PRE-DETECTION OF TERRORISM

Tough problem, but necessary to contemplate

July 25, 2016
Washington, DC

Ted Gordon
Elizabeth Florescu
Yair Sharan
Casualty Expectations

When a SIMAD Might Kill 100,000 or more

Number Killed in a SIMAD Attack

TG
Some planned WMD attacks have been thwarted

- Of 100 cases examined, half were foiled.
  - Jose Pimentel, accused of planning to use pipe bombs in NYC
  - Rezwan Ferdaus pleaded guilty to attempting to use a small drone aircraft
  - Sami Osmaakac found guilty for attempting to use a WMD
  - Amine El Khalifi, sentenced for plotting to attack the US Capitol

- FBI cited many as WMD in indictments
Some Cyber Headlines

- US And China Seek Arms Deal For Cyberspace
- Huge Hack Of US Government Data Affected 21.5 M
- Cyber Attack On U.S. Power Grid Could Cost $1 T
- Hacker: 'Hundreds Of Thousands' Of Vehicles Are At Risk China Acknowledges That It Hacker Units
- Ransomware Porn App Takes Photos Of Users And Holds Phone Hostage
- United (Airlines) Should Thank, Not Ban, Researcher Who Pointed Out A Major Security Flaw
Future Technologies: New Threats

- Future Technologies might give rise to new threats
- Fields like Nano, Bio, Robotics and Materials open new opportunities for people with malicious intentions
- The future terrorist/LW will be more technologically-skilled.
- Weapons will be smaller, cheaper, easier to hide, easier to obtain
Anticipated Future Threats(1)

- **Synthetic Biology** will lead to easy production of contagious Bio-agents (at home labs...)
- **3-D printers** will be cheap and wide spread in each home. Guns, explosives and other weapons could be produced covertly by almost anyone
- **Programmble matter** will be developed. Materials programmed to self assemble, alter their shape and properties. A toy converted into a gun...

TG
Some New Weapons

- **Synthetic Biology:** home production of contagious bio-agents in aerosol form
- **3-D printers:** wide spread, covert weapon production
- **Swarm Robotics:** Tiny robots for many applications (4 millimeter) could be mass-produced in swarms.
- **Cyborg insects:** electronic insects to spread bio-agents or poisons
- **Cybercrime:** Hospitals, financial system, power grid
Technology - Counter Measures

- New threats including SIMADs are seen in the technology horizon
- Likelihood of threats increases with time. There is time to prepare counter measures
- The same families of new technologies enable also development of future counter measures.
- Many of the future threats can be prohibited.

TG
Likelihood to pose a security threat - Nanotechnology

(1=very unlikely   5=very likely)
Likelihood to pose a security threat – Biotechnology

(1=very unlikely   5= very likely)
Likelihood to pose a security threat – Robotics

(1=very unlikely  5= very likely)
Likelihood to pose a security threat – New Materials

(1=very unlikely   5= very likely)
If you can't afford a doctor, go to an airport - you'll get a free x-ray and a breast exam, and; if you mention Al Qaeda, you'll get a free colonoscopy.
The RTD Detection Technologies

1. Multi-spectral sensors
2. Monitor social media
3. Improved "no fly" list
4. Robots security guards
5. 3rd party reporting
6. New codes of ethics
7. Mandatory test reporting
8. Finding suspicious mail
9. DNA analysis
10. Use of brain fMRI
11. Tracking movements
12. Identifying purchasers of proscribed materials
13. Psychological tests
14. Assigning risk scores
15. Video scanning
16. Advanced firewalls
17. Administrative jailing
18. Solutions to stigma
19. Expanded stings
2. Software systems for automatic monitoring of social media. Several kinds: key word searches -- who talks to whom and networks that may connect suspect individuals, and message content – in which individuals may reveal their intent or past activities.

Assume that warrants may be required; the NSA program continues and expands its depth and that most encryption techniques have been broken.
Automated Video Scanning

15. Full-time, real-time automated video scanning near to spot persons who shows up sensitive target inappropriately or frequently.

Finding persons who are out of place or are drawn to a honey pot
1. Multi-spectral and other sensors that collect biometric data that identify individuals (e.g. facial recognition, gait, olfactory signals, iris patterns, etc.)

