

RISKS OF TERRORIST ATTACKS

PROBABILISTIC ASSESSMENT AND USE OF INTELLIGENCE INFORMATION

M. ELISABETH PATÉ-CORNELL

Professor and Chair

Department of Management Science & Engineering

Stanford University

Terrorism Risk Analysis Symposium

USC

January 15, 2005

©Elisabeth Pate-Cornell, Stanford
University

A copy of this presentation has been
provided for viewing purposes only and
is not for reproduction.

OBJECTIVE:

DEVELOP METHODS OF RISK ANALYSIS FOR DHS AND INTEL. COMMUNITY

- **Use of Systems analysis & Bayesian Probability**
- **To assess**
 - **Prob. of attack scenario: threats and vulnerabilities**
 - **Spectrum (and distribution) of damage levels**
- **Dynamic analysis:**
 - **Updating based on intelligence regarding threat**
 - **On analysis and statistical data given changes in system and new information for vulnerabilities**

TERRORIST RISK STUDY

(Ref. Mil. OR with Seth Guikema)

SET PRIORITIES IN THE FACE OF CONFUSION

- Rank threat scenarios
- Identify *weaknesses* in physical and organizational systems: set priorities in *vulnerability* assessments
- Identify and prioritize *countermeasures*
- Set priorities in *intelligence* gathering and analysis

THREATS AND VULNERABILITIES

- **Not independent**
- **Probabilistic analysis of threat (attack) scenarios => loads on systems (physical and organizational)**
- **Use of PRA in the vulnerability assessment (e.g.: banking network) => systems capacity**
- **Countermeasures and damage control**

CHALLENGES: THREATS

- **Threat identification: start with terrorist groups**
- **Attack scenarios include for each terrorist group**
 - Weapons, Targets, Means of delivery, Time window
 - Probabilities based on attractiveness feasibility and effectiveness (*terrorists objectives, supply chain, vulnerability of targets*)
- **Sources of data: Prior knowledge of terrorists' objectives and means, intelligence over time.**
- **Challenges: uncertainty, contradictory information and constant change. Communicate spectrum of possibilities. Time window problem.**

CHALLENGES: VULNERABILITIES

- **Probability of failure under**
 - Different types of attack (ex: explosions vs. fires for structures)
 - Severity of load
 - => Analysis includes both access (opportunities) and system's capacity for different load types
- **Sources of data**
 - Tests
 - Experience
 - Engineering models and probabilistic analysis
 - Expert opinion
- **Challenge: setting priorities among vulnerability assessment tasks**

AN OVERALL MODEL STRUCTURE



VARIABLES AND REALIZATIONS

AN INCOMPLETE, ILLUSTRATIVE LIST

Terrorist groups/Individuals

e.g., Islamic terrorist groups, Disgruntled American, Foreign disgruntled

Terrorist objectives (attributes of value for a successful outcome)

e.g., Symbolism of target, damage and casualties, disruption of U.S. life and economy

Threats (weapons)

e.g., Nuclear (war heads or “dirty bombs”), bio-attacks, conventional explosions

VARIABLES cont.

Means of delivery

e.g., Trucks and cars, people, airplanes, ships, etc.

Targets:

e.g., Main, visible, symbolic buildings, civilian and military infrastructures, embassies, crowded urban areas, religious buildings etc.

Terrorist groups supply chain:

People, skills, communications, transportation, cash, and materials

Outcome evaluation from the U.S. standpoint (Attributes):

Lives lost, economic damage, instability, loss of liberties, restriction of movement, loss of international influence, prestige and leadership

BASES OF PROBABILISTIC SCENARIO ANALYSIS

$p(\text{Successful Attack}) = p(\text{Intent}) \times p(\text{Successful Planning} \mid \text{Intent}) \times p(\text{Implementation} \mid \text{SP \& I}) \times p(\text{No U.S. interference} \mid \text{Impl., etc.})$

Ex: Nuclear warheads (Islamic Fundamentalists)

Unlikely given obstacles. BUT: probability of successful attack =

$p[X:\text{they own loose nuke(s)} \& Y:\text{code known} \& Z:\text{inside the US} \& W:\text{no detection}]$

