03-31-619191134_x.htm

NEFA. (2010). *United States v. Shnewer et al. - Ft Dix trial*. The NEFA Foundation. Retrieved from http://www1.nefafoundation.org/ftdixdocs.html

New York Police Department [NYPD]. (2007). *Threat Analysis: Fort Dix, New Jersey Terror Plot*. NYPD Shield. Counter-Terrorism Bureau.

Palmer, D. & Whelan, C. (2006). Counter-terrorism across the policing continuum. *Police Practice and Research*, 7(5), 449–465.

Piette, J. (2009, May 10). Meeting exposes Fort Dix 5 frame-up. *Workers World*. Retrieved from http://www.workers.org/2009/us/fort_dix_5_0514/

Program Manager’s Information Sharing Environment [ISE]. (2010a). *Nationwide Suspicious Activity Reporting (SAR) Initiative*. Retrieved from http://www.ise.gov/pages/sar-initiative.aspx

Program Manager’s Information Sharing Environment [ISE]. (2010b). *Final Report: Information Sharing Environment (ISE) - Suspicious Activity Reporting (SAR) Evaluation Environment*. Retrieved from http://nsi.ncirc.gov/documents/NSI_EE.pdf

Program Manager's Information Sharing Environment [ISE]. (2008). *Information Sharing Environment Functional Standard for Suspicious Activity Reporting*. Retrieved from http://www.ise.gov/docs/ctiss/ISE-FS-00SARFunctionalStandardIssuanceVersion1.0.pdf

Ratcliffe, J. H. (In Press). Intelligence-led policing: Anticipating risk and influencing action. In M. B. Peterson, B. Morehouse and R. Wright (Eds.) *INTELLIGENCE 2010: Revising the Basic Elements*. International Association of Law Enforcement Intelligence Analysts.

Ratcliffe, J. H. (2008). Intelligence-Led Policing. Cullompton, UK: Willan.

Riley, K. J., Treverton, G. F., Wilson, J. M, & Davis, L. M. (2005). *State and Local Intelligence in the War on Terrorism*. Rand Corporation. Pittsburgh, PA.

Ripley, A. (2007, December 6). The Fort Dix Conspiracy. *Time Magazine*. Retrieved from http://www.time.com/time/nation/article/0,8599,1691609-2,00.html

Russakoff, D. & Eggen, D. (2007, May 9). Sic Charged in Plot to Attack Fort Dix. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/05/08/AR2007050800465.html

Sageman, M. (2004). *Understanding Terror Networks*. University of Pennsylvania Press. Philadelphia.

Shane, S. & Mekhennet, S. (2010, May 8). Imam's Path from Condemning Terror to Preaching Jihad. *The New York Times*. Retrieved from http://www.nytimes.com/2010/05/09/world/09awlaki.html

Sherwell, P. & Spillius, A. (2009, November 7). Fort Hood shooting: Texas army killer linked to September 11 terrorist. *Telegraph*. Retrieved from http://www.telegraph.co.uk/news/worldnews/northamerica/usa/6521758/Fort-Hood-shooting-Texas-army-killer-linked-to-September-11-terrorists.html

Silber, M. D. & Bhatt, A. (2007). *Radicalization in the West: The Homegrown Threat*. New York Police Department. Intelligence Division.

Stansbury, P. (2007). *98th Range Wing Antiterrorism Program*. Intelligence Threat Assessment. U.S. Air Force. Nellis, NV.

Washington Post. (2010, January 1). *Clues left by Fort Hood suspect raise haunting question: Should Army have seen it coming?* Retrieved from http://www.dallasnews.com/sharedcontent/dws/dn/latestnews/stories/010110dnmethasanclues.3f4b199.html

White House. (2007). *National Strategy for Information Sharing*. President George W. Bush. Retrieved from http://georgewbush-whitehouse.archives.gov/nsc/infosharing/NSIS_book.pdf

USA Today. (2008, March 31). *Man sentenced in Fort Dix plot case.* Associated Press. Retrieved from http://www.usatoday.com/news/nation/2008-03-31-619191134_x.htm

Wheeler, J. (2005). *An independent review of airport security and policing for the Government of Australia*. Canberra: Australian Government.

Whitelaw, K. (2009, December 16). *U.S. Ponders How To Stop Homegrown Terrorism*. National Public Radio. Retrieved from http://www.npr.org/templates/story/story.php?storyId=121510640