NEW ANALYSIS TOOLS FOR PRE-DETECTING TERRORIST INTENT

by
Theodore J Gordon; tejgordon@gmail.com; 1 Smilax Dr., Old Lyme, CT 06371

A troubling terrorist scenario involves a self-radicalized lone wolf terrorist who develops a weapon of mass destruction, unknown to the intelligence and police agencies, and suddenly appears ready to strike. We, and many others, believe there are people working on large-scale means of killing and destruction in the misguided belief that they are serving their Gods, making themselves immortal, or righting some wrongs of history. Or they may simply be insane psychopaths. In the past, such people have used poisons, bombs, and machine guns; now, they also have new tools such as infectious man-made viruses and bacteria, stolen or diverted nuclear material or weapons, and intrusive cyber attacks on crucial systems. The scale of potential destruction is huge: capable of destroying billions of dollars of infrastructure or killing millions of people. In our previous work we have designated such an individual as a SIMAD (single individual massively distractive).[1]

One example of a potential SIMAD is the Times Square Bomber, Faisal Shahzad, who was accused of building a bomb from gasoline, propane, and fertilizer and placing the components in an SUV parked in Times Square, and setting the triggering device. Two street vendors discovered the out- of-place SUV and alerted the police. Shahzad was captured at the Kennedy Airport ready to depart on a flight to Dubai. The FBI indictment listed a number of charges; the first "Attempted use of a weapon of mass destruction." He was sentenced to life in prison. Detection in this case was a lucky random event and little analysis was required.

The problem we address in this white paper is the design of an analysis system that improves the chances of detecting a potential SIMAD before he or she has a chance to act. The key word here is *system*; that is the effective combination of detection measures that

[1] The term SIMAD (Single Individual Massively Destructive) was coined by The Millennium Project in the study "Future S&T Management Policy Issues; 2025 Global Scenarios". The Millennium Project, 2003. http://www.millennium-project.org/millennium/scenarios/st-scenarios.html.

leads to a high pre-detection success rate with minimum false positives and negatives, while minimizing adverse impacts on the quality of our lives.

Because of concern about the evolution of terrorism toward SIMAD, the author and several colleagues from the Millennium Project have conducted two Real Time Delphi studies involving more than 100 invited experts. The first study explored the futures of the Lone Wolf phenomenon and the second, the prospects for pre-detection of potential SIMADs.[2] These studies resulted in publication of technical papers in peer reviewed journals and several NATO sponsored workshops in the US and Israel.[3] The information was also presented in a workshop sponsored by the DNI Science and Technology Intelligence Committee (STIC), Data Analysis Working Group. The general conclusions of this work are that large-scale SIMAD attacks are indeed plausible (median opinion: an attack killing and injuring 5,000 people will occur prior to 2027) and that attractive[4] pre-detection measures can (and are being) pursued. But we note that levels of agreement among participants in these studies were low, and many detection measures require compromises- some serious- with freedoms that are familiar to us. The most attractive pre-detection measures were judged to be:

- Software systems for automatic monitoring of social media
- Full-time, real-time automated video scanning near sensitive targets
- Expanded sting operations by police and law enforcement agencies
- Biometric data collection systems that identify individuals

---

[2] Theodore Gordon, Yair Sharan, Elizabeth Florescu, "Prospects for Lone Wolf and SIMAD terrorism," *Technological Forecasting and Social Change* 02/2015; 95. DOI:10.1016/j.techfore.2015.01.013 and "Potential Measures for the Pre-Detection of Terrorism," August 31, 2016, in pre-publication review.

[3] The most recent workshop was held in Washington DC from July 24 – 27, 2016; this meeting resulted in the unclassified report: "Identification of Potential Terrorists and Adversary Planning; Emerging Technologies and New Counter-Terror Strategies;" in preparation; available from the author.

[4] "Attractiveness" is the name of a property used in the study that combined estimates of probability, likelihood, and ease of implementation.

- Computer firewalls that identify the originator of digital messages

Other less obvious measures were also considered, including the use of advanced psychological screening, the use of functional MRI to identify brain anomalies associated with mal-intent,[5] and genetic analysis to search for genetic markers of potentially violent persons. One research team reported that a combination of an abusive childhood and low activity of promoter levels for the monoamine oxidase-A (MAOA) gene resulted in high propensity for anti-social behavior.[6]

Because no single measure seems to hold the key to "pre-crime" detection, we envision the evolution of a layered analysis system in which warning signs from many sources are combined to identify individuals who seem to have a higher chance than others of exhibiting violent behavior in the future. Not surprisingly, an analysis approach that combines measures was judged in our studies to be more effective than any single measure standing alone. But just what would an analysis system that combines several measures look like? We take the credit reporting system as a model. A credit score is a quick look at the overall status of one's credit worthiness. It is composed of several factors such as payment history, late payments, bankruptcies, judgments, and liens. These factors are time weighted: in most credit score algorithms, the older the data, the less important to the overall score. The credit scores is used as a predictor of whether or not an individual is likely to make timely payments in the future.

