

---

# Counterterrorism

## Reasoning About Rare Events

**Tod S. Levitt**

**Information Extraction & Transport, Inc.**  
Arlington, Virginia

**September 20, 2007**

# Rare Events: Philosophical Issues

---

- Is “ $p(\text{terrorist-event} \mid \text{evidence})$ ” an admissible expression?
- If there can be such a distribution, how might it be estimated?
- If it is estimable, what experiment can be done to sample it?

# Rare Events: Philosophical Answers

---

- **Is “ $p(\text{terrorist-event} \mid \text{evidence})$ ” an admissible expression?**
  - Classical: no ; Bayesian: yes
  - See L.J. Savage; Foundations of Statistics; 1954
- **If there can be such a distribution, how might it be estimated?**
  - Evidential accrual via hierarchical Bayesian inference
  - Posterior probability at level  $n$  is the prior probability for level  $n+1$
- **If it is estimable, what experiment can be done to sample it?**
  - Suitably constrain the event space over actors, targets and durations
  - Note Ramsey–De Finetti theorem: Bayesian updating converges to distribution when sampling from an exchangeable event space

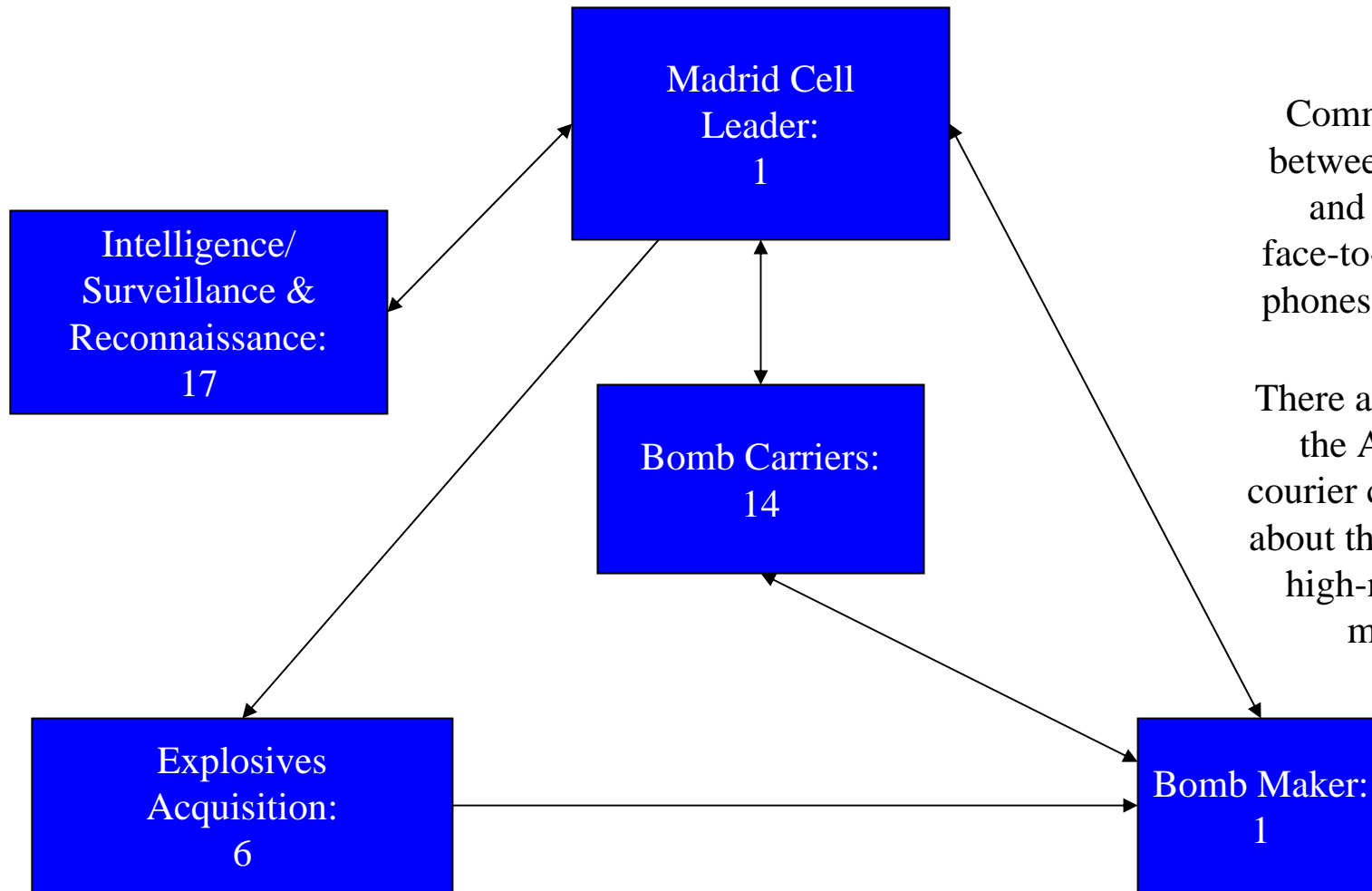
# Analyst Reasoning Issues

---

- Analysts do not usually attempt to estimate  $p(\text{terrorist-event} \mid \text{evidence})$
- Leads to behaviors as if underestimating  $p(\text{terrorist-event} := \text{false} \mid \text{evidence})$
- Given terrorist attack hypothesis there is a tendency to search only for confirming evidence
- This leads to over-focus on specific hypotheses and missed hypothesis opportunities
- Our objective is a mathematical basis and computable approach to estimate  $p(\text{terrorist-event} \mid \text{evidence})$

# Terrorist Events: Rare & Causal

## The Madrid Railway Attack, March 2004



Communications between cell leader and members: face-to-face, mobile phones and internet.

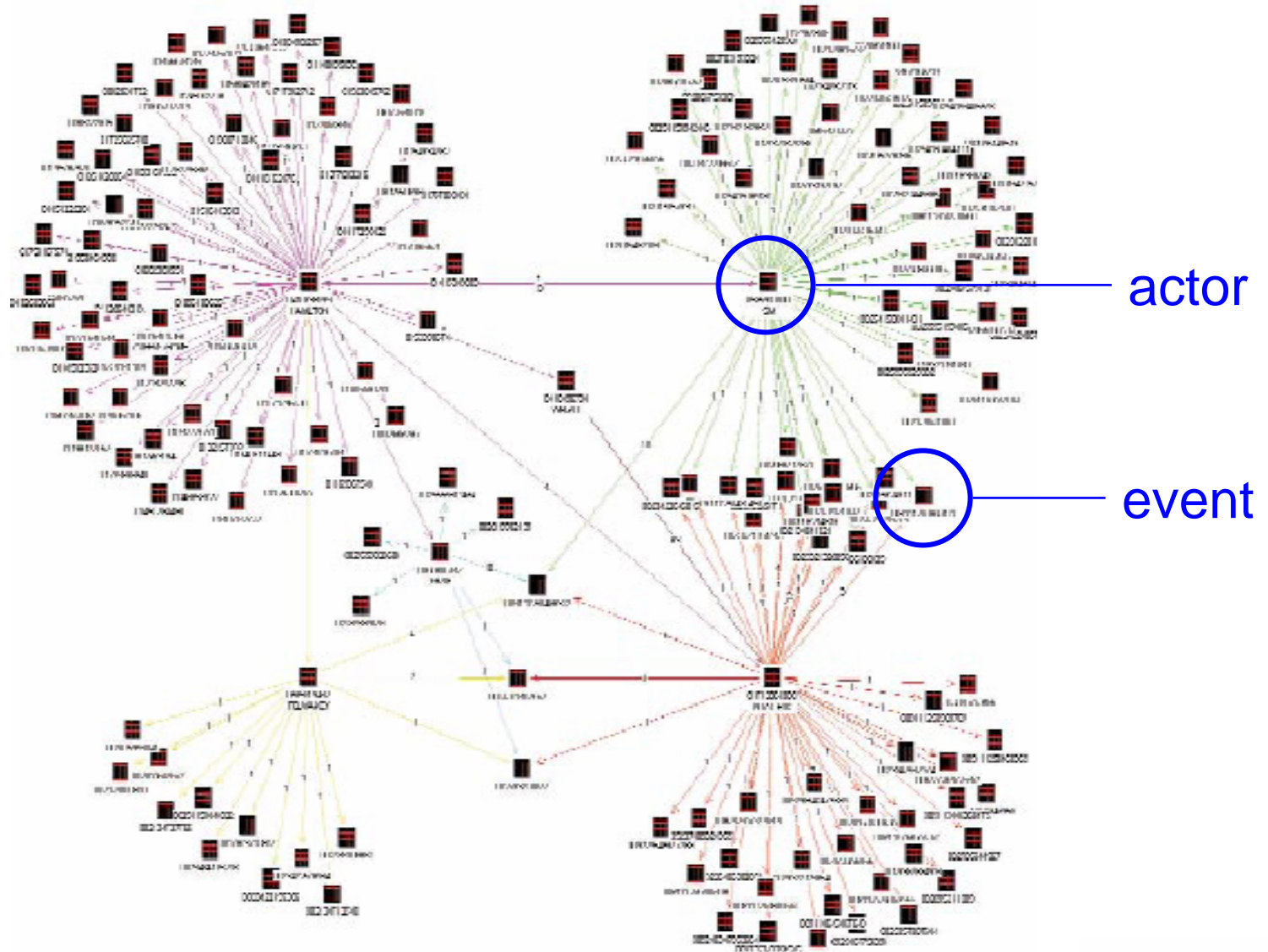
There are indications the AQ-Europe courier conveyed data about the operation to high-ranking AQ members

