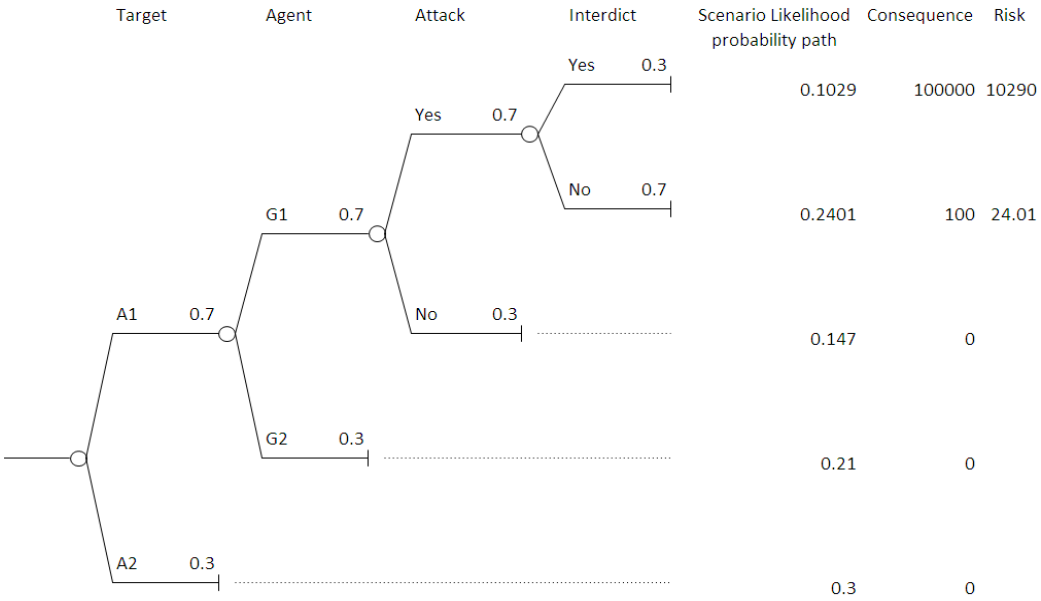
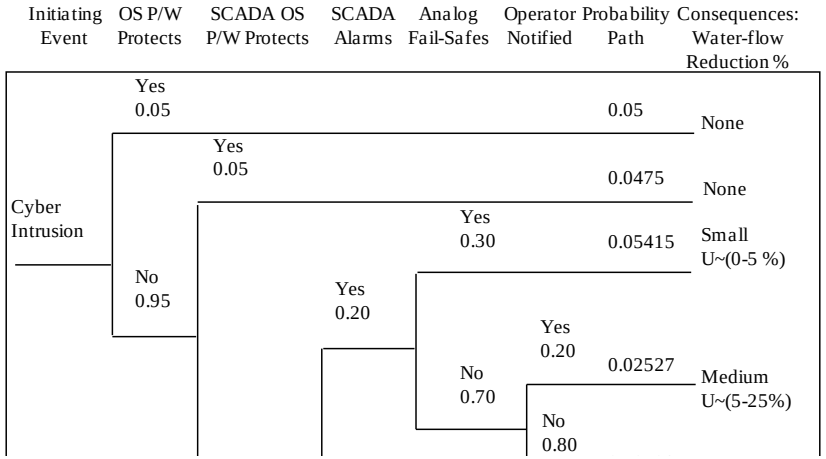
Probabilistic Risk Analysis and Terrorism Risk



By
Barry C. Ezell, Ph.D.
Virginia Modeling, Analysis, and Simulation Center
Old Dominion University
01.757.802.1649
bezell@odu.edu



Context, Purpose & Outline

- Context: Integrated CBRN risk analysis
- Purpose: to provide information on different types of modeling approaches used in risk analysis
- Outline
  - Background and motivation
  - Tree types, properties, and uses
  - Advantages and Disadvantages
  - Summary

Integrated CBRN Risk Assessment (iCBRNra) Requirements

Required by Homeland Security Presidential Directive (HSPD) 18: *Medical Countermeasures against Weapons of Mass Destruction*

§ 14 (c)

"The Secretary of Homeland Security shall develop a strategic, integrated all-CBRN risk assessment… Not later than June 1, 2008, the Secretary of Homeland Security shall submit a report to the President…which shall summarize key findings…and shall update those findings when appropriate, but not less frequently that every 2 years."

Motivation

- Considerable effort has been applied to the challenge of risk analysis in the security domain.
- DHS, industry, and the academic risk analysis communities have all invested heavily in the development of tools and approaches that can assist decision makers in effectively allocating limited resources across the vast array of potential investments that could mitigate risks from terrorism and other threats to the homeland.
- While considerable progress has been made in approaches for terrorism risk analysis, there remain a number of challenges and limitations to each method currently in use.
- With the threat of terrorism quite real, decision makers expect decision support analysis that is balanced, and that identifies limitations and assumptions with the understanding that no single method currently solves all challenges in terrorism risk analysis.

Motivation

- For more than thirty years, probabilistic risk analysis (PRA) has been a major tool for assessing risks and informing risk management decisions by government and businesses, in areas as diverse as industrial safety, environmental protection, and medical decision making.
- The more recent application of PRA to terrorism risks is new however, and not uncontroversial.
- A major challenge in risk analysis of terrorism is the fact that terrorists, unlike natural systems, are “intelligent adversaries” and may adapt to our defensive measures.
- The National Research Council on Methodological Improvements to the Department of Homeland Security’s (DHS) Biological Agent Risk Analysis has argued that because of this adaptive nature, alternative tools like decision trees, game theory, and agent-based modeling are needed to assess the risks of terrorist events.

