RESEARCH BRIEF

Institute for Homeland Security Solutions
Applied research • Focused results

May 2009

Building on Clues: Methods to Help State and Local Law Enforcement Detect and Characterize Terrorist Activity

Project Leads

John Hollywood, PhD, RTI International Kevin Strom, PhD, RTI International

Mark Pope, MS, RTI International

Statement of Problem

State and local law enforcement agencies are important partners in preventing terrorism, with responsibilities that include identifying and investigating local terrorist threats and protecting potential targets from attack. To meet these responsibilities, law enforcement must develop better ways to find and analyze pieces of information that could spotlight potential terrorist activity. However, to date, the federal government has provided limited guidance to law enforcement agencies on how to collect, analyze, and disseminate data that could be used for counterterrorism purposes. Such data could include information that is routinely collected by law enforcement, such as crime incident and suspicious activity data. While state and local law enforcement agencies are involved in fusion centers that seek to blend data from different sources, the Congressional Research Service (CRS) has noted a general lack of true data integration going on in fusion centers, as well as a shortage in training for law enforcement

analysts (Masse, O'Neil, & Rollins, 2007). Some guidelines have been presented on fusion center capabilities (DOJ and DHS Global Justice Information Sharing Initiative, 2005, 2008), information sharing (DOJ Bureau of Justice Assistance, 2003), and law enforcement analytic standards and data sources (International Association of Law Enforcement Intelligence Analysts, 2004). Yet, there has been limited direction on specific methods, tools, and data sources that law enforcement agencies can use for counterterrorism purposes (Hoyt, 2008).

This research brief will focus on describing methods for finding and analyzing information indicating potential terrorist activity. Within this context, we address two central challenges:

- how to find initial "clues" or "cues"—information indicative of potential terrorist activity, especially if these pieces of information are obscured within large volumes of data across disparate data sources and formats, and
- as part of a follow-up investigation, how to collect additional information to determine whether an attack really is being planned, and if so, how to characterize the plot.

While our focus is on the role of state and local law enforcement agencies in terrorism prevention, the information presented is also relevant to federal agencies tasked with protecting U.S. citizens and infrastructure.

Background

Soon after the 9/11 attacks, some officials recommended that "large-scale" data mining be used as a method for identifying potential terrorist activity (Edelstein, 2003). At its core, data mining involves finding previously unknown patterns or relationships in large databases through the use of automated algorithms (Palace, 1996). The idea was that agencies could assemble numerous types of data on individuals (such as commercial data consolidators' personal dossiers, credit card information, and airline passenger data), trawl the resulting data sets, and find patterns of activity that would identify potential terrorists. The best example of this approach is the now-defunct Total Information Awareness (TIA) program, which attempted to assemble a federation of numerous databases containing personal information (including transactional and biometrics data) from which to detect patterns of activity related to terrorism (Associated Press, 2003; Markoff, 2002; Stevens, 2003).

However, two principal concerns about large-scale data mining quickly were raised. The first concern was that analyzing personal records without cause for any prior suspicion would violate individuals' privacy (Executive Committee on ACM Special Interest Group on Knowledge Discovery and Data Mining, 2003). Civil liberty advocates were alarmed at the amount of personal data that TIA and other proposed systems relied on, and advocates have felt that these methods represent a dramatic escalation of government intrusion into the lives of U.S. citizens (Electronic Privacy Information Center, 2005). The second concern was that any large-scale data mining approach would generate so many errors that the results would be operationally useless. Because data mining algorithms rely on previously known examples of

terrorist activity to develop predictive models, there is a high likelihood that some proportion of incoming records will be classified incorrectly. False positives could consume tremendous resources in tracking down false leads, even if the error rate is low. For example, for a database containing records on 200 million individuals, a false-positive rate of 1% would lead to flagging 2 million individuals as potential suspects (Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, 2008; McCullagh, 2008).

While concerns regarding privacy and reliability must be considered, past experiences have shown that there is value in the underlying philosophy behind the proposed data mining approaches—identifying and analyzing data describing suspicious and criminal behaviors. The Sidebar in this research brief summarizes 25 recent disrupted terrorist plots reported by the media (distinguishing convictions from accusations), describing both the reported objectives of the plots and the initial clues leading to their foiling. Although the specific details vary greatly*, 80% of the initial clues in these cases came from properly observing, reporting, and acting on unusual behaviors,* while only 20% came from traditional intelligence efforts. These clues then triggered investigations that led to the unraveling of the various plots.

Thus, a framework for identifying and characterizing potential terrorist activity can be divided into two phases. The first phase consists of finding and analyzing the initial clues indicating terrorist activity may be in progress (emphasizing that the "may" really means "probably not, but could be"). The second phase consists of conducting a follow-up investigation, using the initial clues as starting points. The core of the second phase requires growing a network of information—including people, locations, assets, incidents, and their relationships—around the initial clues. This network provides the information required to assess whether a terrorist plot is in progress, and, if so, how to characterize the nature of the plot. Both phases face challenges, which are described in more detail below

Challenges in Finding Initial Clues

As shown in the Sidebar, the types of suspicious activity reported to law enforcement as initial clues can vary widely. In the most serendipitous cases, law enforcement literally had plots fall into their laps, such as in the "Millennium Plot" case, in which a routine vehicle search by a U.S. Customs agent discovered bomb components. In other cases, however, the initial clues were far more indefinite.

