The Journal of Public and Professional Sociology

Volume 8 | Issue 1 Article 6

March 2016

Tracking Lone Wolf Terrorists

Rodger A. Bates
Clayton State University, rodgerbates@clayton.edu

Introduction

As a social construct, terrorism takes place within specific historical and social contexts (Schmid, 1992). Terrorism is a politically motivated form of premeditated violence perpetrated against noncombatant targets. As a complex phenomenon, numerous attempts have been made to differentiate terrorism based upon the kinds of goals pursued, the types of acts manifested, the motivations for these acts, the levels of organizational hierarchy encountered and the social and psychological profiles of participants (Bates, 2011, 2012).

Terrorism is associated with a structural environment characterized by an imbalance of power between different ideological groups (Black, 2004). In the tradition of the 19th century Russian anarchist group, the People's Will, it is propaganda by deed (White, 2014). Also, it is a tactic that morphs as terrorist groups evolve and change (Lesser, 1999). As a strategy and tactic, terrorism may include bombing, hijacking, arson, kidnapping, or hostage taking – all of which can be enhanced by force multipliers like transnational support, technology, media coverage and ideological and/or religious extremism (Jenkins, 1983). These force multipliers have contributed to the rise of terrorism as a major threat in the last half of the 20th and early 21st centuries.

Modern terrorism has taken many forms. It has been an important strategy in the wars of independence by many former colonies and emerging nations. The Chinese and Cuban revolutions, Vietnam War, and the many conflicts in South America, the Middle East, and Southwest Asia were marked by numerous acts of terrorism by all participants. Increasingly, world news is rife with reports of terrorist groups known by an escalating number of alphabet-challenging letters who use terrorism as a means to promote their causes, challenge their enemies and intimidate populations.

Terrorists can be differentiated in terms of their objectives and organizational structure. The U.S. Army (2007) describes terrorist groups as separatist, ethnocentric, nationalist and revolutionary. They also can be characterized in terms of organization and structure (Bates, 2011). Today, groups such as al Qaeda, ISIS (DAESH), Hamas, Hezbollah and other groups employ terrorism as a tactic. They deploy units or individuals to carry out directed or inspired attacks. As such, however, they are vulnerable to detection and interdiction. The intelligence and related agencies in the United States and abroad have increasingly been successful in identifying, tracking, and in a number of cases eliminating or significantly degrading these groups (Maras, 2013).

The extensive efforts to identify and track today's terrorists, however, have contributed to the growth of another form of terrorism which is much more difficult to identify, track and counter. Self-radicalized, lone wolf terrorists are the response by groups to promote and recruit individuals and motivate them to action while operating beyond the awareness and response of the increasingly more effective agents of counterterrorism (Bates, 2012).

The Lone Wolf Threat

The rise of lone wolf terrorism has created an increasing dilemma in today's security environment. With more effective counterterrorism practices, leaderless resistance has emerged as one of the most difficult forms of terrorism to anticipate and counter. Most recently, lone wolf terrorism has been associated with right-wing reactionaries and religiously radicalized Islamic jihadists (Bates, 2012).

Lone wolf terrorism involves self-radicalized individuals who commit violent acts to promote a cause or support a belief system. These acts, or propaganda by deeds, are extremely difficult to counter because they appear to be isolated and avoid many of the traditional organizational characteristics used to identify and track traditional terrorist groups. Though usually not capable of large-scale attacks, the modern lone wolf terrorist has access to a range of weapons with greater capacities for terror-inspiring events. However, the power of the lone wolf terrorist is not necessarily the actual level of harm potentially experienced, but the level of intimidation that the threat of such random acts of violence can exert on a community.

Today's media has played a major role in providing visibility so that others can be motivated and follow the lead of previous successful lone wolf attacks (Matusitz, 2015). Osama bin Laden, in the 2003 jihadist Internet forum "Sada Jihad," urged his followers to take action without waiting for instructions (Baker and deGraaf, 2010). Likewise, al Qaeda leader Abu Jihad al Masri promoted lone wolf terrorism in 'How to Fight Alone (Clemons, 2010). Recently, ISIS called upon its followers around the world to pick up a knife, gun or any weapon and become personal warriors for the cause (Love & Yan, 2014).

The research on lone wolf terrorism has dramatically increased in the past decade. In February 2010, both the director of the FBI and the director of the CIA stated that lone wolf terrorism was a major concern of their agencies (Sage, 2011). Typologies suggest that these terrorists may range from reactionary rightwing individuals, opponents of abortion, environmental or animal rights advocates, hate group members, or advocates of radical Islam like al Qaeda and ISIS.

In a single dimensional typology, Phillips and Pohl (2011) identify two-types of lone wolf terrorists: risk aversion and risk seeking. Looking at types of justification, Lisa Andrews (2001) identifies lone wolf terrorists in terms of moral justification, religious conviction, social change orientation, level of political antagonism, commitment to revenge, desire for attention, and importance of symbolism. In addition, Artiga (2011) suggests that lone wolves are trying to send a message or promote an ideological position, raise awareness for a cause, shape the political process, spread fear, defame a major social institution, or correct a major injustice. Others note that lone wolves may be motivated by ideological, social, psychological, monetary, threats, or greed.