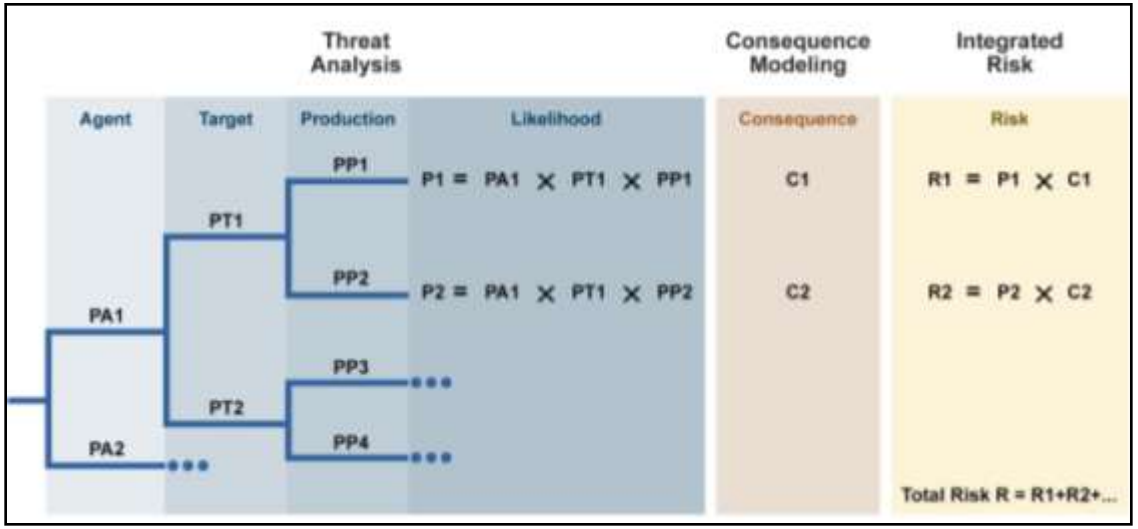
DHS technical response to the Committee can be found at http://www.dhs.gov/xabout/structure/gc_1222807486868.shtm

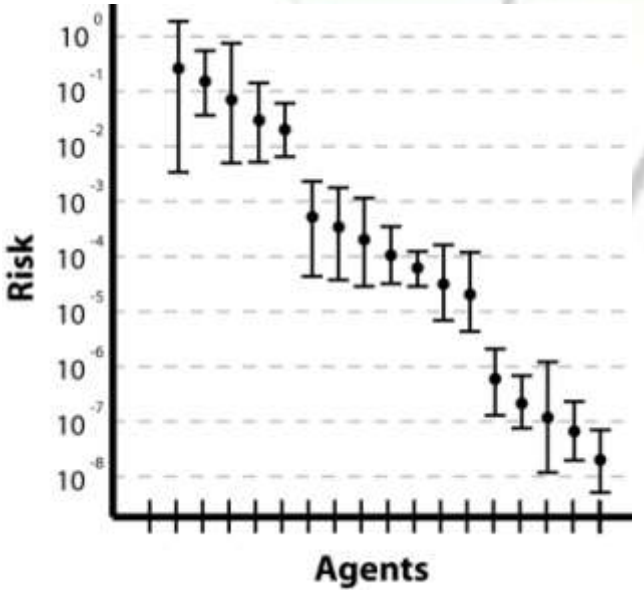
A risk primer…and my bias*…

- Risk Assessment (Kaplan and Garrick)
  - What can go wrong?
  - What is the likelihood?
  - What is the consequence?
- Risk Management (Haimes)
  - What can be done?
  - What are the tradeoffs?
  - What are the impact of current decisions on future options?

* My “risk” worldview is heavily influenced by Professors: Yacov Haimes, Greg Parnell, and Chuck Keating

iCBRNra Components: Bioterrorism Risk Assessment (BTRA)





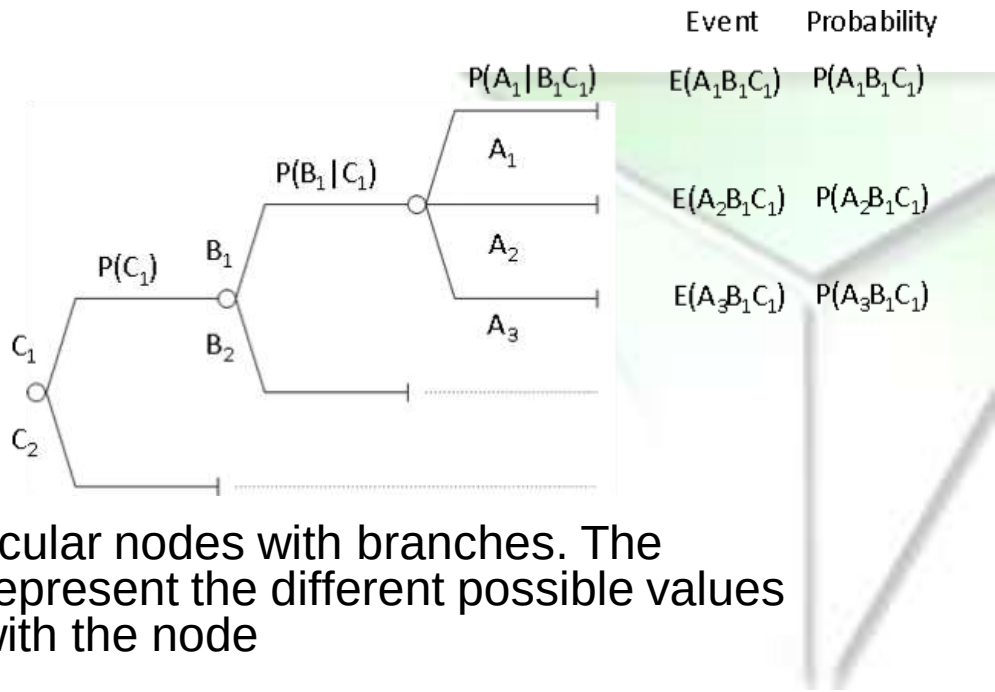
- Required by HSPD-10; first assessment delivered to HSC in January, 2006. Updated assessments are due every two years.
- 2008 update scheduled for delivery 31 January 2008 – many significant expansions and improvements.