Broadly speaking, there are three types of initial clues:

- Discoveries adjacent to law enforcement investigations. These can be discoveries made during routine law enforcement activities, as in the case of the plot to bomb a Florida Islamic center, in which police discovered weapons and plot details while responding to a domestic dispute call. These discoveries can also result from efforts to monitor people and activities known to be of interest; for example, the "Liquid

Explosives Plot" to destroy transatlantic airlines was discovered as part of police efforts to monitor a person of interest (in this case, searching the suspect's luggage).

- Direct reports that a person or group is planning an attack. Examples include reports from an informant, a telephone or e-mail tip that a person is planning a terror attack, or an investigative report. Reports from intelligence agencies describing the threat posed by a person or group can also be included in this category.
- Reports on suspicious behavior that may pertain to terrorist activity. The Memorial Institute for the Prevention of Terrorism has found that the following types of activity "consistently" precede a terrorist attack: acquiring explosives, weapons, or chemical precursors; conducting site surveillance (especially taking video, pictures, or notes of private areas and structural components of potential targets); conducting supply staging, as indicated by abandoned vehicles or concealed packages; carrying out "odd activity" (most commonly involving chemical odors or stains); and leading criminal activity to finance the attack (Memorial Institute for the Prevention of Terrorism, 2007). Data sources for suspicious activity include call-in or e-mail tips, police incident and field interview reports, 911 calls for service, suspicious financial transactions, and suspicious travel reports. Some of the reports are formerly labeled as suspicious activity reports (SARs) potentially related to terrorist activity. Other events are obscured in larger data sources reporting on more innocuous activity, including "ordinary" forms of crime (e.g., loitering, trespassing, theft, fraud, robbery).

There are multiple types of challenges involved in both the initial reporting of incidents and in recognizing the significance of particular events. These include challenges related to (1) people (i.e., how well individuals involved are trained to recognize, handle and share the reports of suspicious activity), (2) process (i.e., how well processes exist to capture and analyze the reports), (3) organization (i.e., how well the organizations involved are structured to capture and analyze the reports), and (4) technology (i.e., how effective information technology methods and tools are at filtering, storing and analyzing the reports).

With respect to "people," training of both law enforcement personnel and the general public is critical if suspicious activity reports are to be made in the first place. The importance of training is evidenced by the "Millennium Plot" to blow up Los Angeles International Airport, in which an alert border agent picked up on the suspect's suspicious behavior, helping lead to his detainment (WGBH Educational Foundation, 2008). Conversely, prior to the 2002 Paradise Hotel bombing in Kenya, a farmer saw the vehicle that would carry out the attack and noted the occupants behaving suspiciously, but he did not know of any way to report the activity (Wax, 2002). More recently, in the 2008 Mumbai attacks, fishermen reported the arrival of the terrorists to local police, describing them as foreign trespassers who told them to "mind their own business," but the local police did not respond (Moreau & Mazumdar, 2008). Training must be discriminating, teaching both examples of genuine suspicious activity and examples of activity that may seem suspicious but is not, such as explaining differences between tourists taking photos and actual instances of site surveillance. The general public also must be given clear directives on how to report suspicious activity.

Even when reports are made, process and organizational shortfalls can lead to a lack of recognition of the significance of these events. For example, it has been reported that the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) failed to share information that two men with terrorist connections had entered the United States. These two individuals, Khalid al-Midhar and Nawqa Alhazmi, went on to help carry out the 9/11 attacks (Johnston, 2003). Similarly, FBI field offices made several pre-9/11 reports of suspicious activity by students at U.S. flight schools, but these reports did not trigger further investigations (Shenon, 2002).

Process and organizational measures also are needed to ensure proper responses to different types of reports. The response to finding a car full of bomb components must be very different than the response to someone observed videotaping structural elements of a bridge; in the latter case, although there is some cause for suspicion, the individual is likely to be innocent of any wrongdoing.

The final challenge area related to the reporting and prioritization of potential terrorist activity is technology. Technology itself cannot stop a terrorist attack, but it can play a key role in managing data efficiently and in filtering and analyzing incoming reports. Because the volume of data that must be filtered often exceeds human capabilities (for example, there are millions of 911 calls per year in a major urban area), automated tools are needed to identify, link, and prioritize cases of interest. One of the most pressing problems that law enforcement agencies face is understanding what current data filtering and searching tools can do and how these tools can best be tailored to fit into their operational analysis processes (Hoyt, 2008).

As an example of how technological tools and methods might help, there are many types of SARs that law enforcement personnel encounter that do not have formal labels tying them to terrorism. These include 911 calls for service, nonemergency calls to police (e.g., calls to 311 systems), and private security “suspicious activity” reports broadly linked to crime (e.g., trespassing or theft). While these reports may include instances of behavior related to terrorism, there are few procedures in place to recognize and report them as such. For example, if 911 calls are made on consecutive days concerning an individual taking photos on a bridge overpass, but no formal police report is generated from these calls, it is highly unlikely that the pattern of these events will ever be recognized manually. In these situations, technological tools could be of great help in finding and linking relevant records.

Some progress has been made in filtering large amounts of data by identifying descriptive data indicative of terrorism-relevant records. One approach is to focus on fields and keywords describing the time, space, and nature of suspicious incidents to find groups of incidents possibly indicating terrorist activity (McCue, 2006). This approach has been used to find potential target surveillance and probe reports in 911 call databases and to assess risks to city landmarks and infrastructure (Hollywood, Strom, & Pope, 2008).