Multidimensional typologies of lone wolf terrorists include White's (2012) Tactical Typology of Terrorism with its emphasis on the type of activity (criminal/political), the level of terrorist activity, and the form of response by control agents. Likewise, Pantucci's (2011) "A Typology of Lone Wolves: A Preliminary Analysis of Lone Islamist Terrorists" focuses on the means and contexts of self-radicalization, tactics of engagement, and the framework of available support. The loner, the lone wolf, the lone wolf pack and the lone attacker have been popular categories of Islamist terrorists. In addition, Bates' (2012) General Model of Lone Wolf Terrorism is a four dimensional (Rubik's Cube) perspective which looks at the influence of the extent of involvement in the radicalization process (self/group), type of motivation (altruistic/egoistic), form (chaos/career), and risk management (aversion/taking).

Identifying Lone Wolf Terrorists

These more complex perspectives have allowed scholars and security agencies to identify possible combinations of types and to better understand the social, psychological, and structural components that create environments conducive to the emergence of lone wolf terrorism. With over 60 U. S. cases prosecuted in 2015 and 900 investigations in all 50 states, we can better understand the level of threat as well as the backgrounds and characteristics of these terrorists (Bergen, 2016).

Identifying terrorists in general, and lone wolf terrorists in particular, is difficult. Almost fifty years ago Hacker (1976) and others attempted to profile terrorists. They suggested that terrorists were young, unmarried, middle class males with some university training and with an understanding or affinity for left-wing political philosophy, which was considered at the core of the terrorist actions of the day (Russell and Miller, 1983). However, these generalizations did not facilitate any useful strategies of identification. Attempts at psychological profiling by Stevens (2005) and McCaulley and Moscalenko (2014) offered some interesting insights but little basis for practical intelligence. Specifically, Staub (2002) found that terrorists were linked to three types of social groups: those identifying with a suffering group; those who respond to suffering in their own group; and alienated individuals who find purpose in joining a terrorist group. Likewise, McCaulley and Moscalenko stated that terrorists may manifest personality types represented by revolutionaries drawn to a cause, those who try a variety of revolutionary or terrorist causes, those who have had a sudden conversion experience, and those who find acceptance in a committed peer group (White, 2014). On the other hand, Laqueur (1999), Pape (2003) and Borum (2004) suggested that as terrorism changes over time, the profile changes. Interestingly, Horgun (2009) wrote that as a complex phenomenon, identifying the roots of terrorism is not as fruitful as identifying the routes.

With the rise of leaderless resistance and interest in the radicalization process, identifying lone wolf terrorists has emerged as a prominent concern. Specifically, violent radicalization, alienation and self-estrangement have been identified as social-psychological precursors to terrorism (Jenkins, 2009; White, 2014). These processes focus on interpretations of reality in which individuals perceive that their existence is threatened by powerful, evil and depraved forces, thus freeing them from normative restraints.

Gill, Horgan and Deckart (2014) analyzed the socio-demographic characteristics of 119 convicted lone-actor terrorists in the United States and Europe, focusing on ideological commitment and network support structures. They categorized lone-actors in terms of gender, age of first terrorist act, relations status and family characteristics, education, employment history/status, military experience, ideological justifications, awareness of intentions, pre-event behaviors, degree of perceived social isolation, behavior within a wider network, and links to a wider network. The results of their analysis suggested seven significant findings: (1) no uniform profile; (2) prior to the events, others knew of their radicalization and intent to act; (3) a significant range of events or actions preceded their attacks; (4) many but not all were socially isolated; (5) there was involvement with like-minded others; (6) their actions were not sudden or impulsive; (7) despite the diversity of lone-actor terrorists, there were distinguishable differences between subgroups. Their findings indicated the importance of focusing on behavior rather than only on semi-stable (at best) socio-demographic characteristics.

Hamm and Spaaj (2015) developed one of the most comprehensive databases on domestic lone wolf terrorists. They suggested that, in terms of lethality, lone wolf terrorism is not on the rise in the U.S., but the targets are increasingly police and military personnel and the use of firearms is now the preferred tactic. Though they found no standard profile, many are unemployed, single white males with criminal records and are prone to mental illness. Their research supports previous studies that radicalization is associated with a combination of personal and political grievances which have formed the basis for an affinity with other online sympathizers. A triggering event is usually associated with some public statement, blog, post or manifesto. Unfortunately, much of the data upon which this study was based included domestic, right wing or special interest causes. It did not include the growing number of jihadist-inspired acts.

Historically, the roots of terrorism are most often found in the socio-economic, political and/or religious fabric of society. Addressing the perceived inequalities between majority and minority populations is the logical strategy in minimizing or eliminating the causes of asymmetric conflict in general and the specific instances of lone wolf terrorism. However, in a multi-cultural world with extensive boundaries between diverse groups, addressing these roots of conflict is challenging. Because of these conditions, identifying potential terrorists in general and lone wolf terrorists in particular is very difficult. Social scientists have, as we have seen, attempted to develop psychological and social profiles, but they have not been specific enough to facilitate the tracking and control of these threat agents. Therefore, the routes to terrorism have been suggested as a more useful strategy. These more complex perspectives have allowed scholars and security agencies to identify possible combinations of types and to better understand the social, psychological, and structural components that create environments conducive to the emergence of lone wolf terrorists and to identify and track them.

