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

Kevin J. Strom, Ph.D.
RTI International
November 4, 2010
IHSS Research Summit
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
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
Phase I: Case Studies of Prior Terrorist 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
Organization of “Terrorist Groups” Responsible for Plots Within the US, 1999-2009

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
Phase I - 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: Structured Interviews Regarding SARs with Subject Matter Experts
Phase II - Purpose

- Understand how SARs are processed at state & local level
- Interview topics cover:
  - Collection and initial reporting
  - Processing and review
  - Analysis and prioritization
  - Sharing and dissemination
  - Follow-up and feedback
- To date conducted interviews with nearly 20 individuals representing local law enforcement, state and regional fusion centers, military, and private contractors
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 : Toward an Analytic Approach for SARs
Phase III – Approach

• Collect samples of various data sources that capture suspicious activity
  – Field interview forms
  – Crime incident forms
  – Online tip line forms
  – 911 data
  – SAR templates used by fusion centers

• Review and categorize common variables associated with these different reporting formats (*includes both structured and unstructured/text narrative fields*)

• Describe the life cycle for each data source

• Describe the strengths and weaknesses of each data source
Phase III – Approach

• Develop “best practice” analytic strategies and knowledge management that account for the characteristics of each data source
  – 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?
Questions?

Contact:
Kevin Strom
kstrom@rti.org
919-485-5729