

# **Risk estimation and national security: introduction and overview**

A. John Bailer

Department of Mathematics and Statistics  
Miami University  
Oxford, Ohio 45056

[baileraj@muohio.edu](mailto:baileraj@muohio.edu)

**Acknowledgments:**

- \* David Banks – for organizing this session and inviting me to participate
- \* Bill Kastenberg – for sharing notes and perspectives on risk from a nuclear engineering perspective
- \* Numerous colleagues for insights and discussions associated with risk assessment

**Caveats/confession:**

- \* Background in health risk assessment and estimation issues

205-230

Risk Estimation and National Security: Introduction and Overview

A. John Bailer\* +

Risk estimation might be used to set exposure limits to chemicals in the workplace, to determine allowable contaminant levels for wastewater treatment plants or to establish engineering targets for operating characteristics of the space shuttle. Other examples include the risk of failure of safety systems in nuclear power plants or buildings in response to seismic events. Concerns for the risk of terrorism are not far from conscious thoughts in days of color-coded travel alerts. These concerns reflect a low probability-high impact hazard. In this overview, an introduction to risk assessment ideas including hazard identification, exposure assessment, dose-response modeling and risk characterization will be presented. The distinction between risk assessment for chemical agents and failure of complex systems will be discussed and risk of terrorism will be placed in this context.

230-255

Biosurveillance and the BioSense Program

Henry Rolka and John Copeland\* +

Empirical biosurveillance systems frequently use temporal and geographic contexts to establish a baseline against which to compare recent data. Numerous varieties of data types are used in varying levels of geographic scope across levels of public health. There are many components all of which must develop and function in concert in order for success in early event detection or situational awareness. A brief background and history of what has been done in this area at CDC will be presented with an update of the BioSense Program.

255-320

Risk Analysis at Los Alamos National Laboratory

Alyson G. Wilson\* +

Risk analysis at Los Alamos focuses around the analysis of complex systems. This talk focuses around the steps that we use to develop analyses: representing the systems, mapping the data, analyzing the data, and making decisions about future data collection. These are the steps used for risk assessment and risk management. Each step is illustrated using examples from the Department of Defense, Department of Energy, or Department of Homeland Security.

## Outline:

0. Preliminaries ...
1. Risks and hazards
2. Components of a (health) risk assessment
3. Risk assessment in engineering
4. Risk assessment and national security

Aside: Other areas where RA encountered (finance, actuarial applications) though not discussed here.

## 0. Preliminaries ...

What is risk analysis?

An answer to the following questions ...

- i. What can happen? (i.e. what can go wrong?)
- ii. How likely is it that that will happen?
- iii. If it does happen, what are the consequences?

(Kaplan S and Garrick BJ (1981) On the quantitative definition of risk. *Risk Analysis* 1: 11-27.)

Risk Analysis (risk assessment and risk management) answers...

- i. What are the risks imposed by human activities and rational phenomena on society and the environment?
- ii. Are these risks acceptable?
- iii. What are the options for reducing these risks?
- iv. On what basis should we choose among these options?

(Kastenbergs course notes 2005)

$$\text{Risk Analysis} = \text{Risk Assessment} + \text{Risk Management} \\ = (\text{PF}|\text{HI}|\text{EA}|\text{DR}|\text{RC}^1) + (\text{actions/options to agent}^2)$$

<sup>1</sup> Risk Assessment includes a number of steps that will be discussed soon (PF=problem formulation; HI = hazard identification; EA=exposure assessment; DR = dose-response modeling; RC=risk characterization)

<sup>2</sup> Risk assessors and risk managers meet early to plan and scope the assessment. In addition, some possible management options may be put in play for consideration in the assessment.