Tracking Terrorists

Unlike military units, terrorist groups are hard to track. A terrorist's affiliation may be to non-state entities, and often they operate with or without the knowledge of any official authority. Their anonymity and mobility may mask the origins or specific locations of their infrastructures or even bases of operation. In such situations, there are limited political channels that a government can apply to lessen the threat of many terrorist groups (Strickland, 2014). Also, in some countries governmental authority isn't strong enough to crack down on terrorist groups, and in others governments may share similar beliefs and philosophies with these groups. These governments might not put forth much effort to end terrorist activity. When governments are unable to gather international support to pressure another government to end hostile activities, there are few political channels to curtail terrorism.

Extensive efforts have been directed to understand the terrorism process, including studies of motivation, recruitment, retention, and structurally conducive social, economic, political and religious environments (Bates, 2011). Strategies and tactics for identifying and tracking terrorists have been developed by counterterrorism agencies using psychological profiling, forensic accounting, communication intercepts, social media monitoring, biometrics and a number of other classified techniques (Lichtblau and Risen, 2006). Early in the war on terrorism the Terrorist Finance Tracking Program (TFTP), with its links to the Society for Worldwide Interbank Financial Telecommunications (SWIFT), provided significant information for the identification and arrest of a number of terrorists operating in the U.S. However, concerns raised by the release of the Snowden documents over the legality of extensive data mining by the NSA, FBI, CIA and the U.S. Treasury Department resulted in a number of international treaties and more restrictive regulations. This reduced access to forensic accounting information (TFTP, 2014). Likewise, the development of the Terrorist Identities Datamart Environment (TIDE, 2014), with 680,0000 to a million subjects on the government watch list as well as over 860,000 biometric files, reflects the extensive resources brought to bear by counterterrorism agencies.

Communication monitoring and intercepts have been successful in limiting the ability of terrorist groups to plan and coordinate their activities. The National Security Agency (NSA, 2016) is the primary U.S. agency responsible for cryptology and Signals Intelligence (SIGNT) and Information Assurance (IA) products and services. Using sophisticated monitoring technology (classified), the NSA provides world-wide access to electronic communications. Though restricted by federal law against domestic monitoring, other federal and state agencies, with restrictions, have been able to provide valuable intelligence related to terrorist threats within the U.S.

Concerns about personal privacy and the legality of domestic communication monitoring have given rise to the growth of commercial encryption software, which has helped terrorists avoid detection. Though counterterrorism agencies have invested in enormous programs to automatically collect and analyze electronic communications, the growing sophistication of terrorists has contributed to an ongoing electronic struggle for data access and security (Scheiner, 2013). Nevertheless, the NSA has access to a huge amount of data, especially through the communication trunks that move Internet data. If it cannot get access through agreements with telecommunication companies, it has been suggested (Snowden) that the NSA surreptitiously monitors communication channels by tapping undersea cables, intercepting satellite communications, and other data sources. Through its ability to quickly sift large amounts of meta-data, it can identify the sources of communications, its content, and the individuals involved.

Open source intelligence activities, like monitoring magazines, newspapers, radio and television broadcasts, are another important tool to track terrorists. Many terrorist organizations provide valuable information about themselves in their public communications and propaganda campaigns (Prunckun, 2015). Al Qaeda's broadcasts and publications have provided significant information on the goals and objectives of the group. While also mobilizing and communicating with actual and potential terrorists, the digital crumbs associated with the dissemination of magazines, such as INSPIRE and Al SHAMIKA, provide access to the potential identity and location of those who appear to at least be interested in their cause (Bates and Mooney, 2014).

The Internet has become a crucial tool for global terrorism (Matusitz, 2015). Their web sites number over 7,000, and terrorists have been successful in hacking other sites to post propaganda videos. In a process called steganography, they also embed messages within text or videos (Lau, 2003). Nevertheless, the NSA and other federal agencies have developed effective counter measures to thwart electronic encryption and covert communications channels (Branch, Armitage and Branch, 2007).

The Dark Web also has become a source of terrorist activity. Using the onion.link router and software such as TOR, terrorists raise funds via bitcoin and put up mirrored sites to support sites regularly deleted on the World-Wide Web. As Cox (2015) noted, terrorists have used the Dark Web to post propaganda videos like the documentary, *The Flames of War,* and to rally jihadists in the Balkan countries. However, as verified in the Snowden leaks, the NSA is using a program known as XKeyscore, which automatically identifies anyone attempting to download TOR. Though this program identifies individuals using TOR, it does not capture what they are accessing on the Dark Web. Former Department of Homeland Security Directors Michael Chertoff and Toby Smith (2015) believe that law enforcement and other security agencies should monitor TOR users and sites. In particular, they recommend mapping the hidden service directory, customer data monitoring, social site monitoring, hidden service monitoring and marketplace profiling.