# CT Analysis: Link Diagrams

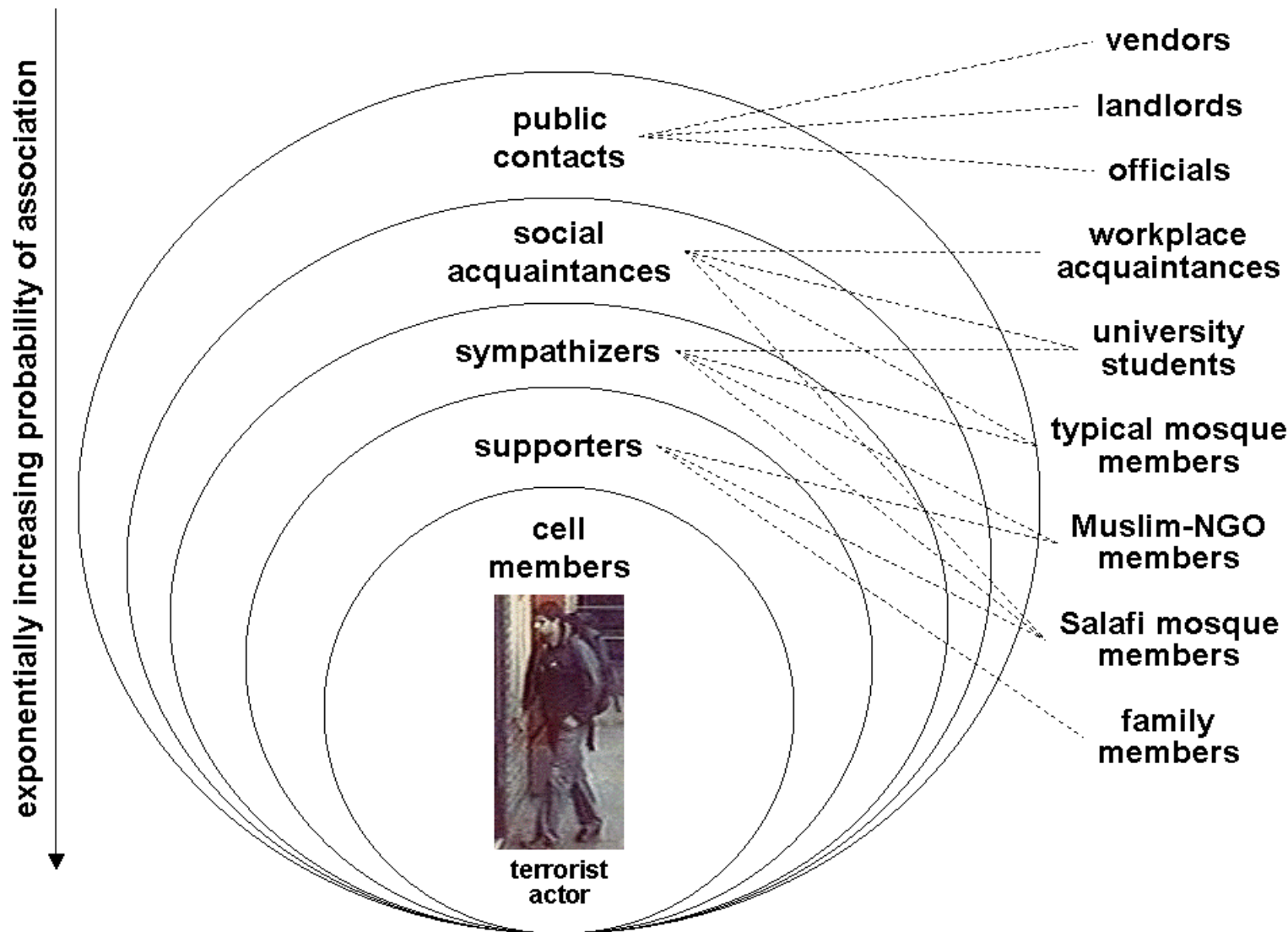
actors



situated  
acts

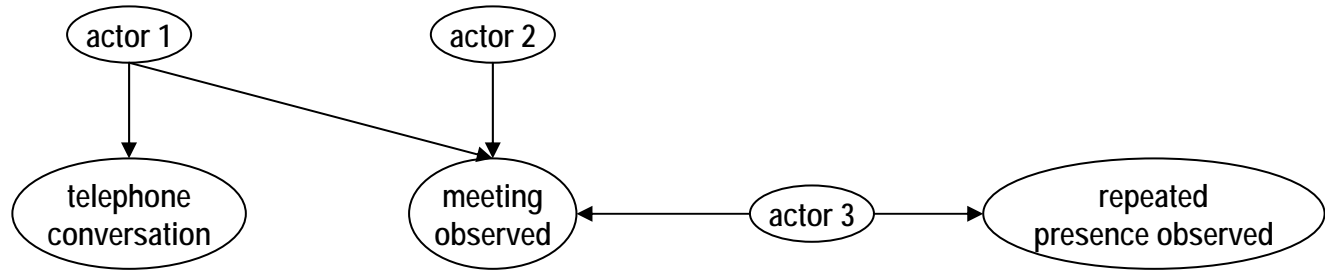


# Links Sample Space Concept

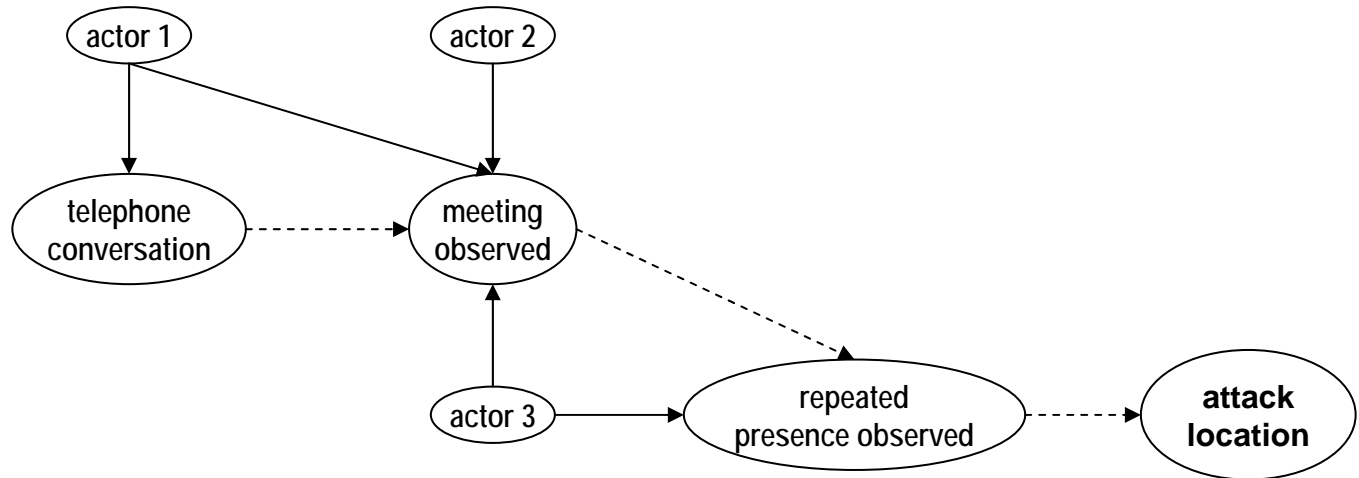


# From Links to Chains

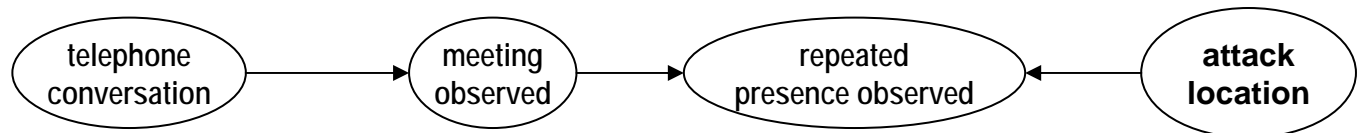
**Linked:**



**Inducted:**



**Causal:**



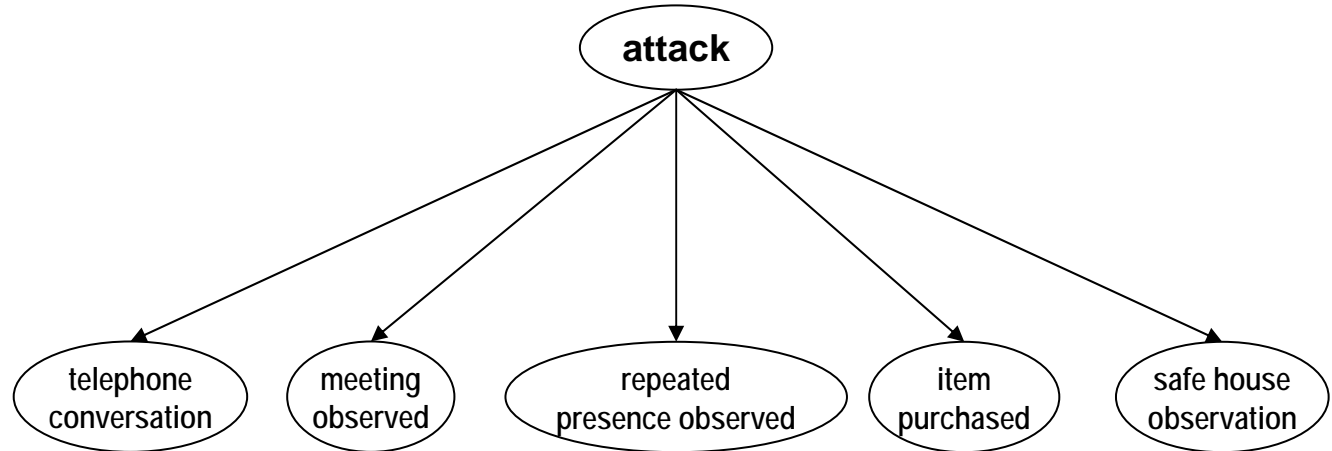
# Link-Direct Evidential Accrual

---

Hypothesis:

attack

Evidence:



Objective: Quantify belief in attack given evidence

Methodology: Bayesian probabilistic evidential accrual

# Enabling Reasoning Belief Quantification

---

