Innovative Technology =

Security-enabling Technologies

Brian Seagrave
Vice President, Homeland Security
May 9, 2008
Security-enabling Technologies

- Situation Assessment – The Threat of Terrorism
- Mitigating the Threat
- Necessary Evolution of Technology
- An idea for the petrochemical industry
Threat Vector: Convergence, Migration, Escalation

Here Today:

- Increasing certainty of detection and apprehension at POEs and on the border
- $64 billion annual illegal drug trade (US only)
- Known links between terrorist and drug trafficking organizations
- High profile, coordinated cyber attack on Estonia
- Hackers demanding cash kill power to several African cities ... with inside help
- Proliferation of anti-forensic hacker tools
- Counterfeit routers, switches, and interface cards
- Escalating violence on law enforcement and border security officers
- 70 new smuggling tunnels found in 2008 as of May 4

Tomorrow?

- Unholy trinity of hackers, terrorists and traffickers with aligned objectives and strength through synergy
- Threat shifts first to the POEs, then onto the web, and via recruitment of personnel in the interior
- Innovation and increased sophistication in attacks
- Use of IEDs on domestic US targets

Keep in mind: they are already inside
As early as December 1993, a team of al Qaeda operatives had begun casing targets in Kenya, Senegal, Tanzania, and Djibouti.

Nairobi, Kenya
213 killed, 4500 injured
August 7, 1998

Khobar Towers, KSA
19 killed, hundreds injured
June 25, 1996

Dar Es Salaam, Tanzania
11 killed, 85 injured
August 7, 1998

Hezbollah operatives were detected conducting surveillance as early as four years before the attack.
Q: If you are Al Qaeda or Hezbollah, How do you outshine 9/11?

A: Recreate Bhopal, India
8,000 killed, 500,000 injured
December 3, 1984

Threat Escalation is Inevitable...Where are they Probing Now?
5 Success Factors in a Terrorist Attack

1. **Plant**
   - Put people in place or recruit people at locations to carry out attacks

2. **Probe**
   - Conduct surveillance & reconnaissance and trial runs on potential targets to detect weaknesses, assess impact, and develop knowledge for planning attack

3. **Procure**
   - Acquire equipment and materials, and get access to put them in place

4. **Pretend**
   - Hide, blend in, deceive personnel and authorities as to intent and identities

5. **Perform**
   - Command and control executing the operation

Tools: Money, People, Networks, Software, Hardware, Access, Identities, Mobility

To prevent a terrorist attack, it is critical to detect the discreet but identifiable indicators of the pre-attack preparations.
Threat Vector Summary

Fanaticism, desperation, money, and evolving tools combine to enable criminal and terrorist operations as sophisticated as an espionage/special forces agency.

A single integrated corps uses a variety of tools to probe for vulnerabilities in **all perimeters**, including from the inside, across multiple potential targets owned/operated by different organizations ... narrowing targets, learning how to penetrate defenses and planning their operation.
Early Warning is Key

- A **Common Security Picture (CSP)** is needed across a single organization’s assets, personnel, networks and information systems, facilities, and supply chain to detect and recognize all threats and suspicious links and patterns
  - Correlation of event data is key

- Must be structured for information sharing – not just technically, but in policy – **between separate organizations**
  - A consortium of neighboring assets messaging incident data between them
  - Using intelligent technology to detect common suspicious events and surveillance/probing
    - facial recognition, intelligent video, image analysis, license plate readers, network policy deviation, facility policy deviation, Network Operations Center, Security Operations Center … convert data to a blinded descriptive message and see who else has similar event data
  - Irrespective of ownership, liability, or security provider
Common Security Picture Concept

Step One: Deploy an Enterprise Security Common Operating Picture (COP)

Correlation across your security domains to detect patterns and links of interest

Your COP

<table>
<thead>
<tr>
<th>Surveillance</th>
<th>Facility Events</th>
<th>IT Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Mining</td>
<td>System Failures</td>
<td>Network Intrusions</td>
</tr>
<tr>
<td>LPR</td>
<td>Incidents</td>
<td>DDoS</td>
</tr>
<tr>
<td>Facial Recognition</td>
<td>Facility Intrusions</td>
<td>Stolen Identities</td>
</tr>
<tr>
<td>Digital Forensic Analysis</td>
<td>Thefts</td>
<td></td>
</tr>
</tbody>
</table>
Step Two: Common Security Picture

- Actor-identifying information
- Geospatial proximity
- Fusion (time, space)
- Matching, linking, pattern & anomaly detection

Lead sharing:

- Airport COP
- Port COP
- MTA COP
- Financial Institution COP
- NSSE COP

Indicators and warnings:
Security Technology Convergence

Drivers of Convergence: Need/threat and Internet Protocol
Security Technology Convergence

Drivers of Convergence: Need/threat and Internet Protocol
What’s on the Back Side?

Drivers of Convergence: Need/threat and Internet Protocol
The Availability of Intelligence is the 4th Factor in Security Technology Convergence
Availability of Information

Correlation and Sharing of Suspicious Events are the Key to Strong Security
The Upshot

- A single, integrated solution for managing security in all three domains is inevitable
  - The “ERP of Security”
  - Better security for lower cost
- Correlation is key
- The more data available for correlation, the more complete situational awareness becomes, and the more proactive and therefore stronger you get
  - Inter-domain incident data
  - Intra-enterprise incident data
  - Open source intelligence

Prevent the next attack through automated vigilance
An Idea for the Petrochemical Industry
Security Must Be a Layered Defense with Integration across Domains

- Extend surveillance and intelligence to provide prediction for expanded response time
- Expand detection arrays
- Correlate innocuous event data
- Increase response window: Deploy monitored tactical infrastructure to slow down intruder and speed up responders
- Position mobile response assets to reduce Time to Respond
- Integrate mix of overlapping sensors chosen to fit the attributes of each increment

The right mix of people, processes, technology & infrastructure changes for effectiveness in each tier
Active Deterrence

Q:
How do you delay a determined intruder until responders arrive, without collateral damage from lethal force?

A:
The Ray Gun
Silent Guardian™ Protection System
For Critical Infrastructure Protection

Silent Guardian™ projects high power millimeter wave directed energy

- A new less-than-lethal tool providing long range protection
- Deters and repels aggressors with zero casualties
- Establishes intent in real-time
- Repel phenomenology creates a compelling human flight response
- Effect is temporary and does not cause injury
- De-escalates aggression and outbreaks of violence
- Provides a zone of protection
- Speed of light delivery
- Commercial product is a 4th generation technology evolution

Flexible employment
- Pier-side
- Tug escort
- Helo-loaded

Relocatable protection
- High value assets
- Sensitive cargos
- Keep-out zones

Infrastructure, Chemical & Energy Protection
Port & Maritime Protection