\* Warning: Risk analysis may be defined by different organizations in different ways

## 1. Risks and hazards

- \* risk corresponds to the probability of some adverse outcome
- \* magnitude or severity of an adverse outcome is often part of the consideration of risk

Kaplan and Garrick (1981) argue that "Risk" can be defined as a collection of triplets –  $R = \{ (s_i, p_i, x_i) \} i=1, \dots, N$

where

$s_i$  = scenario

$p_i$  = Pr(scenario  $s_i$ )

$x_i$  = measure of damage associated with scenario  $s_i$

Commonly,  $R = \sum x_i p_i$

## 2. Components of a (health) risk assessment

- \* most familiar paradigm for risk assessment was published by the National Research Council (NRC, 1983) – **hazard identification, exposure assessment, dose-response assessment, risk characterization**
- \* Common revisions include a **problem formulation** component where scope, breadth and context of the risk assessment are defined

## **Hazard identification**

- \* uses available scientific and engineering data to determine whether some agent is a hazard.
- \* epidemiologists evaluate the strength of human studies to evaluate whether the association between exposure and an adverse response is one of cause-and-effect (e.g. employees at a microwave popcorn processing plant that exhibited severe pulmonary symptoms- Kreiss et al. (2002))
- \* toxicologists examine animal studies, structural activity relationships, etc.
- \* may be the result of observing a series of unusual cases

## **Exposure assessment**

- \* often requires the expertise of nutritionists, industrial hygienists (for occupational exposures), engineers and hydrologists (for waterborne hazards), meteorologists (for airborne hazards), and analytical chemists.
- \* provides a description of the individuals / organisms / entities experiencing exposure to a particular hazard
- \* provides a description of the pattern or "profile" of exposure

## **Dose-response modeling or exposure-response modeling**

- \* develop models that predict adverse response as a function of dose or exposure
- \* requires the input of statisticians, epidemiologists, and modelers
- \* big question: how is exposure measured?