Technology also can serve as a “signal booster,” helping to further discriminate between genuinely suspicious incidents and incidents that, while atypical, are not cause for concern.

For example, one can look for trends and patterns in activity over time—finding multiple instances of individuals videotaping structural elements of the bridge, as well as trespassing on the bridge, heightens suspicion. Similarly, finding multiple instances of questionable shipments on bills of lading by a single company heightens suspicion.

The key feature of these uses of technology is that they are highly focused. While they may access very large databases (e.g., 911 calls-for-service databases), the queries employed return only small numbers of records meeting precise criteria relevant to certain kinds of suspicious activity. This approach is in sharp contrast to the blunderbuss approach used in large-scale data mining concepts.

Challenges in Conducting Subsequent Investigations

Once an initial clue (or clues) warranting follow-up action has been discovered, the subsequent investigation is a recursive process—finding the initial clue helps law enforcement agencies find associated people, events, and assets, which, in turn, leads to finding still more associated people, events, and assets. As the additional information is discovered, investigators assess the information, developing and testing hypotheses about whether there is a terrorist plot in progress, and if so, about the nature and extent of the plot (Hollywood, Snyder, McKay, & Boon, 2004). The overall approach has been compared to the types of activities law enforcement investigators would perform to track down a fugitive, as well as the social network supporting the fugitive (Jonas & Harper, 2006).

Methodologies for conducting these investigations appear to be more mature than methods for finding the initial clues. Because there are persons of interest with names and other personally identifying information to be investigated at this stage, querying transactional data about the suspects—phone directories, financial transactions, phone transactions, travel transactions, activity reports—is highly relevant to growing a larger network around the initial clue (Krebs, 2008). Given the fairly low rate of initial clues triggering investigations and the online access to many transactional databases, it is feasible (albeit not ideal) to run such investigations manually. Furthermore, state, local, and federal agencies have conducted joint planning and exercises in which they have built out networks around a suspected terror plot, given a strong lead, focusing on the information sharing and coordination needed to follow up on discovered persons and events (Harris, 2007).

Analytic approaches in this phase are largely centered around social network analysis (SNA), the discipline “focused on uncovering the patterning of people’s interactions” (Freeman, 2008). SNA is principally focused on relationships between people. Example applications include ways to determine who are the “most important” and “most in the know” in a social network. The idea being that capturing and questioning these individuals would do the most organizational damage to the group (Krebs, 2002). Network analysis for counterterrorism typically extends SNA to include “entities” such as organizations, events, assets, locations, financial transactions, and communications (phone calls, e-mails) needed to reflect what is

known about a specific group. In either case, the principal output is a network graph or "link chart" representing the entities as nodes and relationships as links. Geospatial maps showing the locations of the entities are also valuable. Link charts and maps can be drawn manually using Microsoft Office tools to track entities and links and draw diagrams or can be created using specialized link charting and geospatial analysis software (Police Foundation Crime Mapping Laboratory, 2004). Network analysis has been further extended to support agent-based modeling to predict network efficiency and performance given changes to relationships (Carley, 2003). There are also analysis tools to scan network data to find previously hidden relationships between the nodes, such as individuals using similar aliases (Zetter, 2002).

Still, some challenges do remain related to the processing and analysis of data as part of subsequent investigations. First, training and processes need to support smooth transitions from low levels of suspicion (most initial clues) to high levels of suspicion (up to arrests). Investigators must carefully assess what sorts of collection efforts are warranted and permitted at each stage of the investigation, from initial efforts to court-ordered searches and, finally, to arrests. The initial clues also need to be taken into account. Second, despite significant efforts on information sharing, organizational barriers between agencies remain. Many of these barriers are in place to protect individuals' privacy, as well as to protect data security and integrity; the issue is to design processes and structures that best permit needed information sharing, while maintaining safeguards.[1]

With respect to technology, analysts must collect and enter data into social network analysis tools manually, which can be a labor-intensive, time-consuming, and error-prone process. This has led to interest in automated tools that parse text reports and articles across multiple repositories to build entity networks. Accuracy, however, can be a significant problem because a tool can easily take a statement such as "The victim was shot on Alabama St." and turn it into the entity network [State of Alabama] → shot → [Victim]. An alternate approach is to demonstrate to analysts which entities are statistically associated with an initial entity of interest, without attempting to formally determine the relationship (Saffron Technology, 2008).

Synthesis

Approaches to conducting investigations following initial clues appear to be maturing. Network analysis tools are commonly available. Federal, state, and local authorities develop plans and conduct exercises to jointly investigate possible plots once an initial lead has been provided. The principal challenge is to continue building on the progress to date.

[1] For discussions of data privacy issues relevant to the Department of Homeland Security (DHS), see DHS Privacy Office. (October 10, 2008). *The Privacy Office of the U.S. Department of Homeland Security.* Retrieved January 28, 2009, from http://www.dhs.gov/xabout/structure/editorial_0338.shtm.

However, approaches to find the initial clues have made much less progress. Initial post-9/11 experiments in using wholesale data mining of personal information databases quickly ran into fundamental privacy and accuracy barriers. While much has been done to provide for the collection and sharing of relevant data through the creation of fusion centers and information-sharing standards, less has been done to develop methods that support the cooperative filtering and analysis of the data. Improving capabilities to find initial clues is more a matter of improving analytic processes, structures, and training than it is of technologies. A secondary need is to examine the large number of existing data management, filtering, query, and analysis tools available to law enforcement to determine how they might be best employed and how they can be improved.

