SECONOMICS

Scenario Based Adversarial Risk Analysis on Transport Infrastructures

J. Cano[1] D. Ríos Insua[2] A. Tedeschi[3] U. Turhan[4]

[1]URJC

[2]Royal Academy of Sciences, Spain

[3]DeepBlue Srl, Italy

[4]Anadolu University, Turkey

XXII MCDM. Málaga. June 17, 2013

SEVENTH FRAMEWORK PROGRAMME

Outline

Description of the problem

Defender's problem

Attacker's problem

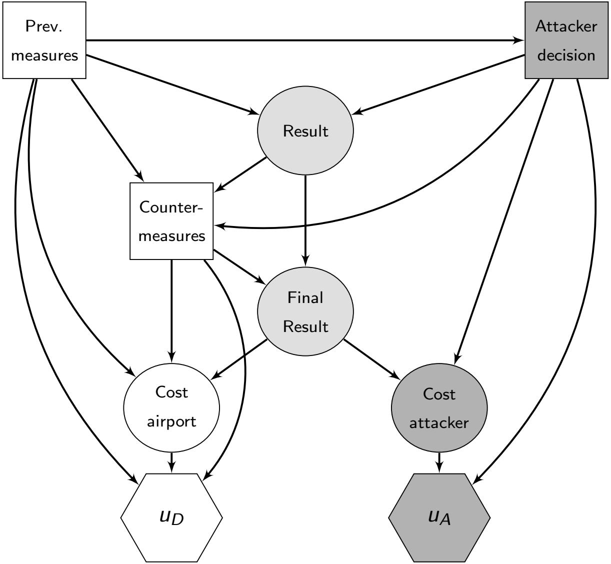
Results

1. Description of the problem

General overview

- Unlawful access to ATC Tower.
- ATC Tower attached to terminal building.
  - Gate located in terminal main lounge.
  - Covered by CCTV cameras.
- Attackers plan to enter ATC Tower, taking hold of air traffic.
- After first security checks, they could enter ATC Tower, capture ATCOs and interfere with air traffic.

Influence diagram. Seq D-A-D



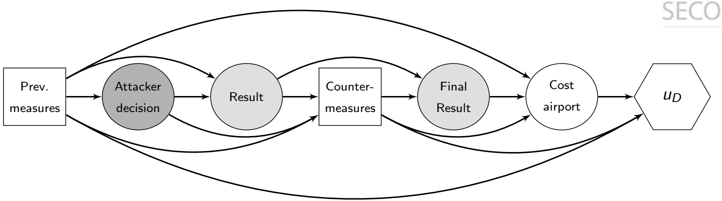
Relevant elements

SECONOMICS

- "Prev. measures" and "Countermeasures", Defender's first and second decisions, $d_1 \in \mathscr{D}_1$, $d_2 \in \mathscr{D}_2$.
- "Attacker decision" undertaken by terrorists, $a \in \mathscr{A}$.
- "Result", only relevant uncertainty, $s_1 \in \mathscr{S}_1$ (depends on (d_1, a)),
- "Final Result", $s_2 \in \mathscr{S}_2$ (liberate ATC Tower, cost what it may).
- "Cost airport" depends on $(d_1, s_1, d_2, s_2) \longrightarrow$ utility u_D.
- "Cost attacker", depends on $(a, s_1, d_2, s_2) \longrightarrow$ utility u_A.