Logic trees are important tools for exploring the scenario space, analyzing uncertain events, defining scenarios, and assessing risk[1].

- Probability tree
- Event tree
- Decision tree
- Fault Tree

[1] Dillon-Merrill, R. L., Parnell, G. S., and Buckshaw, D. L., Logic Trees: Fault, Success, Attack, Event, Probability, and Decision Trees, Wiley Handbook Of Science & Technology for Homeland Security, John G. Voeller, Editor, 2008.

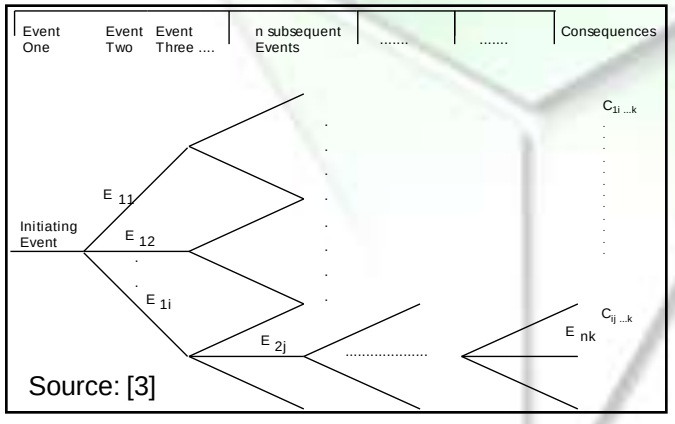
Probability Tree



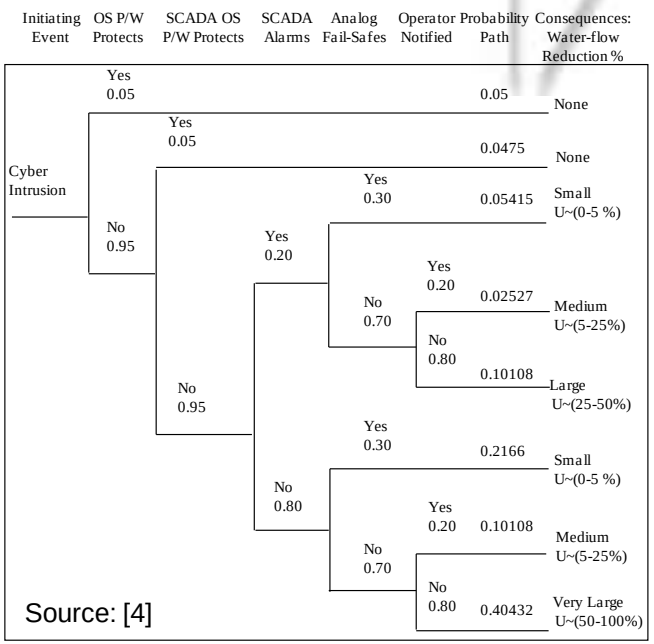
- A probability tree is a succession of circular nodes with branches. The branches emanating from each node represent the different possible values of the uncertain variables associated with the node
- Properties
  - Events (nodes) and branches
  - Forward logic
  - Downstream events conditioned on previous events
- Uses
  - A graphical way to represent the fundamentals of probability theory
  - To describe the probabilistic relationship between two or more events
  - Logic diagrams
    - Event Tree
    - Decision Tree

Event Tree

- An event tree models the sequence of events that lead to consequences.[1]
  - Properties
    - Events (nodes) and branches
    - Forward logic
    - Downstream events conditioned on previous events
    - An extension of probability trees by adding: initiating event and mitigating events
    - Consequences are added for each probability path
  - Uses
    - Used in PRA at the "systems" level [2]
      - Nuclear reactor safety (1975)
      - Cyber risk to SCADA systems (1998)
    - Helps to understand how an outcome occurs as it transitions through mitigating events.
    - Consequences are conditioned on the occurrence of the initiating event and subsequent mitigating events.
    - In PRA, multiplying the consequence times the probability path equals risk.