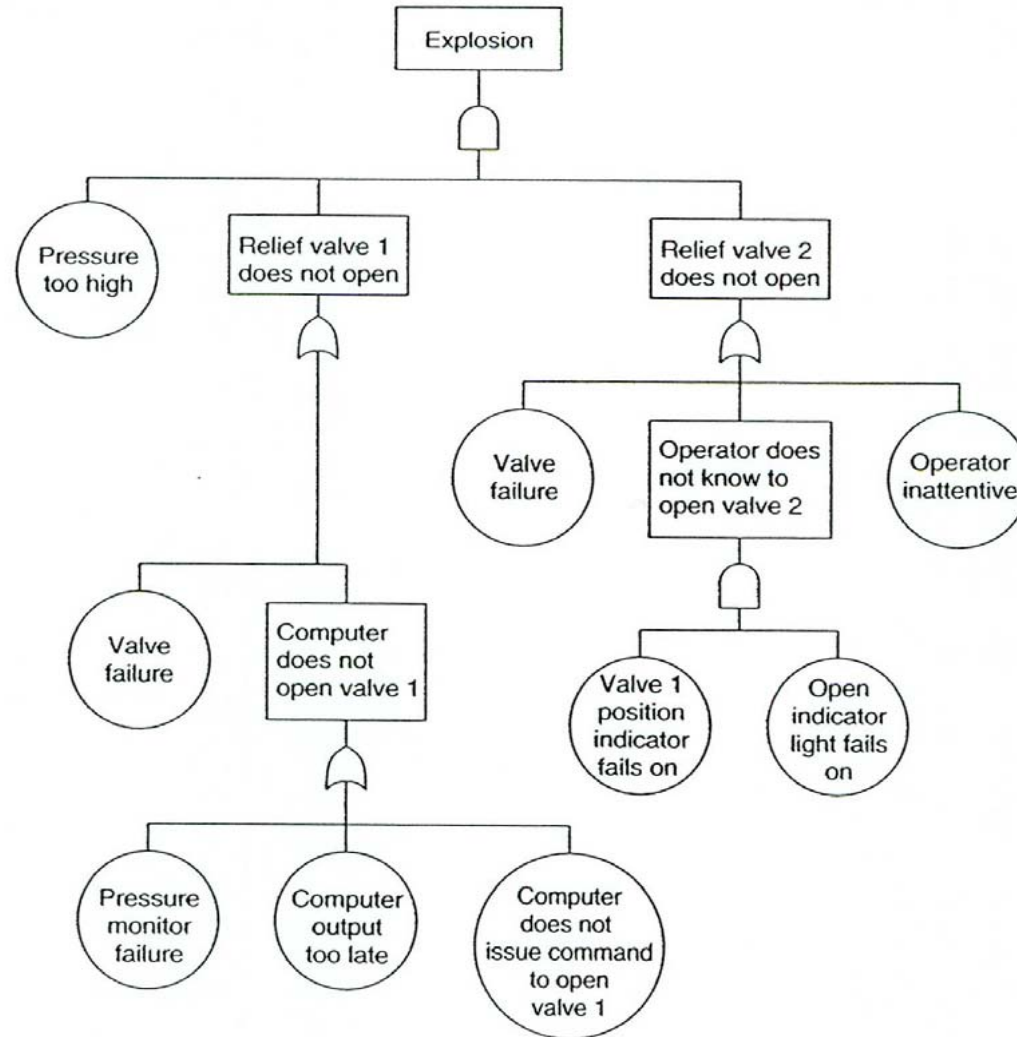
## **Risk characterization**

- \* involves all of the disciplines described above and many others.
- \* integrates the first three components into a full picture of what is known about the effects of exposure, of a specific kind and intensity, on specific populations or persons.
- \* various control options might be compared with respect to their potential benefits in reducing the risk associated with exposure to some hazard.
- \* place where important sources and impacts of uncertainty are considered

### 3. Risk assessment in engineering

- \* Failure of engineered systems provides a different set of challenges.
- \* Led the development of RA (aerospace) and PRA (nuclear industry)
- \* Engineered systems are typically comprised of a collection of interconnected components, often with redundancy built as a safeguard for successful operation of the system even if particular elements fail.
- \* Fault trees are one demonstration
- \* fault tree example ([www.nepss.org/presentations/Risk\\_26June02.ppt](http://www.nepss.org/presentations/Risk_26June02.ppt))

Fault tree (top level=outcome; lower levels=events with AND/OR gates)



4. Risk assessment and national security – DHS as the center of this concern

\* much of this section is based on Masse et al. (2007) *Congressional Research Service Report on DHS Risk Assessment Methodology: Evolution, Issues, and Options for Congress* - a great review of RA thinking in the evaluating risks associated with security preparations.

- \* So, how does security RA differ from health/engineering RA?
1. Security RA or terrorism is "adversial risk assessment" (Banks)
  2. Health endpoints are now TARGETS
  3. Exposure is a now a SCENARIO of attack
  4. Exposure assessment is Terrorist Threat Characterization (Hall R (2005) Assessment guidelines for counter terrorism. CREATE Draft report #05-017.)
  5. Risk Managers = DHS + nuclear power plant operators + ...

In addition, need to consider (Hall, 2005) ...

- \* Weapons used
- \* Adversary characteristics – persistence/educ.-sophist./commitment/mobility/motivation/org. scope-scale + may adjust to countermeasures
- \* Target characteristics – criticality/human occup.-vulnerability/damage vulnerability/symbolism/protection
- \* Scenario – event sequence of particular attack
- \* Outcome – human losses/financial losses/symbolic losses
  
- \* Security Risk assessment has evolved over time (Masse et al. 2007; Fig. 1) highlighted the following stages:

Stage 1 (2001-2003): Risk = Population ( $R=P$ )

Stage 2 (2004-2005): Risk = Threat + Critical Infrastructure + Pop'n Density ( $R=T+CI+PD$ )

Stage 3 (2006-today): Risk = Threat\*Vulnerability\*Consequence ( $R=T*V*C$ )

Stage 1 ( $R=P$ ) implies that security risk = population size.

\* size of the risk  $\propto$  size of the exposed population.

Stage 2: ( $R=T+CI+PD$ )

\* additive in characteristics that were scored but not evaluated as probabilities

Stage 3 ( $R=T*V*C$ )

\* risk as a product of factors:

$T=$ Threat =likelihood of attack ( $T=$ Threat)

$V =$  vulnerability

$C =$  consequence ( $V, C$ ) where  $V=1$  by assignment.