2. Defender's problem

Preventive/recovery measures



- Cameras (preventive), (x_1, c_1).
- Metal detectors (preventive), (x_2, c_2).
- X-ray devices (preventive), (x_3, c_3).
- Airport police (preventive/recovery), (x_4, c_4).
- Airport private security (preventive/recovery), (x_5, c_5).
- **Special police force (government, recovery).**

Countermeasures $(x_1, x_2, x_3, x_4, x_5)$ ***deterrent*** *aspect, reducing Attacker's probability of success. Recovery measures aim at* ***minimizing consequences*** *of attack,* ***recovering*** *from it.*

Defender's dynamics

- Invest $(x_1, x_2, x_3, x_4, x_5)$, incurring in a cost

$$c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5.$$

- Observe terrorists' attack, and (if successful) take appropriate recovery measures.
  - Try to recover as soon as possible, no matter the costs.
- Face consequences of attack.
  - Cost of a life, c_{life}.
  - Flight diversion/cancellation, $c_{\text{div-cancel}}$.
  - Image and political costs, c_{image}. Difficult to assess.
- Get utility (depends on costs of preventive measures, and possible damages/casualties caused by attack).
  - Assume risk aversion $u_D(c_D) = -\exp(k_D \cdot c_D)$.

Solving Defender's problem

1. Compute maximum utility action at node "Countermeasures"

$$d_2^*(d_1, s_1) = \arg\ \max_{d_2 \in \mathscr{D}_2} u_D(d_1, s_1, d_2).$$

   - Need $u_D(d_1, s_1, d_2)$, $\forall (d_1, s_1)$.

2. Compute expected utility at node "Result"

$$\psi_D(d_1, a) = \int u_D(d_1, s_1, d_2^*(d_1, s_1)) p_D(S_1 = s_1 | d_1, a)\, \mathrm{d}s_1.$$

   - Need $p_D(S_1 = s_1 | d_1, a)$, $\forall (d_1, a)$.

3. Compute expected utility at node "Attacker decision"

$$\psi_D(d_1) = \int \psi_D(d_1, a) p_D(A = a | d_1)\, \mathrm{d}a,\ \forall d_1.$$

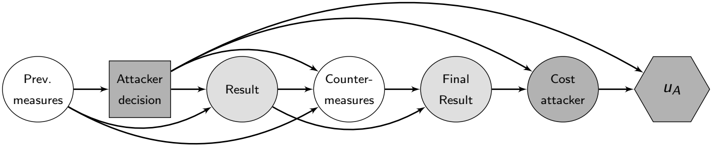
   - Need $p_D(A = a | d_1)$ (key point, solve Attacker's problem!).

4. Find max. expected utility decision at node "Prev. measures"

$$d_1^* = \arg\ \max_{d_1 \in \mathscr{D}_1} \psi_D(d_1).$$

3. Attacker's problem

Possible attacks



- Two possibilities:
  - Terrorists decide to attack ATC Tower.
    - 1–5 terrorists (influence on attack success and impact).
  - They decide to do nothing.

Attacker's dynamics

- See security measures deployed $(x_1, x_2, x_3, x_4, x_5)$.
- Decide attack $a \in \mathscr{A}$.
- Face operational costs.
  - In general, little preparation needed.
- Suffer consequences of recovery measures.
- Get utility (depends on operational costs, revenues from successful attack and recovery measures).

Consequences for Attacker

- Upon launching an attack to ATC Tower
  - Take control over air traffic operations.
    - Panic situation.
    - Force authorities to some negotiation.
    - Cause as much economic and political damage to airport and government.
    - Not all directly monetized, but high utility for Attacker.
  - Terrorists' lives lost.
    - For some terrorists (suicide), not an issue.
- Attacker's utility aggregates both aspects

$$u_A(a, s_1, d_2) = w_1 u_1(\text{revenues}) + w_2 u_2(\text{casualties}).$$

Uncertainty about Attacker's elements

- Defender has uncertainty about
  - Attacker's utility $\longrightarrow U_A(a, s_1, d_2)$, typically through

    $$u_A(c_A) = \exp(k_A \cdot c_A),\ k_A \sim \mathscr{U}(0, K_A).$$

  - Attacker's beliefs on success of attacks $\longrightarrow P_A(S_1 | d_1, a)$. We use beta distribution centered around Defender's own beliefs.
  - Attacker's beliefs on Defender's response $\longrightarrow P_A(D_2 | d_1, a, s_1)$. Typically, Attackers expect Defender to respond similarly to first stage.
- Uncertainty propagated to compute $p_D(A = a | d_1)$.

