RESEARCH BRIEF

"Connecting the Dots" in Intelligence

Detecting Terrorist Threats in the Out-of-the-Ordinary

Abstract

In today's heightened security environment, accurate and timely intelligence information is critical. But managing the flood of available data has never been more fraught with challenges. A RAND team has devised a new approach to gathering and interpreting information based on a computer network able to single out warning signs while protecting individual privacy. Atypical situations would be the starting point. The network would detect these suspicious signals and then project them into a realistic context so that analysts could assess whether they really do indicate a possible terrorist attack and initiate any necessary preemptive action.

RAND RESEARCH AREAS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND HOMELAND SECURITY
TRANSPORTATION AND INFRASTRUCTURE

Corporate Headquarters
1776 Main Street
P.O. Box 2138
Santa Monica, California
90407-2138
TEL 310.393.0411
FAX 310.393.4818

www.rand.org

"I think anything out of the ordinary routine of life well worth reporting."

—Sherlock Holmes

Effective intelligence gathering plays a vital role in detecting and preventing terrorist attacks. But in the information age, it has become tremendously challenging to identify and understand the signals that could point to plans for an attack. Every day, the intelligence community receives huge amounts of data from many different sources—countless unsystematic "dots" of information. Yet with few clues about which data from this enormous flow are related to possible terrorist activity, great uncertainties about what the data mean, and little indication of how to put all the information together, the community can easily miss critical warning signs.

With a mandate to design new ways to "connect the dots" in intelligence, a team from the RAND National Security Research Division (NSRD) has created a concept for an analytic tool that can improve the ability to identify terrorist-related data and comprehend links among them. The results of the study are documented in *Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior.*

The new concept is based on the idea of studying the atypical—out-of-the-ordinary signals that deviate significantly from an established status quo. It envisions a network of computers that can handle a flow of data far too large for analysts to work with directly. The network would take in streams of raw data, filter them to extract information that could be related to terrorist activity, and then test the information to identify observations that truly indicate a serious threat. By prioritizing information in this way, the network would help human analysts focus on the most relevant and important discoveries.

Why Is There a Need for a New Approach to Analyzing Intelligence?

In the past, the intelligence community searched for threats to homeland security by harvesting large amounts of data from sources worldwide. Computers and analysts then filtered the data for individual "nuggets" that fit preestablished patterns of suspicious behavior. This approach worked both because the volume of data to process was comparatively limited and the adversaries were large, not very agile, and typically attacked in similar ways.

In today's dramatically changed security environment, however, new realities undermine the traditional approach. The volume and scope of available data far exceed the ability of conventional approaches to process the information directly. The nature of the adversaries has also changed: They are smaller and more scattered than in the past—and much more elusive. Nor will they necessarily attack the same way twice. Consequently, looking

for established patterns of suspicious behavior can actually be counterproductive. Finally, in the era of electronic databases, approaches centered on collecting and storing all available data on individuals have raised serious privacy concerns.

The Atypical Signal Analysis and Processing (ASAP) Concept Offers a Promising Alternative

To meet current security demands, the NSRD team departed from traditional thinking about intelligence analysis, turning instead to a process used by history's highly astute problem-solvers, such as the fictional Sherlock Holmes. This process locates suspicious behavior not in established patterns, but in out-of-the-ordinary situations. Problem-solvers first establish expectations for what is "normal" in a given situation. They then closely observe the situation for behavior that deviates significantly from the status quo. When they see a "flag," solvers search for additional data to confirm that the behavior is not only truly unusual but also real cause for concern. They next seek to understand the meaning of the behavior, first searching for related information that enables them to put that behavior in context and then testing hypotheses about what the deviations suggest. In the final stage of the process, the solvers act upon all they have learned. For Sherlock Holmes, this would involve naming the culprit. In a situation such as a terrorist attack, it would entail taking preemptive action to eliminate or minimize the risk.

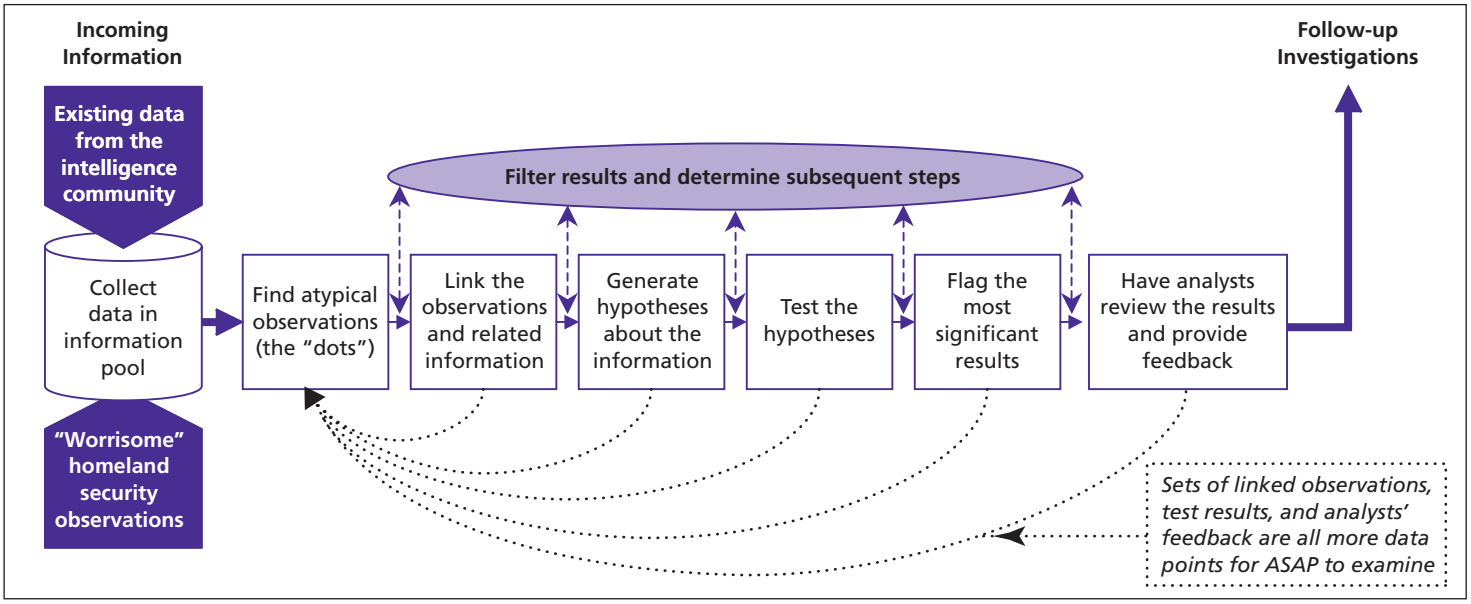
Drawing on this problem-solving process, the NSRD team created the Atypical Signal Analysis and Processing (ASAP) concept. This concept calls for a powerful tool that would use this method to sift through vast quantities of data and evaluate different ways of understanding suspicious information. Fresh discoveries about harvested information would be continuously incorporated into interpretations of what it means.

