Institute for Homeland Security Solutions

Applied research • Focused results

Building on Clues: Examining Successes and Failures in Detecting U.S. Terrorist Plots, 1999-2009

October 2010

Authors

Kevin Strom, RTI International

John Hollywood, RAND Corporation

Mark Pope, RTI International

Garth Weintraub, RTI International

Crystal Daye, RTI International

Don Gemeinhardt, RTI International

Table of Contents

List of Figures

List of Tables

Executive Summary

Since 2001, the intelligence community has sought methods to improve the process for uncovering and thwarting domestic terrorist plots before they occur. Vital to these efforts are the more than 17,000 state and local U.S. law enforcement agencies whose role in the counterterrorism process has become increasingly recognized. As part of an on-going study for the Institute for Homeland Security Solutions (IHSS), this report examines open-source material on 86 foiled and executed terrorist plots against U.S. targets from 1999 to 2009 to determine the types of information and activities that led to (or could have led to) their discovery. Our findings provide law enforcement, homeland security officials, and policy makers with an improved understanding of the types of clues and methods that should be emphasized to more reliably prevent terrorist attacks, including the need to:

- **Recognize the importance of law enforcement and public vigilance in thwarting terror attacks.** More than 80% of foiled terrorist plots were discovered via observations from law enforcement or the general public. Tips included reports of plots as well as reports of suspicious activity, such as pre-operational surveillance, para-military training, smuggling activities, and the discovery of suspicious documents.
- **Continue to investigate Al Qaeda and Allied Movements (AQAM), but do not overlook other groups, and pay particular attention to plots by "lone wolves."** Less than half of U.S. terror plots examined had links to AQAM, and many non-AQAM plots, primarily those with white supremacist or anti-government/militia ties, rivaled AQAM plots in important ways. Additionally, plots by single actors ("lone wolves") have proven particularly successful, reaching execution nearly twice as often as plots by groups.
- **Ensure processes and training are in place that enable law enforcement personnel to identify terrorist activity during routine criminal investigations.** Almost one in five plots were foiled "accidentally" during investigations into seemingly unrelated crimes. Training is needed to recognize when ordinary crimes may be connected to terrorism.
- **Work to establish good relations with local communities and avoid tactics that might alienate them.** Approximately 40% of plots were thwarted as a result of tips from the public and informants. Establishing trust with persons in or near radical movements is jeopardized by tactics such as racial, ethnic, religious, or ideological profiling.
- **Support "quality assurance" processes to ensure initial clues are properly pursued and findings shared.** Investigating leads and sharing information across agencies led to foiling the vast majority of terrorist plots in our sample. Similarly, breakdowns in these basic processes led to lost opportunities to thwart some of the worst attacks, including 9/11.
- **Expand the federal standards for categorizing suspicious activity reports (SARs).** A large majority of the initial clue types we identified, including public and informant tips, as well as law enforcement observations made during routine criminal investigations, are only indirectly referenced in the current national SAR standards. Expanding them would enable more comprehensive reporting and greater information sharing of potential terrorist activity.

Introduction

Since 2001, the intelligence community has sought methods to detect and disrupt terrorist plots as far "left of the boom" as possible (Carafano, 2009). The process of thwarting such plots typically proceeds in three steps: (1) finding an initial clue that alerts law enforcement that terrorist activity may be underway, (2) finding sufficient evidence to warrant the allocation of law enforcement personnel and resources to investigate the initial lead, and (3) conducting a full-scale investigation. To more reliably thwart terror plots requires improvements to all three steps.

Key to this effort are the more than 17,000 state and local law enforcement agencies that collectively represent terrorism's "first-line preventers" (Kelling & Bratton, 2006). Despite the vast size of this network and the growing recognition of their importance in the counterterrorism process, state and local resources are still commonly underutilized. While regional and state fusion centers have helped promote partnerships and information sharing, considerable challenges remain.

Particularly problematic has been the lack of coordination and standardization of counterterrorism practices at the state and local levels. For example, in the absence of federal guidance, local jurisdictions have developed different procedures for collecting and prioritizing suspicious activity reports (SARs)—reports of activities and behaviors potentially related to terrorism collected from incident reports, field interviews, 911 calls, and tips from the public. This lack of standardization has impeded the sharing and analysis of such information (Suspicious Activity Report Support and Implementation Project, 2008).

The Nationwide SAR Initiative (NSI) was launched in part to remedy this deficiency by establishing "a unified process for reporting, tracking, and accessing of (SARs)" (National Strategy for Information Sharing [NSIS], 2007, p. A1-7). The U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and Department of Defense (DOD), among others, are presently working on identifying what those standardized processes should be. Completed as part of a larger study for the Institute for Homeland Security Solutions (IHSS), this project report informs the development of those standards by determining the types and sources of information that have proven most influential in thwarting terror plots.

In this analysis, we examine all identified terrorist plots against U.S. targets from 1999 to 2009, including both foiled and executed plots, to determine what types of suspicious behaviors and means of reporting most frequently led to (or could have led to) their discovery and ultimate prevention. Specifically, this study seeks to (1) identify and assess the meaningful characteristics of terrorist plots; (2) characterize the initial clues of terrorist activity; (3) characterize the evidence that led to full-scale counterterrorism investigations; (4) characterize how these full-scale investigations progressed; and (5) analyze plots that ended in an attack to

determine if there were clear indicators that could have been detected. Together, these analyses provide state and local law enforcement partners with an improved understanding of the types and sources of clues that should be emphasized to more effectively detect and disrupt terrorist activity before it occurs.

While there has been no shortage of counterterrorism research in recent years, this study is unique in two key respects. First, unlike small-*n* qualitative case studies, which typically suffer from an inability to generalize findings (Goldthorpe,1997; Lieberson, 1991), or large-*n* statistical analyses that are often too general and thus not useful to investigators at a practical level (Brady & Collier, 2004; Mahoney & Rueschemeyer, 2003), this study seeks the middle ground. Specifically, this study uses quantitative techniques to characterize qualitative case studies of terrorism incidents in order to provide practical recommendations to law enforcement. Second, unlike most counterterrorism research, which has focused on the types of activities terrorists engage in prior to attack (e.g., Smith, Damphousse, & Roberts, 2006; Memorial Institute for the Prevention of Terrorism, 2007), this study focuses on the activities of law enforcement and the public at large that have proven most effective at thwarting plots.

Methods

Defining Cases to Include

Determining which cases to include in a study on terrorism is a task that has long been fraught with confusion and disagreement. Despite numerous efforts, there remains no clear consensus on what constitutes terrorism. In this study, we included recent cases of U.S. terrorism satisfying the following criteria:

- *The case fits the definition of "terrorism" as defined in the Global Terrorism Database (GTD).* Specifically, the case reflects an "intentional act of violence or threat of violence by a non-state actor" meeting two of the three following requirements: (1) the act was aimed at attaining a political, economic, religious, or social goal; (2) the act included evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) other than the immediate victims; or (3) the act was outside the precepts of International Humanitarian Law (START, 2010).
- *The case can include a plot that reached execution, a plot foiled prior to reaching execution, or material support to a terrorist organization clearly in service of a future plot.* "Executed" plots include those that were actually carried out, even if they did not result in casualties or were stopped during the moment of execution (e.g., the Christmas day bombing plot was counted as an executed plot despite the bomb failing to detonate). "Foiled" plots include only thwarted plots that were deemed as legitimate threats; hoaxes and cases in which alleged perpetrators were subsequently acquitted were excluded. Cases of "material support in service of a future plot" typically involved suspects conducting site surveillance of U.S. landmarks to assist terrorist groups in determining which landmarks to attack; cases of recruiting U.S. persons to train with or fight for the Taliban or other radical groups overseas were not included.

