Red Teaming the Terrorist Threat to Preempt the Next Waves of Catastrophic Terrorism

Dr. Joshua Sinai
ANSER
Tel: 703/416-3578
joshua.sinai@anser.org

14th Annual NDIA SO/LIC Symposium & Exhibition
12 February 2003
Sept. 11 Attacks Represented “Pearl Harbor” for CbT Community

• Numerous I&W indicators were present prior to 9/11
  – In al Qaida training manual, missions include:
    • “Blasting and destroying the embassies and attacking vital economic centers” – WTC
    • “Freeing the brothers who are captured by the enemy”
      – September 12 sentencing date for African embassy bombings

• Al Qaida MO - “If you don’t succeed, try again”
  – 1993 bombing of the World Trade Center
  – December 1994 GIS hijacking of Air France aircraft
  – USS Cole bombing preceded by a failed attack against the USS Sullivan

• Al Qaida operatives trained to fly commercial airplanes
  – Iraqi Salman Pak training camp, south of Baghdad
  – U.S. flight schools
Red Team Can Create Incubation-Period Observables

- High-impact & CBRN/Cyber terrorist attacks usually require longer “incubation” periods than Low Impact attacks
  - February 1993 World Trade Center bombing plot began in October 1992 (5 months)
  - March 1995 Aum Shinrikyo sarin gas attack was preceded by a series of attempts to kill adversaries using various gas spraying devices in 1994 (1 year+)
  - April 1995 Oklahoma City bombing plot began 6 months earlier in Fall 1994
  - October 2000 USS Cole attack reportedly planned for 8 months
  - September 2001 WTC/Pentagon attacks preceded by 2-year incubation period

- RT Objective: create pre-incident “attack” observables during the “incubation” that can be identified and monitored
Identifying CLI Incubatory Phases

• Identifying CLI preparation for an attack is more difficult because of the short time frame involved, generally 3-5 days or less
  – Palestinian suicide bombers
  – ETA attacks
  – Al Qaida attacks against foreigners in Saudi Arabia or Pakistan

• Even with CLI, always anticipate new types of attacks and new profiles of operatives
  – In the case of suicide bombers, the use of women, teenagers, dyeing one’s hair blonde, university students, fathers, using ambulances for transportation
Pre-Incident Terrorist Activities vs. Govt. Response

**Intention + Capability = Threat**

**Threat + Indications (observables/activities) = Warning/Tracking/Preemption**

**Group Formation**       **Plan**       **Develop**       **Execute**

**Terrorist Activities**

---

- **Enough**
  - Operational Intelligence to Preempt or Prevent Attack

- **Tracking**

- **Warning**

---

**Indications**

Multidisciplinary collection and analysis to track CLI/CHI/CBRN warfare proclivity

---

**Government Response**

- Preempt

---

**Tactical Response Measures**

---
Traditional Red Teams

• The traditional Red Teaming process grew out of the Military Services’ readiness and evaluation programs, where a unit’s readiness, capability and campaign plan (the “Blue Team”) is tested against an Opposing Force (OPFOR) (the “Red Team”).

• The Red Team projects itself imaginatively into the terrorists’ minds to devise adversary strategies, operations and tactics

• The Blue Team tries to design countermeasures
‘Blue’ Buy-in of Red Teaming

• Forming a Red Team requires the Blue Team planners’ acceptance of Red as a \textit{valid, value-adding group}

• Two basic \textit{requirements} facilitate the Blue Team’s “\textit{buy-in}”:
  – First, officials need to make clear that Red Teaming is the \textit{product of their own initiative}
  – Second, Red Team members must have \textit{credibility}, which is the product of their \textit{expertise and experience}
**Alternative Names for Red Teaming**

- War Games
- Scenarios (alternative)
  - Best case, most likely, intermediary, worst case etc.
- Simulations
- Tabletop Exercises
- Tiger Teams (Navy concept)
- Peer Review
  - Also, red teaming proposals
- A pilot “chair-flying” a mission before execution
Requirements for Effective Red Teaming – Peter Probst

• In Red Team models, assess vulnerabilities by using databases that terrorists would use, not necessarily RT members’ expert knowledge of what might be U.S. vulnerabilities, because what we consider vital, terrorists may not.