US NSA: "a biometric system provides an automated method of recognizing an individual based on biometric characteristics, including fingerprint, face, iris, voice, signature, vein pattern, and hand geometry."
19. Expanded sting operations by police and law enforcement agencies

Includes consideration of new types of stings such as cyber honey pots (web sites designed to appear attractive and offer support to would be terrorists).
Identification of Gun Purchasers

12. Advanced means of identifying purchasers of guns and materials thought to be useful in making terror weapons

Involves use of real time facial recognition at points of sale and possibly real time DNA analysis
16. Computer firewalls that identify the originator of digital messages and make computers essentially impervious to attack

Greatly improved safeguard against computer virus intrusion; warns of intrusion attempts and begins the hunt for perpetrators; possibly recognizes stolen passwords
8. Collecting subtle markers from suspicious mail and packages that will help identify the person who packed and mailed them, and the contents without opening the envelope or box.

Markers would include DNA, checks against an improved "no fly" list, addressed to notable or political persons, directed to a published but intentionally incorrect address.
5. Extended public 3\textsuperscript{rd} party reporting (if you see something....)

Would involve an extended social marketing program (like anti-smoking). But the campaign would recognize that it could go too far and have neighbor accusing neighbor and revive a new form of McCarthyism.
2016 Study Objectives

- Overall: reduction of terror events including WMD cases
- Study new technologies of detection and interdiction
- Likelihood, effectiveness, ease of implementation, and unintended consequences of specific developments
The RTD Panel

- 145 people signed in; 100 provided answers
- 30 countries
- Many disciplines:
  - Security: 31.34
  - Education: 11.94
  - Politics: 7.46
  - Business and Trade: 6.72
  - Environment: 6.72
  - Economics: 4.48
  - Futures: 2.99
  - Energy: 2.24
  - Health/medicine: 2.24
  - Psychology: 1.49
  - Demography: 0.75
  - Psychiatry: 0.75
  - Other: 20.15

Well Experienced
- > 20 years: 59.68
- 10-20 years: 21.77
- 5-10 years: 8.87
- 0-5 years: 4.03
- Student/well read: 5.65

Gender
- Male: 83%
- Female: 17%
The Pre-Detection RTD

Imagine two worlds. One employs this approach, the other does not. If the world that does not employ this approach were to have 10 attacks, how many do you think would occur in the world that uses it?

7

Changes are OK  WPM: 6.83 (77)

Submit only this cell  go

Please provide reasons for your answers click here

In the year 2025 how likely is the use of this approach by more than 50% of the security programs of developed countries?

- Very high  (32)
- High  (38)
- Mid range  (8)
- Low  (3)
- Very Low  (0)

Changes are OK  WPM: 8.79 (68)

Submit only this cell  go

Please provide reasons for your answers click here

Considering factors such as cost, training, and negative unintended consequences, please rate the difficulty of introducing this technique?

- Very high  (6)
- High  (28)
- Medium  (35)
- Low  (10)
- Very low  (3)

Your answer has been entered, and you may change it at any time.

Submit only this cell  go

Please provide reasons for your answers click here

Imagine two worlds. One employs this approach, the other does not. If the world that does not employ this approach were to have 10 attacks, how many do you think would occur in the world that uses it?

6

Changes are OK  WPM: 8.79 (68)

Submit only this cell  go

Please provide reasons for your answers click here

In the year 2025 how likely is the use of this approach by more than 50% of the security programs of developed countries?

- Very high  (34)
- High  (25)
- Mid range  (14)
- Low  (2)
- Very Low  (0)

Changes are OK  WPM: 8.79 (68)

Submit only this cell  go

Please provide reasons for your answers click here

Considering factors such as cost, training, and negative unintended consequences, please rate the difficulty of introducing this technique?

- Very high  (4)
- High  (16)
- Medium  (30)
- Low  (22)
- Very low  (3)

Your answer has been entered, and you may change it at any time.

Submit only this cell  go

Please provide reasons for your answers click here

Submit all rows
Row 1 of 21

Submit all rows
Row 2 of 21

TG
The Questions

- For each given technology
  - Effectiveness
  - Likelihood
  - Difficulty of introducing
  - Reasons for all answers

- Also asked about
  - New detection techniques
  - Unintended impacts on freedoms
  - Combined approaches

TG
## Highest Likelihood

<table>
<thead>
<tr>
<th>Item</th>
<th>Measure</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Software systems for automatic monitoring of social media.</td>
<td>79.94</td>
</tr>
<tr>
<td>1</td>
<td>Multi-spectral and other sensors that collect biometric data that identifies individuals</td>
<td>79.43</td>
</tr>
<tr>
<td>16</td>
<td>Computer firewalls that identify the originator of digital messages</td>
<td>77.24</td>
</tr>
<tr>
<td>15</td>
<td>Full-time, real-time automated video scanning near sensitive targets</td>
<td>76.20</td>
</tr>
<tr>
<td>11</td>
<td>Tracking movements of suspected terrorists and people who meet with them</td>
<td>72.54</td>
</tr>
<tr>
<td>19</td>
<td>Expanded sting operations by police and law enforcement agencies</td>
<td>71.09</td>
</tr>
</tbody>
</table>
## Highest Effectiveness