- *The planned or executed acts of violence in the case were intended to cause casualties or catastrophic damage to critical infrastructure.* During our initial search for incidents, we uncovered a significant number of small-scale attacks against property, almost all of which were conducted by animal rights and environmental groups (e.g., vandalism of auto dealerships, arsons of new housing developments, destruction of lab equipment). Although the cumulative financial impact of these attacks is undoubtedly large, including them in our study posed significant challenges. First, such attacks have generally received little national coverage, and thus information about them was severely limited. Second, small-scale attacks directed only at property are typically given lower investigative priority. In fact, none of the more than 135 animal rights and environmental group attacks against property we identified were foiled prior to execution. Including such cases, therefore, would likely produce an imbalanced analysis. We thus discarded small-scale attacks intended strictly to damage property, unless the targets were deemed to be critical infrastructure (e.g., dams, power plants, bridges).
- *The plot was directed against a U.S. target outside of a conflict zone.* This criterion includes targets within U.S. boundaries, as well as U.S. embassies, consulates, and military bases abroad. However, U.S. targets in countries with high insurgent or terrorist paramilitary activity, such as Iraq, Afghanistan, and Pakistan, were excluded.
- *The case took place between January 1, 1999 and December 31, 2009*. In selecting our study period we sought to evaluate a minimum of 10 years of data. Selecting 1999 as a start date also ensured that some of the first wave of Al Qaeda and Allied Movements (AQAM) plots (notably the Millennium Plot) as well as several major militia and Y2K plots were included.
- *The case can include plots of any ideological motivation*. While AQAM and AQAM-inspired violence has received a great deal of attention since 9/11, we examined cases across the full range of ideological motivations, including broadly Leftist ideologies, animal rights causes, the environment (besides animal rights), opposition to abortion, opposition to governmental authority (militia groups), and white supremacist (including Neo-Nazi) beliefs. In a few cases, the exact motivations of the plotters were either not known or not clearly ideological in nature.
- *Information about the case was publicly available*. Only cases discussed in open sources are included. Sources used include media accounts, legal records, government publications, research databases, and listings by terrorism "watchdog" groups.

We believe that the cases included in this analysis are representative of recent activity that is generally considered terrorism against U.S. targets. We recognize that restricting the cases to those publicly known is a limiting factor that may skew the specific numbers in this study (notably, plots foiled through intelligence efforts that never became public and plots that ended on their own are likely underreported). However, we believe that the general trends in our findings are valid and informative.

Identifying Cases

Cases were identified from a variety of publicly available information sources. Research databases included the GTD from 1999 to 2007, augmented with the Worldwide Incidents and

Tracking System (WITS) for 2008 to 2009. Government sources included publications and reports from the FBI, DOJ, DHS, and the White House. We also reviewed media accounts and summaries, which proved particularly helpful for information regarding more recent incidents.

Terrorist incidents were also identified from incident summary lists maintained by several advocacy groups, including the Heritage Foundation (tracking predominantly AQAM and AQAM-inspired groups), the Southern Poverty Law Center (tracking anti-government groups and those motivated by racial, ethnic, religious, or other types of bias), and the Fur Commission (tracking environmental and animal rights groups). Although information from these advocacy groups was useful in identifying cases of interest, we drew from other sources to code the fields of interest wherever possible.

Coding Process and Analytic Methods

Identified cases were added to a customized Microsoft Access database, which served as the central repository for all information collected or extracted. All cases were reviewed independently by multiple project staff to verify that they were accurately and consistently coded and that they satisfied the stated criteria for inclusion. Cases were coded for a number of attributes, including group ideology/motivation, group size, means of attack, nature of attack, target type, the initial clue that led to (or could have led to) the plot's discovery, source of the initial clue, and the secondary clue that led to a full-scale investigation. These codes were developed after all cases were identified and refined to ensure they accurately characterized the types of clues and activities identified. A list of the variables and the codes used can be found in **Appendix A**. The full dataset is available upon request.

Using this coding scheme, we identified cases with similar attributes to establish trends and patterns within the dataset. We emphasize that given the incompleteness of the data these counts should not be confused with statistical analyses. Similarly, many of the counts are very small (e.g., a plot was foiled a certain way only once or twice) and could not be used to draw meaningful statistical inferences, even if perfect data were available. Additionally, cases known only to intelligence agencies are likely underreported, as mentioned. Furthermore, it is unlikely that we found every relevant case through our searches. While these limitations should be noted, we believe that the general trends and patterns in the cases are informative.

Results

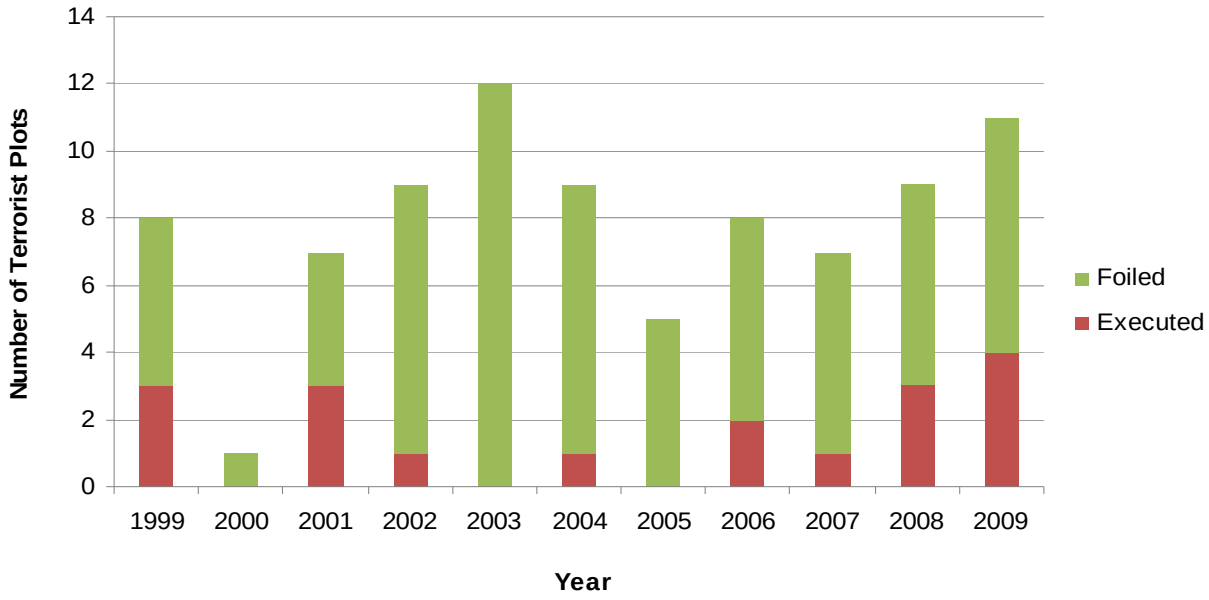
Characterizing Terrorist Plots in the United States, 1999–2009

We identified 86 cases that met the specified criteria. Of these 86 cases, 18 plots reached execution and caused—or were intended to cause—casualties. The remaining 68 cases were plots that were intended to cause casualties but were thwarted prior to execution. Assuming

these identified cases are generally representative, the United States is interdicting about 80% of terrorist plots intended to cause casualties or destroy critical infrastructure.

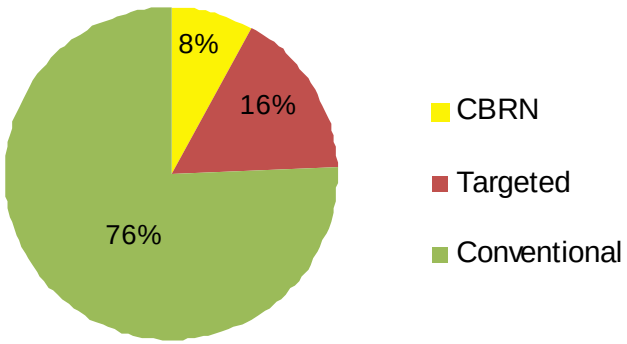
From 1999 to 2009, our data indicate an average of approximately 8 plots (1.6 executed plots and 6.2 foiled plots) per year. However, the number of plots varied significantly from year to year, ranging from a low of 1 in 2000 to a high of 12 in 2003, as illustrated in **Figure 1**.