Source: [3]

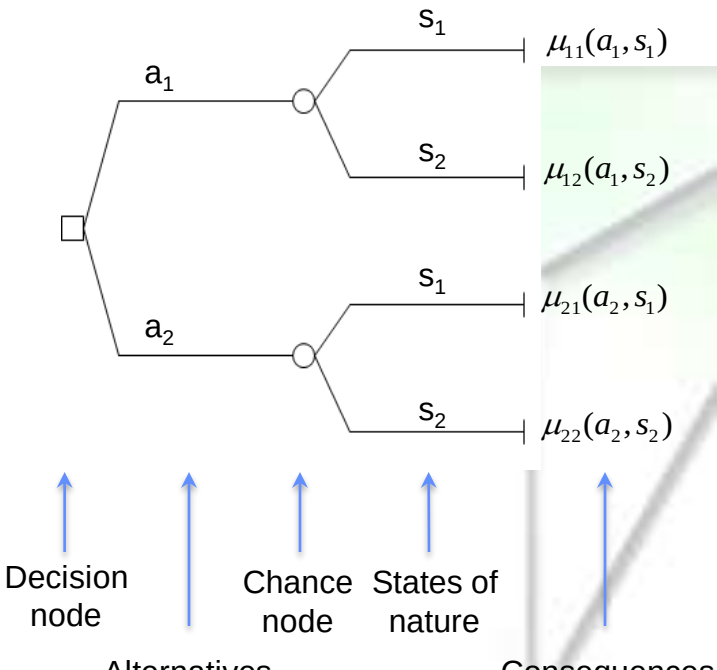


Source: [4]

[1] Kumamoto, H. and Henley, E.J., *Probabilistic Risk Assessment and Management for Engineers and Scientists*, IEEE Press, Piscataway, NJ, pp. 98-101, 1996.
[2] Homeland and Security Risk Assessment, RP04-024-01a, Nov. 2005.
[3] Ang, A., and Tang, W., *Probability Concepts in Engineering Planning and Design, Vol. 2: Decision, risk, and reliability*, NY., 1984.
[4] Ezell, B., Haimes, Y., and Lambert, J., "Risks of Cyber Attack to Water Utility Supervisory Control and Data Acquisition Systems", *Military Operations Research*, Vol. 6, No. 2, 2001.

Decision Tree

- A decision tree is a diagram of a decision, read left to right. [1]
  - Properties
    - Leftmost node in a decision tree is called the root node in the shape of a square, called a decision node.
    - Branches emanating to the right from a decision node represent the set of decision alternatives that are available.
    - Small circles in the tree are called chance nodes that represent uncertainty in outcomes.
    - The right end of each path through the tree is called an endpoint, and each endpoint represents the final outcome of following a path from the root node of the decision tree to that endpoint.
  - Uses: In decision analysis, used as a decision support tool to calculate and the best expected value for an alternative.

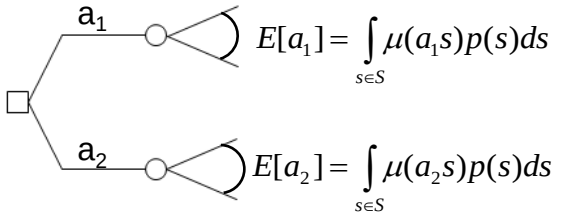


$$E[a_1] = \sum_{j=1}^{2} p(s_j)\mu_{1j} \qquad E[a_2] = \sum_{j=1}^{2} p(s_j)\mu_{2j}$$

Objective Function

$$\underset{1 \le j \le 2}{Max} \sum_{j=1}^{2} p(s_j)\mu_{ij} \quad \text{or} \quad Max\{E[a_1], E[a_2]\}$$

Stochastic Decision Tree

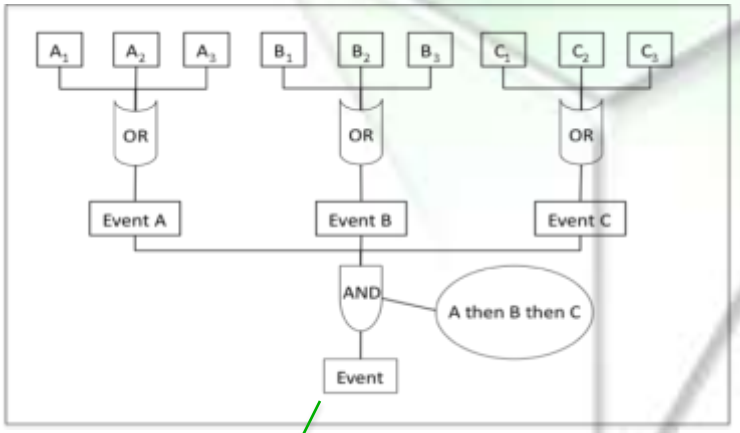


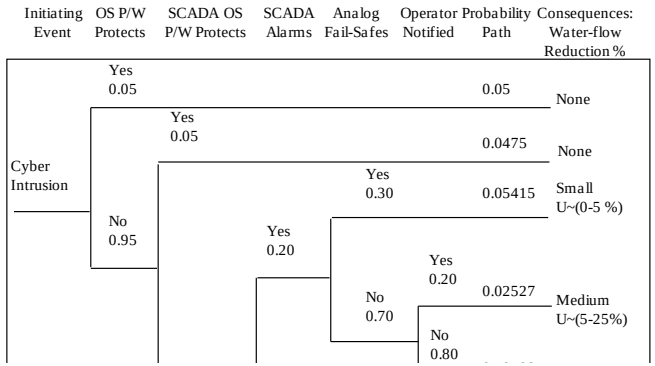
$$Max\{E[a_1], E[a_2]\}$$

[1] http://www.public.asu.edu/~kirkwood/DAStuff/decisiontrees/index.html
[2] Haimes, Y., Risk Modeling, Assessment, and Management 3rd Edition, Wiley, NJ., 2009.