<table>
<thead>
<tr>
<th>Item</th>
<th>Measure</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Combined three or four approaches you considered most effective</td>
<td>4.31</td>
</tr>
<tr>
<td>4</td>
<td>Robots acting as security guards for high value infrastructure and crowd scanning</td>
<td>4.12</td>
</tr>
<tr>
<td>2</td>
<td>Software systems for automatic monitoring of social media.</td>
<td>4.11</td>
</tr>
<tr>
<td>11</td>
<td>Tracking movements of suspected terrorists and people who meet with them</td>
<td>4.10</td>
</tr>
<tr>
<td>15</td>
<td>Full-time, real-time automated video scanning near sensitive targets</td>
<td>4.10</td>
</tr>
<tr>
<td>1</td>
<td>Multi-spectral and other sensors that collect biometric data that identifies individuals</td>
<td>4.10</td>
</tr>
</tbody>
</table>
Will Effective Measures be Implemented?

**Likelihood vs. Effectiveness**

- Combination of three or four approaches considered most effective
- Software systems for automatic monitoring of social media
- Robots security guards for high value infrastructure and crowd scanning
- Biometric data collection that identifies individuals
- Use of brain imaging (fMRI) to find anomalies that suggest future violent behavior
- Solutions to stigma associated with false identification of malintent.
<table>
<thead>
<tr>
<th>Item</th>
<th>Measure</th>
<th>Ease to Implement (10= very easy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Extended public 3(^{rd}) party reporting (if you see something....)</td>
<td>5.30</td>
</tr>
<tr>
<td>19</td>
<td>Expanded sting operations by police and law enforcement agencies</td>
<td>5.13</td>
</tr>
<tr>
<td>2</td>
<td>Software systems for automatic monitoring of social media.</td>
<td>5.08</td>
</tr>
<tr>
<td>15</td>
<td>Full-time, real-time automated video scanning near sensitive targets</td>
<td>4.99</td>
</tr>
<tr>
<td>8</td>
<td>Collecting markers from mail and packages to identify the person who mailed them</td>
<td>4.75</td>
</tr>
<tr>
<td>12</td>
<td>Advanced means of identifying purchasers of guns and materials</td>
<td>4.61</td>
</tr>
</tbody>
</table>
## Attractiveness (product of ease and effectiveness)

<table>
<thead>
<tr>
<th>Item</th>
<th>Measure</th>
<th>Attractiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Software systems for automatic monitoring of social media.</td>
<td>20.88</td>
</tr>
<tr>
<td>15</td>
<td>Full-time, real-time automated video scanning near sensitive targets</td>
<td>20.46</td>
</tr>
<tr>
<td>5</td>
<td>Extended public 3rd party reporting (if you see something....)</td>
<td>20.19</td>
</tr>
<tr>
<td>19</td>
<td>Expanded sting operations by police and law enforcement agencies</td>
<td>19.70</td>
</tr>
<tr>
<td>12</td>
<td>Advanced means of identifying purchasers of guns and materials</td>
<td>18.03</td>
</tr>
</tbody>
</table>
Attractiveness vs. Likelihood

- Real-time automated video scanning near sensitive targets
- Software systems for automatic monitoring of social media.
- Extended public 3rd party reporting (if you see something...)
- Biometric data collection that identifies individuals
- DNA analysis to find genetic evidence that suggests future violent behavior
- Use of brain imaging (fMRI) to find anomalies that suggest future violent behavior
Increasing Parallel Measures

Effect of Adding Members to the Set

Probability of the Set

Number of Members in the Set

- Blue line: 0.40
- Red line: 0.30
- Green line: 0.20
**Combined Measures**

- Measures the respondents combined
  - Multispectral sensors for identifying individuals (1)
  - Robots acting as security guards (4)
  - Means for tracking suspected terrorist (11)
  - Full-time video scan near sensitive targets (15)

