Critical Infrastructure Protection Metrics and Tools; Techniques for Adversary Threat Probability Assessment [June 5-7, 2008] [video]
Techniques for Adversary Threat Probability Assessment

William L. McGill

06 June 2008

First Principles ➞ The Basic Model ➞ Some Examples ➞ Discussion
Basic Definitions

- **Risk** is the potential for harm or loss
- A **hazard** is a source of risk in general
- A **threat** is a source of risk that is plausible with respect to a DM’s specific circumstances
Risk = Threat × Vulnerability × Consequence

*RISK* is the **COMBINATION** of the set of **THREATS**, **CONSEQUENCES**, and **VULNERABILITIES**
The Risk Triplet

\[ R_{ij} = \langle e_i, p_{ij}, c_j \rangle \]

1. What are the plausible initiating events?
2. What are the consequence of concern?
3. How likely is this combination of cause and consequence?
The Basis of Risk

\[ p_{ij} = \Pr(e_i,c_j) = \Pr(e_i)\Pr(c_j|e_i) \]

- Probability of Initiating Event (threat probability)
- Probability of Consequence \( c_j \) given Occurrence of Initiating Event \( e_i \) (vulnerability to \( c_j \) from \( e_i \))

[See McGill and Ayyub 2008]
### Table I. Scenario List

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Likelihood</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td>$p_1$</td>
<td>$x_1$</td>
</tr>
<tr>
<td>$S_2$</td>
<td>$p_2$</td>
<td>$x_2$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$S_N$</td>
<td>$p_N$</td>
<td>$x_N$</td>
</tr>
</tbody>
</table>

---

#### Hazard Likelihood and Consequence Analysis

- **Casualty Loss (Fatalities)**: Casualty loss from different scenarios is shown on the x-axis, ranging from 0 to 1,000,000 fatalities.
- **Annual Exceedence Rate**: The annual exceedence rate is shown on the y-axis, ranging from $1.E-09$ to $1.E+01$.

#### Membership Analysis

- **Probability of Exceedance**: The probability of exceedance is shown on the y-axis, ranging from 0 to 1.
- **Loss in Fatalities**: The x-axis represents the loss in fatalities, ranging from 0 to 10,000 fatalities.

#### Hazard Types

- Major Hurricane
- Tornado
- Drought
- Winter Storm
- Nuclear Attack
- Explosive Attack
- Airplane as Projectile
- Biological Attack
- Industrial Accident
- Regional Total
• Probability that a hazardous initiating event $e_i$ will occur:
  – At a given location?
  – Of a given type?
  – At a given time?
Types of Hazardous Events

- Explosives
- CBRN
- Sabotage
- Novel types (e.g., RF)
- Kinetic
- Others...

All Hazards

Natural
- Meteo
- Astro
- Geo

Anthropic
- Techno
- Accident
- Malicious
All Possible Scenarios

- No Event Occurs
- A NATURAL Event Occurs
- A NATURAL Event Occurs
- Technological Event Occurs
- An Accident Event Occurs
- A Malicious Attack Occurs
A Malicious Attack Occurs Against Something the Doesn’t Matter to Me
An Explosive Macro Occurs Against Something That Matters to Me.

Stadium

Office Building

Power Substation

Train Station

Hospital

- P1
- P2
- AP3
- P4
- P5
- P6
- P7
- AP8
- P9
- P10
- AP11
- P12
Scenarios and Surprise

“The unilateral advantage gained by the introduction of a new weapon (or by the use of a known weapon in an innovative way) in conflict against an adversary who is either unaware of its existence or not ready with effective countermeasures, the development of which requires time.”

Adapted from: Cynthia Grabo, Anticipating Surprise: Analysis for Strategic Warning

- Knowledge of plausible alternative scenarios is an essential element of defeating surprise
- In general, the scenario identification is the most important step of the risk analysis process
### Threat Types

<table>
<thead>
<tr>
<th>Cyber</th>
<th>Radiological</th>
<th>Sabotage</th>
<th>Biological</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laser</td>
<td>Projectile and Impact</td>
<td>Explosive</td>
<td>Assault</td>
</tr>
</tbody>
</table>

### Critical Elements

<table>
<thead>
<tr>
<th>Building</th>
<th>Computer Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipeline</td>
<td>People</td>
</tr>
<tr>
<td>HAZMAT Storage</td>
<td>Railcars</td>
</tr>
</tbody>
</table>

The set of threat scenarios consists of all possible threat scenario - susceptible critical element pairs.