Operationally,

$$\text{THREAT} = \text{Pr}\{ \text{attack} \}$$

$$\text{VULNERABILITY} = \text{Pr}\{ \text{successful} \mid \text{attack} \}$$

$$\text{CONSEQUENCE} = E\{ \text{Loss} \mid \text{successful attack} \}$$

From CRS (2007) Report

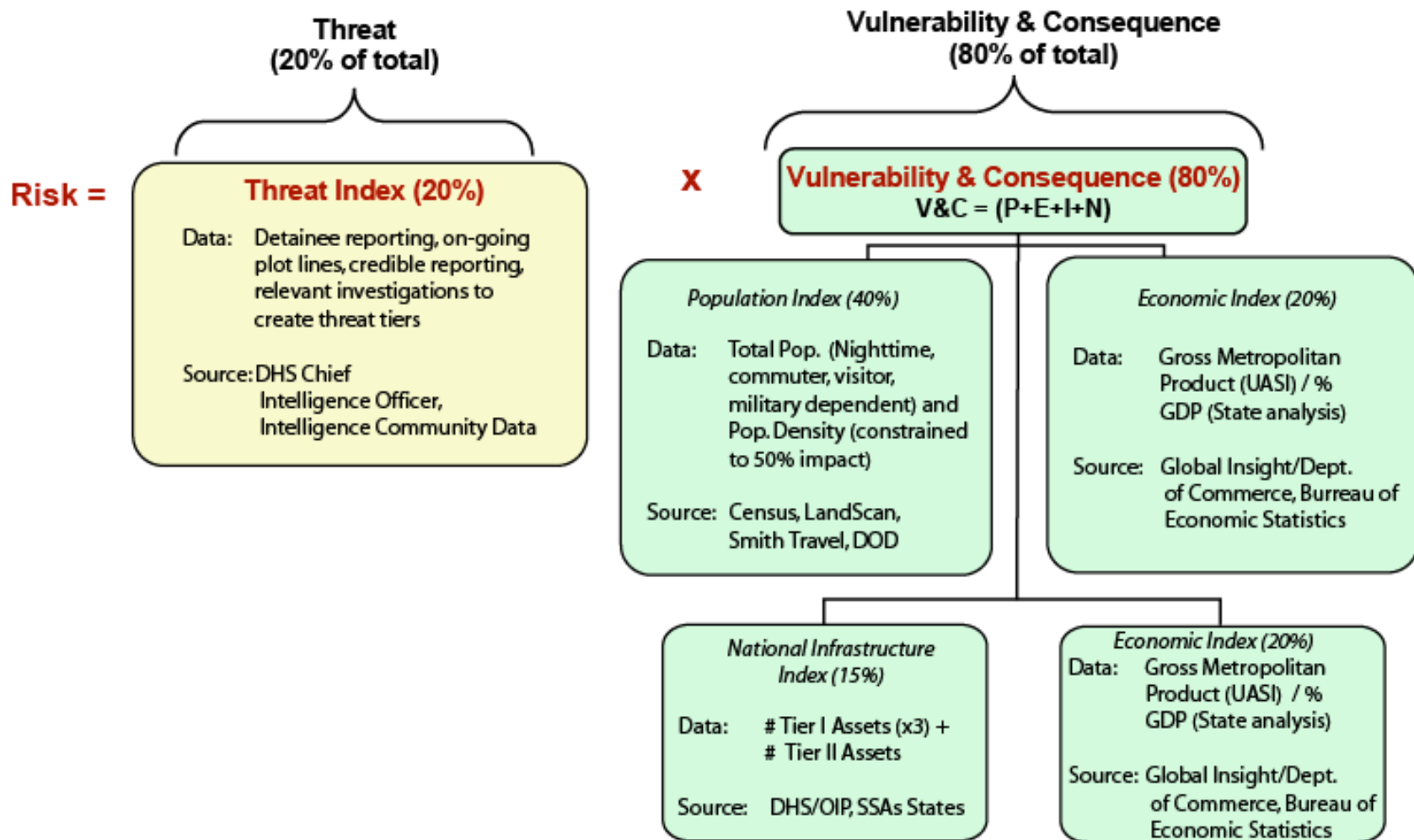


Figure 1 displays this relationship and provides description of sources for these categories.