- How much improvement
  - Effectiveness of the combined approach 4.31.
  - Average score 19 pre-detection measures 3.41
  - Best score: single measure 4.17 (Robot guards)
  - 25% improvement over the average effectiveness.
<table>
<thead>
<tr>
<th>Commonly Expressed Opinions:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inhibitors</strong></td>
<td><strong>Promoters</strong></td>
</tr>
<tr>
<td>Bureaucratic ineptitude</td>
<td>Costs are plunging</td>
</tr>
<tr>
<td>Chances for misuse</td>
<td>Difficult to fool</td>
</tr>
<tr>
<td>Cost</td>
<td>Easy to implement</td>
</tr>
<tr>
<td>Entrapment perceptions</td>
<td>Existing infrastructure</td>
</tr>
<tr>
<td>Intrusion on freedoms</td>
<td>Unlikely to stir opposition</td>
</tr>
<tr>
<td>Legal, ethical considerations</td>
<td>Will become more</td>
</tr>
<tr>
<td>Many false positives</td>
<td>common, like sex offender</td>
</tr>
<tr>
<td></td>
<td>lists</td>
</tr>
</tbody>
</table>
New Detection Technologies

- Synergistic approaches to reduce false positives
- Positive identification to use in passports
- Quantum encryption
- Software that can auto review big data, synthesize, infer (like fraud detection)
- Real time (remote ?) DNA analysis for instant and irrefutable identification
- National or international identity cards with DNA identifiers built in.
# Unintended Consequences

<table>
<thead>
<tr>
<th></th>
<th>Number of Respondents</th>
<th>Average Answer (100 = serious, lasting, and deep)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of privacy</td>
<td>63</td>
<td>72.38</td>
</tr>
<tr>
<td>Loss of trust in government</td>
<td>54</td>
<td>57.39</td>
</tr>
<tr>
<td>Increased public anxiety</td>
<td>59</td>
<td>56.98</td>
</tr>
<tr>
<td>Unwarranted stigma</td>
<td>54</td>
<td>53.44</td>
</tr>
<tr>
<td>Other</td>
<td>5</td>
<td>42.40</td>
</tr>
<tr>
<td>Economic downturn</td>
<td>48</td>
<td>32.21</td>
</tr>
<tr>
<td>Increased threat level</td>
<td>49</td>
<td>30.20</td>
</tr>
</tbody>
</table>
The best intentions can lead to disastrous results. *Most pre-detection measures can create collateral damage that could be worse than the terrorism they help avoid.*

- A police state; cover for abusive or totalitarian approaches.
- Might become just a new kind of arms race.
- Deepen the security gap between developed and developing countries
- System errors
- Stereotyping & false positives
- Transparency reduction -- to protect against certain programs
- Opportunities for corruption and personal revenge
- Weakened security due to inconsistent deployment, competence and supporting regulations.
Technology can help reduce terror attacks but the question is how to reduce religious radicalism and ideologies that instigate to terrorism. *There is no such thing as one cockroach.*

Bureaucratic and legal limitations ensure that there is NEVER a comprehensive and seamless system of access and sharing such information, even among allies with common identification of threat categories.

It is a fundamentally futile concept to expect to find, and react to, tactical terrorist functionaries in the field if no mechanism is in place to curb the source and support of them.

*There is a distinction between criminal behavior, tendency toward violence, and terrorist intent and different pre-detection measures might be required for each.*

All these techniques are totally dependent on the continuous availability of electricity, which makes them 100% vulnerable to hostile cyber attacks.

*For better or worse, everyone is now a security stakeholder and more often than is now recognized, a security participant.*
Conclusions

- Public perception is key in determining acceptability
- Detection will fall short: helps avoid totalitarianism
- Guard data, warn of intrusion, what has been done
- Safeguards synthetic biology like those for pilots
- Some pre-detection measures need to be invented:
  - a method for positive identification at a distance
  - an identity card (drivers’ license) that cannot be counterfeited.
  - computer firewalls that identify the originator of digital messages
Vexing problems.
- False positives and associated lasting stigma.
- How can authorities compensate for their errors?
- Can the judicial system cope?
- Will the specter of massive attacks be so strong that compromises with freedoms will be tolerated, and to what extent?
Authors

- Theodore Jay Gordon, futurist, consultant, co-founder of the Millennium Project, founder The Futures Group, co-founder The Institute for the Future.

- Dr. Yair Sharan, Col (ret) in the IDF, director of the FIRS2T group, Co-Director of the Israeli Millennium project node, formerly director of the Interdisciplinary Center for Technological Analysis and Forecasting (ICTAF) at Tel Aviv University, Israel

- Elizabeth Florescu, Director of Research at The Millennium Project, and co-author of the annual “State of the Future” reports. She was one of the principal investigators on many studies including scanning reports for the US Army Environmental Policy Institute, assessing new technologies-related issues.