Fault, Attack, and Success Trees

- A fault tree is a tool for analyzing, visually displaying, and evaluating failure paths in a system to evaluate system level risk. [1]
  - Properties
    - Uses Boolean algebra, reliability theory, and probability theory
    - fault trees provide insight into why mitigating events on an event tree fail
    - Attack trees categorize the different ways in which a system can be attacked.
    - Success (defend) trees are the compliment of fault trees.
  - Uses
    - 1961- Minute Missile
    - 1966- Aircraft design
    - 1971 Nuclear power plant safety
    - Many more..
    - Attack trees are special case of fault trees that have been used to represent an adversary's successful defeat of a firewall system, networks, etc.





Fault trees are often used in conjunction with event trees.

[1] Ericson, C., Fault Tree Analysis – A History, A History from the Proceedings of the 17th International System Safety Conference, 1999.

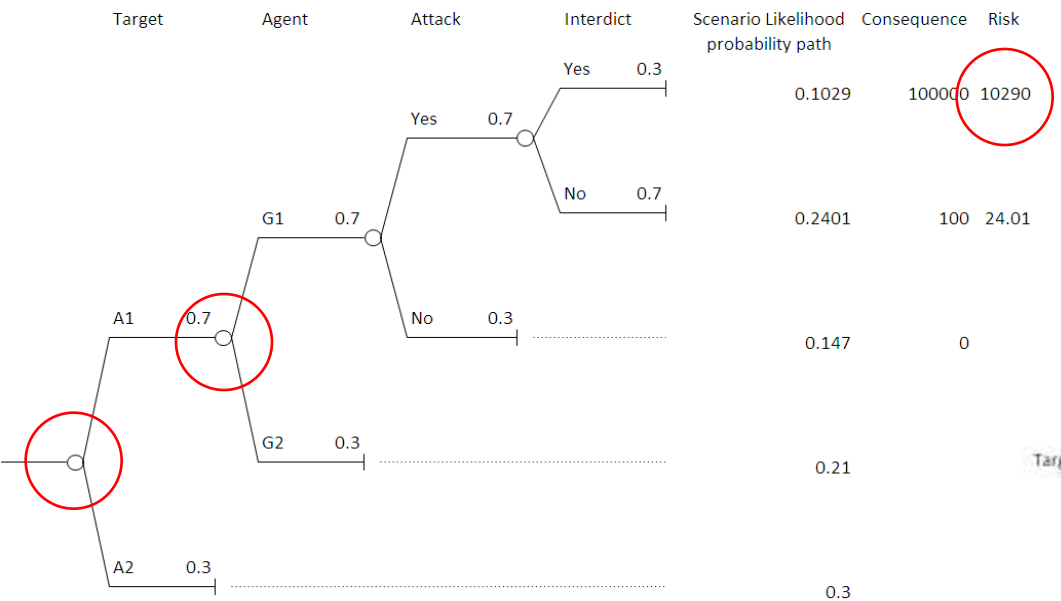
Assumptions: Event and Decision Tree

- Event Tree
  - Intelligent adversary (IA) decisions are modeled as probability estimates
    - Assumes: Intelligence Community expert knowledge about the IA preferences and capabilities (*).
    - Limitations:
      - terrorist choices are not random events such as failure events in engineered system or natural hazard events
      - terrorist are not static and change their preferences based on what we chose to do.
      - … a snapshot in time…
- Decision Tree
  - IA decisions are modeled as decision nodes with branches being alternatives
    - Assumes ideal intelligence and rationality [1] We **know** the IA risk preference of consequences:
      - Intelligence (the agent's representational and computational capacities) [1,2]:
        - IA goal is to maximize his consequence.
      - Rationality: IA does not make irrational choices
  - Limitations:
    - Adversaries' objective functions and level of ability to predict tree outcomes are unknown
    - Decision trees assume we *know* the intelligent adversary's true utility

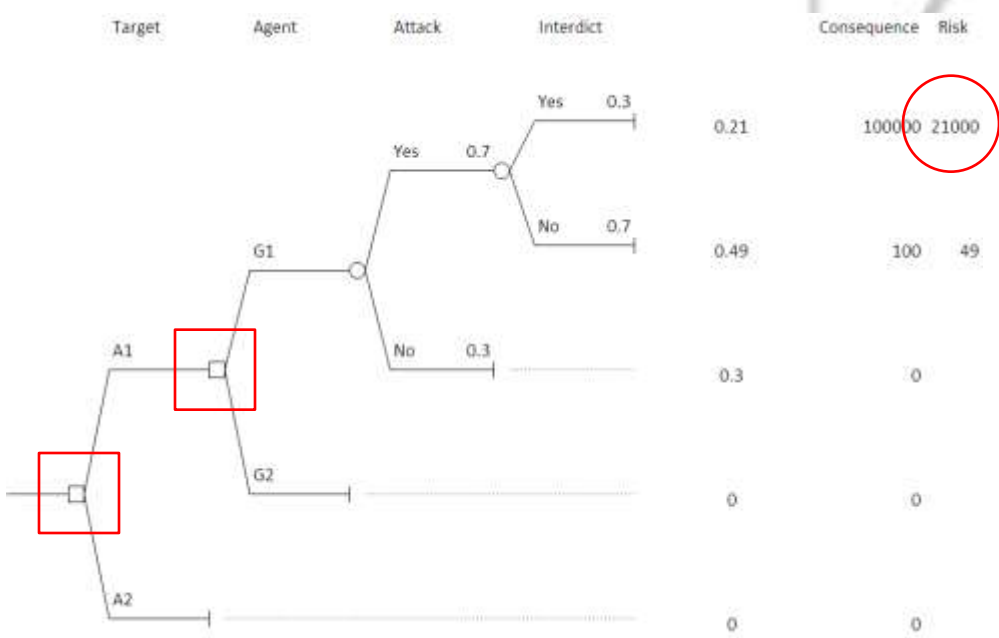
[1] Hees, M., and Roy, O., "Intentions, Decisions and Rationality", May 2007 (Web: http://www.illc.uva.nl/Publications/ResearchReports/PP-2007-21.text.pdf)
[2] [Myerson, 1991] Myerson, R. B. (1991). Game Theory: Analysis of Conflict. Harvard UP, 1997.
[3] [Savage, 1954] Savage, L. J. (1954). The Foundations of Statistics. Dover Publications, Inc., New York.

