RESEARCH BRIEF

Using Behavioral Indicators to Detect Potential Violent Acts

Government organizations have put substantial effort into detecting and thwarting terrorist and insurgent attacks by observing suspicious behaviors of individuals at transportation checkpoints and elsewhere. Data, methods, and technologies to do so abound, but their volume and diversity can be overwhelming. Their effectiveness is also not clear, or at least not clearly backed in extant research.

To help set priorities for special attention and investment in integrating multiple approaches, the Office of Naval Research asked the RAND Corporation to review relevant literature in behavioral sciences related to threat detection. This work built on earlier RAND efforts on predicting suicide attacks; assessing social science on counterterrorism; and identifying indicators of chemical, biological, radiological, and nuclear weapon development by subnational terrorist groups.

Key findings:

- **Data, methods, and technologies to detect behaviors possibly leading to violent acts abound, but their effectiveness is not always clear.**
- **Multiple, independent layers are necessary in any detection system: Nothing on the horizon presents a "magic bullet" for threat detection.**
- **Effective information fusion, particularly that focusing on man-machine cooperation and not just automation, is critical if analysis of behavioral indicators to detect violent acts is to achieve full potential.**

Technology and Methods

The RAND researchers focused on new or nontraditional technologies and methods and how the data gathered with them might, especially when used with other information, help detect potential violent attacks, such as those by suicide bombers or insurgents placing improvised explosive devices. The researchers highlighted technologies and methods in three cross-cutting classes of data: communication patterns, "pattern-of-life" data, and data relating to body movement and physiological state. The authors focused on what is technically possible, but flagged profound civil-liberties and privacy issues that arise in implementing these technologies. They also noted methods for mitigating some of the related problems.

Efforts to analyze communications patterns have focused on online communications, text analysis and natural-language processing, and speech analysis of content. The expanding technologies for online communications are likely to make other interactions available for data collection. At the same time, methods for analyzing communication patterns have not been well tested and have a low "signal-to-noise" ratio. Text analysis and natural-language processing could improve detection of deception, hostility, or extremist patterns. Such techniques could also quickly analyze large amounts of data. Doing so, however, depends on context and culture and has not been adequately tested in operational settings. Speech analysis has been validated in laboratory settings but faces challenges for real-world implementation, such as the fact that physiological drivers, including anxiety and changes in vocal tone, vary by individual.

Pattern-of-life data include information gathered from mobile devices, existing records, and machine-learning techniques. Mobile devices that enable tracking are increasingly widespread, but users can turn them off, disable them, or not carry them. Existing records may include school records, criminal records, interrogation reports, footage from surveillance cameras, and records of computing use, but there are many challenges involved in extracting and combining these disparate types of data. Machine-learning and big-data analysis may find previously undetected patterns but require massive amounts of data and can be vulnerable to "noisy" data.

Physiological data include information on kinetics and gross motor movements and observations of physiological state. Existing technology can collect data on kinematic patterns (movement), and surveillance and reconnaissance platforms can monitor individuals as they maneuver before an attack. More naturalistic (or real-world) observations are needed for improving current detection systems and protocols. Observing physiological state also holds promise for detecting deception and other behaviors. Such methods may include polygraph testing, electroencephalograms (EEGs), and facial-expression analysis. Two problems with such methods, however, are that physiological indicators may stem from many causes, most of them benign, and such indicators also vary by individual.

Cross-Cutting Themes

The researchers found several cross-cutting themes.

Multiple, independent layers are needed in any detection system, such as screening based on many types of information, including background checks, overtly observable characteristics (including the carrying of weapons), and behavioral cues. A constant issue in screening is how to trade off detection rate against false-alarm rate. Doing so should depend on context. For example, during a period of high alert, security personnel can use less-discriminate cues if they have additional temporary resources. During such a period, the public also tends to be more forgiving of inconvenience and somewhat higher false-alarm rates are tolerable.

Probing to stimulate behavioral responses can sometimes improve detection effectiveness significantly. Such intentional stimulating of behavioral responses may include verbal questioning, anxiety-raising changes of procedure or process, subliminal stimuli, or polygraph tests. It may be polite or obtrusive. Further research could address trade-offs between benefits for detection effectiveness and negative consequences for civil liberties, commerce, and the perceived legitimacy of the security system.

Countermeasures can pose a big problem to detection systems, though they are seldom or poorly employed and can create their own indicators. The operational value of detection systems may be enhanced by making observations from a distance, automatically, or without subjects being aware of the observation.

Nothing on the horizon presents a "magic bullet" for threat detection. This increases the potential importance of effective information fusion, including networked real-time or near-real-time integration of information. Heuristic and simple-model methods, including checklists and risk indexes, are especially suitable for on-the-scene security personnel. More-sophisticated integration methods might seek to incorporate behavioral indicators. A constant challenge in this effort is sorting through evidence from sources and sensors that often produce imprecise and conflicting reports.

Problems associated with high false-alarm or failure-to-detect rates can be addressed by improving system effectiveness, reducing the effects of false alarms on dignity and perceived violations of civil liberties (e.g., by transparency, explanation, fairness, apology, and compensation), and deterring abuse by those within the security system.

Conclusions and Recommendations

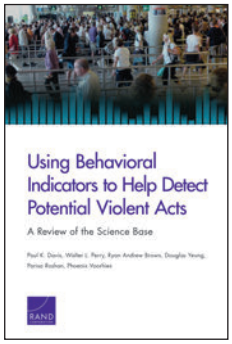
Information generation, retrieval, and integration will tax both automated methods and human-machine interactions. Machines can process vast amounts of data, but interpretations will continue to depend on human expertise and judgment. Efforts to optimize systems should therefore focus on man-machine cooperation, and not automation.

Such integrated systems raise profound issues of privacy and civil liberties, although many private organizations exploit relevant technologies and change notions of privacy. Many of the technologies and methods reviewed are highly controversial—both scientifically and because of potential conflicts with civil liberties and privacy. The RAND researchers attempt to clarify such controversies, not to resolve them.

Regarding new investments, the researchers find that new technologies and methods for using behavioral indicators to detect potential violent attacks should be routinely and consistently subjected to objective peer review and adequate community scrutiny, although sometimes within a classified domain. Vulnerability to countermeasures should be a prime consideration in evaluating investment programs. Investment decisions about individual technologies and methods should be informed by a structured portfolio-analysis approach.

The researchers also recommend more research on mitigating the costs of false alarms, not just by reducing the false-alarm rate but also by mitigating their consequences, including wasting the time of those falsely detained, raising their fears, insulting their dignity, and invading their privacy. These and other measures (e.g., deterring abuse by those with access to information) could be very important in dealing with civil-liberty considerations.

Finally, the researchers recommend that more effort be put toward developing methods for effective information fusion. This is critical if behavioral indicators are to achieve their potential. Fusion should occur not just within a given method, but with heterogeneous information across activities and phases. Yet it remains to be seen how much can realistically be accomplished.



This research brief describes work done for the RAND National Defense Research Institute documented in *Using Behavioral Indicators to Help Detect Potential Violent Acts: A Review of the Science Base* by Paul K. Davis, Walter L. Perry, Ryan Andrew Brown, Douglas Yeung, Parisa Roshan, and Phoenix Voorhies, RR-215-NAVY, 2013 (available at http://www.rand.org/pubs/research_reports/RR215.html). The RAND Corporation is a nonprofit research institution that helps improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

www.rand.org

RB-9724-NAVY (2013)