$$\text{Risk} = T * V * C = E\{ \text{Loss} \mid \text{successful attack} \} \times \\ \text{Pr}\{ \text{success} \mid \text{attack} \} \times \text{Pr}\{ \text{attack} \}$$

Complications include:

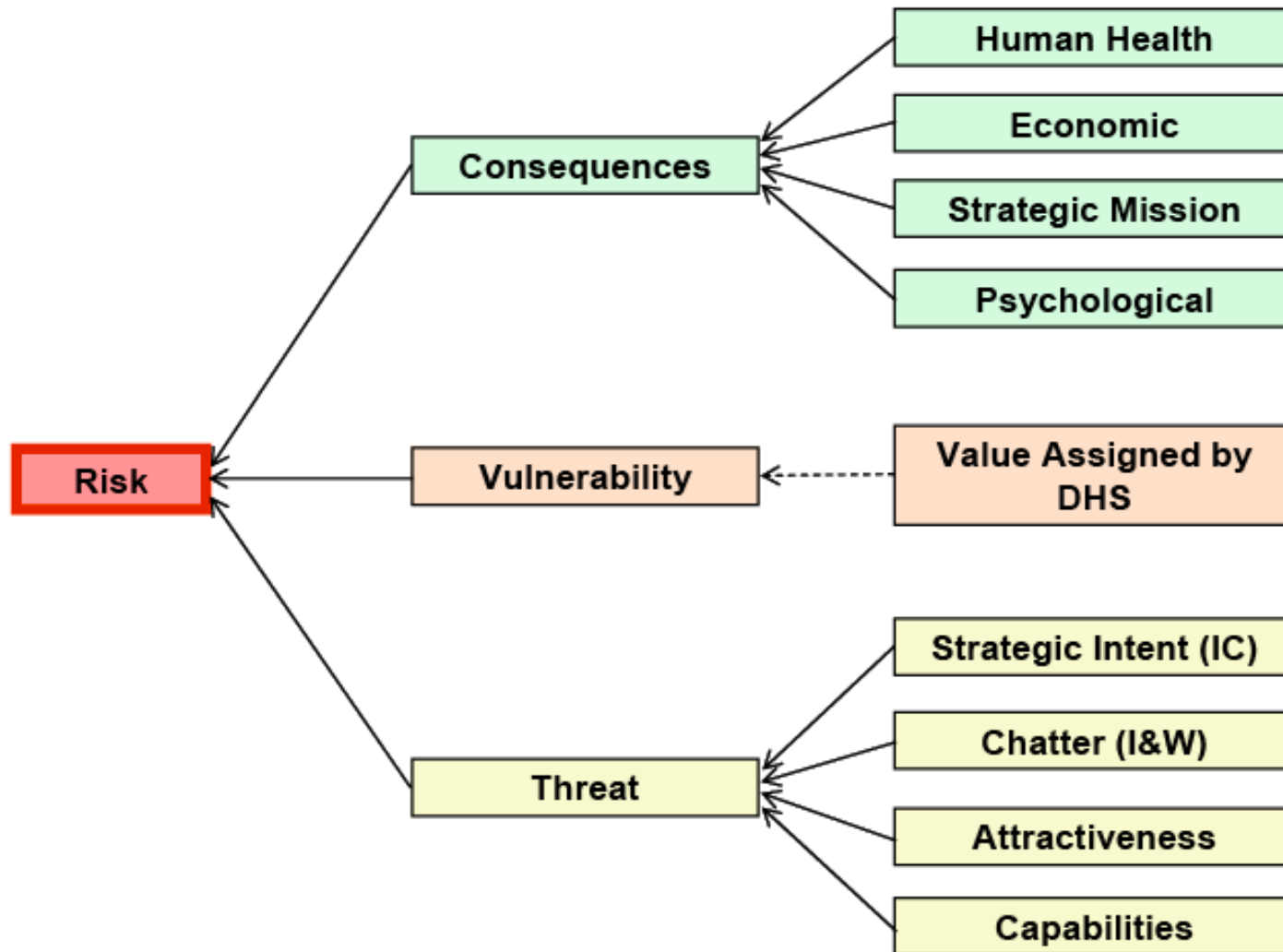
- 1) multiple assets are candidates for attack;
- 2) the probabilities listed above are uncertain (perhaps only obtainable via expert elicitation);
- 3) the planning of defense for possible attack must allocate resources to multiple targets recognizing that terrorists may not be considering the same suite of potential targets.