We imagine that a "composite threat index" for individuals could be similar in many respects: it would also be used to anticipate future behavior; it would be based on the synthesis of results of several time weighted measures, many of which would be derived

---

[5] Telling Truth From Lie In Individual Subjects With Fast Event-Related fMRI. Langleben DD, Loughead JW, Bilker WB, Ruparel K, Childress AR, Busch SI, Gur RC.Hum Brain Mapp. 2005 Dec;26(4):262–72. Medline: http://www.ncbi.nlm.nih.gov/pubmed?term=Langleben%20DD%5BAuthor%5D&cauthor=true&cauthor_uid=16161128.

[6] Caspi A1, McClay J, Moffitt TE, Mill J, Martin J, Craig IW, Taylor A, Poulton R., "Role of Genotype in the Cycle of Violence in Maltreated Children," Science, August 2, 2002: Vol. 297 no. 5582 pp. 851-854 http://www.ncbi.nlm.nih.gov/pubmed/12161658

from public records; it would be dynamic; and would be available to the individual, and under limited circumstances, to others; it could be contested and changed. An automated system of this sort might be used to form a composite risk number associated with an individual; the higher the number, the more carefully the person would be monitored. It is a systematic way to form an advanced "no fly" list.

The measures that make up a composite threat index would be those that promise to be effective, near term, less intrusive on human rights and that already exist in diverse databases, for example by referencing printed emails and other documents originated by an individual, photographs, and videos, tracking purchases of critical materials, reviewing arrest records, scanning self-published information about intent, accessing manifestos that incite to terror, reviewing MAOA levels in the brain and other such specialized information if available, results of psychological and other test taken in the course of enrollment, enlistment, job applications, security checks, etc. and the frequency of communications with known mal-intents. As more independent measures are added to a detection strategy, even better results can be obtained, since one technique can find signals that others miss. Nevertheless, this system could easily violate privacy norms and may require judicial oversight but finding individuals with high threat scores could lead to effective "vigilant monitoring." If this approach were to be used, measures would have to be developed to minimize false accusations and assure privacy-- a tough prescription.

As many respondents pointed out there are limits to what pre-detection measure can be expected to achieve, either individually or in combination. While some warned that "you CANNOT stop them all", there was optimism that with "Big Data, collecting everything and using deep learning/neural nets and fast machines we are increasingly being effective in thwarting attacks, and we are exponentially getting better at it."[7]

We advocate creating one or more in depth studies to:

[7] Respondent comment from Gordon, et. al, "Potential Measures For The Print Detection Of Terrorism Assessment Using Real Time Delphi," August 31 2016, in peer review.

- Identify existing data that might serve as measures in a composite threat index for individuals and means for weighting these measures. This is a daunting problem since the historical data on which a regression analysis could ordinarily be made, is so sparse. This work should include assessment of data reliability, availability, level of privacy compromise, utility, and others such factors.
- Evaluate alternate algorithms that might be used in forming a composite threat index including their reliability, chances for false negatives and positives, susceptibility to hacking, limitations, efficiency, etc.
- Create scenarios that depict futures in which such indexes are used and that include both successful and unsuccessful outcomes. These scenarios should be tested against randomly chosen "shock" events that could facilitate or impede the intent of policies included in the scenarios.
- To the extent reasonably possible, test the ability of the best algorithms to predict examples of terrorist behavior using historical cases with known outcomes.
- Collect opinions from decision makers and experts about the practicality of using the most promising approaches found here and their alternatives, if any.

Most pre-detection measures can create collateral damage that could be worse than the terrorism they help avoid. Respondents in the RTD studies used words like despotism, totalitarian, Hitler, Orwellian, Minority Report, and Stalin to describe consequences that could flow from some pre-detection measures. An unfortunate but inevitable consequence of finding terrorists before they can act is the possible loss of civil liberties. Unless we are careful in implementing these measures, we could lose what we are trying to protect, and we will have done it to ourselves.