Future Directions

We recommend that future research proceed in several directions. First, work should be conducted to improve interorganizational processes and methodologies for processing and analyzing the various types of suspicious activity reports that may provide initial clues. This work should include (1) developing training material that more precisely characterizes different types of activity of interest, (2) developing processes for handling reports of varying degrees of interest (from “probably not, but could be” through “plot discovered”), and (3) developing methods for filtering data to isolate records most likely associated with various types of potentially terrorist-related activity.

Second, there should be an evaluation of existing processing and analysis tools to identify those applications that provide the best operational value for counterterrorism. This should include a focus on tools and approaches that can help identify the reports of genuine concern obscured within large volumes of data. In addition, tools should be identified that do not require the purchase of additional expensive software or extensive training for end users. This evaluation of analysis tools should take place in partnership with state or local agencies or fusion centers.

The result of these projects should be a guide describing practical analysis processes and methodologies for law enforcement analysts with counterterrorism responsibilities, both in fusion centers and in state and local police departments. This guide should focus on user-friendly methodologies that require limited technical training, are relatively inexpensive, and provide operationally actionable results. The guide should describe the organizational structures and processes needed to employ the methodologies. The guide should also describe when and how to use particular computing tools to address specific analysis needs. As appropriate, the guide should also include simple tools (such as Microsoft Office tools and macros) to help automate some of the most valuable approaches.

Contact Information

John S. Hollywood

RTI International

3040 Cornwallis Road

Research Triangle Park, NC 27709

jhollywood@rti.org

John S. Hollywood is an operations researcher with RTI, where he conducts research on data mining and predictive analysis for law enforcement and homeland security purposes. He also conducts research on the design and management of complex policy solutions, primarily in the area of information technology. He has developed a concept for finding hidden terror threats by analyzing and detecting unusual behavior (published in *Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior*) and a concept for managing information networks to satisfy the needs of end users. Dr. Hollywood has a PhD in operations research from the Massachusetts Institute of Technology. Prior to joining RTI, Dr. Hollywood worked for the RAND Corporation.

Kevin J. Strom is a criminologist with RTI. His research interests include studying law enforcement responses to community violence and interagency coordination in response to terrorism. Dr. Strom has led terrorism-related projects for the National Institute of Justice (NIJ), including a study that examined interagency coordination and response to the July 2005 terrorist attacks in London. He also led the recently completed NIJ-funded project on which RTI collaborated with the Washington, D.C., Metropolitan Police Department to examine whether suspicious activity reports in 911 data can be analyzed for terrorism prevention. He has a PhD in criminology from the University of Maryland, College Park. Prior to joining RTI, Dr. Strom was employed with the Bureau of Justice Statistics.

Mark W. Pope is a research analyst in RTI's Crime, Violence and Justice Program. He conducts research in the areas of prisoner reentry, law enforcement, homeland security, and violence prevention. His research interests include using information technology to develop data-driven solutions for crime, violence, and terrorism. He recently worked on an NIJ-funded project that examined 911 calls-for-service data to identify potential instances of terrorist surveillance. He has an MS in information science from the University of North Carolina at Chapel Hill.

References

Ankarcrona, A. (2008, December 22). Five found guilty of plotting to kill Fort Dix soldiers. *CNN*. Retrieved January 12, 2009, from http://www.cnn.com/2008/CRIME/12/22/fortdix.case/.

Associated Press. (2003, September 25). Pentagon's "Terror Information Awareness Program" will end. *USA Today*. Retrieved November 20, 2008, from http://www.usatoday.com/news/washington/2003-09-25-pentagon-office_x.htm.

Associated Press. (2004, August 6). Cops: Chicago man had bomb plot. *Fox News*. Retrieved January 12, 2009, from http://www.foxnews.com/story/0,2933,128156,00.html.

Associated Press. (2006a, April 13). Anti-government white supremacist guilty. *Boston.com*. Retrieved January 12, 2009, from http://www.boston.com/news/nation/articles/2006/04/13/anti_government_white_supremacist_guilty.

Associated Press. (2006b, September 1). U.S. judge schedules closed hearing to discuss classified information in terrorism case. *International Herald Tribune*. Retrieved January 12, 2009, from http://www.iht.com/articles/ap/2006/09/01/america/NA_GEN_US_Terrorism_Closed_Hearing.php.

Associated Press. (2007, December 14). 2 plead guilty in Southern California terror plot: Suspects accused of plotting attacks on Southern California military and Jewish targets. *WCBSTV.com*. Retrieved January 12, 2009, from http://wcbstv.com/topstories/levar.washington.plea.2.611202.html.

Associated Press and Seattle Times Staff. (2003, July 18). Attorney calls bomb-threat charge excessive. *The Seattle Times*. Retrieved January 12, 2009, from http://community.seattletimes.nwsource.com/archive/?date=20030718&slug=threats18m.

Brush, P. (2002, March 1). Montana militia busted: "Project 7" group planned assault on elected officials, authorities say. *CBS News*. Retrieved January 12, 2009, from http://www.cbsnews.com/stories/2002/03/01/national/main502580.shtml.

Carley, K. (2003). Dynamic network analysis. In R. Breiger & K. Carley (Eds.), *The summary of the NRC workshop on social network modeling and analysis* (pp. 133–145). Retrieved November 20, 2008, from http://stiet.cms.si.umich.edu/sites/stiet.cms.si.umich.edu/files/archivedHTML/researchseminar/Winter%202003/DNA.pdf.