**Hypothesis H: Terrorists executing attack plan on site**

- States: true, false

**Evidence E: Surveillance at site**

- States: true, false

## Bayes Rule

$$p(H|E) = p(E|H)p(H)/p(E)$$

$$p( E=true | H=true ) = .999$$

$$p( E=true | H=false ) = .001$$

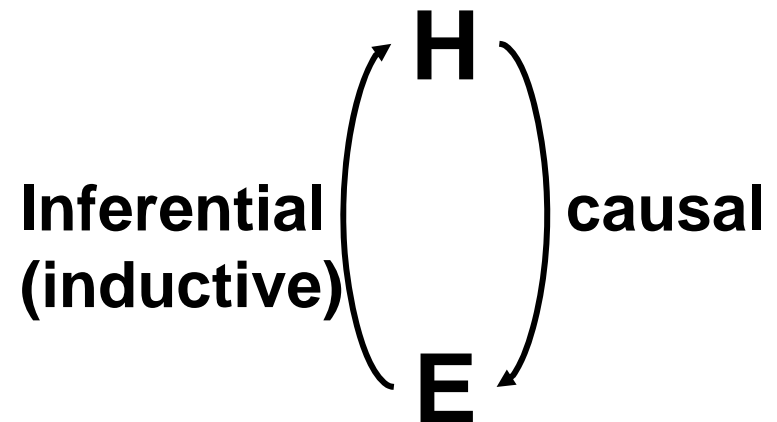
$$p( E=false | H=true ) = .001$$

$$p( E=false | H=false ) = .999$$

$$L_E = p(E|H=true) / p(E|H=false)$$

$$L_{E=true} = .999/.001 = 999$$

$$L_{E=false} = .001/.999 = .001001$$



# Rare Versus Weak Evidence

---

- **Weak Evidence:**  $L_E = p(E|H=\text{true}) / p(E|H=\text{false})$  is close to 1
- **Rare Evidence:**  $p(E|H=\text{true})$  and  $p(E|H=\text{false})$  are close to 0
- Weak evidence is not necessarily rare
- Rare evidence is not necessarily weak
- Weak evidence inference order doesn't matter
- Rare evidence inference order matters a lot

# Rare & Weak Evidence Examples

---

Consider  $p(\text{Presence Pattern} \mid \text{Terrorist Surveillance})$

Presence Pattern	Explanation	Classification
twice in one week	tourist	not_rare & weak
once a month for a year	monthly lecture	rare & weak
seven days in a row	terrorist	rare & not_weak
five days in a row	security guard	not_rare & not_weak

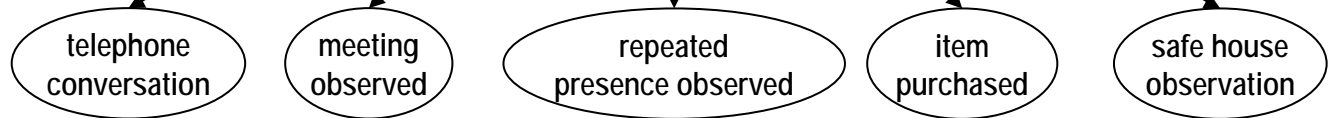
# Link-Direct Evidential Accrual

---

Hypothesis:



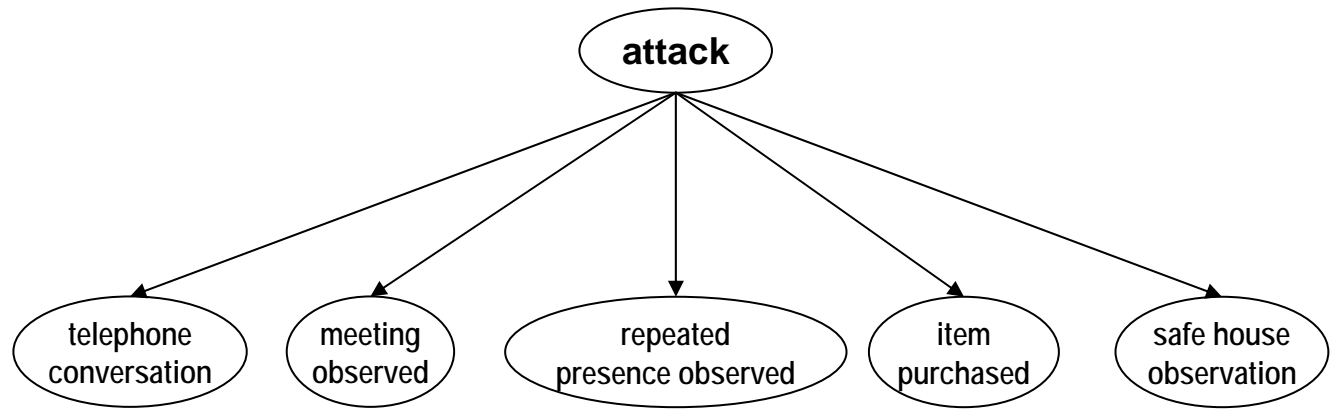
Evidence:



$$\begin{aligned} & p(\text{attack} \mid t \ \& \ m \ \& \ r \ \& \ i \ \& \ s) \\ & = p(t \ \& \ m \ \& \ r \ \& \ i \ \& \ s \mid \text{attack}) p(\text{attack}) / p(t \ \& \ m \ \& \ r \ \& \ i \ \& \ s) \\ & = p(t \mid \text{attack}) p(m \mid \text{attack}) p(r \mid \text{attack}) p(i \mid \text{attack}) p(s \mid \text{attack}) \\ & \quad p(\text{attack}) / p(t \ \& \ m \ \& \ r \ \& \ i \ \& \ s) \end{aligned}$$

# Link-Direct Evidential Accrual Issues

Hypothesis:



Evidence:

Prior Conditionals:

$p(\text{evidence} \mid \text{attack})$  not reasonably estimable

attack \ evidence	true	false
true	$p(t t)$	$p(t f)$
false	$p(f t)$	$p(f f)$

Other Issues:

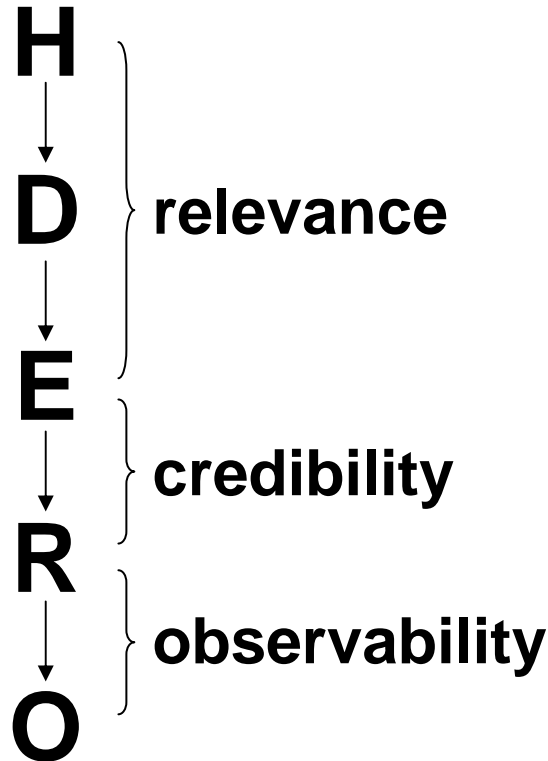
- $p(\text{telephone\_conversation} \mid \text{attack}:=\text{false})$  is high, but analyst likely ranks low
- Exchangeability of events assures that order of evidence arrival does not affect result of Bayesian updating in the limit of infinite pieces of evidence (Ramsey-DeFinetti theorem)
- But ordering update effects are important in finite sequences of evidence