Terrorist activities on the Dark Web and the Visible Web are not only monitored by governmental security agencies, but they are also viewed by private citizens concerned about terrorism and potential hate crimes. Groups of researchers, hackers, and maverick computer geeks, who cyber-stalk terrorist networks, are now active in both the

United States and abroad. Aaron Weisburd, founder of Internet Haganah and director of the Society for Internet Research, works out of his Carbondale, Illinois home and describes his organization as a "global non-governmental ad-hoc intelligence network" modeled after al Qaeda's very own network. His organization has assisted in shutting down numerous sites linked to networks affiliated with groups such as Hezbollah, Hamas, al Qaeda and ISIS (Rosenblatt, 2007).

Terrorist groups like the Islamic Cyber Caliphate Army have responded by developing hackers who have attacked government, commercial, and private web sites. They have hacked sites, uploaded propaganda, and released personal and confidential information about military, police and government officials. With posts on both the Visible and Dark webs, these cyber terrorists have encouraged lone wolf attacks on identified individuals and their families (SIG, 2016). Recently, they also targeted a number of world leaders and even Weisburd and his group.

The struggle between terrorists and counterterrorism agencies also takes place within the environment of social media. Terrorists, and in particular lone wolf terrorists, often seek affirmation or opportunities to promote their radical perspectives through social media sites. Carmon and Stalinsky (2015) suggest that American companies like Twitter, FaceBook, Google, Apple, Microsoft, YouTube, WhatApp, Skype, Tumblr and Instagram have served as propaganda vehicles for global jihadists. Through graphic beheadings and other executions, ISIS has gained attention and recognition as the new leader in global jihad. The power of social media, as reflected in the Arab Spring, has been a significant force multiplier in the world of terrorism. Not only groups of terrorists, but also single actors are mobilized, directed or at least inspired through the constant flow of posts, tweets and other forms of social media.

Just as advertisers and marketing specialists have learned to monitor and mine social media for commercial purposes, so too have security agencies. Using false identities, called “sock puppets,” social media can be used to identify, track and manipulate participants (Prunckun, 2015). Online fake agents, employing sophisticated computer-generated algorithms based on narrative and statistical probabilities, penetrate radical forums and disseminate false information.

Along with profiling, forensic accounting, communication monitoring, and Internet and social media scrutiny, terrorist tracking also involves other covert techniques. At the international level, satellites and drones identify and track groups and individual terrorists and locate training camps and related infrastructure. Recently, the U.S. military and special operation entities have begun using miniature satellites known as Cubesats to track specific terrorist targets (Klotz, 2014). Even private citizens have contributed to tracking activities through Google Earth technology (Noak, 2014). The military also has been using drone technology to track and interdict terrorists in current combat zones. Likewise, drones are now being used for border security in the U.S. and for immigration and homeland security purposes (Gunderson, 2015).

Human intelligence (HUMINT) also continues to play a vital role in the identification and tracking of terrorists. Clandestine and covert operatives provide vital and specific information on terrorist activities. The use of informants and agents to gather information is, however, a high risk activity. Therefore, specifics on this form of terrorist tracking will not be presented. However, community-based surveillance programs, such as Community Oriented Policing (COP) like the Green Bay Way, illustrate the many benefits of embedded neighborhood policing. COP often encourages information on criminal and possible terrorist radicalization. The similar strategy of Mosaic Engagement, found in the United Kingdom's Preventing Violent Extremism Strategy (Prevent), is another example of engaging local communities to identify radicalization and terrorism (Southers, 2013).

Tracking Lone Wolf Terrorists

While identifying potential lone wolf terrorists is difficult, tracking them is even more so. Part of that difficulty is that they may be associated with a variety of causes and groups. Today, the threat of inspired or directed radical Islamic jihadist terrorism dominates the news. The major attacks in Paris, Brussels, Nice, Ft. Hood, San Bernardino, Orlando and other sites, both foreign and domestic, have focused our attention on this group. However, numerous other domestic terror threats have been associated with a variety of other groups. The FBI has tracked white supremacist groups like the KKK, Aryan Nation and related hate groups. Single-issue groups like the Animal Liberation Front (ALF), Earth Liberation Front (ELF) and anti-abortion groups also have spawned lone wolf terrorist attacks. The Southern Poverty Law Center tracks 148 "patriot groups" which include anti-tax and anti-government organizations, various militia groups, and the Sovereign Citizens, all of which have been associated with violence and lone wolf attacks (Somashekhar and Leonnig, 2015). However, law enforcement and the Department of Homeland Security face practical, legal and political challenges when investigating and tracking these domestic groups.

The increasing threats from radical Islamic terrorist groups and their advocates have gained national attention. As Bergen (2016) notes, self-radicalized lone wolf attackers in the U.S. are a greater threat than returning ISIS fighters from Syria and Iraq, but finding them remains difficult since they do not fit any ethnic profile and the only thing in common is their connection to social media. On the other hand, Weiman (2015) suggests that the lone wolf label may be a detriment to addressing this problem. The belief that terrorists of this type act alone is incorrect; they are inspired or directed by others. Wolves do not hunt alone; they hunt in packs. In this instance, a virtual wolf pack inspires or directs these acts. Lone wolves are often recruited, trained and directed by others online. They use the Internet to find everything from instructions on how to make a bomb, diagrams of public buildings, and names of police, government and military to target. YouTube videos and Twitter postings provide inspiration, direction and personal contacts with other jihadists and also fighters in Iraq and Syria. In 2015, the Brookings Institute identified over 46,000 Twitter accounts used by ISIS activists (Millar, 2015).