Casciani, D. (2008, September 9). Airline urges liquids review after trial. *BBC News*. Retrieved January 12, 2009, from http://news.bbc.co.uk/2/hi/uk_news/7564184.stm.

Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council. (2008). *Protecting individual privacy in the struggle against terrorists: A framework for program assessment*. Washington, DC: The National Academy Press. Retrieved from http://books.nap.edu/catalog.php?record_id=12452#toc.

Eddy, M., & Associated Press. (2007, September 6). Germans seeking more suspects in terror plot. *The New York Sun*. Retrieved January 12, 2009, from http://www.nysun.com/foreign/germans-seeking-more-suspects-in-terror-plot/62075/.

Edelstein, H. (2003). *TIAin't: Data mining in depth.* Retrieved November 18, 2008, from http://www.dmreview.com/issues/20030401/6512-1.html.

Electronic Privacy Information Center. (2005). *Terrorism (Total) Information Awareness page* (index of news articles and opinion pieces about TIA, mostly critical). Retrieved November 20, 2008, from http://epic.org/privacy/profiling/tia/.

Executive Committee on ACM Special Interest Group on Knowledge Discovery and Data Mining. (2003). *Data mining is NOT against civil liberties*. Retrieved November 18, 2008, from http://www.acm.org/sigs/sigkdd/civil-liberties.pdf.

Faiola, A., & Mufson, S. (2007, June 3). N.Y. airport target of plot officials say. *Washington Post,* p. A01. Retrieved January 12, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2007/06/02/AR2007060200606.html.

Freeman, L. (2008). *What is social network analysis?* Buffalo, NY: International Network for Social Network Analysis. Retrieved November 18, 2008, from http://www.insna.org/sna/what.html.

Glod, M., & Markon, J. (2003, May 19). Tracking hate groups aids terrorism fight: Federal agents turn to domestic front. *Washington Post,* p. B01. Retrieved January 12, 2009, from http://www.washingtonpost.com/ac2/wp-dyn/A7672-2003May18.

Hamblett, M. (2008). 2nd Circuit upholds convictions in terror financing sting. *New York Law Journal*. Retrieve from http://www.law.com/jsp/article.jsp?id=1202422768877.

Harris, S. (2007). *How they connect the dots. Government Executive*. Retrieved from http://www.govexec.com/story_page.cfm?filepath=/features/0907-01/0907-01s2.htm.

Hollywood, J., Snyder, D., McKay, K., & Boon, J. (2004). *Out of the ordinary: Finding hidden threats by analyzing unusual behavior (MG-126-RC)*. Santa Monica, CA: RAND Corporation. Retrieved November 19, 2008, from http://www.rand.org/pubs/monographs/2004/RAND_MG126.pdf.

Hollywood, J., Strom, L., & Pope, P. (2008). Using 9-1-1 calls to identify potential instances of terrorist surveillance. *The Police Chief, 75*(10), 160–165.

Horowitz, C. (2004, November 29). Anatomy of a foiled plot: Two would-be bombers of the Herald Square subway station find that three is a crowd. *New York Magazine*. Retrieved January 12, 2009, from http://nymag.com/nymetro/news/features/10559/.

Hoyt, J. (2008). *DHS Science and Technology Directorate's programs.* Paper presented at the Technologies for Critical Infrastructure Protection Conference, Chicago, IL.

Hurdle, J. (2007, July 13). U.S. man convicted of pipeline, energy attack plan. *Reuters*. Retrieved January 12, 2009, from http://www.alertnet.org/thenews/newsdesk/N13358494.htm.

International Association of Law Enforcement Intelligence Analysts, Inc. (2004). *Law enforcement analytic standards*. Retrieved November 19, 2008, from http://www.it.ojp.gov/documents/law_enforcement_analytic_standards.pdf.

Iskioff, M., & Hosenball, M. (2003, June 18). Terror watch: America's secret prisoners. *Newsweek*. Retrieved January 12, 2009, from http://www.newsweek.com/id/58521.

Johnston, D. (2003, July 24). 9/11 Congressional report faults FBI – CIA lapses. *New York Times,* p. A12. Retrieved May 5, 2009, from http://www.nytimes.com/2003/07/24/us/9-11-congressional-report-faults-fbi-cia-lapses.html.

Jonas, J., & Harper, J. (2006). Effective counterterrorism and the limited role of predictive data mining. *Policy Analysis*, 584.

Krebs, V. (2002). Mapping networks of terrorist cells. *Connections, 24*(3), 43–52.

Krebs, V. (2008). *Connecting the dots: Tracking two identified terrorists.* Retrieved November 18, 2008, from http://www.orgnet.com/prevent.html.

Lubrano, A., & Shiffman, J. (2006, February 12). Federal authorities say W-B man is a terrorist. *Philadelphia Inquirer*. Retrieved January 12, 2009, from http://www.shannenrossmiller.com/media/RossmillerArticle,PhillyInquirer21206.pdf.

Markoff, J. (2002, November 9). Pentagon plans a computer system that would peek at personal data of Americans. *New York Times*. Retrieved November 18, 2008, from http://query.nytimes.com/gst/fullpage.html?res=9F05EFD61431F93AA35752C1A9649C8B63.

Masse, T., O'Neil, S., & Rollins, J. (2007). *Fusion centers: Issues and options for Congress*. (CRS Report for Congress RL34070). Washington, DC: Congressional Research Service.