* Capability in the military sense is the ability to execute a specified course of action (DOTMLPF).

Event trees express our uncertainty in the intelligent adversary's true utility

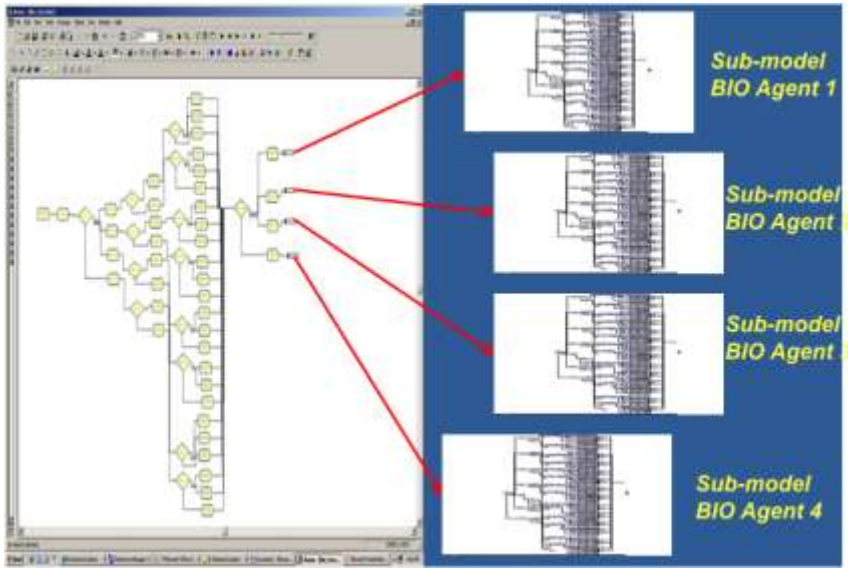


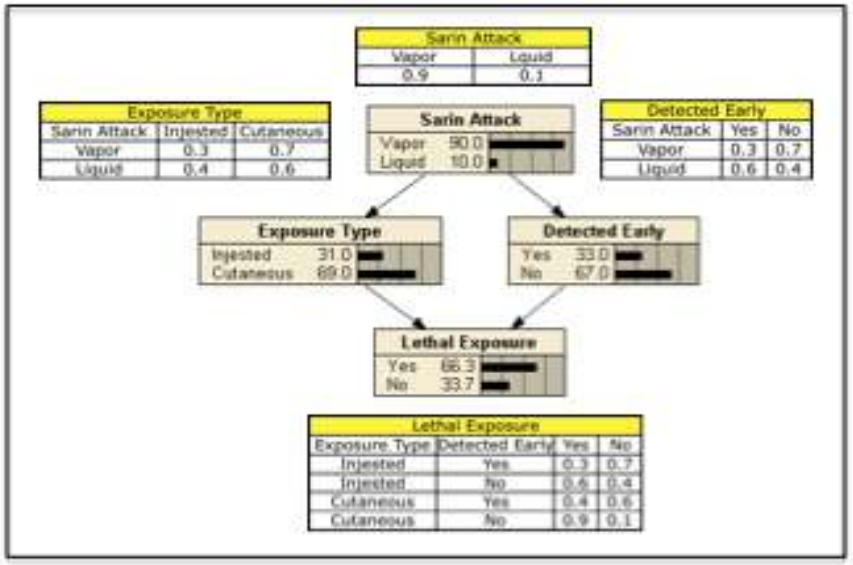
Decision trees assume we ***know*** the intelligent adversary's true utility