In their study of 119 lone actor terrorists, Gill, Horgan and Deckart (2014) found that they regularly engaged in detectable and observable activities with a wide range of individuals, social movements, or terrorist organizations. Using the Internet, YouTube, Twitter or similar forms of social media, these individuals have posted manifestos, diatribes or pleas calling for violence, and, in their minds, justifiable acts against others. Thus, one of the first steps to identify and track potential lone wolf terrorists is to monitor these sites.

Whereas al Qaeda is an elitist radical Islamic terror group, ISIS is a populist group and uses the Internet to open its ranks to almost anyone willing to further their goals. Their form of lone wolf terrorism encourages ex-post-facto declarations of identification with the movement. This provides greater security and anonymity for self-radicalized jihadists and minimizes their prior identification and tracking. However, even the most independent attacks involve some prior public or virtual commitment. For this reason, friends, relatives and the public are critical in countering terrorists, in the same way as law enforcement deals with single-shooters.

Gill, Horgan and Deckart (2014) also found that lone-actor terrorist events were rarely sudden and impulsive. Evidence of some form of virtual or hands-on training as well as strategic or tactical planning was associated with most attacks. This planning and acquisition of skills, weapons and/or other related resources provide for the discovery of lone wolf terrorists. Obviously, travel to a terrorist training facility, either domestic or abroad, is a trackable activity. The acquisition of weapons or bomb-making supplies provides additional evidence of an impending terrorist action. The Boston Marathon bombers accessed INSPIRE magazine to make a pressure cooker-based explosive device. They also purchased fireworks for the black powder to build the bombs (Weiman, 2015). Timothy McVeigh followed the Anarchist's Cook Book's recipe to make the fertilizer fuel oil-based explosive (ANFO) used in the Oklahoma City bombing (Fire, 1995). Because of their potential danger, people purchasing quantities must provide personal documentation. However, the attacks in Paris and Brussels involved the explosive TATP (triacetone-triperoxide), also called the "Mother of Satan" because of its instability, which is available in nail polish remover and hydrogen peroxide found in most homes. Nevertheless, geospatial analysis of these precursors may prove useful to track potential terrorists (Smith, et. al., 2005).

As previously noted, it is difficult to profile lone wolf terrorists. However, despite their diversity, researchers have noted distinguishable differences between subgroups. Compared to right wing and single-issue lone wolves, those inspired by radical Islamic groups (al Qaeda, ISIS, Boko Haram) are generally younger, are often students and are likely to have sought legitimation from epistemic authority figures. They are more likely to have been radicalized and trained through virtual sources. Right wing lone wolves, on the other hand, are usually unemployed, less educated, have made verbal statements to friends and families about their intent or beliefs, and have engaged in dry runs or have obtained assistance from others in procuring weapons (Gill, Horgan and Deckart, 2014).

Created by Congress in 2003, the Department of Homeland Security's mission includes preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience (DHS, 2016). The DHS is committed to operating a multifaceted team of 22 government agencies and organizations to stop terrorism before it occurs. These agencies include the Secret Service, the Border Patrol, Immigration and Customs Enforcement, and the Coast Guard and other agencies responsible for transportation security and port security, plus a number of intelligence organizations. Because of its size, the complexity of the agencies involved, and the diversity of some of their missions, coordination and cooperation have been problematic (White, 2014).

The FBI allocates billions of dollars to support counterterrorism efforts (Strickland, 2014). The National Counterterrorism Center (NCC) coordinates these efforts, including the Joint Terrorism Task Force (JTTF) of over 4,000 members nationwide from 500 state and local agencies and 55 federal agencies. The JTTF provides a one-stop source for information, including the terror watch list, which enables a shared intelligence base across many agencies. However, because lone wolf terrorism in the U.S. is a national issue, many of the government agencies such as the NSA and CIA are restricted from operating domestically. Though the Patriot Act has expanded the powers of our domestic intelligence agencies like the FBI, the clash over civil liberties has limited the tools and tactics of counterterrorism within the U.S.

As a domestic issue, lone wolf terrorism is a major responsibility of state and local law enforcement agencies. Using JTTF information and undercover or cyber operations by the FBI, local agencies investigate, track and respond to domestic threats. A variety of law enforcement agencies like the Law Enforcement Information Network, the National Crime Information Center, and the fusion centers around the country provide important information to local law enforcement (White, 2014). Thus far, state and local law enforcement has been reasonably successful – with the help of the above agencies. However, the anonymity and mobility of potential lone wolf terrorists still poses a significant challenge.

A Potential Response

Enhanced communication and intelligence sharing is necessary between external and internal homeland security agencies and state and local law enforcement. Since lone wolf terrorism is, for the most part, an internal security threat at the community level, local law enforcement must identify, track, and interdict them. To do this, they must move beyond their traditional roles and include more attention, training and intelligence gathering to counterterrorism.