McCue, C. (2006). *Data mining and predictive analysis: Intelligence gathering and crime analysis*. Burlington, MA: Butterworth-Heinemann.

McCullagh, D. (2008, October 7). Government report: Data mining doesn't work well. *CNet News*. Retrieved November 20, 2008, from http://news.cnet.com/8301-13578_3-10059987-38.html.

Memorial Institute for the Prevention of Terrorism. (2007). *Terrorism warnings (poster)*. Retrieved November 21, 2008, from http://www.mipt.org/terrorism/files/pdf/Terrorism-Indicators-Warnings-Poster.pdf.

Moreau, R., & Mazumdar, S. (2008, November 27). India-Pakistan tensions grow in wake of attacks. *Newsweek International*. Retrieved January 28, 2009, from http://www.newsweek.com/id/171056.

Murphy, J. (2003, November 13). FBI: Abortion bomb plot thwarted: Suspected leapt into Biscayne Bay to avoid arrest. *CBS News*. Retrieved January 12, 2009, from http://www.cbsnews.com/stories/2003/11/13/national/main583390.shtml.

Murphy, J. (2004, August 18). Error in Albany "terror" case: Terror camp document said defendant was "brother," not "commander." *CBS News*. Retrieved January 12, 2009, from http://www.cbsnews.com/stories/2004/08/05/terror/main634129.shtml.

Palace, B. (1996). Data mining. Technology note. Prepared for Management 274A. *Technology Note, Anderson Graduate School of Business at UCLA.* Retrieved November 20, 2008, from http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/index.htm.

Police Foundation Crime Mapping Laboratory. (2004). *Users' guide to mapping software for police agencies* (6th ed.). Report to the Office of Community Oriented Policing Services Cooperative Agreement #2004-CK-WX-K003. Retrieved December 22, 2008, from http://www.policefoundation.org/pdf/UsersGuideMapping04.pdf.

Russakoff, D., & Eggen, D. (2007, May 9). Six charged in plot to attack Fort Dix: "Jihadists" said to have no ties to Al-Qaeda. *Washington Post,* p. A01. Retrieved January 12, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2007/05/08/AR2007050800465.html.

Saffron Technology, Inc. (2008). *Saffron technology, Inc.* Retrieved November 20, 2008, from http://www.saffrontech.com/.

Shenon, P. (2002, May 18). Traces of terrorism: The warnings; FBI knew for years about terror pilot training. *New York Times,* pp. A1–A2. Retrieved May 5, 2009, from http://www.nytimes.com/2002/05/18/us/traces-of-terrorism-the-warnings-fbi-knew-for-years-about-terror-pilot-training.html?pagewanted=2.

Stevens, G. M. (2003). *Privacy: Total Information Awareness programs and related information access, collection, and protection laws* (Congressional Research Service Report RL31730). Retrieved November 20, 2008, from http://www.fas.org/irp/crs/RL31730.pdf.

U.S. Attorney's Office, Eastern District of New York. (2006). *Shahawar Matin Siraj convicted of conspiring to place explosives at the 34th Street subway station. Press release.* Retrieved May 24, 2006, from http://www.usdoj.gov/usao/nye/pr/2006/2006may24.html.

U.S. Attorney's Office, Northern District of Ohio. (2008). *Three convicted of conspiring to commit terrorist acts against Americans overseas. Press release.* Retrieved January 12, 2009, from http://cleveland.fbi.gov/dojpressrel/2008/terroristacts061308.htm.

U.S. Attorney's Office, Southern District of Texas. (2007). *Ronald Grecula sentenced to prison in plot to sell bomb to terrorists. Press release.* Retrieved January 12, 2009, from http://www.usdoj.gov/usao/txs/releases/February%202007/070209-Grecula.htm.

U.S. Department of Justice (DOJ). (2003). *Iyman Faris sentenced for providing material support to Al Qaeda.* (Government Press Release 03-589). Washington, DC: U.S. Department of Justice. Retrieved January 12, 2009, from http://www.usdoj.gov/opa/pr/2003/October/ 03_crm_589.htm.

U.S. Department of Justice (DOJ) and DHS Global Justice Information Sharing Initiative. (2005). *Fusion center guidelines: Developing and sharing information and intelligence in a new world*. Retrieved November 19, 2008, from http://www.it.ojp.gov/documents/fusion_center _guidelines.pdf.

U.S. Department of Justice (DOJ) and DHS Global Justice Information Sharing Initiative. (2008). *Baseline capabilities for state and major area fusion centers: A supplement to the fusion center guidelines*. Retrieved November 19, 2008, from http://www.it.ojp.gov/documents/baseline capabilitiesa.pdf.

U.S. Department of Justice (DOJ), Bureau of Justice Assistance. (2003). *The national criminal intelligence sharing plan.* Retrieved November 19, 2008, from http://www.it.ojp.gov/documents/NCISP_Plan.pdf.

U.S. fears home-grown terror threat. (2006, June 24). *BBC News*. Retrieved January 12, 2009, from http://news.bbc.co.uk/2/hi/americas/5112354.stm.

U.S. Federal Bureau of Investigation (FBI). (2006a, July 7). FBI busts "real deal" terror plot aimed at NYC-NJ underground transit link. *Fox News*. Retrieved January 12, 2009, from http://www.foxnews.com/story/0,2933,202518,00.html.

U.S. Federal Bureau of Investigation (FBI). (2006b). Terrorism 2002–2005. Retrieved May 5, 2009, from http://www.fbi.gov/publications/terror/terrorism2002_2005.htm.