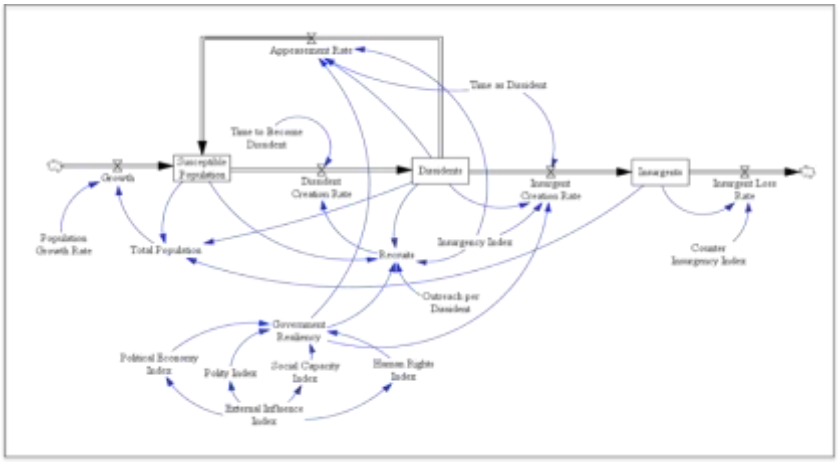


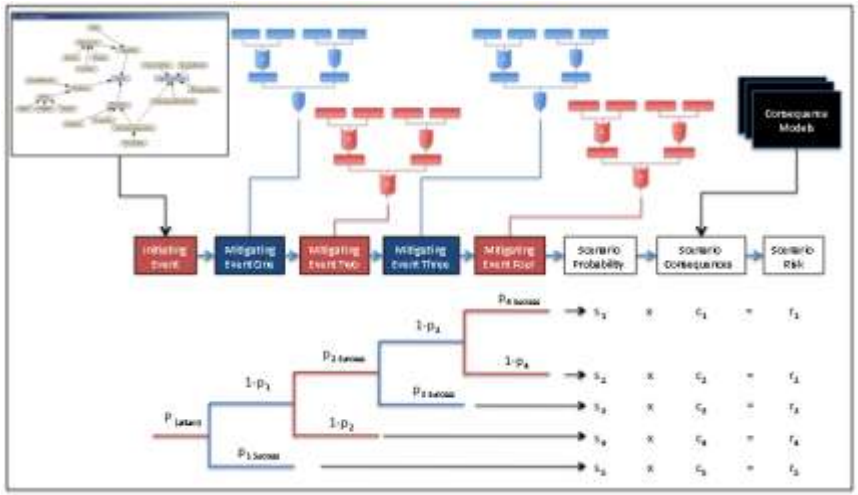
Logic trees alone, are limited in how they cover the landscape of terrorism risk analysis. There are ways to improve them; some more mature than others.

Alternative Approaches









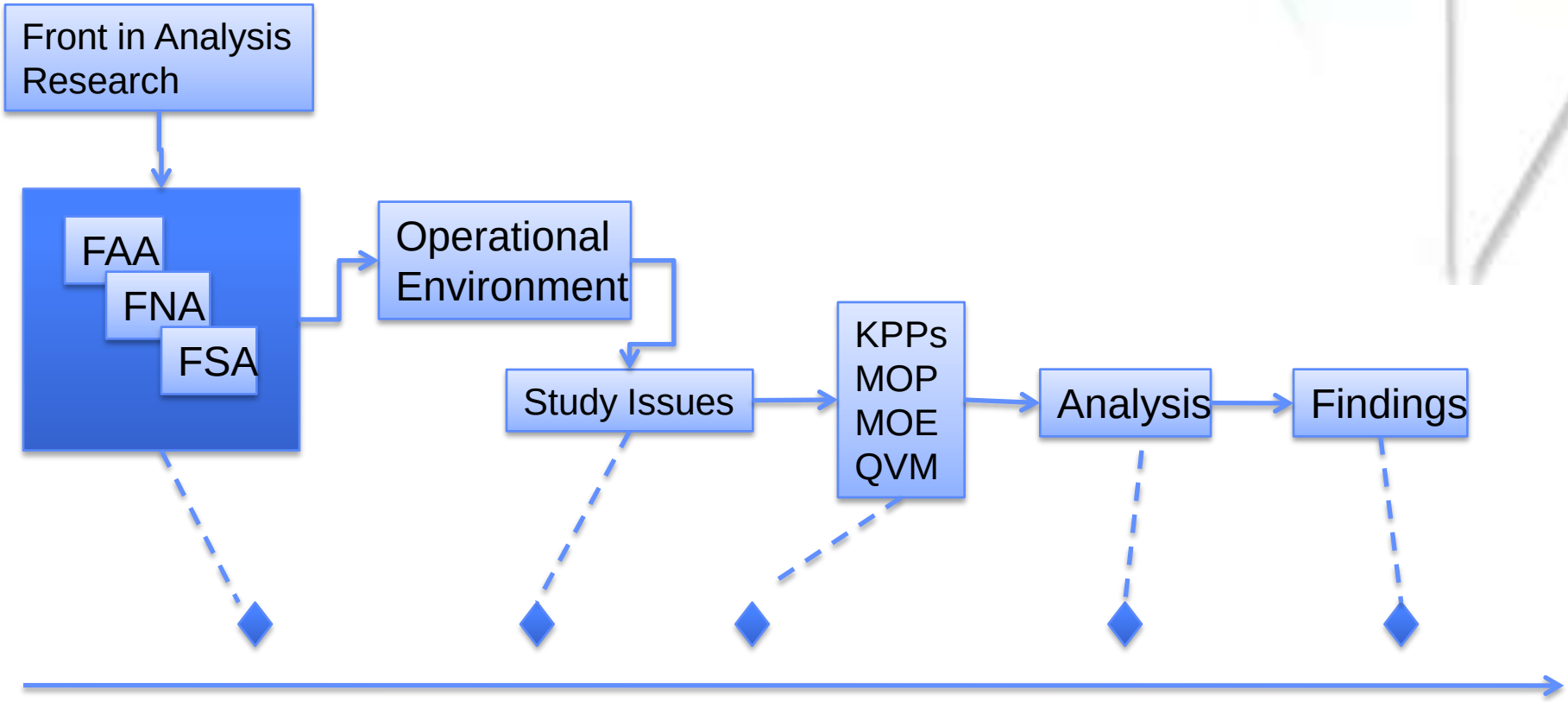
Another “Call for change” for maturing bioterrorism risk analysis might be the manner in which the community recommends risk analysis improvements to DHS.

For example, capability based assessment is a useful framework for structuring alternative recommendations to DHS.

- Functional Area Analysis: determines gaps in current methodology
- Functional Needs Analysis: prioritizes gaps in methodology
- Functional Solutions Analysis: produces a set of alternatives to cover gaps

A vetted list of alternatives that address priority gaps in current risk analysis methods and models would allow DHS to systematically evaluate alternatives and decide on the maturation strategy of terrorism risk analysis.

