Surveillance Detection

Prevention vs. Mitigation
MR. RICHARD KIRCHNER, JR.

CHIEF, SURVEILLANCE DETECTION
ANTITERRORISM FORCE PROTECTION DIRECTORATE
PENTAGON FORCE PROTECTION AGENCY
U.S. DEPARTMENT OF DEFENSE

20 SEPTEMBER 2011
Would you like to…

• Reduce the amount of people deployed in security
• Reduce the potential for terrorist or criminal activity
• Reduce operational deficiencies by focusing on threat vs. risk
• Enhance the capabilities of your security technology
• Enhance the security image of the organization

Proactively identify criminal & terrorist operations

Exploiting the Terrorist’s Greatest Vulnerability
Background

Historical Security Focus
- Perimeter Security / Target Hardening
- Access Control
- Incident Response

DHS Has Invested $30B+
- Physical Security
- First Responders

Impact
- Improved Damage Mitigation Profile
- More Efficient Response
Results of Focusing on Physical Security
Khobar Towers

Tanzania

Mumbai
Khobar Towers

Casing began 18-21 months before the attack
3-person team – 40 occasions
Vehicle sighted on ten separate occasions
Several other targets also cased

19 killed – 372 wounded
Terrorist Surveillance in the US

Al Qaeda surveillance operations:
- Prudential Financial Center
- NYSE, Citigroup Headquarters
- IMF, and World Bank

More than 100 photos of the Prudential Center
- Details of site security measures and ways to defeat them
- Types of badges worn by employees
- Dossiers on individual security guards
Mumbai

179 killed – 300+ wounded

Casing began at least 16 months prior to attack
Attack team had never been in the city
UNSUCCESSFUL (TERRORIST)

Fort Dix (NJ) May 2007
Daniel Patrick Boyd, Hysen Sherifi, Mohammad Omar Aly Hassan, Ziyad Yaghi, Zakariya Boyd, Dylan Boyd & Anes Subasic, arrested and charged with conducting surveillance on Quantico Marine Base and planning to attack US military members
Our Focus Must Equally Be:

PREVENTION vs. MITIGATION

Physical Security Improvements Are Not Sufficient
Every successful terrorist assault (and many criminal acts) have been preceded by extensive surveillance, reconnaissance, and logistics activity.
WHO HAS THE WILLINGNESS AND CAPABILITY TO ATTACK US?
SUSPICIOUS ACTIVITY?
SUSPICIOUS ACTIVITY?
MY BUILDING
RED SHIRT W/ SUNGLASSES…
FOREIGN NATIONAL ARMY MAJOR
Attack Cycle
Terrorist’s Greatest Vulnerability

The Intelligence Gathering Process

*Exploit This Vulnerability*

- Identify
- Gather
- Collate
- Share
- Analyze

To Identify

Patterns of Behavior Indicative of Pre-Attack Surveillance

Suspicious Activity Reports
Methodology

- Understand Surveillance
- Know The Terrorist Operational Planning Cycle
- Identify Surveillance Vulnerabilities / Zones
- Improve Observational Awareness Skills
- Effectively Employ Technology
Basic Objectives of Surveillance

• Collect Intelligence
• Avoid Detection
Specific Surveillance Objectives

- Identify facility vulnerabilities and surveillance targets
- Identify locations from which surveillance can be undertaken [RED ZONES]
- Identify and describe electronic security measures (number, location, type and coverage of cameras)
- Document security procedures
- Study security force (size, gender, ethnicity, locations, dress, weapons, competency)
- Determine First Responder response times, locations
POTENTIAL VEHICLE OBSERVATION POINTS (FIXED, FOOT & VEHICULAR)

Cafe
Deli
Parking
Taxi Stand
Parking
Signage
Basic Training

- Understand Surveillance
  - Objectives
  - Techniques
  - Methodologies
- Improve Observational Awareness
- Pay Careful Attention to Surveillance Zones
- Consider Surrounding Environments
SURVEILLANCE DETECTION TRAINING

**SD Operations Instruction & OJT**
- Types of surveillance
- Identifying Hostile Surveillance Locations
- "Reverse Engineering" what a Hostile Surveillant can see and its value
- Window matrices
- Surveillance Point diagrams
- Neutralization and exploitation
- Establishing baseline activity
- Target Analysis
- Surveillance indicators and anomalies
- Observation and reporting skills
- Surveillance Detection Routes
- Surveillance Case studies
- SD Team operations

**Counterintelligence Training**
- Counterintelligence fundamentals
- FIS Operations and Methodology
- Demeanor in a hostile real-world environment
- Changing clothes in the field
- Cover Legend (Cover for Status)
- Elicitation/Counter-Elicitation
- Foreign Nat’l and Cultural Awareness
- Overview of modern day TSCM threats
- Advanced covert camera & video usage
- Elements & signatures of espionage tradecraft

**Suicide Bomber/Behavioral Pattern Recognition (BPR) Training**
- Physiological and psychological signs associated with suicide bombers
- Critical differences between combating terrorism and criminal acts
- Design, construction, concealment and delivery of Type I, II, III improvised explosives devices (IED)
- Legally defensible suicide bomber identification techniques
- Case analysis related to studies on modern suicide bombing events
- Instruction/perform physical techniques, interception tactics and other practical skills required to effectively counter suicide bombing tactics
- Instruction/perform physical techniques and firearms skills associated with deadly-force and non-deadly force encounters (interceptions)
- Instruction/perform decision making under stress, firearms/Simunition training specific to unconfirmed and confirmed suicide bomber encounters in proximity to queued individuals and unstructured crowds.
- Stress Reflex Indicators (SRI)
- Physiological/psychological manifestations associated with BPR/SRI
- Articulation of behaviors/indicators and reasonable suspicion
- Proactive application of BPR/SRI techniques to detect imminent suicide bombing attacks
- Role and limitations of visual analysis
- Facial analysis, expressions and micro-behaviors
- Emotional speech analysis
- Gesture analysis
- General expressivity
- Sensory parameter dependent physiological responses
Multifaceted Functionality

- Detect Hostile Surveillance
- Detect Countersurveillance activities
- Support Counterintelligence Functions
- Support Executive Protection
- Provide Protective Intelligence
- Conduct Awareness Training
- Assist in Vulnerability Assessments
- Provide overwatch Special Unit activities
- Support to Incident Command
- Tactically Engage Extreme Threats
Employ Technology to Exploit Terrorist Vulnerabilities
Technology Should:

• Capture Events Quickly
  - Location, Time, Activity, Description, Image (no PII dependence)
• Establish Institutional Memory
• Structure Information to Facilitate Analysis
• Identify Patterns of Behavior Indicative of Pre-Attack Surveillance
  - Collect, collate, and analyze suspicious activity reports to detect patterns indicative of pre-attack surveillance
• Provide Immediate Feedback on Suspicious Individuals, Vehicles, etc.
• Automate Threat Information Sharing Across Regions and Industries
• Enable Ad Hoc Queries Across the Database
“...premier Surveillance Detection Program in DoD.”

- 2010 Joint Services Vulnerability Assessment (JSIVA) Team
QUESTIONS?

Surveillance Detection

Semper Vigilans - Amo Haud Alius
Always Vigilant – Like No Other

Rik Kirchner
Surveillance Detection
Division