# Rare Evidence Order Sensitive

	Case 1	Case 2	Case 3	Case 4	Case 5
$p(i A)$	0.999	0.999	0.999	<b>0.099</b>	0.999
$p(i A^c)$	0.001	0.001	0.001	<b>0.001</b>	0.001
$p(r A)$	0.999	0.999	<b>0.099</b>	0.999	0.999
$p(r A^c)$	0.001	0.001	<b>0.001</b>	0.001	0.001
$p(m A)$	0.999	<b>0.099</b>	0.999	0.999	0.999
$p(m A^c)$	0.001	<b>0.001</b>	0.001	0.001	0.001
$p(t A)$	<b>0.099</b>	0.999	0.999	0.999	0.999
$p(t A^c)$	<b>0.001</b>	0.001	0.001	0.001	0.001
$L_s(A)$	<b>25.12</b>	<b>8.38</b>	<b>5.38</b>	<b>4.09</b>	<b>25.12</b>

# Structuring Evidence for Accrual

---



**Evidence O: Repeat observation of suspect person**

- States: true, false

**Evidence R: Reliability of report**

- States: high, neutral, suspect

**Evidence E: Surveillance at site**

- States: true, false

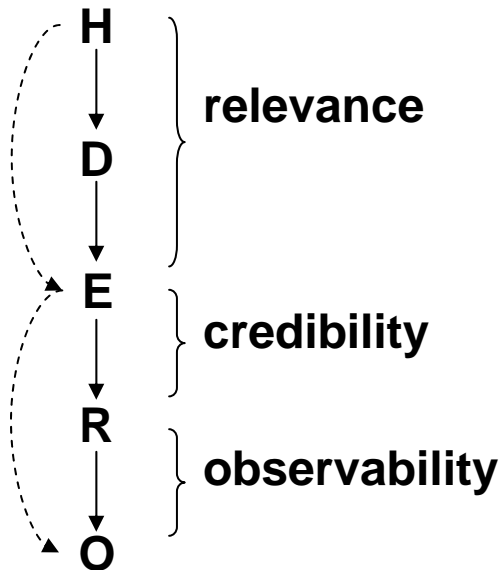
**Evidence D: Site is a terrorist target**