Figure 1. Foiled and Executed Terrorist Plots by Year, 1999–2009



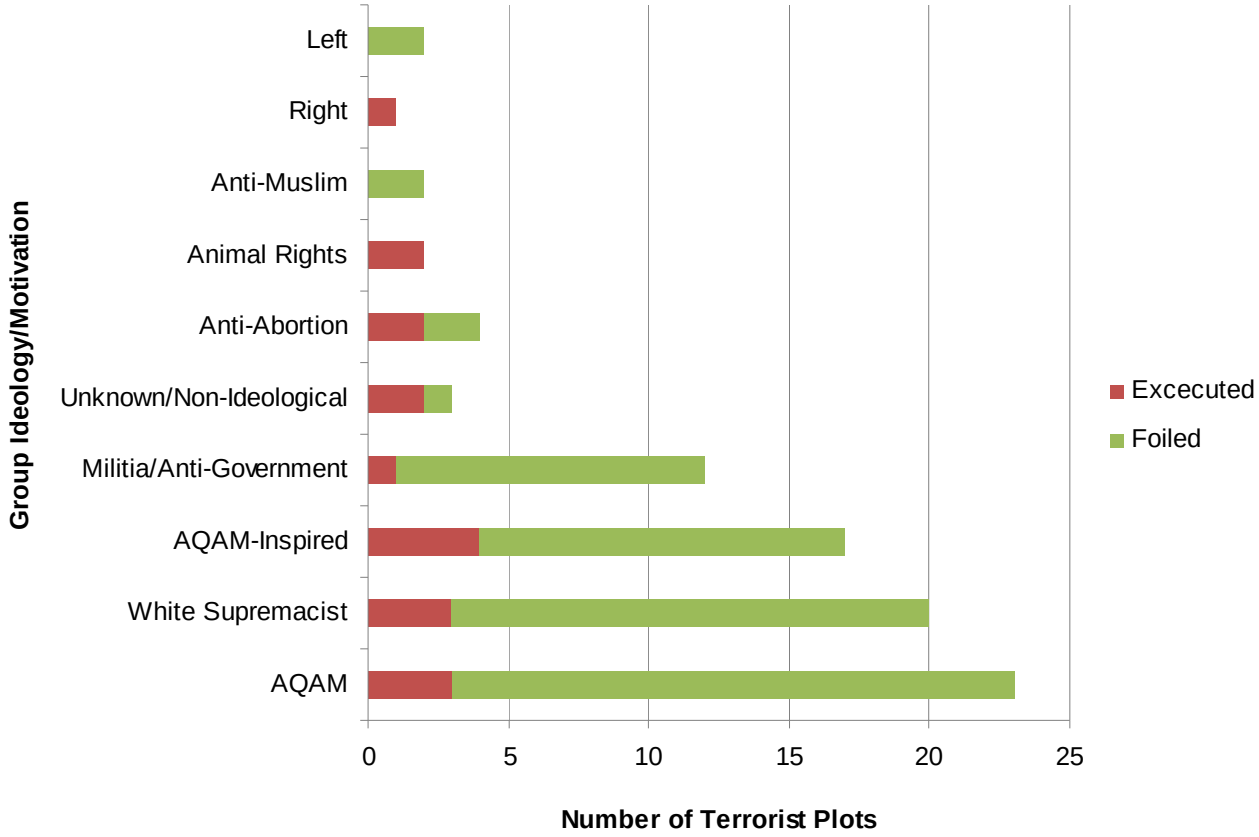
The nature of these plots also varied widely (see **Figure 2**). In the majority of plots (65 cases, 76%), the plan was to carry out a conventional attack, including bombings and mass shootings, to inflict casualties. By contrast, chemical, biological, radiological, or nuclear (CBRN) attacks were planned in only seven cases (8%). In 14 cases (16%), a particular person or small group was targeted (typically assassinations).

Figure 2. Nature of Terrorist Plots, 1999–2009



The frequency of plots also varied by group ideology/motivation. From the 86 cases examined, we were able to identify ten distinct ideological or motivational categories. **Figure 3** provides a breakdown of these group types and the number of plots associated with them. In the figure, we distinguish between "AQAM" plots (those sponsored directly by a foreign AQAM organization) and "AQAM-Inspired" plots (those planned or carried out by individuals who did not receive direct support or training from AQAM but were nevertheless influenced by them). AQAM-inspired plots are frequently characterized by the media as "homegrown" terrorist plots, and recent research has highlighted their growing importance in the U.S. (Bergen & Hoffman, 2010).

Figure 3. Terrorist Plots by Group Ideology/Motivation, 1999–2009

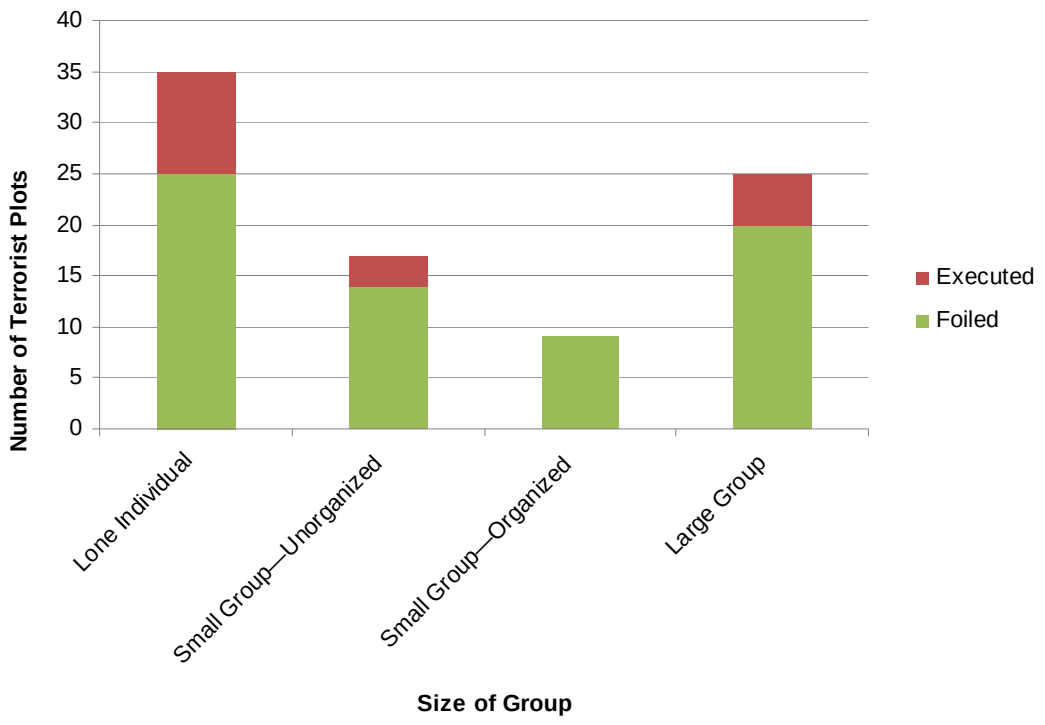


Since 9/11, U.S. discourse on terrorism has tended to focus on AQAM and associated "Jihadists" (e.g., Sageman, 2008; Hoffman, 2003; Ackerman & Tamsett, 2009). However, our analysis indicates that non-AQAM attacks are also important. Although AQAM and AQAM-inspired plots were responsible for a plurality of attacks in our study (40 out of 86), white supremacist and militia/anti-government groups were also responsible for a significant number of attacks (20 and 12 plots, respectively).