Wax, E. (2002, December 2). Kenyan farmer spotted bombers. *Washington Post*. Retrieved November 19, 2008, from http://media.www.dailyiowan.com/media/storage/paper599/news/2002/12/02/Nation/Kenyan.Farmer.Spotted.Bombers-334722.shtml.

WGBH Educational Foundation. (2008). Ahmed Rassam's millennium plot. *Frontline*. Retrieved November 21, 2008, from http://www.pbs.org/wgbh/pages/frontline/shows/trail/inside/cron.html.

Whitlock, C. (2007, July 5). Homemade, cheap and dangerous: Terror cells favor simple ingredients in building bombs. *Washington Post,* p. A01. Retrieved January 12, 2009, from http://www.washingtonpost.com/wp-dyn/content/article/2007/07/04/AR2007070401814.html.

Wilkinson, M., & Hall, C. (2006, February). 3 charged in terror plot; local suspects planned attacks in Iraq, U.S. says: Men accused of trying to build bombs. *Toledo Blade*. Retrieved January 12, 2009, from http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20060222/NEWS03/60222005.

Zetter, K. (2002). *Tracking terrorists the Las Vegas way.* Retrieved November 20, 2008, from http://www.pcworld.com/article/103692/tracking_terrorists_the_las_vegas_way.html.

Appendix

Table 1 summarizes 25 recent disrupted terrorist plots reported by the media, (the table distinguishes convictions from accusations), describing both the reported objectives of the plot and the initial clue leading to its foiling. Of these 25 foiled plots, only 5 (20%) of the initial clues came from intelligence operations (CIA, FBI, and the U.S. Department of Defense). Eight (32%) came from unexpected discoveries made during police investigations. Six (24%) came from tips reporting a potential plot to law enforcement. Finally, six came from following up on suspicious activity—two (8%) from direct police action in response to observing suspicious activity and four (16%) from following up on tips reporting suspicious activity. Overall, 80% of the initial clues came from observing, reporting, and properly acting on behavior of concern, including both directly threatening behavior (such as openly discussing plans for terror attacks) and suspicious activity (such as conducting target site surveillance).

Table 1. Initial Clues Leading to the Foiling of 25 Reported Terrorist Plots[2]

Plot Description	Initial Clue
Yassin Aref and Mohammed Hossain. Convicted of plotting to use a rocket propelled grenade to assassinate a Pakistani diplomat (Hamblett, 2008)	**Intelligence.** Aref's name and address were found in a notebook in northern Iraq, plus other classified intelligence (Murphy, 2004)
Russell Defreitas et al. Accused of plotting to blow up fuel pipelines and fuel tanks at John F. Kennedy airport in New York	**Intelligence.** CIA operations in South America and the Caribbean (Faiola & Mufson, 2007)
Assem Hammoud et al. Accused of plotting to attack New York–New Jersey transit lines	**Intelligence.** FBI monitoring of Internet chat rooms used by extremists (FBI, 2006b)
Iyman Farris. Convicted of plotting to destroy the Brooklyn Bridge using blowtorches, as well as derail a Washington, D.C.-area train (DOJ, 2003)	**Intelligence.** Interviews of 9/11 mastermind Khalid Sheikh Mohammed and searches of his residences (Iskioff & Hosenball, 2003)

[2] The incidents listed in this table were initially identified in the following sources, along with two other cases widely reported in the national media ("Millennium Plot" and Hanau, Germany, plot): (1) Office of the Press Secretary of the President. (2005, October 6). *Fact sheet: Plots, casings, and infiltrations referenced in President Bush's remarks on the War on Terror.* Retrieved January 9, 2009, from http://www.whitehouse.gov/news/releases/2005/10/20051006-7.html. (2) U.S. Department of Justice, Federal Bureau of Investigation (DOJ, FBI). (2006). *Terrorism 2002-200*5. Retrieved February 6, 2009, from http://www.fbi.gov/publications/terror/terrorism2002_2005.pdf. (3) Carafano, J. J. (2007, November 13). *U.S. thwarts 19 terrorist attacks against America since 9/11* (Backgrounder No. 2085). Washington, DC: The Heritage Foundation. Retrieved January 9, 2009, from http://www.heritage.org/research/HomelandDefense/upload/bg_2085.pdf.

Table 1. Initial Clues Leading to the Foiling of 25 Reported Terrorist Plots (continued)