#### Threat Scenarios

<table>
<thead>
<tr>
<th>Explosive</th>
<th>Building</th>
<th>Projectile</th>
<th>HAZMAT</th>
<th>Assault</th>
<th>People</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projectile</td>
<td>Building</td>
<td>Incendiary</td>
<td>HAZMAT</td>
<td>Explosive</td>
<td>Computers</td>
</tr>
<tr>
<td>Incendiary</td>
<td>Building</td>
<td>Explosive</td>
<td>HAZMAT</td>
<td>Incendiary</td>
<td>Computers</td>
</tr>
<tr>
<td>Explosive</td>
<td>Pipeline</td>
<td>Sabotage</td>
<td>HAZMAT</td>
<td>Radiological</td>
<td>Computers</td>
</tr>
<tr>
<td>Sabotage</td>
<td>Pipeline</td>
<td>Projectile</td>
<td>HAZMAT</td>
<td>Radiological</td>
<td>Computers</td>
</tr>
<tr>
<td>Explosive</td>
<td>Rat Car</td>
<td>Chemical</td>
<td>People</td>
<td>Sabotage</td>
<td>Computers</td>
</tr>
<tr>
<td>Sabotage</td>
<td>Rat Car</td>
<td>Radiological</td>
<td>People</td>
<td>Sabotage</td>
<td>Computers</td>
</tr>
<tr>
<td>Explosive</td>
<td>People</td>
<td>Laser</td>
<td>People</td>
<td>Sabotage</td>
<td>Computers</td>
</tr>
</tbody>
</table>

#### Relevant Attack Profiles for Explosive – HAZMAT Scenario

- **On Person – Via Back Road**
  - On Person
  - Ground Vehicle (A) – Via Back Road
  - Ground Vehicle (B) – Via Back Road
  - Ground Vehicle (C) – Via Back Road
  - Aerial Vehicle (Human) – Via Back Road
  - Waterborne Vehicle (Human) – Via Back Road
- **On Person – Via Main Access Road**
  - On Person – Via Main Access Road
  - On Person – Via Water
- **On Person – Via Forest**
  - On Person – Via Forest
  - Aerial Vehicle (Human) – Via Air
- **Waterborne Vehicle (A) – Via Water**
  - Aerial Vehicle (Human) – Via Air
  - Aerial Vehicle (Human) – Via Water
  - Waterborne Vehicle (A) – Via Water

#### Attack Profiles Compatibility Matrix

Threat scenarios are defined as the pairing of threat type to a susceptible critical element via a target susceptibility matrix.

#### Attack Profiles Compatibility Matrix

Attack profiles are defined as the pairing of threat delivery systems to compatible intrusion paths via an attack profile compatibility matrix.

#### Delivery Systems for Explosive Threats

- On Person
  - Ground Vehicle (Human)
  - Ground Vehicle (Human)
  - Waterborne Vehicle (Human)
- Waterborne Vehicle (Autonomous)
- Aerial Vehicle (Human)
- Aerial Vehicle (Human)

#### Intrusion Paths

- Via Back Road
  - Via Main Access Road
  - Via Water
  - Via Forest
  - Via Air

The set of attack profiles consists of all representative delivery system – compatible intrusion path pairs.
• The probability of realizing an attack profile given an event:

\[
\Pr(P) = \Pr(P \mid S, A) \Pr(S \mid A) \Pr(A)
\]

or

\[
\Pr(P) = A_P A_S A_A
\]

where:

• \(A_P\) = Relative attack profile attractiveness
• \(A_S\) = Relative scenario attractiveness
• \(A_A\) = Relative asset attractiveness
• \(\lambda_0\) = Baseline threat rate of occurrence
Generic Profile Utility:

\[ U_P = \max \left( G^* P_S^* - L^* (1 - P_S^*) - C^*, 0 \right) \]

Relative Attack Profile Attractiveness:

\[ A_P = \frac{U'_P}{\sum_P U'_P} \]

\[ U'_P = \delta_P U_P \]

Scenario Utility:

\[ U'_S = \delta_{S_i} \max \left( U_P \right) \]

Relative Scenario Attractiveness:

\[ A_S = \frac{U'_S}{\sum_S U'_S} \]

Asset Utility:

\[ U'_A = \delta_{A_i} \max \left( U_S \right) \]

Relative Asset Attractiveness:

\[ A_A = \frac{U'_A}{\sum_A U'_A} \]
Conservative Assumptions

- **Perfect Knowledge:** The adversary has perfect knowledge of everything.

- **Zero-sum game:** The adversary’s gain exactly balances the defender’s loss.
Prototypical Adversaries

• The “rational” adversary

\[ U_P = G^* P_S^* \]

• The “gain maximizer”

\[ U_P = G^* \]

• The “success maximizer”