How Would the ASAP Tool Work?

The tool envisaged within the ASAP concept is a computer network that would use a wide variety of "agents"—software applications that perform a specific function on data they receive as inputs—to collect, link, and analyze "dots" of intelligence information. These agents would move data through a series of steps (see the figure).

1. **The network would gather information from a set of external databases.** This information would mainly consist of observations on "watched" entities—people, places, things, and financial activities already suspected as being relevant for terrorist operations. Reports from members of the intelligence and homeland-security communities of highly unusual and suspicious behavior would also be part of the incoming stream.
2. **The network would store this data within a structured information pool.**
3. ***Detection agents* would find the "dots" in this pool.** These agents would filter the information in the pool, looking for out-of-the-ordinary signals.
4. ***Relationship agents* would search for other information related to the "dots."** These agents would scour the ASAP information pool, as well as relevant external databases, to find relationships between new and existing dots. They would also search for pertinent data that had previously gone unnoticed.
5. ***Hypothesis agents* would create possible interpretations of what the linked dots mean.** These agents would identify which data may indicate a real threat by placing the dots into a larger context that would provide clues about their meaning.
6. ***Testing agents* would run tests to determine whether these hypotheses are correct.** If a hypothesis that indicates certain linked data are threatening proved to be accurate, the data would warrant significant concern. Hypothesis and testing

ASAP Analysis Is an Iterative, Multidirectional Process



agents would provide the basis for singling out linked "dots" for further investigation.

7. **The network would prioritize the results of the tests, forwarding high-priority outcomes to human analysts.** In this way, analysts would become aware of the most unusual and suspicious phenomena among the flood of incoming intelligence information. They could then do the definitive analysis and decide on appropriate actions.

At the same time as data are moving through this sequence of steps, the output of every step becomes an additional data point for the network to analyze, feeding back into the process at the early "detection" stage. This allows the flows through the ASAP network to be iterative and multidirectional—continually adapting to the most recent results. For example, an ASAP network might evaluate whether certain linked "dots" would be more significant if considered as a complete set rather than individually. If that were the case, the entire set would flow back into the network as a new data point. A network control function (the oval in the figure) manages these multidirectional flows, filtering the results of each step and determining what steps to take next.

The ASAP Concept Would Protect Individual Privacy

The ASAP network would work with only a restricted set of data. Data streams initially flowing into the system would consist solely of existing intelligence and homeland security information. Personal records would be introduced only if suspicion were great enough to subpoena that information under existing U.S. legal and law-enforcement statutes. Algorithms built into the network, along with judicial review of any request to subpoena personal records, would ensure that those statutes were being followed.

What Would Implementation Involve?

Fully implementing the ASAP concept would involve an extensive three-phase research effort. In phase 1, researchers would develop an architectural blueprint for the network and a scenario to test the architecture. During phase 2, researchers would create design specifications for the software agents. In phase 3, a prototype network would be built.

In the meantime, certain initial steps could be taken:

- Distribute within the intelligence community standardized profiles of organized behavior in "watched" fields.
- Establish electronic posting boards where members of the community can report and read about "unusual" phenomena.
- Develop semi-automated tools, such as Google-like search engines, to help analysts identify and connect relevant postings.

Implementing these stopgap measures would enable human analysts to link "dots" more effectively until an automated ASAP network became fully functional. ■

This research brief describes work overseen by the RAND National Security Research Division and documented in *Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior* by John Hollywood, Diane Snyder, Kenneth McKay, and John Boon, MG-126-RC (available at http://www.rand.org/publications/MG/MG126), 2004, 188 pages, $27.50, ISBN: 0-8330-3520-7. MG-126-RC is also available from RAND Distribution Services (phone: 310.451.7002; toll free: 877.584.8642; or email: order@rand.org).

RAND Offices Santa Monica • Washington • Pittsburgh • New York • Doha • Berlin • Cambridge • Leiden

RB-9079-RC (2005)