Through federal grants, many local agencies have upgraded their tools and tactics to deal with terrorist threats, but most are focused on response. SWAT team training, increased firepower and special assault-style vehicles will help, but it takes enhanced intelligence and investigative capabilities to deter local terrorist activities. For example, 720 municipal law enforcement agencies that integrate community policing with the new mandates from the DHS have increased their counterterrorism preparedness – and have also lowered their local crime rates (Adcox, 2014).

Local agencies can access federal counterterrorism information. The terror watch list is available, including the FBI Terrorist Screening Center's password-protected App (application) via a smart phone. The Digital Terror + Hate App from the Simon Weisenthahl Center lists information on jihadists, white supremacists, anti-Semitic and other hate groups. While the federal government has extensive resources to track terrorists, most local agencies may have one or two individuals, at best, who deal with digital surveillance. These Apps can help. The website addresses and social media accounts of locals who run solo hate campaigns provide a geographic search function to identify the sources and support networks of lone wolf terrorists (Koebler, 2015).

Local communities can prioritize the types of terrorist threats because of increased access to relevant terrorist-related intelligence. Given a community's demographics, the patterns of social media content observed, and the types of groups or individuals identified by federal or regional agencies, police can improve their focus on potential threats. Some communities are more likely to be a source of jihadist radicalization, yet others may have a higher risk of anti-government or white supremacist activities. Police auxiliary officers, with adequate cyber training, can provide intelligence information pertinent to local threats just as Weisburd 's Society for Internet Research (Greenberg and Cooper, 1996).

Most lone wolf terrorists engage in some prior acts. Frequenting known hate groups or mosques with extremist reputations may be an additional part of the mosaic of radicalization. Local police could make routine checks to find buyers of large amounts of fertilizer or similar components for improvised explosives, with special attention to locals on the terror watch list. They could also monitor local concealed carry permit applications, especially for those who were turned down. Local gun shows could be monitored for those purchasing weapons from private sellers, which bypasses the federal firearms background check requirement (Bates, 2015). Local law enforcement could work with area gun stores to identify individuals who did not pass the required background check or who appear suspicious (Cutway, 2016).

Enhanced community engagement activities by local police also can provide a more conducive environment for counterterrorism awareness. If local police have sufficient diversity in their staff, they may be better able to make and maintain contacts in the community. If little diversity is present, local police may seek community support to create outreach opportunities. A ministerial alliance, including leaders of local mosques or similar religious groups, can improve community solidarity. It also might identify those groups that avoid interaction or cooperation with others.

Tracking lone wolf terrorists in a local community is difficult. Limited resources and legal restraints are significant impediments. A balance must be maintained to avoid the alienation of individuals. However, improved coordination between federal and local agencies, combined with the use of open-source data and increased community engagement can foster the identification and tracking of potential lone wolf threats.

Conclusions

As the threat of domestic and international terrorism increases, the identification and tracking of terrorists is the most important component of counterterrorism. Given the diversity of the sources of terrorism, each threat is associated with different structural environments and potential participants. Profiling terrorists is very difficult. However, focusing on the routes to terrorism has allowed us to better understand the recruitment, radicalization, and related activities associated with terrorism in general and lone wolf terrorism in particular. Digital crumbs left as they become radicalized and move from spectator to potential threat provide clues for their identification. At the international and national levels, forensic accounting, the monitoring of the Internet and the Dark Web, and the use of undercover cyber operatives play important roles in effective counterterrorism. Local law enforcement can use the information developed by other agencies and can provide community awareness and local engagement to address the threat of lone wolf terrorists. The most important element remains the vigilance and involvement of citizens and even family members. While lone wolf terrorists are hard to identify and track, learning more about their routes and behaviors gives us the tools and tactics for more effective counterterrorism.

References:

Adcox, K. (2014) "Community-oriented Counterterrorism: Incorporating National Homeland Security Into the Local Community Policing Philosophy." Dudley Knox Library (Dissertation). Retrieved from: http://calhoun.nps.edu/handle/10945/44507.

Andrews, L. (2001) "Motivations for Terrorism." Developmental Psychology Newsletter.

Artiga, V. (2010) "Lone Wolf Terrorism: What We Need to Know and What We Need to Do" TAK Response Conference. San Jose, CA Sept. 14-16. Retrieved from: http://www.takresponse.com/index/homeland-security/lone-wolf_terrorism.html.

Bakker, E. and B. de Graaf, (2010) "Lone Wolves: How to Prevent This Phenomenon?" International Center for Counter-Terrorism – The Hague. Expert Meeting Paper.

Bates, R. A. (2011) "Terrorism within the Community Context," *Journal of Public and Professional Sociology.* Vol. 3.

Bates, R. (2012) "Dancing with Wolves: Today's Lone Wolf Terrorists." *Journal of Public and Professional Sociology. Vol. 4 (1).*

Bates, R. (2015) "Gun Shows: The Social Construction of an Armed Event." *Journal of Public and Professional Sociology. Vol. 7 (2).*

Bates, R, and M. Mooney (2014) "Psychological Operations and Terrorism: The Digital Domain." *Journal of Public and Professional Sociology. Vol. 6 (1).*

Bergen, P. (2016) "How Big Is U.S. Terror Threat," CNN Mar. 24. Retrieved from: http://www.cnn.com/2016/03/22/opinions/terrorism-threat-united-states-bergen/.