Furthermore, white supremacist and militia/anti-government plots rivaled AQAM plots in other ways. For example, the majority of CBRN plots were hatched by non-AQAM groups—three plots were by white supremacist groups, and two attacks were for unknown or non-ideological reasons (with the latter including the October 2001 anthrax attacks). Some types of non-AQAM attacks with relatively few plots are worth mentioning as well, as they were disproportionately likely to reach execution. These include plots by animal rights groups, anti-abortion activists, right wing groups, and attacks carried out for unknown or non-ideological reasons. Although the small number of such plots makes statistical inferences problematic, anecdotally, our data suggest that authorities have been less successful at thwarting these types of plots.

Analysis of terrorist plots by group size reveals that the vast majority of attacks were by single actors and small groups, as illustrated in **Figure 4** below.

Figure 4. Executed and Foiled Plots by Group Size, 1999–2009



More than 40% (35 cases) of terrorist plots from 1999 to 2009 were planned or carried out by single individuals, or “lone wolves” (individuals not directly under the command structure of a group or movement but who sympathize with a particular cause). “Lone wolves” have also been more successful in executing attacks; nearly 30% of plots by single actors reached execution, compared to a 16% average execution rate by small and large groups.

Plots by large groups (including 23 AQAM plots and 2 attacks by the Animal Liberation Front [ALF]) were responsible for approximately 29% of identified plots. Although large groups were less successful than lone wolves, they were more successful than small groups, executing 20% of their intended attacks. We note, however, that while we classify both AQAM and ALF as large groups, operationally, the majority of their attacks have been perpetrated by small groups of individuals, often acting with a large degree of autonomy.

Of the remaining plots, approximately 20% (17 cases) involved small unorganized groups (small groups with no formal structure, such as the father and son duo Wade and Christopher Lay, who plotted to assassinate Texas officials involved in the 1993 Waco standoff), and 11% (9 cases) involved small organized groups (groups with names and formal organizational structures, such as the Jamiyyat Ul-Islam Is-Saheeh [JIS] group, which formed in a California prison and allegedly conspired to attack Army National Guard facilities, synagogues, and other targets throughout southern California). Overall, attacks by small groups were found to be the least successful, reaching execution in just 3 of the 28 incidents plotted (11%).

Initial Clues of Terrorist Activity

In this section, we limit our analysis to the foiled plots (68 cases) in order to understand what characteristics these plots had in common that allowed them to be thwarted. We first consider initial clues—reports that tipped off law enforcement or members of the intelligence community that there was a reasonable suspicion of future terrorist activity.

To conduct this analysis, we developed a coding scheme to categorize the clues that first brought these plots to the attention of authorities. The categories of initial clue types and examples of each are described in greater detail below in **Table 1**. In the table, we list the federal standards for categorizing suspicious activity reports potentially related to terrorism as defined in the newly created *Information Sharing Environment* (*ISE) SAR Functional Standard*, Version 1.5 (Program Manager for the Information Sharing Environment, 2009). Note that the *ISE SAR Functional Standard* focuses on suspicious activity as traditionally defined (e.g., people photographing locations that are not normally photographed). Thus, many of the initial clues identified from the plots in our dataset had no matching ISE SAR code, or a code that was only tangentially related—for example, coding a tip that a specific conspiracy was underway as “Expressed or Implied Threat.” We therefore use our own coding schema in the analysis rather than the ISE SAR codes to provide a more detailed and complete list of clue types.

Table 1. Types of Initial Clues or Activities That Brought Attention to a Plot

Initial Clue	Description	ISE SAR Equivalent Code
Associations with known suspects	Authorities note meaningful associations between a known terror suspect(s) and a new suspect. (e.g., Authorities observe terrorism suspects meeting secretly with previously unknown persons.)	No equivalent
Prior terrorist activity	Authorities investigate non-violent acts of terrorism (typically against property) and find plans and material to carry out more violent attacks. (e.g., Authorities investigate suspects for nighttime arsons at churches and discover plans and material to bomb a church during services.)	Sabotage/Tampering/ Vandalism
Solicitation of an undercover agent or informant	A would-be terrorist solicits an undercover agent or informant to participate in a plot. (e.g., A member of a group asks a perceived fellow extremist to help him or her acquire explosives to blow up a government building.)	Expressed or Implied Threat; may also include Acquisition of Expertise
Online solicitation	A would-be terrorist attempts to recruit others to join a plot, or expresses interest in joining a plot, in online media (chat rooms, discussion boards, etc.). (e.g., A person asks to join an AQAM group and receive training to blow up a government building.)	Expressed or Implied Threat; may also include Acquisition of Expertise
Unsolicited public tip reporting a specific plot	A member of the general public (including associates of the perpetrator not already acting as police informants) contacts authorities to report a plot (e.g., A former member of an extremist organization learns that other members are plotting an attack and voluntarily reports this to the police.)	Expressed or Implied Threat
Direct threat from perpetrator	A would-be terrorist makes an explicit threat directly to the intended target who then reports it to authorities. (e.g. An individual sends a letter to the IRS threatening to kill any employee who attempts to collect his/her taxes and the threat is reported.)	Expressed or Implied Threat
“Ordinary” crime	Authorities investigate criminal activity with no known links to terrorism and discover evidence of a plot. (e.g., Authorities respond to a report of domestic violence and find attack plans at the home.)	No equivalent
Precursor crime	Authorities investigate crimes known to be associated with terrorism (e.g., counterfeiting, identity theft, robbery) and discover evidence of a plot. (e.g., Authorities arrest would-be plotters for multiple gas station robberies during adjacent searches and discover plans to carry out a terrorist attack.)	Can be Theft/Loss/ Diversion, depending on the type of crime

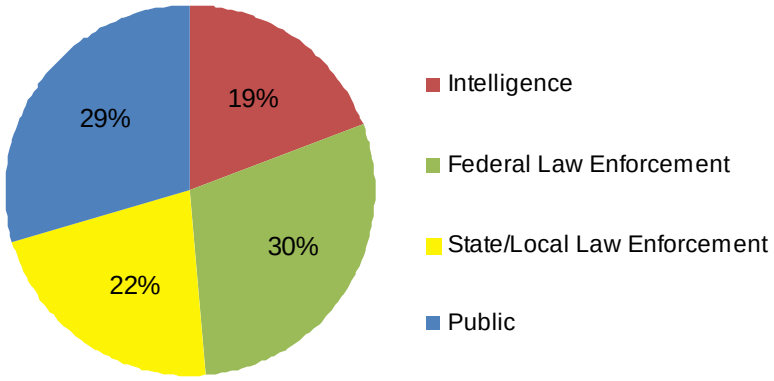
(continued on next page)

Table 1. Types of Initial Clues or Activities That Brought Attention to a Plot (continued)