This CRS report also highlights a number of questions, both raised in this report and extracted from other sources including RAND. Example questions include:

- \* what is the risk to?
- \* from what sources does the risk originate?
- \* should resources be allocated based on risk, risk reduction, other? (RAND)
- \* how can terrorism risk be estimated?
- \* what are the tolerable levels of risk?

DHS differentiates between two types of risk – asset-based (see fig. 3) and geographic based. Asset-based RA has T/threat estimated from the intelligence community while geographic-based risk looks at regions without considering assets in these areas.

Figure 3 (from CRS 2007 report) **Asset-Based Risk Analysis Attributes**

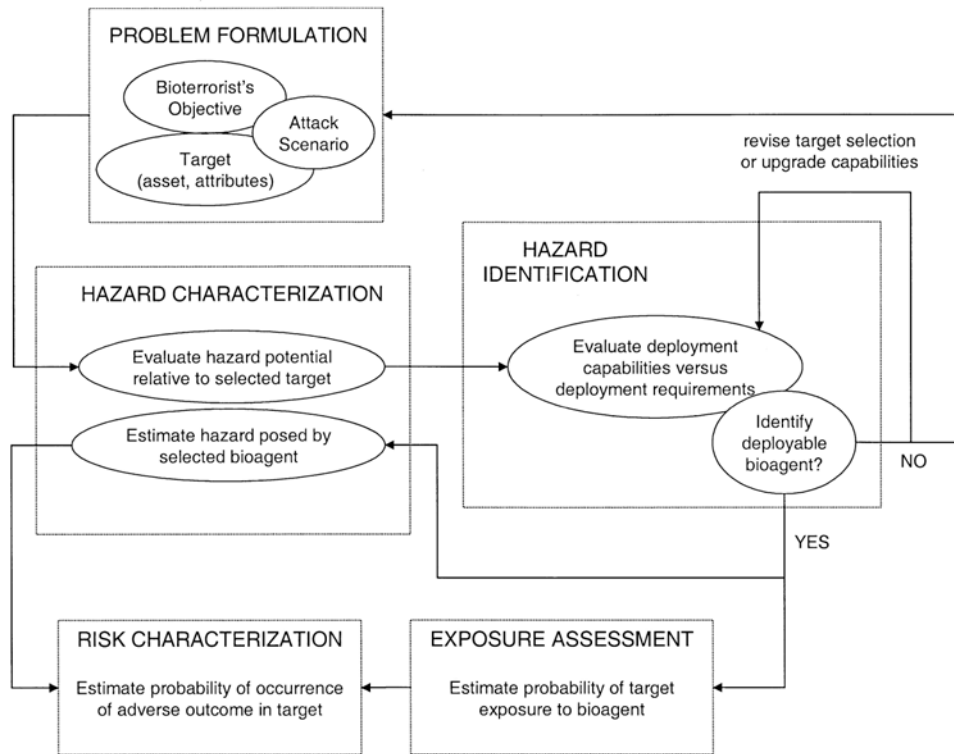


Can the ideas from Health risk assessment and Engineering risk assessment help with security risk assessment?

