

Understanding & Countering Adversary Methodologies for Identifying, Selecting & Targeting Urban Infrastructure





AGENDA

- 7 Steps of the Attack Cycle
- Disrupting the Cycle
- Threats, Risks & Countermeasures
- Security Plans
- Case Studies
- Challenges
- Conclusion



7 Steps of the Attack Cycle



OFFLINE SOLUTIONS

STEP 1 – INITIAL TARGET SELECTION

Collecting information on a number of targets

Diverse sources of information, including:

- + Internet
- + Media and newspapers
- + Informants, insiders

Potential targets are screened for vulnerabilities

Targets showing vulnerabilities receive additional attention



OFFLINE SOLUTIONS

STEP 2 – INITIAL SURVEILLANCE

This phase can last days, weeks, months...even years

Adversary is looking for:

- + Existing security measures
- + Vulnerabilities (weakness)
- + Predictability
- + Complacency of guards, staff, employees, etc.



OFFLINE SOLUTIONS

STEP 3 – FINAL TARGET SELECTION

Determined by:

- + Objectives & goals
- + Capabilities
- + Resources available
- + Probability of success



OFFLINE SOLUTIONS

STEP 4 – DETAILED SURVEILLANCE & PLANNING

Information gained is used to:

- + Develop detailed security assessments & prepare operations
- + Procure base of operations in target area
- + Design & test escape routes
- + Decide on type of weapon or attack
- + Penetration testing



OFFLINE SOLUTIONS

STEP 5 – FINAL SURVEILLANCE

Purpose of this phase is to:

- + Improve chances of success
- + Confirm planning assumptions
- + Develop contingency plans
- + Ensure nothing significant has changed in environment



OFFLINE SOLUTIONS

STEP 6 – DEPLOYMENT & ATTACK

Adversaries have important advantages:


- + Element of surprise
- + Choice of time, place & conditions of attack
- + Diversions or secondary attacks
- + Security & support positions to neutralize response



OFFLINE SOLUTIONS

STEP 7 – ESCAPE & EXPLOITATION

- Escape plans are usually well rehearsed
- The exception is suicide attacks, however...
- Media campaign – maximizing effect




OFFLINE SOLUTIONS

DISRUPTING THE CYCLE

There are three **phases** in the cycle where adversaries can be:

- + Deterred
- + Detected
- + Delayed
- + Disrupted



Initial Target Selection	Initial Surveillance	Final Target Selection	Detailed Surveillance	Final Surveillance	Deployment	Escape & Exploitation
--------------------------	----------------------	------------------------	-----------------------	--------------------	------------	-----------------------




OFFLINE SOLUTIONS

TYPES OF THREATS

Multiple threats to individuals & organizations:

- Theft
- Assault
- Work Place Violence
- Fire
- Kidnapping
- Terrorism
- Natural Disaster



OFFLINE SOLUTIONS

THREAT

CAPABILITY

- History

INTENT

- Can be very difficult to discern
- Might be announced in advance (i.e., social media)
- May be discovered by well-trained staff & employees

TARGETING



OFFLINE SOLUTIONS

CARVER

C – Criticality

A – Accessibility

R – Recognizability

V – Vulnerability

E – Effect

R – Recoverability



OFFLINE SOLUTIONS

RISK

What is Risk?

- Probability of being targeted
- Severity of impact from a successful attack

Severity of Risk is Determined by:

- Threat
- Vulnerability
- Consequences (impact)




OFFLINE SOLUTIONS

RISK

Criticality of Risk:

- Business
- Reputation
- Life
- Duty to Care

There are human costs and asset costs



OFFLINE SOLUTIONS

RISK

Dealing with Risk:

- Reduce
- Avoid
- Shift
- Accept

Risk Management Strategies:

- Deter
- Detect
- Deny
- Delay
- Respond (consequence management)
- Mitigate
- Recover




OFFLINE SOLUTIONS

COUNTER-MEASURES

- Threat Assessments (know the threat)
- Vulnerability Assessments (know yourself)
- Risk Assessments (know the plan)

Threat Awareness:

- This is on us!
- The warnings are there to see
- Public-Private sector partnerships are critical (fusion cells)




OFFLINE SOLUTIONS

SECURITY PLANS

Risk Assessments allow you to:

- + Prioritize & allocate limited resources
- + Develop effective plans based on identified risks
- + Test the plan (Red Teams, rehearsals, table-top exercises, etc.)
- + Implement the plan
- + Manage the plan
- + Update the plan



OFFLINE SOLUTIONS

CASE STUDIES



OFFLINE SOLUTIONS

MUMBAI 2008


- Lashkar-e-Tayyiba x 10
- 2+ years planning
- Multiple target selection
- Active shooter + multiple IEDs



- 164 Dead
- 600+ Injured





OFFLINE SOLUTIONS



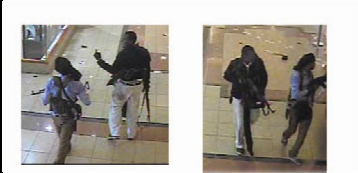
OSLO 2011

- Lone Wolf
- VBIED + Active Shooter
- 8 + 69 Dead
- 209 + 110 Injured







OFFLINE SOLUTIONS



WESTGATE 2013

- Al-Shabaab x 4
- Active Shooters + IEDs
- 67 Dead
- 175 Injured






OFFLINE SOLUTIONS

BESLAN 2003

- Chechen Separatists
- Hostage Situation
- 385 Dead
- 700+ Injured






OFFLINE SOLUTIONS

OKLAHOMA CITY 1995




- Lone Wolf
- 1+ years planning
- Multiple target selection
- VBIED (2,200kg)
- 168 Dead
- 324 Injured
- Cost: USD 3,500




OFFLINE SOLUTIONS

BOSTON 2013



- Lone Wolf x 2
- IED x 2
- 3 Dead
- 264 Injured



OFFLINE SOLUTIONS

CHALLENGES

- Slow acceptance of a changing situation
- Difficult to assess the situation
- Difficult to acquire accurate information
- Determining risk threshold
- Low Probability – High Impact

CONCLUSION

"Security is both a feeling and a reality but they are not the same"



OFFLINE SOLUTIONS

Ulitsa Iza Laze 9
Split 21000 - Croatia
Office: +385 21 347 607
Fax: +385 21 770 627
Iridium: 8816 224 39 396
Email: info@offlinesolutions.net
Web: offlinesolutions.eu