Initial Clue	Description	ISE SAR Equivalent Code
Criminally suspicious activity	Authorities receive reports of criminal activity or behavior indicating the possibility of a terrorist attack. (e.g., Passersby see a man parked outside a synagogue with a rifle and call police.)	Expressed or Implied Threat
Suspicious activity—paramilitary training/travel	Authorities receive reports of individuals either setting up paramilitary training events or trying to travel overseas to receive paramilitary training. (e.g., (1) Authorities investigate reports of people regularly firing assault rifles in a mining pit. (2) A person reports that a family member is trying to book travel to receive paramilitary training in Pakistan.)	Acquisition of Expertise
Suspicious activity—potential surveillance activity	Authorities receive reports of behavior potentially related to target probing and surveillance. (e.g., Authorities detain and question people trespassing in and photographing military barracks.)	Breach/Attempted Intrusion, Eliciting Information, Testing or Probing of Security, Photography, and/or Observation/Surveillance depending on the incident
Suspicious activity—extremist rants	Authorities receive reports of an individual carrying out "violent" or "threatening" rants justifying terrorist attacks and implying the individual would like to participate. (e.g., Authorities investigate a person who routinely calls for "Jihad" against the U.S. government and who invites "trusted" individuals into secret meetings with him.)	Expressed or Implied Threat
Suspicious activity—smuggling-like behavior	Authorities investigate suspicious activity associated with smuggling contraband, typically onto an airplane or at a point of entry. (e.g., Authorities investigate a man at a border crossing who seems extremely nervous, repeatedly glances at the vehicle's trunk, and is unable to answer simple questions about his travel plans.)	Sector-Specific Incident for security checkpoints
Suspicious activity—suspicious documents found	Authorities discover documents that appear relevant to a terrorist plot. (e.g., site surveillance plans, false identification documents, or e-mail discussing a person's participation in a plot)	"Evidence" of Explicit or Implied Threats, Misrepresentation, or Observation/Surveillance depending on the content

The initial clues of the 68 thwarted plots are presented below by the source (**Figure 5**) and type (**Figure 6)** of clue. "Source" refers to the person or organization that initially observed and reported the clue—state or local law enforcement, federal law enforcement,[1] the intelligence community, or a member of the general public who voluntarily provides information to authorities (i.e., not already working as an informant). "Type" refers to the means by which the clue initially came to the attention of law enforcement, broadly categorized as investigations of crimes, reports of suspicious activity, reports of specific terrorist plots, or the discovery of associations with known or suspected terrorists.

Figure 5. Source of Initial Clues in Foiled Plots, 1999–2009



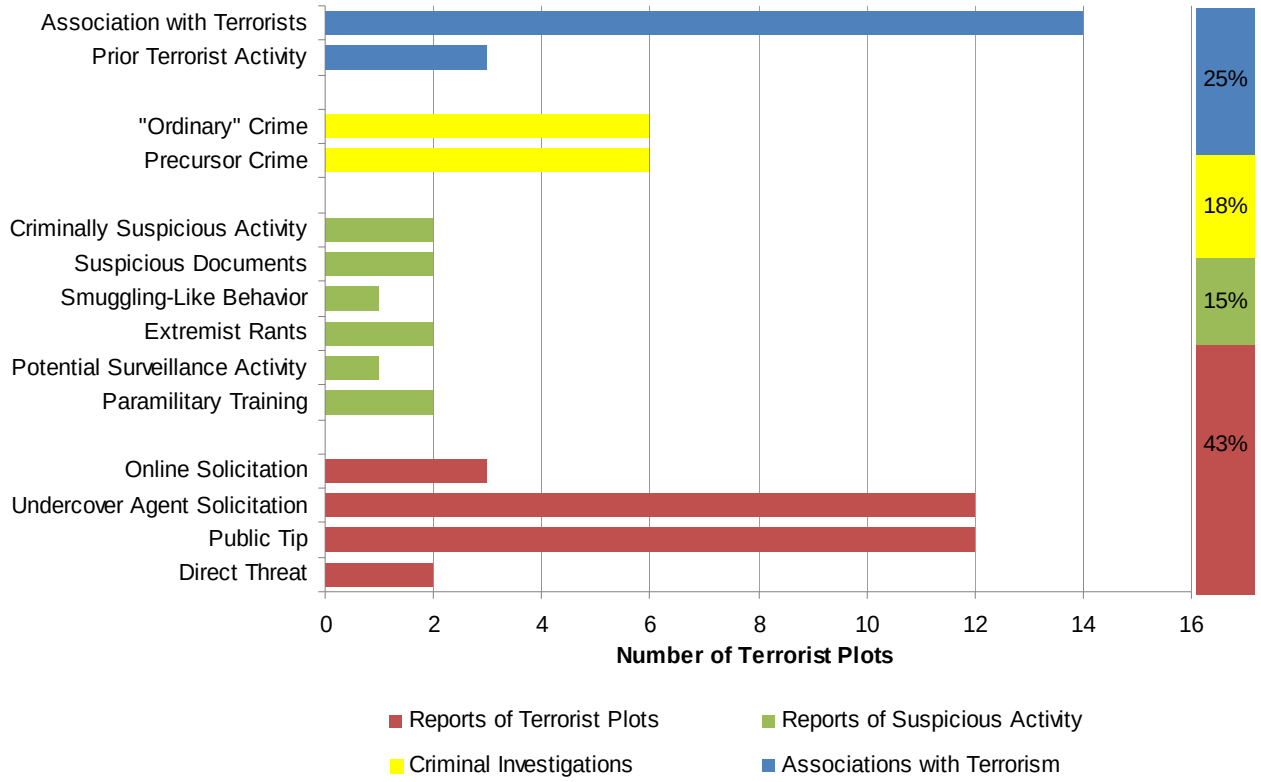
Our analysis indicates that law enforcement, assisted by the public, is generally the first line of defense in detecting terrorist plots. In over 80% of the foiled plots in our dataset, the initial clue came from law enforcement (20 federal cases and 15 state/local cases) or from public reporting (20 cases). By contrast, intelligence reporting was found to be the source of initial clues in just 13 cases (19%). As noted earlier, we acknowledge that the actual number of cases foiled by intelligence is likely higher. Nevertheless, the importance of the general public and state and local law enforcement in foiling terror plots is clear.

In **Figure 6**, we summarize the types of initial clues that ultimately foiled terrorist plots. In most cases (29 plots, 43%), the initial clue was a report of a specific plot. The vast majority of these reports (24 of 29 plots) were split between tips from the general public (12 cases) and

[1] We recognize that certain agencies (notably the FBI) perform both intelligence and law enforcement functions. Therefore, when categorizing the source of initial clues, we consider both the agency involved and the type of activities the agency was engaged in which produced the clue. For example, if the FBI discovers a plot during the course of its intelligence collection activities, such as phone or other communication intercepts authorized by the Foreign Intelligence Surveillance Act (FISA), the source is classified as "Intelligence." Similarly, if the FBI discovers a plot during the course of a criminal investigation, the source is classified as "Federal Law Enforcement."

would-be terrorists soliciting an undercover agent or informant (12 cases). In two cases, the plot was foiled after the perpetrator made a direct threat to their target. Only three plots were reportedly discovered through Internet monitoring activities that found suspects conspiring online to participate in terrorist activities, although we note that the open-source nature of our information may underestimate these types of activities.

Figure 6. Type of Initial Clues in Foiled Plots, 1999–2009



In 10 cases (15%), the initial clue came from a report of suspicious activity. The types of suspicious activities included criminally suspicious actions (2 cases), suspicious documents (2 cases), smuggling-like behavior (1 case), extremist rants (2 cases), and paramilitary training (2 cases). Only one case was identified in which the initial clue came from a report of possible surveillance activities, a somewhat surprising finding given the large amount of attention this type of pre-operational behavior has received.

Non-terrorism related criminal investigations also led to a significant number of plots being foiled (12 cases, 18%). In half of these (6 cases), investigations into precursor crimes (e.g., robbery, theft, counterfeiting) revealed the larger plot, and in the other half law enforcement came upon the plots “by surprise” while investigating unrelated “ordinary” crimes (e.g., parole violations, traffic stops). The link between the investigation of criminal or “suspicious” activity and terrorism was thus significant, thwarting nearly one in three identified terrorist plots overall.

Clues Triggering Full Investigations

The second step in foiling a terrorist plot is amassing enough evidence to warrant a full-scale investigation (generally associated with the legal standard of probable cause). Often, this evidence is found as a result of authorities responding to the initial clue. Sometimes, however, the initial clue itself is sufficient to launch a full-scale investigation. In other instances, a full investigation is launched when a connection to another ongoing investigation is discovered. **Table 2** describes the types of evidence that led to full-scale investigations in the 68 foiled plots we examined and maps them to the ISE SAR code equivalents.

