Building on Clues: Improving Methods to Help Detect and Characterize Terrorist Activity

Kevin J. Strom, Ph.D.
RTI International

December 1, 2010

funded by the Institute for Homeland Security Solutions
www.ihssnc.org
Project Overview

• **Problem**: Limited guidance on *how* to collect, analyze and share counterterrorism-related data
  - Emphasis has focused more on *what* to do and less on *how* to do it

• **Response**: Develop methods for collecting, prioritizing, and analyzing information potentially related to terrorism including suspicious activity reports
  - Identify best approaches to finding the initial clues of terrorist activity and establishing reasonable suspicion
  - Identify effective approaches for analyzing unstructured, narrative data
Project Phases

I. Used open-source analysis to assess foiled terrorist plots and executed attacks
   – Developed database of 86 foiled and executed plots against U.S. targets from 1999 – 2009

II. Conduct interviews with subject matter experts including law enforcement, regional and state fusion center personnel
   – Identify what is working well and what needs improving

III. Develop and test analytic processes for prioritizing and analyzing suspicious activity reports (SARs) potentially related to terrorism
Findings from Case Studies of Prior Plots
Case Selection Criteria

- Included cases in which–
  - A terrorist plot against a US target was executed;
  - A terrorist plot to injure or kill at a US target was foiled; or
  - Material support to terrorist organization in service of a future plot

- The planned or executed plots were intended to cause casualties or catastrophic damage to critical infrastructure

- Plots could be from any ideological motivation

- Cases were identified from public information sources

- Limitations
  - Do not include plots that were never reported publically –
    - Plots that are only known to intelligence agencies
    - Plots that “self-foiled”
  - Every plot relevant to our study may not have been identified in our searches
Characteristics of Terrorist Plots in the United States From 1999 – 2009

- Identified **18 plots reaching execution** that caused, or were intended to cause, casualties
- Identified **68 foiled plots** intended to cause casualties during the same time period

Among identified cases, findings demonstrate that the US is interdicting about 80% of terrorist plots intended to cause causalities or destroy critical infrastructure
Similar numbers of AQAM and AQAM-inspired plots (n=40) and White Supremacist / Militia/Anti-Government (n=32) 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 the general public (20 cases).
Types of Initial Clues in Foiled Plots

- 43% - Reports of specific plots
  - Generally split between tips from the general public and would-be terrorists soliciting an undercover agent or informant

- 25% - Associates of known terror suspects
  - Individual were first identified through links to known suspects

- 18% - Criminal investigations
  - Includes crimes known to be related to terrorism (e.g., robbery, counterfeiting) and “ordinary” crimes (e.g., parole violations, traffic stops)

- 15% - Various types of suspicious activity
  - Planning activity: paramilitary training, suspicious documents
  - Preparatory activity: smuggling-like behavior during attempts to move incriminating material, target site surveillance
Types of Initial Clues in Foiled Plots - Detail

- 25% Association with Terrorists
- 18% Suspicious Documents
- 15% Precursor Crime
- 25% "Ordinary" Crime
- 12% Criminal Solicitation
- 12% Undercover Agent Solicitation
- 10% Online Solicitation
- 8% Paramilitary Training
- 6% Potential Surveillance Activity
- 6% Extremist Rants
- 4% Smuggling-Like Behavior
- 2% Suspicious Activity
- 2% Precursor Crime
- 0% "Ordinary" Crime

Bar chart showing the number of terrorist plots:
- Reports of Terrorist Plots: 14
- Reports of Suspicious Activity: 6
- Associations with Terrorism: 3
- "Ordinary" Crime: 6
- Criminal Solicitation: 6
- Undercover Agent Solicitation: 12
- Online Solicitation: 3
- Paramilitary Training: 2
- Potential Surveillance Activity: 1
- Extremist Rants: 2
- Smuggling-Like Behavior: 2
- Suspicious Activity: 2
- Precursor Crime: 0
- "Ordinary" Crime: 0
- Criminal Solicitation: 0
- Undercover Agent Solicitation: 0
- Online Solicitation: 0
- Paramilitary Training: 0
- Potential Surveillance Activity: 0
- Extremist Rants: 0
- Smuggling-Like Behavior: 0
- Suspicious Activity: 0
- Precursor Crime: 0
Evidence Triggering Full Investigations in Foiled Plots