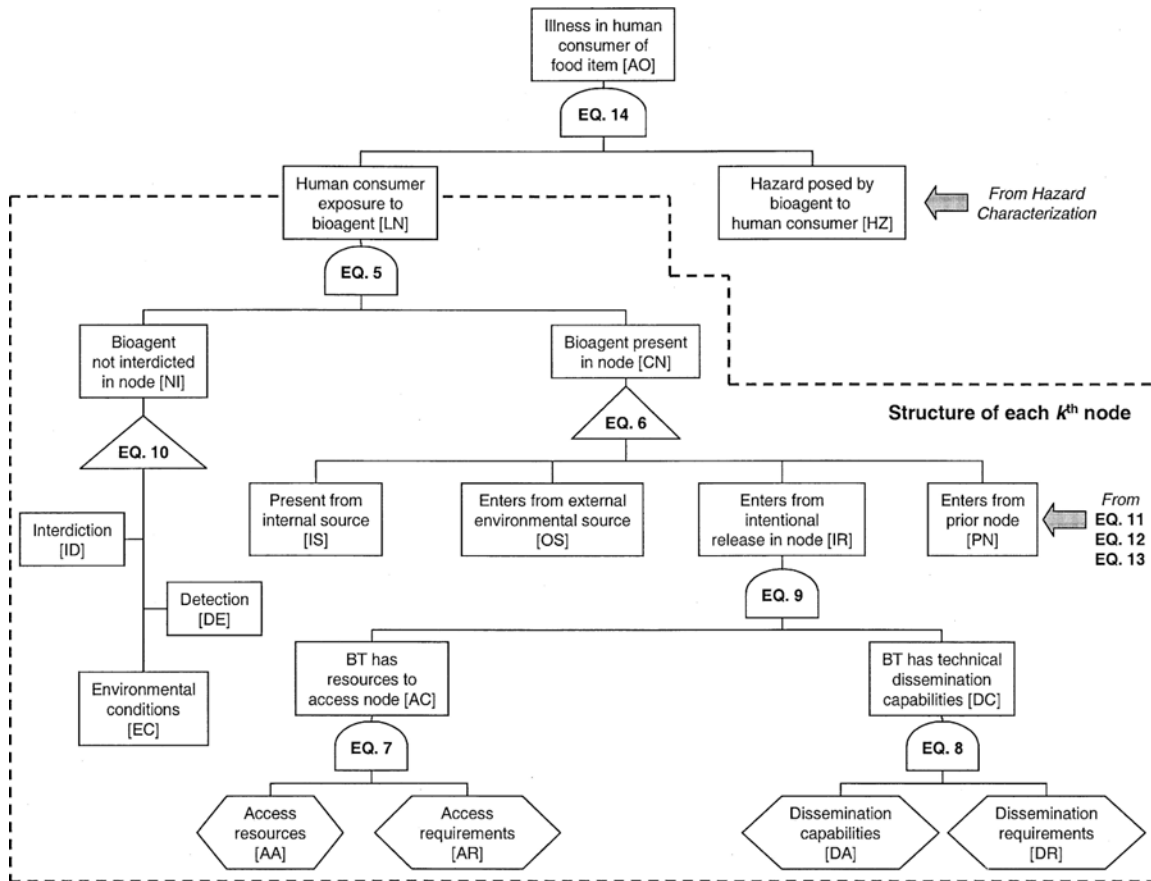
The (health) risk assessment paradigm and fault trees were applied to an analysis of the bioterrorism risks to US Food Supply (Hope, B (2004) Using fault tree analysis to assess bioterrorist risks to the US food supply. *Human and Ecological Risk Assessment* **10**: 327-347).

The following two figures come from this paper ...

(Bio)Terrorism risk from health RA perspective [Hope (2004) Fig. 1]



Fault Tree and the food supply (Hope (2004) Fig. 3)



Does Security RA require additional tools beyond health and engineering risk tools?

Not surprising, yes.