Table 2. Descriptions of Clues Triggering Full Investigations

"Triggering" Clue	Description	ISE SAR Code
Initial Clues Sufficient to Launch a Full Investigation		
Details of plot from intelligence	Information provided from intelligence efforts is sufficient to launch a full investigation.	No equivalent
Details of plot from public tip	Information provided in a tip about a terrorist plot is sufficient to launch a full investigation.	Expressed or Implied Threats
Details of plot from solicitation	Information provided by group members soliciting an undercover informant or agent is sufficient to launch a full investigation.	Expressed or Implied Threats
Explicit threats from suspect	Suspect made written or oral threats sufficiently concerning to launch a full investigation.	Expressed or Implied Threats
Threatening behavior by suspect	Suspect's observed behavior is sufficiently concerning to launch a full investigation.	Expressed or Implied Threats
Evidence Collected from Investigating Initial Clues Used to Launch Full Investigation		
Search following SAR that is potentially terrorism-related	Adjacent search following a report of activity potentially related to terrorism finds evidence triggering a full investigation. Evidence could include attack plans, target surveillance reports or video, weapons stockpiles, explosives material, or detonator components.	Material Acquisition and Storage or Weapons Acquisition; may be other types, depending on materiel found
Search following criminal activity	Adjacent search investigating a previous crime or criminally suspicious activity finds evidence triggering a full investigation.	Material Acquisition and Storage or Weapons Acquisition; may be other types, depending on materiel found
Surveillance following SAR that is potentially terrorism-related	Surveillance following a report of suspicious activity finds evidence triggering a full investigation. This could include documentation (video, audio) of suspects meeting with informants or undercover agents to plot an attack or seek training/materiel to carry one out.	Typically Expressed or Implied Threats

(continued on next page)

Table 2. Descriptions of Clues Triggering Full Investigations (continued)

"Triggering" Clue	Description	ISE SAR Code
Confession during interrogation for a SAR that is potentially terrorism-related	Suspect confesses to a plot while being interrogated for activity potentially related to terrorism.	No equivalent
Confession during interrogation for criminal activity	Suspect confesses to a plot while being interrogated for a crime or criminally suspicious activity.	No equivalent
Links from Other Investigations ("Connecting the Dots")		
Links from a terrorism investigation	Suspects named in an initial clue are part of another terror-related investigation.	No equivalent
Links from intelligence	Suspects named in an initial clue previously appeared in intelligence reports or databases.	No equivalent

Figure 7 below provides a breakdown of the type of evidence that triggered full-scale investigations in the 68 foiled terrorist plots we identified.

Figure 7. Evidence Triggering Full-Scale Investigations in Foiled Plots, 1999–2009

In many of the plots examined (46%, 31 cases), the initial clue alone was sufficient to launch a full-scale investigation. However, the majority of plots (50%, 34 cases) required additional investigation or linking, demonstrating the importance of ensuring that initial clues are properly pursued after discovery.

Among the follow-up methods available to law enforcement, surveillance/undercover operations and searches following terrorism SARs proved especially fruitful. Together, these activities triggered full-scale investigations in 17 plots (25%). Equally important, however, were searches adjacent to criminal investigations (14 cases, 21%), in which the officers or agents involved thought they were investigating "ordinary" criminal activity, unaware that it was connected to terrorism. Examples of evidence discovered during these investigations include written plans to carry out an attack, surveillance reports or video, weapons stockpiles, and discovery of bomb components, such as explosives, explosive precursors, or detonators.

Although the media is filled with exhortations that U.S. intelligence and law enforcement agencies need to do a better job of "connecting the dots" (a somewhat ambiguous phrase describing the ability to find patterns or links across large databases that indicate a terrorist plot), our analysis suggests that this ability has been useful in foiling only a few terrorist plots (3 cases, 4%). We note again, however, that the open-source nature of our data undoubtedly underestimates the importance of these technological capabilities. Our results should therefore not be interpreted as implying that investments in these programs are unwarranted. Instead, they highlight the importance of more basic processes, such as ensuring that investigative leads are properly pursued, which unclassified reporting suggest have foiled an order of magnitude more cases (31 cases, 46%).

With respect to the *ISE SAR Functional Standard*, although Material Acquisition and Storage and Weapons Stockpiles events never constituted an initial clue, they provided some of the most frequent secondary clues (i.e., the evidence discovered during follow-on searches). Why reports of stockpiling or suspicious material have never led directly to foiling plots—even though weapons and explosive stockpiles are generally required to carry out a terrorist attack—is an open question.

Missed Opportunities to Prevent Terrorist Attacks

We have found references to initial clues that could have foiled plots in 7 of the 18 executed cases. In four of these cases, it appears that the initial clues were not fully pursued—the clue either was simply disregarded or was not forwarded to appropriate agencies. The following cases are examples of these missed opportunities:

- **9/11 Attacks**: As described in *The 9/11 Report* (9/11 Commission, 2004), the Central Intelligence Agency was aware that two of the hijackers had attended a "terrorism conference" in Malaysia and had traveled to the United States. However, information about the two suspects was not shared with the FBI or the Federal Aviation Administration in a timely manner. FBI Director Robert Mueller has also publicly acknowledged other missteps that could have likely prevented the attack, including

the failure to authorize the search of Mousaoui's computer in August, and the failure to follow up on requests to investigate suspicious individuals seeking flight training in Phoenix (Locy & Johnson, 2002).

- **2009 Attempted "Christmas Bombing" of Northwest Airlines Flight 253**: The attempted bomber's father reported to State Department officials concerns about his son's extremist views, recent disappearance, and possible travel to Yemen. This led to the creation of a file in the National Counterterrorism Center (NCTC) Terrorist Identities Datamart Environment (TIDE). But the record was not added to the Terrorist Screening Database (TSDB) because of a lack of specific information (DeYoung & Leahy, 2009; Lipton & Shane, 2009).
- **2009 Fort Hood Shootings**: Reportedly, the shooter had exchanged at least 18 e-mail messages with a radical Muslim cleric and terrorism supporter (Hess & Gearan, 2009). Screening of the messages by the FBI led to the decision that the exchange was explained by a research paper Hasan was writing (Cyr, 2009). This decision has been controversial, on the grounds that such extensive contacts with a known terrorism suspect should have been reported to the Army.
- **1999 Columbine High School Shootings:**[2] In 1998, almost a full year before the attack, an affidavit for a search warrant was issued for one shooter's home, based on a complaint that the shooter was bragging online about building bombs. Police later found a small bomb matching the online description near his home. However, the lead was somehow dropped, and the search was never carried out (Toppo, 2009).

In another three cases, the attackers were already under investigation or court supervision, but still managed to execute an attack:

- **2003 Attempted "Shoe Bombing" of American Airlines Flight 63**: French officials detected suspicious behavior at the perpetrator's point of departure (Paris), as he had paid for his ticket in cash, had no checked bags, and failed to answer all of their questions. However, an extensive screening did not find the explosives in his shoes, and he was allowed to board a flight the next day. The 1-day delay probably helped prevent the explosives from detonating (Elliot, 2002).
- **1999 Shooting Spree at the North Valley Jewish Community Center in Los Angeles**: The perpetrator had a known history of violent assaults, self-injury, and, fantasizing about violent attacks; he was additionally under parole supervision at the time of the shooting (Egan, 1999).
- **2009 Shooting at the Little Rock, Arkansas, Army Recruiting Office**: The shooter was under investigation by the FBI's Joint Terrorist Task Force after being detained in Yemen for possessing a fake Somali passport and other counterfeit documents (Dao & Johnson, 2009; Thomas, Esposito, & Date, 2009)..