• Red Team members need to understand how a terrorist group goes about deciding on what is important for them to target and what they perceive to be important criteria for measuring the desired impact of an attack.
Red Team Methodologies

• Must think **3-5 moves ahead** of the opponent
  – Action/reaction/re-
    reaction/counteraction/counter-counter
    action/etc.

• A **continuing process** focusing on the **entire plot** rather than a **single component** in an attack
### Three Levels of I&W Observables

<table>
<thead>
<tr>
<th>Terrorist Group/I&amp;W Observables</th>
<th>Strategic</th>
<th>Operational</th>
<th>Tactical</th>
</tr>
</thead>
</table>
| **Federal Government Observables** | - Group motivations  
Group is expanding  
- Hostile intent  
- Capabilities upgraded  
- Activities in safe haven  
- Previous attacks  

-Group’s modus operandi (MO)  
- Types of likely attacks & targeting  
- Conducting specialized recruitment & training  
- High noise level  

- Plots & conspiracies  
- Uncover weapons acquisition  
- Disappearances of operatives  
- Heightened operational security  
- Actual attacks |
| **State & Local Government Observables** | - Warnings from federal agencies  
- CIP vulnerabilities  
- Group interest in attacking high value targets  

- Radical subcultures present  
- Reported presence of cell operatives in city  

- Reported surveillance of targets  
- Reported suspicious activities |
Red Team Organization

Control Group

Analysis Cell

Trusted Agents in Blue HQ

Operation Cell and Observers
  - Leadership/C2
  - Logistics
  - Operations

Operation Cell and Observers
  - Leadership/C2
  - Logistics
  - Operations
Red Teaming Attack Scenarios

Conventional Low Impact

Conventional High Impact

Chemical

Biological

Radiological

Nuclear

Cyber

New/Other
Generic Terrorist Attack Timeline

U.S. and Allied

Political
Intelligence
Military
Information / Public Diplomacy
Commercial / Public Security
Economic/Financial
Law Enforcement

Observables and Indicators & Warning (I&W) Template

STRATEGY
PLANNING
TACTICS
WEAPONIZATION
RECRUITMENT
LOGISTICS
PREPARATION
EXECUTION

Scenario: ________ / Actor: _______

Terrorist Attack Cycle (TAC)
Response Framework
Analysis Template Concept

Observables and I&W Template—Scenario: **CLI**

Observables and I&W Template—Scenario: **CHI**

Observables and I&W Template—Scenario: **Chemical**

Observables and I&W Template—Scenario: **Biological**

Observables and I&W Template—Scenario: **Nuclear**

Observables and I&W Template—Scenario: **Cyber**

Observables and I&W Template—Scenario: **???”
## Tool Kits to Red Team Future Terrorism

### Critical Infrastructure Protection

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Al Qaeda</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>M x C x (SUM T)</td>
<td>100-0%</td>
<td>T'H</td>
<td>100-0%</td>
<td>T'H</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0% T'H Raw Score 100-0%</td>
</tr>
<tr>
<td>Aryan Nation</td>
<td>50%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>31%</td>
<td>0%</td>
<td>0%</td>
<td>50%</td>
<td>100%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>50% 100% 137%</td>
</tr>
<tr>
<td>FARC</td>
<td>50%</td>
<td>75%</td>
<td>75%</td>
<td>50%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>33%</td>
<td>50%</td>
<td>16%</td>
<td>100%</td>
<td>16%</td>
<td>10%</td>
<td>3%</td>
<td>14%</td>
</tr>
<tr>
<td>IRA</td>
<td>0%</td>
<td>100-0%</td>
<td>50%</td>
<td>75%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0%</td>
<td>0%</td>
<td>25%</td>
<td>0%</td>
<td>100%</td>
<td>0%</td>
<td>100-0%</td>
<td>0%</td>
<td>0% 0%</td>
</tr>
</tbody>
</table>