Black, D. (2004) "The Geometry of Terrorism." *Sociological Theory* 22 (1): 14-25.

Borum, R. (2004) *Psychology of Terrorism.* University of South Florida: Tampa, FL.

Branch, S., G. Armitage, and P. Branch, P (2007) "A Survey of Covert Channels and Countermeasures in Computer Network Protocols." IEEE Communications Surveys and Tutorials. Vol. 9 (3).

Carmon, Y. and S. Stalinsky (2015) "Terrorists Use of U.S. Social Media Is a National Security Threat." Forbes/Opinion. (Jan. 30, 2015) Retrieved from: https://ent.siteintelgroup.com.

Chertoff, M. and T. Smith (2015) "The Impact of the Dark Web on Internet Governance and Cyber Security." Paper No. 6 (Feb. 17, 2015) Global Commission on Internet Governance. Retrieved from: https://www.cigionline.org/publications/impact-of-dark-web-internet-governance-and-cyber-security.

Clemons, S. (2010) "The Real Problem with 'Lone Wolf' Terrorism." Retrieved from: http://www.thewashingtonnote.com/archives/2010/04/the real problem.

Cox, J. (2015) "ISIS Now Has a Propaganda Site on the Dark Web." Motherboard. Retrieved from: http://motherboard.vice.com/read/isis-now-has-a-propaganda-site-on-the-dark-web.

Cutway, A. (2016) "Gun Store Owner May Have Thwarted Mass Shooting by Refusing to Sell Weapon." Orlando Sentinel. Retrieved from: http://www.orlandosentinel.com/features/gone-viral/os-gun-store-owner-stops-mass-shooting-20160329-story.html.

DHS (2016) Department of Homeland Security. Retrieved from: htts:www.DHS.gov.

FBI (2016) "Protecting America from Terrorist Attack." Retrieved from: https://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs.

Fire, F. (1995) "ANFO: The Tool of Destruction." Fire Engineering Network, (10/01/1995). Retrieved From: http://www.fireengineering.com/articles/print/volume-148/issue-10/features/anfo-the-tool-of-destruction.html.

Gill, P., J. Horgan and P. Deckart (2014) "Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-actor Terrorists." Journal of Forensic Sciences. Vol. 59 (2).

Greenberg, M. and K. Cooper (1996) "Unused Secret Weapon against Terrorism." Law Enforcement News. (Nov. 15, 1996). Retrieved from: http://www.lib.jjay.cuny.edu/len/96/15nov/html/forum.html.

Gunderson, D. (2015) "Drone Patrol: Unmanned Craft Find Key Role in U.S. Border Security." MPR News: Retrieved from: http://www.mprnews.org/story/2015/02/19/predator-drone.

Hacker, F.J. (1976) *Crusaders, Criminals and Crazies.* New York: Norton.

Halpern, M. (2014) "We Must Track and Trap Lone Wolf Terrorists." Observer, Retrieved from: **http://observer.com/2014/11/we-must-track-and-trap-lone-wolf-terrorists/.**

Hamm, M. and R. Spaaj (2015) “Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies.” Indiana State University #2012-ZA-BX-0001. This report has not been published by the U.S. Department of Justice. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice. 2

Horgun, J. (2009) *Walking Away from Terrorism.* Routledge: New York.

Jackson, G. (2015) “Tracking Terrorists in the Dark Web.” WJLA: Washington, DC. Retrieved from: http://wjla.com/news/government-matters/tracking-terrorists-in-the-dark-web-111942.

Jenkins, B. (1983) *New Modes of Conflict.* RAND: Santa Monica, CA.

Jenkins, B. “Outside Expert’s View .” In D. Gartenstein-Ross and L. Grossman (ed.) *Homegrown Terrorists in the U.S. and U.K.: An Empirical Analysis of the Radicalization Process.* Foundation for the Defense of Democracies: Washington, DC.

Klotz, I. (2014) “Beware Terrorists: Mini Spy Satellites Can Find You.” NBC News (Jun. 7, 2014) Retrieved from: http://www.nbcnews.com/id/43313086/ns/technology_and_science-space/t/beware-terrorists-mini-spy-satellites-can-find-you/#.VvxA1vkrJD8.

Koebler, J. (2015) “How to Track Terrorists from Your Phone.” U.S. News and World Report. (Mar. 8, 2015). Retrieved from: http://www.usnews.com/news/articles/2012/03/08/how-to-track-terrorists-from-your-phone.

Lau, S. (2003) “An Analysis of Terrorist Groups’ Potential Use of Electronic Steganography.” SANS Institute. Retrieved from: http://www.sans.org/reading_room_whitepapers/steganography554.php.

Laqueur, W. (1999) *The New Terrorism: Fanaticism and the Arms of Mass Destruction.* New York: Oxford University Press.

Lesser, I.O. (1999) “Changing Terrorism in a Changing World.” In I.O. Lesser,B. Hoffman, J. Arquilla, D. Ronfeldt, M. Zannia and B. Jenkins (eds.) *Countering the New Terrorism.* RAND: Santa Monica, CA.