Solving Attacker's problem

1. Compute expected utility at node "Countermeasures"

$$\Psi_A(d_1, a, s_1) = \int U_A(a, s_1, d_2) P_A(D_2 = d_2 | d_1, a, s_1) \, \mathrm{d}d_2.$$

   - Need $U_A(a, s_1, d_2)$, $\forall (a, s_1, d_2)$, $P_A(D_2 = d_2 | d_1, a, s_1)$, $\forall (d_1, a, s_1)$.

2. Compute expected utility at node "Result"

$$\Psi_A(d_1, a) = \int \Psi_A(d_1, a, s_1) P_A(S = s_1 | d_1, a) \, \mathrm{d}s_1.$$

   - Need $P_A(S_1 = s_1 | d_1, a)$, $\forall (d_1, a)$.

3. Compute maximum utility action at node "Attacker decision"

$$A^*(d_1) = \arg\ \max_{a \in \mathscr{A}} \Psi(d_1, a), \ \forall d_1.$$

4. Defender's predictive density over attacks given by

$$\int_0^a p_D(A = x | d_1) \, \mathrm{d}x = \Pr(A^*(d_1) \leq a).$$

Monte Carlo estimation of $p_D(A = x|d_1)$

1. For each d_1

   For $k = 1$ to N

   Draw $\left(u_A^k(a, s_1, d_2), p_A^k(S_1|d_1, a), p_A^k(D_2|d_1, a, s_1)\right) \sim F$

   At chance node D_2, compute

   $$(d_1, a, s_1) \to \psi_A^k(d_1, a, s_1) = \int u_A^k(a, s_1, d_2)\, p_A^k(D_2 = d_2|d_1, a, s_1)\, dd_2$$

   At chance node S_1, compute

   $$(d_1, a) \to \psi_A^k(d_1, a) = \int \psi_A^k(d_1, a, s_1)\, p_A^k(S_1 = s_1|d_1, a)\, ds_1$$

   At decision node A, compute

   $$d_1 \to a_i^*(d_1) = \arg\max_{a \in \mathscr{A}} \psi_A^k(d_1, a)$$

2. For any a

   Approximate $\int_0^a p_D(A = x|d_1)\, dx$ through $\#\{1 \le k \le N :\ a_i^*(d_1) \le a\}/N$.

4. Results

Case study: small airport

- Southeastern European small-size international airport.
- International and domestic flight operations.
- Single runway flight operations.
- Runway 3000×45 meters.
- Runway lighted for night flights.
- Radio navigation aids.

Contemplated new preventive measures

SECONOMICS

Measure	Max	Cost (€)/unit	Deterrence	Detection
Cameras	4	450/850	Moderate-high	Moderate (persons)
Metal detectors	1	6,500	Moderate	High (material)
X-ray devices	1	90,000	Moderate	High (material)
Police	5	1,550/1,750	High	High (persons)
Private security	10	1,300	High	Moderate (persons)
Special force	20	Per operation	—	—

- Estimated investment budget 100,000 €.
- Different scenarios depending on:
  - $p_D(S = 1 | a = \{1, 2, 3, 4, 5\}, d_1)$.
  - k_D (forcefulness in fighting against terrorists).
  - Parametrization of attack duration and consequences (Image/political costs).

Main conclusions

- Upon perceived low-level threats, authorities tend to underestimate risk.
  - Attackers see a breach in security (more attackers).
  - Great impact can be caused even with low-profile attacks.
  - Low-cost preventive measures and well-trained personnel could deter attackers or minimize their number.
- Under scenario of high probability of attack.
  - Authorities tend to invest on expensive (sometimes sensationalist and ineffective) measures.
  - Set up security protocols for personnel increase their efficiency.