Since Security RA involves adversaries, other strategies have been suggested including (Kardes E and Hall R (2005) Survey of literature on strategic decision making in the presence of adversaries. CREATE Draft Report #05-006):

\* game theory (Fricker 2006; Banks and Anderson 2006; Bier 2006 – all in Statistical Methods in Counterterrorism – ed. AG Wilson, GD Wilson, DH Olwell)

\* prob. risk analysis including expert elicitation and Bayesian methods

Table 1: Comparing health, engineering and security risks

	Health Risk Assessment	Engineered-System Risk Assessment	National Security Risk Assessment
Problem Formulation	Control exposure to agent	Avoid system failure	People and resources in danger
Hazard Identification	Agent with potential impact identified	Work from failure to cause (e.g. fault trees)	Scenarios of Threats
Exposure Assessment	Measured, eval. from work history, PBPK modeled, etc.	System "load"	Vulnerability of targets, intelligence?
Exposure-Response	Toxicity (animal) and epi (human) data available	Stress tests of system components + subj. probs.	Data?
Risk Characterization	Proportion of pop'n at risk at certain exposure	Propagate probs. in a fault tree	Ordering of risks for targets?

## Conclusion/take-home message:

- \* All risk assessments should provide input for making good decisions in the face of uncertainty
- \* Tools from health and engineering risk assessment are useful for security risk assessment but the adversarial nature adds an important twist.
- \* Many opportunities for statisticians in risk assessment (in general) and in security risk assessment (in particular)
- \* Thanks again to the session organizer and participants!

References (both cited and "bonus" for interested readers):

Banks, DL (2002) Statistics for homeland defense. *Chance* **15**: 8-10.

Major, J.A. (2002) Advanced Techniques for Modeling Terrorism Risk. *The Journal of Risk Finance* \_\_\_\_: 15-24

Masse, T., O'Neil, S. & Rollins, J. (2005) The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress.

National Research Council (1983) ...

Apostolakis, G.E. & Lemon, D.M. (2005) A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. *Risk Analysis* **25**: 361-376

Anderson, E.L., (2002) Assessing the Risks of Terrorism: A Special Collection of Perspectives Articles by Former Presidents of the Society for Risk Analysis. *Risk Analysis* **22**: 401-402

Bier, V. (2005) Choosing What to Protect *Center for Risk and Economic Analysis of Terrorism Events*

Deisler, Jr., P.F. (2002) A Perspective: Risk Analysis as a Tool for Reducing the Risks of Terrorism. *Risk Analysis* **22**: 405-413

Haimes, Y.Y. & Longstaff, T. (2002) The Role of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism. *Risk Analysis* **22**: 439-444

Hall, R. (2005) Assessment Guidelines for Counter Terrorism. *Center for Risk and Economic Analysis of Terrorism Events*

Kardes, E. & Hall, R. (2005) Survey of Literature on Strategic Decision Making in the Presence of Adversaries. *Center for Risk and Economic Analysis of Terrorism Events*

Kulldorff, M., Mostashari, F., Duczmal, L., Yih, W.K., Kleinman, K. & Platt, R. (2006) Multivariate Scan Statistics for Disease Surveillance. *Statistics in Medicine* **26**: 1824-1833

- O'Sullivan, T. (2005) The Uncertain Dynamics of Global Bioterrorism: Smallpox as a Hypothetical Case for Risks and Responses. *Center for Risk and Economic Analysis of Terrorism Events*
- Orosz, M. (2005) Risk Analyst Workbench Design and Architecture *Center for Risk and Economic Analysis of Terrorism Events*
- Rolka, H., Burkom, H., Cooper, Kulldorf, M., Madigan, D. & Wong, W.K. (2006) Issues in Applied Statistics for Public Health Bioterrorism Surveillance Using Multiple Data Streams: Research Needs. *Statistics in Medicine* **26**: 1834-1856
- Rose, J., Haas, C., Page, A. & Clark, M. (2006) Assessing the Risk from Biological Threats: A Government/Academia Partnership for Homeland Security. *United States Environmental Protection Agency*
- Wulf, W.A., Haines, Y.Y. & Longstaff, T.A. (2003) Strategic Alternative Responses to Risks of Terrorism. *Risk Analysis* **23**: 429-444
- (2007) Homeland Security Centers of Excellence.
- (2006) Survey of DHS Data Mining Activities. Department of Homeland Security, Office of Inspector General