### “Trophy Targets” Risk Prioritization

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Golden Gate Bridge</td>
<td>75%</td>
<td>38%</td>
<td>50%</td>
<td>53%</td>
<td>48%</td>
<td>44%</td>
<td>100-0%</td>
<td>T'H</td>
<td>100-0%</td>
<td>T'H</td>
<td>100-0%</td>
<td>T'H</td>
<td>100-0%</td>
<td>T'H</td>
<td>100-0%</td>
<td>100-0%</td>
<td>100-0% 137%</td>
</tr>
<tr>
<td>JFK Airport Terminal</td>
<td>100%</td>
<td>50%</td>
<td>75%</td>
<td>39%</td>
<td>20%</td>
<td>10%</td>
<td>10%</td>
<td>4%</td>
<td>26%</td>
<td>14%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0% 0% 75%</td>
</tr>
<tr>
<td>Carnival Cruise Vessel</td>
<td>50%</td>
<td>25%</td>
<td>100%</td>
<td>53%</td>
<td>75%</td>
<td>36%</td>
<td>5%</td>
<td>2%</td>
<td>29%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0% 0% 82%</td>
</tr>
<tr>
<td>Union Station</td>
<td>70%</td>
<td>35%</td>
<td>30%</td>
<td>16%</td>
<td>25%</td>
<td>12%</td>
<td>10%</td>
<td>4%</td>
<td>17%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0% 0% 49%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability/risk</th>
<th>4:1 Security, Hardness, Reconnaissance, Replaceability</th>
<th>Rough Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security/risk</td>
<td>1:0.5 Security, Hardness, Reconnaissance, Replaceability</td>
<td>Rough Risk</td>
</tr>
<tr>
<td>Security/risk</td>
<td>0:1 Security, Hardness, Replaceability</td>
<td>Rough Risk</td>
</tr>
<tr>
<td>Vulnerability/risk</td>
<td>4:1 Security, Hardness, Reconnaissance, Replaceability</td>
<td>Rough Risk</td>
</tr>
<tr>
<td>Vulnerability/risk</td>
<td>1:0.5 Security, Hardness, Replaceability</td>
<td>Rough Risk</td>
</tr>
<tr>
<td>Vulnerability/risk</td>
<td>0:1 Security, Replaceability</td>
<td>Rough Risk</td>
</tr>
</tbody>
</table>

### Notes
- **Threat Score**: Combined Threat Potential against Transport Targets
- **Risk**: Vulnerability/risk + Rough Risk
Difficulties and Constraints

• Cultural
  – Need to mesh contrasting organizational cultural orientations between Red Team and government bureaucracy

• Operational
  – Easier said than done
  – Need to obtain “buy in” for Red Team activities from affected government agencies
  – Need to coordinate Red Team activities with affected government agencies
    • Issue of “need to know,” who will be “read” into the exercise, etc.

• Political
  – Policy makers don’t always have the required range of response options recommended by a Red Team
    • Some Red Team recommendations may be too controversial

• Safety
  – Cooperation of security officers may be required for some aspects of the exercises
Summary

• Benefits of Red Teaming
  – Broaden spectrum of intelligence I&W analytical processes to strengthen preemptive capabilities
  – Provides for policy, operational and intelligence fusion
  – Generate government-wide Red Teaming expertise to expand reservoir of experts who are “recycled” back to their parent agencies
Conclusion

• **Think Like the Enemy** - always anticipate and prepare to counteract new types of attacks and targeting because terrorists seek to exploit new vulnerabilities and inflict maximum damage
  – Past trends do not necessarily reveal future attack patterns

• Red Team “Out of the Box” Threat/Risk Assessments
  – Focus on multi-dimensional, not uni-dimensional, baskets of potential threats