[2] Although the Columbine shootings did not have a traditional political objective, there was a clear desire to terrorize as many people as possible, including a failed attempt to blow up the school prior to the shootings. As such, the Columbine shootings were included in the GTD, and thus in our analysis.

While it is obviously alarming that these attacks were carried out by individuals already under supervision/investigation, it must be noted that in one case (the “shoe bombing” attempt) the investigation probably helped foil the execution, and in the other two cases (shootings), the attacks appear to have been fairly impulsive, making them extremely difficult to detect.

Conclusions and Recommendations

This study has generated findings relevant to detecting and preventing terrorism. Results demonstrate that, while the threat from AQAM groups is significant, other groups should not be ignored. In total, less than half of identified plots were sponsored or inspired by AQAM. The majority of plots outside of AQAM’s ideology have been from persons with white supremacist or antigovernment/militia ideologies. Of note, attacks from non-AQAM groups rivaled AQAM-related plots in many respects, including a greater likelihood of involving chemical or biological weapons. In addition, a large majority of plots have been conducted by single actors (“lone wolves”) and small groups. Lone wolf plots have also been the most successful, reaching execution more than twice as often as plots by groups.

A second category of findings concerns the initial clues that helped support additional investigation and dedication of law enforcement resources. Perhaps most important was the finding that over 80% of initial clues came from law enforcement (roughly split between federal and state/local) or from the general public. By contrast, intelligence reporting provided initial clues in 19% of plots, although the open-source nature of our data likely underestimates its actual importance. Analysis also revealed that in most instances, the initial clue was a report of the plot, either from a member of the public knowledgeable of the plot or from a would-be terrorist soliciting an undercover agent.

Finally, our results reiterate the importance of both fully investigating potential leads and recognizing signs of potential terrorist activity during the course of routine criminal investigations. Investigations into seemingly unrelated criminal activity, together with suspicious activity reports, led to the discovery of initial clues in nearly a third of the foiled terrorist plots identified. Furthermore, in half the foiled plots examined, law enforcement had to pursue initial clues further to establish enough evidence to launch a full-scale investigation and, in four of the 18 executed plots examined (including 9/11), clues that could have thwarted plots were not fully investigated or shared.

Study Recommendations

Recognize the importance of law enforcement and the general public in preventing attacks, and support them through investments in education and reporting. More than four in five foiled terrorist plots were discovered via observations from law enforcement and the general public. Accordingly, many larger jurisdictions have instituted suspicious activity

reporting systems. For example, the Los Angeles Police Department (LAPD) has the iWatchLA community awareness program, encouraging the public to report suspicious activity, and New York has the New York Police Department (NYPD) Shield program, which partners law enforcement with private industry (LAPD, 2010; NYPD, 2010). However, for these programs to work as intended, it is crucial that stakeholders are properly trained. Failure to do so may result in an inordinate number of low-value tips for which resources must be devoted or a failure to recognize behavior that is important. In this study, suspicious activity reports most commonly associated with an actual plot included the following:

- Reports of a person or group conspiring to carry out an attack, either from the general public or from an informant. These were the most common types of initial clues.
- Persons seeking paramilitary training. These included persons trying to train within the U.S., as well as persons traveling (or planning to travel) overseas to receive training.
- Persons conducting surveillance of a possible target.
- Behavior associated with smuggling, typically of weapons or explosives.
- Criminal activity intended to raise money, such as thefts, frauds, and robberies.

Continue to investigate AQAM, but do not overlook other types of terrorist groups, and pay particular attention to "lone wolves." Most U.S. terrorist plots have not originated with AQAM. Although a large proportion of would-be terrorists have been inspired by AQAM, white supremacist and anti-government/militia ideologies have also motivated a large proportion of terrorist plots. Others have been inspired by animal rights, anti-abortion, and personal beliefs to commit violent attacks. Nor does AQAM have a monopoly on the most destructive types of attacks, as evidenced by the fact that the majority of CBRN attacks were outside of AQAM. There was also a strong trend that most attacks were committed by single actors ("lone wolves") or small groups of people. This trend is particularly noteworthy as lone wolves were found to be almost twice as likely as groups to successfully execute attacks.

Ensure processes and training are in place that enable law enforcement personnel to identify terrorist activity during routine criminal investigations. Nearly one in five thwarted plots were foiled "accidentally" as a result of investigations into seemingly unrelated crimes. Law enforcement personnel need proper training and the necessary checks and balances within their agencies to ensure that they identify and follow-up on situations where an investigation of an ordinary crime may be potentially terrorism-related.

Work to establish good relations with local communities and avoid tactics that might alienate them. Of the 68 foiled plots examined, approximately 40% were thwarted as a result of tips from the public or reports by informants. Acquiring information from these sources depends on the ability to establish good relationships between law enforcement and communities with persons in or near radical movements, an ability that is jeopardized by indiscriminately targeting individuals and groups due to their race, ethnicity, religion or ideology.

Support "quality assurance" processes and systems to ensure that initial clues are properly pursued and findings shared. For cases in which initial clues did not immediately trigger a full investigation, doing the basics of investigating leads and sharing information across agencies led to foiling the vast majority of plots. Proper training, information technology, and oversight are needed to support the coordination and "quality assurance" of pursuing leads and sharing of findings. Specifically, law enforcement must ensure (1) leads are investigated, whether through interviews, contact with informants or agents, or searches, as appropriate; (2) relevant information is shared with other agencies responsible for the investigation of terrorism suspects and those responsible for safeguarding access to U.S. points of entry and aircraft; and (3) investigations are escalated when sufficient evidence has been found.

Expand the ISE SAR Functional Standards to include reports beyond traditional SARs. In a majority of the foiled plots examined, the initial clue came from a public/informant tip or a discovery during what was initially considered a "routine" criminal investigation. These types of clues are at most indirectly referenced in the ISE SAR Functional Standard. Adding them would permit the ISE SAR Functional Standard (and Nationwide SAR Initiative) to be used for all major types of reports associated with state and local law enforcement discovering terrorist activity, significantly expediting information sharing and subsequent investigations.

References

9/11 Commission (2004). *Final report of the national commission on terrorist attacks upon the United States.* Washington, DC: National Commission on Terrorist Attacks

Ackerman, G., & Tamsett, J. (2009). *Jihadists and weapons of mass destruction*. Boca Raton, FL: CRC Press.

Bergen, P., & Hoffman, H. (2010) *Assessing the terrorist threat: A report of the Bipartisan Policy Center's National Security Preparedness Group*. Bipartisan Policy Center. Retrieved September 10, 2010 from http://www.bipartisanpolicy.org/sites/default/files/Final%20NSPG%20Threat%20Assessment%20Report%20Sept%202010%20report%20w%20cover.pdf

Brady, H. E., & Collier, D. (Eds.) (2004). *Rethinking social inquiry: Diverse tools, shared standards*. Lanham, MD: Rowman and Littlefield.