AoA Methodology Example

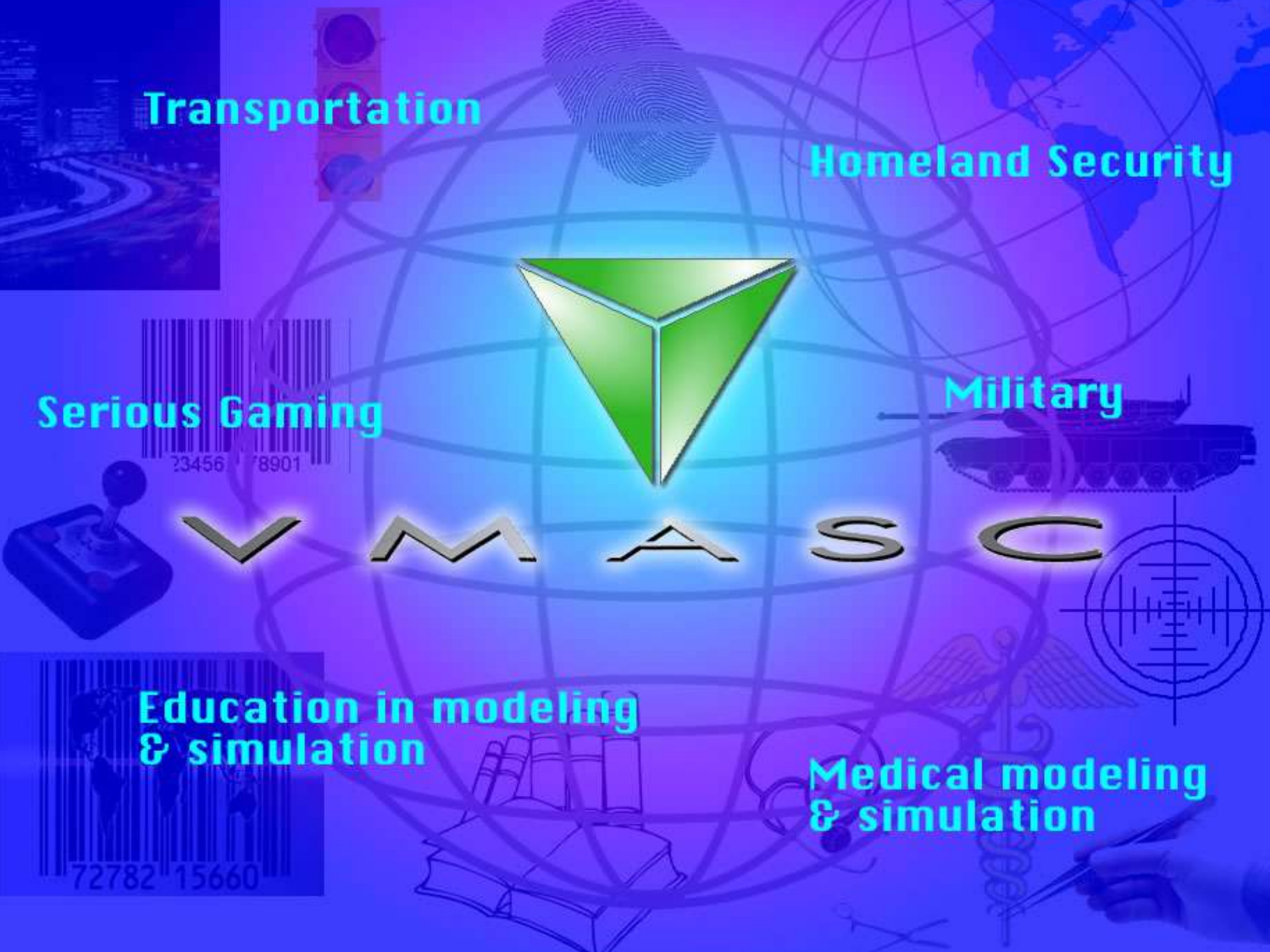


Summary: Final Thoughts

- Logic trees are useful in terrorism risk analysis.
  - Event trees express our uncertainty in the intelligent adversary's true utility.
  - Decision trees assume we know the intelligent adversary's true utility.
- Each approach has assumptions that bound the context of their usefulness.
- To the point that event trees assign probabilities to intelligent adversary choices, consider the following:
  - There is only one kind of uncertainty stemming from our lack of knowledge concerning the truth of a proposition. Distinctions between probabilities are merely for our convenience in investigating complex phenomena. There is only one logical and workable interpretation of probability and it is that of degrees of belief – George Apostolakis (1990)
- To the point that decision trees are the solution to terrorism risk analysis, consider the following:
  - "No single model or methodology can effectively meet all the challenges of tracking terrorism through scenario generation and structuring, updating and quantifying the value of intelligence, assigning priorities to the scenarios in a well-established risk-based methodology, or track terrorists' attack plans." – Yacov Haimes (1998, 2004, 2009)

Two papers:

1. Barry C. Ezell and Detlof von Winterfeldt (2009), Probabilistic Risk Analysis and Bioterrorism Risk, *Biosecurity and Bioterrorism.*
2. Barry C. Ezell, Steven Bennett, Detlof von Winterfeldt, John Sokolowski, and Andrew J. Collins (2009), Probabilistic Risk Analysis an Terrorism Risk, Risk Analysis (RA-00156-2009).


Transportation
Homeland Security
Serious Gaming
Military
VMASC
Education in modeling
& simulation
Medical modeling
& simulation