Lichtblau, E. and J. Risen. "Bank Data Is Sifted by U.S. in Secret to Block Terror,” *New York Times*, June 22, 2006. Accessed June 23, 2006.

Love, J, and H. Yan (2014) “Western Allies Reject ISIS Leader’s Threats Against Their Civilians,” CNN. Retrieved from: http://www.cnn.com/2014/09/22/world/meast/isis-threatens-west/.

McCauley, C. and S. Moskalenko (2014). "Toward a Profile of Lone Wolf Terrorists: What Moves an Individual from Radical Opinion to Radical Action." *Terrorism and Political Violence* 26:69-85.

Maras, M. (2013) *Counterterrorism.* Jones and Bartlett Learning: Burlington, MA.

Matusitz, J. (2015) *Symbolism in Terrorism: Motivation, Communication, and Behavior.”* Rowan and Littlefield: Lanham, MD.

Millar, L. (2015) "Islamic State: U.S. Terror Experts Say Tracking Down Lone Wolf Attackers Remains Difficult." ABC News (May 7, 2015). Retrieved from: http://www.abc.net.au/news/2015-05-08/countering-islamic-state-sympathisers-in-us/6454142.

Noak, R. (2014) Here's How to Track Terrorists on Google Earth." Washington Post (Aug. 26, 2014), Retrieved from: https://www.washingtonpost.com/news/worldviews/wp/2014/08/26/heres-how-to-track-terrorists-on-google-earth/.

NSA (2016) National Security Agency: Washington, DC. Retrieved from: https://www.nsa.gov/index.shtml.

Pantucci, R. (2011) " A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists." The International Center for the Study of Radicalisation and Political Violence.

Pape, R. (2005) *Dying to Win: The Strategic Logic of Suicide Terrorism.* New York: Random House.

Phillips. P. & Pohl, G. (2011) "Economic Profiling: Can Economics Provide Behavioral Investigative Advice?" Retrieved from: http://ssm.com/abstract=1858975.

Prunckun, H. (2015) *Scientific Methods of Inquiry for Intelligence Analysis.* Second Edition. Rowan and Littlefield: Lanham, MD.

Rosenblatt, A. (2007) "Cyber-Spies Tracking Terror on the Web." CNN. Retrieved from: http://www.cnn.com/2007/TECH/05/29/internet.spying/.

Sage (2011) "Terror Threat." Retrieved from: http://www.ereference.com/defense- secretary-leon-panetta-terror-threat.

Scheiner, B. (2013) "NSA Surveillance: A Guide to Staying Secure." The Guardian. Retrieved from: http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance.

Schmid, A. P. (1992) "The Response Problem as a Definitional Problem." *Terrorism and Political Violence* 4 (4) (Winter)*:* pp. 7-25.

SIG (2016) "Islamic Cyber Caliphate Army." Site Intelligence Group. Retrieved from: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=757&Itemid=1355.

Somashekhar, S, and C. Leonnig (2012) "Lone Wolf Domestic Terrorism Threats Are Hard to Track." Washington Post (Aug. 8, 2012). Retried from: https://www.washingtonpost.com/politics/lone-wolf-domestic-terrorism-threats-are-hard-to-track/2012/08/08/fd5de712-e172-11e1-a25e-15067bb31849_story.html.

Smith, B., J. Cothren, P. Roberts and K. Damphouse (2008) "Analysis of Terrorist Activities: The Identification of Spatial and Temporal Patterns of Preparatory Behavior of International and Environmental Terrorists." U.S. Department of Justice: Washington, DC.

Southers, E. (2013) *Homegrown Violent Extremism.* Elsevier: Oxford, UK.

Staub, E. (2002) "Notes on Terrorism: Origins and Prevention." *Peace and Conflict: Journal of Peace Psychology. Vol. 8 (3).*

Stevens, M. (2005) "What Is Terrorism and Can Psychology Do Anything to Prevent It?" Behavioral Sciences and the Law. Vol. 23 (4).

Strickland, J. (2014) "How Are Terrorists Tracked, and What Does It Cost?" How Stuff Works – Culture. Retrieved from: http://people.howstuffworks.com/how-are-terrorists-tracked.htm

TFTP (2014) "Terrorist Tracking Program." U.S. Department of Treasury. Retrieved from: http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx

TRAC (2015) A large data base which tracks terrorist groups. Retrieved from: http://www.trackingterrorism.org/

Tucker, P. (2015) "How the Military Will Fight ISIS on the Dark Web." Defense One. Retrieved from: http://www.govexec.com/insights/reports/joint-enterprise-licensing-agreements/126893/?oref=WA.

Weiman, G. (2015) "There Is No Such Thing as a Lone Wolf in Cyberspace." Blog – Great Debate/ Reuters: June 25, 2015. Retrieved from: http://blogs.reuters.com/great-debate/2015/06/25/theres-no-such-thing-as-a-lone-wolf-in-cyberspace/.

White, J. (2014) *Terrorism and Homeland Security 8th Edition.* Cengage: Belmont, CA.