- 46% - Initial clue alone sufficient
- 50% - Additional investigations/linking required after initial clue
- 4% - Links from other ongoing investigations
Evidence Triggering Full Investigations in Foiled Plots - Detail

- **Links From Intelligence**: 1
- **Links from a Terrorism Investigation**: 2
- **Confession During Interrogation**: 3
- **Surveillance Following Terrorism SAR**: 11
- **Search Following Criminal Activity**: 6
- **Search Following Terrorism SAR**: 14
- **Threatening Behavior by Suspect**: 1
- **Explicit Threats from Suspect**: 3
- **Details of Plot from Solicitation**: 11
- **Details of Plot from Tip**: 11
- **Details of Plot from Intelligence**: 5

![Bar Chart](chart.png)

- **Initial Clues Sufficient**: 46%
- **Evidence from Investigation of Initial Clues**: 4%
- **Links from Other Investigations**: 50%
Case Studies – Conclusions and Recommendations

- Recognize importance of law enforcement and the public in preventing attacks, and support them through investments in education and reporting.
- Continue to investigate AQAM, but do not overlook other types of terrorist groups, and pay particular attention to “lone wolves.”
- Ensure processes and training are in place that enable law enforcement personnel to identify terrorist activity during routine criminal investigations.
- Work to establish good relations with local communities and avoid tactics that might alienate them.
- Support “quality assurance” processes and systems to ensure that initial clues are properly pursued and findings shared.
- Expand the federal standards for categorizing suspicious activity reports (SARs).
Phase II – Preliminary Findings

- No uniform reporting format for SARs creates a knowledge management issue between the various SARS data sources
- Lack of a systematic approach for determining whether a SAR is potentially terrorist-related and warrants additional review
- Tendency is to pass reports that are remotely terrorist related up the chain ultimately ending up at the FBI
  - The potential result of this trend is that federal databases will be ‘watered down’ with low value information
- Frustration expressed by individuals at the local level that they rarely learn the outcome of information they pass up
Phase III – Approach

- Develop “best practice” analytic and knowledge management strategies that account for the characteristics of each SAR data source (e.g., tip lines, 911 calls, field interview reports, etc.)
  - Data cleaning, processing, and filtering
  - What are appropriate “triggers” that indicate the activity in question warrants additional inquiry?
  - What is the process for ensuring that pertinent information is not dropped or missed?
  - Which reports should be prioritized ahead of others?
State and Local Analysts Have Expressed a Desire for SAR Evaluation Criteria and Feedback

• Phase II Findings:
  – Lack of a standardized model to determine whether a SAR is potentially terrorist-related and warrants additional review
  – Individuals at the local level rarely learn the outcome of information they pass up the chain

• Recommendations:
  – A “one-size-fits-all” model is probably not realistic. However, can develop an instructional model that relies heavily on prior cases and subject matter expertise
  – Provide routine feedback on SARs submitted by state/local
    • Does not need to provide outcome of an investigation – feedback can be limited to whether SARs “like this one” were useful, and why
Key Lessons Learned from Phase 1 – Following Up on Initial Clues

- **Critical success factor**: *following up on initial clues*, which includes finding links, direct action and information sharing
  - *Finding links* involves searching for related activity – same types of suspicious activity, same people, organizations, vehicles, bank accounts, etc.
  - *Direct action* includes tasking resources – searches, interviews, surveillance
  - *Information sharing* is bidirectional – same nodes send and receive

- **Implicit requirements**:
  - “Scheduling” mechanism to task follow-up activities to be completed by specified times / dates
  - “Quality control” mechanism to ensure follow-ups occur and that needed feedback is provided
  - *Finding*: these measures are partially addressed, but need bolstering
Why This is Important – 4 of the 5 Executed Plots With the Highest Casualties (or Potential Casualties) Had Dropped Initial Clues…