$= p(X) \times p(Y \mid X) \times p(Z \mid X, Y) \times p(W \mid X, Y, Z)$

KEY HYPOTHESES FROM THE US VIEW POINT

1. The probability of each scenario per time unit is proportional to expected utility *for the perpetrator group* weighted by probability of intention for each group for the considered time window (both *as assessed by the US based on available intelligence*)
2. Ranking of threat scenarios by order of expected “disutility” (negative impact) *to the US*. The input used should reflect opinions of appropriate experts in their fields as opposed to intuitive global ranking by experts

DYNAMICS AND GAMES

Dynamic analysis:

Updating of the model for each time period

Game:

- **Moves and countermoves (use of a game theoretic model)**
- **Updating based on new information/intelligence (e.g., outcome of previous operations, the location of a source of material)**
- **Organizational changes (e.g., the emergence of a new group or cell structure)**
- **Political changes (shifts in alliances, objectives, etc.)**
- **Technological changes (e.g., breakthrough in nuclear weapons)**

ROLE OF INTELLIGENCE

1 Pick up signals of potential attacks

- Observe and identify signal out of noise
- Generate possible scenarios
- Assess chances, rank possibilities, generate counterterrorism actions; propose response

B. Go get the information to respond to known threat

- Identify potential sources
- Choose means of detection
- Analyze intelligence, update probabilities, propose response

In both cases, usefulness of Bayesian treatment of information

SEPTEMBER 11, 2001 AND THE FAILURE OF THE INTEL. COM.

- Two “fusion of information” problems
 - Different pieces of information
 - Communications across agencies:
Organizational and cultural problems
- TTIC (Terrorist Threat Integration Center) at DHS
- Connecting the dots while respecting civil liberties: the Markle Foundation report
“Creating a Trusted Information Network for Homeland Security”

INTELLIGENCE: TWO KINDS OF UNCERTAINTY PROBLEMS

- Terrorist attack plans on the U.S. have been foiled in the past (e.g., on LAX in December 1999) and other instances; others were missed (WTC in 1993)
- Two kinds of uncertainty problems:
 - The statistical one of extracting information from background noise (e.g., chatter on the phone system)
 - The probabilistic problem of identifying and gathering information that would confirm (or not) worrisome prospects (e.g., whether specific treat is real).
- Question:
Where to look in the haystack? Monitoring of groups and of their *supply chains*: a probabilistic risk analysis approach

BAYESIAN ANALYSIS OF INTELLIGENCE SIGNAL

- An obvious exercise in theory:
$$p(A|S_1, S_2, \text{etc.}) = p(A) \times p(S_1, S_2, \text{etc.}|A) / P\{S_i\}$$
where the evidence is $E = \{S_i\}$
- The most difficult: $p(E)$ because one has to generate a set of other possible scenarios (properly structured), assess from expert opinions their priors and the likelihood of the evidence, unless the signal and the hypotheses have occurred frequently enough that we have sufficient statistics, which is seldom the case.
- Extremely difficult to implement for two reasons:
 - The analysts have not been trained that way
 - The top decision makers do not understand the language and the pedigree of probability

COMMUNICATION ISSUES

- Public Alert System regarding terrorist attack risk:
Difficulties of communicating risk to the public (especially when the signal is unclear). Ex. The color coded system of the DHS. Would quantification help? Perhaps if it is well done. But what to do at a given time and what to say to the public?
- Officials:
Difficulty of generating and communicating the different alternative hypotheses to the decision makers. The dislike for “two-armed scientists” (analyst) and the incentive to jump on the most likely – or preferred- hypothesis and pretend that that’s it (e.g., intelligence problems). Separation of policy making and intelligence?

CONCLUSIONS

- Fusion of information across agencies is improving
- All data bases cannot be merged
but many links (interfaces) can be and are being established
- The use of Bayesian probability is *not* part of the culture
but I think that we are slowly getting there
- Human intelligence collection and analysis is more important than ever; but technologies offer enormous opportunities

CONCLUSIONS cont.

- Trade-offs between false positives and false negatives are unavoidable; have to be recognized and handled with clear values because we care about protecting both the US and individual rights
- The design of the organization(s) that observe(s) signals and manage(s) the risk is essential to success. Structure, procedures and culture determine information, incentives and the spectrum of possible actions.
- Two very different but thorny communication problems: to the upper-level decision maker(s) and to the public
- And when the intelligence community is successful, no one hears about it...