Carafano, J. (2009, December 28). *Re-learning the lessons from the thwarted Detroit airline bombing*. Heritage Foundation web blog. Retrieved April 7, 2010, from http://www.heritage.org/Research/Reports/2009/12/Re-Learning-the-Lessons-from-the-Thwarted-Detroit-Airline-Bombing

CBS News. (2010, February 4). *Alleged Christmas bomber said to flip on cleric*. Retrieved June 26, 2010, from http://kdka.com/national/Umar.Farouk.Abdulmutallab.2.1471361.html

Cyr, E. (2009, November). *FBI reassessing past look at Fort Hood suspect*. Associated Press. Retrieved February 10, 2010 from http://www.wusa9.com/news/Fort_Hood/story.aspx?storyid=93462&catid=282

Dao, J., & Johnson, D. (2009, June 3). Suspect in soldier attack was once detained in Yemen. *New York Times*. Retrieved February 9, 2010 from http://www.nytimes.com/2009/06/04/us/04recruit.html?_r=1&ref=us

DeYoung, K., & Leahy, M. (2009, December 28). Uninvestigated terrorism warning about Detroit suspect called not unusual. *Washington Post*. Retrieved February 9, 2010 from http://www.washingtonpost.com/wp-dyn/content/article/2009/12/27/AR2009122700279.html

Egan, T. (1999, August 14). Racist shootings test limits of health system, and laws. *New York Times*. Retrieved February 8, 2010 from http://www.nytimes.com/1999/08/14/us/racist-shootings-test-limits-of-health-system-and-laws.html?sec=&spon=&pagewanted=all

Elliot, M. (2002, February 16). The shoe bomber's world. *Time*. Retrieved February 9, 2010 from http://www.time.com/time/world/article/0,8599,203478-1,00.html

Goldthorpe, J. H. (1997). Current issues in comparative macrosociology: A debate on methodological issues. *Comparative Social Research, 16*, 1–26.

Hess, P., & Gearan, A. (2009, November 21). Levin: More e-mails from Ft. Hood suspect possible. *Associated Press*. Retrieved February 9, 2010 from http://abcnews.go.com/Politics/wireStory?id=9143884

Hoffman, B. (2003). Al Qaeda, trends in terrorism, and future potentialities: An assessment. *Studies in Conflict & Terrorism*, *26*(6), 429–442.

Kelling, G. L., & Bratton, W. J. (2006). *Policing terrorism*. New York: Manhattan Institute.

Lieberson, S. (1991). Small N's and big conclusions: An examination of the reasoning in comparative studies based on small number of cases, *Social Forces*, *70*(2), 307–20.

Lipton, E., & Shane, S. (2009, December 27). Questions on why suspect wasn't stopped. *Washington Post*. Retrieved February 9, 2010 from http://www.nytimes.com/2009/12/28/us/28terror.html

Locy, T. & Johnson, K. (2002, May 29). FBI missed 9/11 clues, director says. *USA Today*. Retrieved September 17, 2010 from http://www.usatoday.com/news/washington/2002/05/30/fbi-missed-clues-usat.htm

Los Angeles Police Department (LAPD). (2010). *iWatchLA: iWatch, iReport, I keep us safe*. Retrieved June 26, 2010, from http://lapdonline.org/iwatchla

Mahoney, J., & Rueschemeyer, D. (Eds.) (2003). *Comparative historical analysis in the social sciences*. New York: Cambridge University Press.

Memorial Institute for the Prevention of Terrorism. (2007). *Terrorism warnings* (poster). Retrieved July 1, 2010, from http://www.mipt.org/Websites/mipt/Images/media/Terrorism%20Warnings%20Push%20Card%20-%20New.pdf

National Strategy for Information Sharing (NSIS). (2007, October). *Information sharing: Success and challenges in improving terrorism-related information sharing*. Retrieved April 5, 2010, from http://georgewbush-whitehouse.archives.gov/nsc/infosharing/NSIS_book.pdf

New York Police Department (NYPD). (2010). *NYPD Shield: Countering terrorism through information sharing*. Retrieved June 26, 2010, from http://www.nypdshield.org/public/

Program Manager for the Information Sharing Environment. (2009, May 21). *Information sharing environment functional standard for suspicious activity reporting, Version 1.5*, ISE-FS-200. Retrieved June 24, 2010, from http://www.niem.gov/pdf/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued.pdf

Sageman, M. (2008). *Leaderless Jihad: Terror networks in the twenty-first century*. Philadelphia, PA: University of Pennsylvania Press.

Smith, B. L., Damphousse, K. R., & Roberts, P. (2006). *Pre-incident indicators of terrorist incidents: The identification of behavioral, geographic, and temporal patterns of preparatory conduct*. Washington, DC: National Institute of Justice. NIJ Grant 2003-DT-CX-0003. Retrieved July 1, 2010, from http://www.ncjrs.gov/pdffiles1/nij/grants/214217.pdf

Study of Terrorism and Responses to Terrorism (START). (2010, May). *Global Terrorism Database: GTD variables and inclusion criteria*. Retrieved July 9, 2010, from http://www.start.umd.edu/gtd/downloads/Codebook.pdf

Suspicious Activity Report (SAR) Support and Implementation Project. (2008). Findings and recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project. Retrieved April 5, 2010, from http://iwitnessvideo.info/files/mccarecommendation-06132008.pdf

Thomas, P., Esposito, R., & Date, J. (2009, June 3). Recruiter shooting suspect had ties to extremist locations: Investigators probing attack to determine whether shooting suspect acted alone. *ABC News*. Retrieved February 9, 2010 from http://abcnews.go.com/Politics/story?id=7732467&page=1

Toppo, G. (2009, April 14). 10 years later, the real story behind Columbine. *USA Today*. Retrieved February 8, 2010, from http://www.usatoday.com/news/nation/2009-04-13-columbine-myths_N.htm

Appendix A. Description of Variables and Coding Scheme

The full dataset is available upon request.

Variable	Description
Identifying information	• Unique ID • Short name for the plot • Date plot was executed or thwarted with an arrest • Location of plot/intended target • Whether the plot reached execution
Plot description	Text field describing names, dates, places, and a brief summary of the allegations/convictions
Group ideology/motivation	Structured field describing the group's ideology: • Left (broadly "Leftist" ideologies besides those related to environmental or animal rights causes) • Right (anti-liberal beliefs distinct from militia/anti-government and White supremacist ideologies) • Anti-Muslim • Animal rights • Anti-abortion • Militia/Anti-government (groups rejecting federal governmental authority) • Al Qaeda and Allied Movements (AQAM) • AQAM-inspired (persons who are motivated by AQAM but have no direct connections with an AQAM group; commonly categorized as "homegrown terrorists") • White supremacist (includes both traditional white supremacist and neo-Nazi groups) • Unknown/Non-ideological (persons motivated by unknown ideological reasons or for reasons not clearly ideological but still intended to terrorize a particular community, e.g., the attacks at Columbine
Group size	Structured field indicating the composition of the plotter(s): • Single Individual ("lone wolf") • A small unorganized group (a collective effort with no formal structure) • A small organized group (a collective effort that has a name and a formal structure) • A large group

Variable	Description
Type of target	Structured field describing the type of target: • Abortion (clinic or doctor) • Aircraft (always a commercial jet liner) • Airport • Bank • Bridge • Bus • Community center • Convention (such as the Republican National Convention) • Gas station • Gas storage tanks (natural gas storage tanks) • Government executive (targeted for assassination) • Government building • Home/House • Judicial personnel (judges or law enforcement officials targeted for assassination) • Military base • Power grid (can be power plants or transmission lines) • Religious building (examples have included churches and mosques) • School • Scientist (targeted for assassination) • Shopping mall • Skyscraper • Street (refers to an attempt to shoot or bomb a crowd of people on a street) • Train • Unknown
Nature of attack	Structured field labeling the plot as one of the following: • Chemical, biological, radiological, or nuclear (CBRN)—plots to use weapons of mass destruction in some form • Conventional—plots to use conventional means of attack, such as bombings or shootings to kill people indiscriminately • Targeted—plots to assassinate or injure specific individuals
Type of initial clue	Structured field for the type of the initial clue that tipped off law enforcement (see Table 1 for a full list of the variables used)
Source of initial clue	Structured field for where the clue came from: • Intelligence efforts • Federal law enforcement • State/local law enforcement • Tips from the general public (unsolicited)

Variable	Description
Investigation progression	Text field describing how investigators found sufficient evidence to launch a full investigation
“Triggering” clue	Structured field for the type of evidence that led to a full investigation (see Table 2 for a full list of the variables used)
End result	Text field describing the final outcome of the plot and actions taken against plotters/attackers
Sources	Text field listing the references used in the case