\[ U_P = P_S^* \]
INTRUSION PATHS LEADING TO TANK 1 / 2

1. Ground (Forest)
   - Security Zone 1
   - Not drawn to scale
   - Tank

2. Ground (Main Gate)
   - Security Zone 3
   - Not drawn to scale
   - Tank

3. Water
   - Security Zone 4
   - Not drawn to scale
   - Tank

4. Air
   - Security Zone 5
   - Not drawn to scale
   - Tank

Attack Profile Attractiveness

<table>
<thead>
<tr>
<th>Attack Profile</th>
<th>Intrusion Path</th>
<th>$P_{VP}$</th>
<th>$P^*_{S}$</th>
<th>$G^1$</th>
<th>$U'_{P}$</th>
<th>$A_P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery System</td>
<td>Hand Emplaced</td>
<td>1.0</td>
<td>0.38</td>
<td>67.1</td>
<td>25.3</td>
<td>0.06</td>
</tr>
<tr>
<td></td>
<td>Ground (Forest)</td>
<td>1.0</td>
<td>0.16</td>
<td>67.1</td>
<td>10.5</td>
<td>0.03</td>
</tr>
<tr>
<td></td>
<td>Ground (Main Gate)</td>
<td>1.0</td>
<td>0.53</td>
<td>67.1</td>
<td>35.7</td>
<td>0.09</td>
</tr>
<tr>
<td></td>
<td>Water</td>
<td>1.0</td>
<td>1.00</td>
<td>200</td>
<td>200</td>
<td>0.50</td>
</tr>
<tr>
<td>Ground Vehicle</td>
<td>Ground (Main Gate)</td>
<td>1.0</td>
<td>1.00</td>
<td>200</td>
<td>200</td>
<td>0.50</td>
</tr>
<tr>
<td>Manned Aerial Vehicle</td>
<td>Air</td>
<td>1.0</td>
<td>0.94</td>
<td>76.9</td>
<td>72.3</td>
<td>0.18</td>
</tr>
<tr>
<td>Unmanned Aerial Vehicle</td>
<td>Air</td>
<td>1.0</td>
<td>0.99</td>
<td>57.3</td>
<td>56.5</td>
<td>0.14</td>
</tr>
</tbody>
</table>

Note(1): Gain from success in units of millions of dollars
### Threat Scenario

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Key Element</th>
<th>$P_{VE}$</th>
<th>Max($U'_p$)</th>
<th>$U'_s$</th>
<th>$A_s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explosive Attack</td>
<td>Main Building</td>
<td>0.80</td>
<td>50.1</td>
<td>40.1</td>
<td>0.07</td>
</tr>
<tr>
<td></td>
<td>Personnel</td>
<td>0.80</td>
<td>60.1</td>
<td>48.1</td>
<td>0.09</td>
</tr>
<tr>
<td></td>
<td>Loading Dock</td>
<td>0.60</td>
<td>20.0</td>
<td>12.0</td>
<td>0.02</td>
</tr>
<tr>
<td></td>
<td>Pipeline</td>
<td>0.40</td>
<td>20.0</td>
<td>8.02</td>
<td>0.01</td>
</tr>
<tr>
<td></td>
<td>80-Ton Rail Car</td>
<td>0.80</td>
<td>60.1</td>
<td>48.1</td>
<td>0.09</td>
</tr>
<tr>
<td></td>
<td>Chemical Tank 1</td>
<td>1.00</td>
<td>180</td>
<td>180</td>
<td>0.34</td>
</tr>
<tr>
<td></td>
<td>Chemical Tank 2</td>
<td>1.00</td>
<td>200</td>
<td>200</td>
<td>0.37</td>
</tr>
</tbody>
</table>

*Note (1): Notional maximum attack profile utilities provided for other key elements. Utility expressed in millions of dollars.*

### Attack Profile

<table>
<thead>
<tr>
<th>Delivery System</th>
<th>Intrusion Path</th>
<th>$P_{VA}$</th>
<th>$U'_s$</th>
<th>$A_s$</th>
<th>Baseline Frequency, $\lambda_s$ (Events per Year)</th>
<th>$\lambda_s$ (Events per Year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hand Emplaced</td>
<td>Ground (Forest)</td>
<td>1.0</td>
<td>200</td>
<td>0.01</td>
<td>1/25</td>
<td>9.455E-05</td>
</tr>
<tr>
<td></td>
<td>Ground (Main Gate)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.919E-05</td>
</tr>
<tr>
<td></td>
<td>Water</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.334E-05</td>
</tr>
<tr>
<td>Ground Vehicle</td>
<td>Ground (Main Gate)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7.482E-05</td>
</tr>
<tr>
<td>Manned Aerial Vehicle</td>
<td>Air</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.700E-05</td>
</tr>
<tr>
<td>Unmanned Aerial Vehicle</td>
<td>Air</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.107E-05</td>
</tr>
</tbody>
</table>

---

**Scenario Attractiveness**

**Asset Attractiveness**
### Adversary Characterization

This page specifies the preferences of the adversary.

#### Adversary Focus
- Maximizing Disruption
- Maximiing Economic Losses
- Maximiing Fatalities

#### Convert from Dollars to Utility

#### Convert from Lives to Utility

#### Adversary Utility Shape
- 5.0

<table>
<thead>
<tr>
<th>Attack Profile</th>
<th>VBIED</th>
<th>AVIED</th>
<th>WBIED</th>
<th>HEIED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adversary Loss from Failure</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>Cost to Execute Attack</td>
<td>1.00</td>
<td>4.00</td>
<td>2.00</td>
<td>1.00</td>
</tr>
<tr>
<td>Minimum Scenario Utility</td>
<td>0.00E+00</td>
<td>0.00E+00</td>
<td>0.00E+00</td>
<td>0.00E+00</td>
</tr>
<tr>
<td>Awareness of Attack Profile</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
</tbody>
</table>
Thank you for your time!