<table>
<thead>
<tr>
<th>Plot</th>
<th>Casualties</th>
<th>Dropped clue(s)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/11 attacks (2001)</td>
<td>3000</td>
<td>Yes</td>
</tr>
<tr>
<td>Attempted Christmas-day bombing of NW 253 (2009)</td>
<td>290 (potential)</td>
<td>Yes</td>
</tr>
<tr>
<td>Attempted “shoe bombing” of AA 63 (2001)</td>
<td>197 (potential)</td>
<td>No</td>
</tr>
<tr>
<td>Ft. Hood shootings (2009)</td>
<td>45</td>
<td>Yes</td>
</tr>
<tr>
<td>Columbine shootings (1999)</td>
<td>34</td>
<td>Yes</td>
</tr>
</tbody>
</table>

... and we found only four executed plots with dropped clues
A Notional Process for Processing Clues of Potential Terrorist Activity Involves Multiple Cycles of Evaluation and Application

1. Get initial clue
2. Evaluate clue and associated information
3. Schedule follow-up actions
4. Take actions
5. Get results

- No further action needed
- Start full investigation
- Further action justified
- Probable cause established for a specific plot
- Problems identified
- Take corrective actions

(Repeated evaluations) (Repeated applications)
A State-Transition Model for Processing Clues

1. Find links
2. Post info
3. Share info
4. Do direct action
5. Determine and resolve issues

Get initial clue
Evaluate new clue / new information
Schedule follow-up activities

Scheduled activity
Activity late / other problem
End
Results received
Need search
Need post
Need share
Need action

Probable cause
Actions complete
Action needed
Start full investigation
Close and store
Actions complete
End

Start
Wait
Common Themes in Initial Clues: **TASCS** – Threatening, Atypical, Significant, Credible, and Specific

- **Threatening** – activity described has a clear relationship (“nexus”) to an aspect of terrorism or crime
  - For terrorism, can be descriptions of activity anywhere in the attack chain – not just preparations for specific plot
  - Beyond terrorism to crime – significant number of cases foiled through investigations of what initially seemed to be “routine” crime
- **Atypical** – common, benign explanations for reported behavior are highly unlikely
  - Referencing Heuer: limited evidence for competing hypotheses
  - E.g., photographing a landmark or leaving behind a backpack likely not terrorism – trespassing in secure areas could be a different story
- **Significant** – report describes behavior reflecting personal commitment by suspect
  - Not just sending some inflammatory e-mail or posts – “doing” not “saying”
  - Not just being part of a specific racial/ethnic/ideological group
  - For associations, more than just casual personal or business contacts
- **Credible** – reason to believe the person making the report was a reliable witness
- **Specific** – report of activity at least somewhat precise and detailed
Phase III – Preliminary Findings and Recommendations

- Progress is being made on establishing SAR processes, developing a common data format, and providing training to recognize and report SARs
  - *E.g., Nationwide SAR Initiative and ISE SAR Functional Standard 1.5*

  - **Issue:** Direct tips of terrorist activity and findings during routine criminal investigations are not explicitly part of the SAR process; some other types of relevant activity are only indirect matches (*e.g.,* overseas travel for paramilitary training = “acquisition of expertise”)
  - **Recommendation:** explicitly add these types to the Functional Standard

- **Issue:** Some types of SARs are unidentified in larger data pools (*e.g.,* 911 calls, field interview reports)
  - **Recommendation:** develop secondary screening processes
Phase III – Preliminary Findings and Recommendations

- **Issue**: Scheduling and quality control of SAR follow-up activities are not fully addressed
  - **Recommendation**: explicitly introduce scheduling of follow-up activities, checks on progress and results, and corrective actions, into SAR analysis processes and information flows

- **Issue**: Desire for a standard evaluation model for SARs – however, wide variation in clues seen to date mean a single model is not feasible
  - **Recommendation**: create an “instructional model” that educates based on previous case studies, with overall guidance to look for reports that are “TASCS” (Threatening, Atypical, Significant, Credible, and Specific)
Next Steps

- Publish comprehensive final report on current project
- Continue to maintain US TIPS database and explore possibilities for expansion of variables and scope (e.g., addition of other countries)
- Explore integrating findings with current law enforcement training initiatives
- Continue to explore analytic approaches with SAR data focusing on non-classified local sources
Questions

Kevin J. Strom

kstrom@rti.org