Plot Description	Initial Clue
Dhiren Barot. Convicted of plotting to attack financial targets in New York; Washington, D.C.; and Newark, New Jersey, as well as UK targets (Whitlock, 2007)	**Intelligence.** Interviews with Khalid Sheikh Mohammed; Barot's memo on elementary bomb making was found on a laptop in Pakistan (Whitlock, 2007)
Abdulla Ahmed Ali et al. ("Liquid Explosives Plot"). Accused of plotting to destroy transatlantic airliners using liquid explosives; convicted of plotting a terrorist bombing campaign (Casciani, 2008)	**Discovery during police investigation.** Ali's luggage was searched by UK police and found to contain suspicious material after his return from Pakistan (Ali was already under surveillance by police) (Casciani, 2008)
David Wayne Hull. Convicted of plotting to bomb abortion clinics (Murphy, 2003)	**Discovery during police investigation.** Explosives' construction and plots found by informant during investigation of Hull (Glod & Markon, 2003)
William Joseph Krar. Convicted of plotting to weaponize cyanide gas (FBI, 2006b)	**Discovery during police investigation.** FBI search of residence subsequent to Krar's arrest for delivering false identification badges (FBI, 2006a)
Seas of David group. Accused of plotting to blow up the Sears Tower and FBI headquarters	**Discovery during police investigation.** Group leader asked an undercover FBI agent he thought was affiliated with Al Qaeda for assistance ("U.S. fears home-grown terror threat," 2006)
Syed Haris Ahmed and Ehsanul Islam Sadequee. Accused of videotaping U.S. Capitol and World Bank and sharing tapes with a suspected overseas terrorist, as well as discussing various terror plots against U.S. targets	**Discovery during police investigation.** Identified by law enforcement when they met with three Canadians already under investigation for suspected terrorist activities (Associated Press, 2006b)
Sean Michael Gillespie. Convicted of plotting attacks on Jewish sites (FBI, 2006a)	**Discovery during police investigation.** Investigation subsequent to being arrested for firebombing an Oklahoma City synagogue (FBI, 2006)
Robert J. Goldstein et al. Convicted of plotting to attack the Islamic Center of Pinellas County, Florida (FBI, 2006a)	**Discovery during police investigation.** Local police discovered weapons and a mission statement for an attack during a call for a domestic dispute (FBI, 2006a)
Jamiyyat Ul-Islam Is-Saheeh group. Convicted of plotting to attack Los Angeles Army National Guard facilities, synagogues, and other California targets (Associated Press, 2007)	**Discovery during police investigation.** Local police investigation subsequent to members being arrested for armed robberies of gas stations (Associated Press, 2007)

Table 1. Initial Clues Leading to the Foiling of 25 Reported Terrorist Plots (continued)

Plot Description	Initial Clue
Ronald Allen Grecula. Convicted of attempting to provide an improvised explosive device (IED) to Al Qaeda (U.S. Attorney's Office, Southern District of Texas, 2007)	**Tip reporting a plot.** A confidential source informed the Drug Enforcement Administration (DEA) about Grecula's intentions (Murphy, 2003)
Stephen John Jordi. Convicted of plotting to bomb abortion clinics (FBI, 2006a)	**Tip reporting a plot.** Brother alerted FBI of Jordi's plans (Murphy, 2003)
Project 7 Militia. Accused of plotted assassinations of state and local officials to start an antigovernment war; convicted of various conspiracy and weapons charges (FBI, 2006b)	**Tip reporting a plot.** County sheriff approached by a member of the group who offered to be an informant (Brush, 2002)
Paul Douglas Revak. Accused of plotting to bomb the U.S. Coast Guard station in Bellingham, Washington; convicted of "threatening to use a weapon of mass destruction" (FBI, 2006a)	**Tip reporting a plot.** Fellow student at Western Washington University called authorities after Revak tried to recruit him to assist (Associated Press and Seattle Times Staff, 2003)
Michael C. Reynolds. Convicted of plotting to destroy pipelines and a New Jersey refinery (Hurdle, 2007)	**Tip reporting a plot.** Shannen Rosmiller met Reynolds online through her private efforts in monitoring extremist websites to find potential terrorists (Lubrano & Shiffman, 2006)
Gale William Nettles. Convicted of plotting to assist in blowing up the Dirksen Federal Building in Chicago (FBI, 2006a)	**Tip reporting a plot.** Tip from a prisoner incarcerated with Nettles (Associated Press, 2004)
Ahmed Ressam ("Millennium Plot"). Convicted of plotting to bomb Los Angeles International Airport (WGBH Educational Foundation, 2008)	**Police action in response to suspicious activity.** U.S. Customs agent noticed suspicious activity by Ressam and had his car searched at Port Washington, Washington (WGBH Educational Foundation, 2008)
Islamic Jihad Group members. Accused of plotting to destroy U.S. military facilities in Germany	**Police action in response to suspicious activity.** Suspects discovered conducting surveillance of U.S. military facilities in Hanau, Germany (Eddy & Associated Press, 2007)
"Fort Dix Plot" group. Convicted of plotting to attack service members at Ft. Dix, New Jersey (Ankarcrona, 2008)	**Tip reporting suspicious activity.** Circuit City employee reported a video of group members firing weapons and calling for a Jihad (group members had given the employee the videotape to burn it to a DVD) (Russakoff & Eggen, 2007)
Demetrius Van Crocker. Convicted of plotting to use explosives and Sarin against U.S. targets (Associated Press, 2006a)	**Tip reporting suspicious activity.** Informant alerted authorities of Crocker's "antigovernment rants" (Associated Press, 2006a)

Table 1. Initial Clues Leading to the Foiling of 25 Reported Terrorist Plots (continued)

Plot Description	Initial Clue
Mohammad Zaki Amawi, Marwan Othman El-Hindi, and Zand Wassim Mazloum. Convicted of plotting to build IEDs to attack U.S. forces in Iraq (U.S. Attorney's Office, Northern District of Ohio, 2008)	**Tip reporting suspicious activity.** Tips from the community about the men, as well as assistance from an informant (Wilkinson & Hall, 2006)
James Elshafay and Shahawar Martin Siraj. Convicted of plotting to bomb a New York City subway station during the Republican National Convention (U.S. Attorney's Office, Eastern District of New York, 2006)	**Tip reporting suspicious activity.** Tip to the New York Police Department terrorism hotline about Siraj's "virulent anti-American tirades" (Horowitz, 2004)