- States: true, false

**Hypothesis H: Terrorists executing attack plan on site**

- States: true, false

# Hierarchical Dependencies



**Evidence O: Repeat observation of suspect person**

- States: true, false

**Evidence R: Reliability of report**

- States: highly, neutral, suspect

**Evidence E: Surveillance at site**

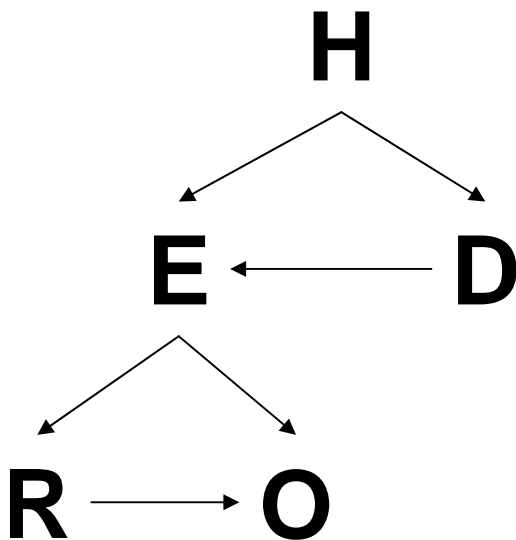
- States: true, false

**Evidence D: Site is a terrorist target**

- States: true, false

**Hypothesis H: Terrorists executing attack plan on site**

- States: true, false

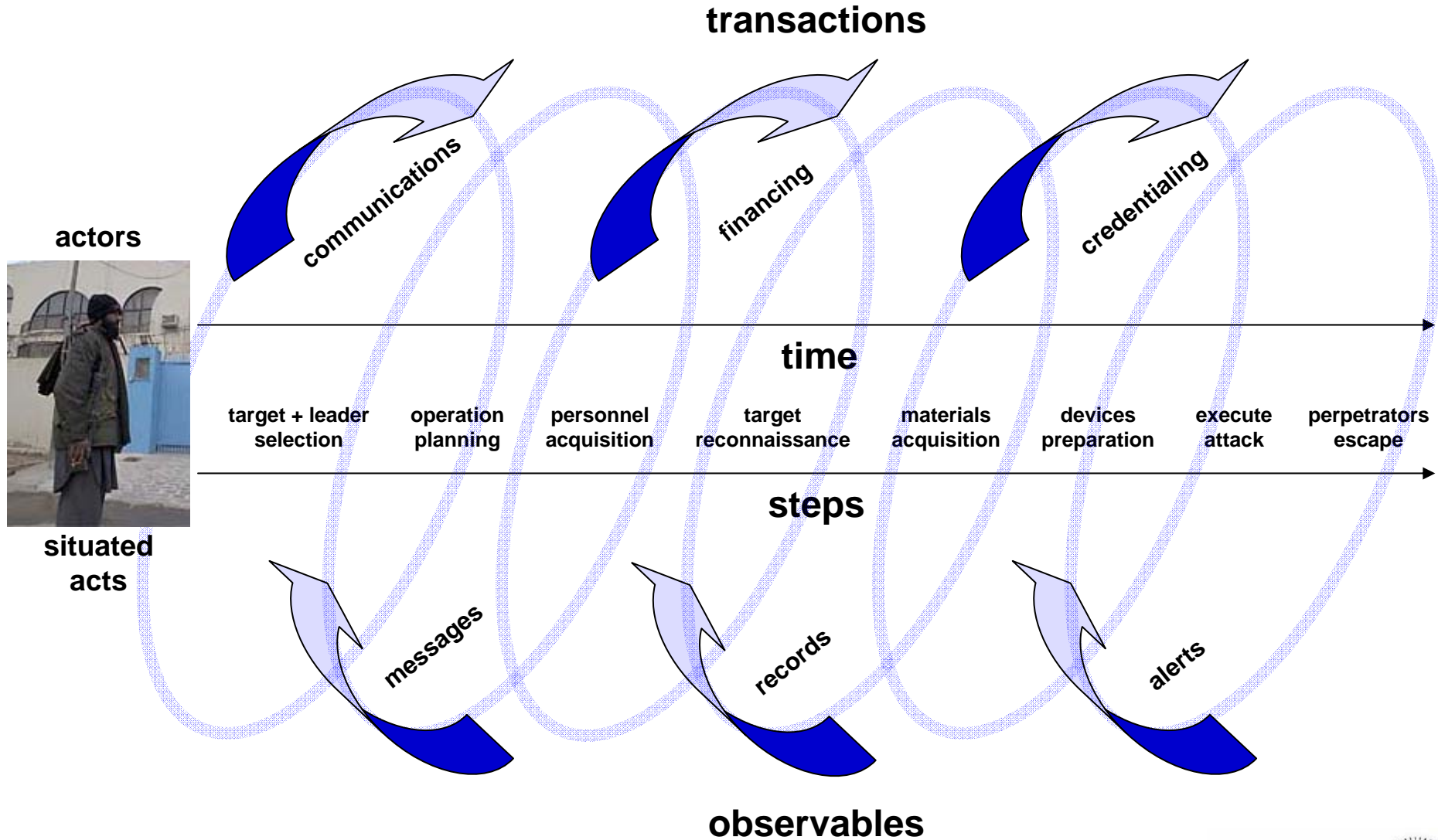


# Hierarchical Bayesian Inference Issues

---

- **Must account for multiple types of uncertainty**
- **Conditional independence cannot necessarily be assumed – variable relations form a directed acyclic graph**
- **Evidence arrives asynchronously in arbitrary order**

# CT Analysis: Causal Reasoning

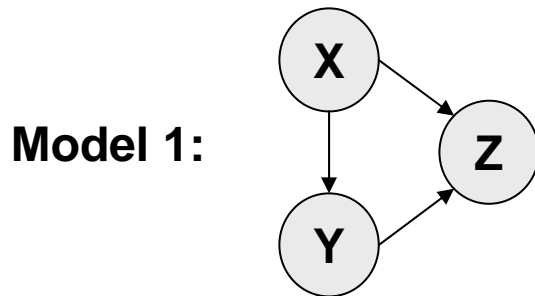


# Causal Reasoning Issues

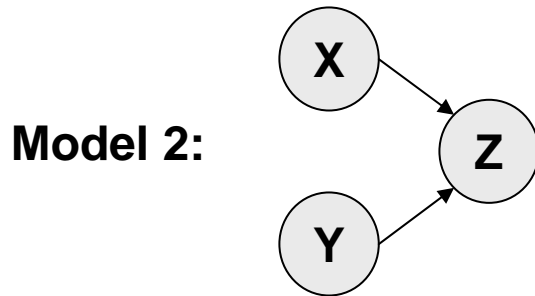
---

- Scientific inference strongly discouraged causal reasoning throughout the 20<sup>th</sup> century
  - R.A. Fisher, The Design of Experiments, 6<sup>th</sup> Ed., Oliver & Boyd, 1951.
- Breakthroughs in Bayesian inference support the principled use of causal scientific reasoning
  - J. Pearl, Causality, Cambridge University Press, 2000.
- Evidential accrual algorithms provide mathematical foundation for well-structured inductive causal inference
  - F. V. Jensen, Bayesian Networks and Decision Graphs, Springer, 2001.

# Bayesian Networks Nano-Tutorial



$$p(X, Y, Z) = \underbrace{p(Z | X, Y) p(Y | X) p(X)}_{\text{prior probability densities}}$$



$$p(X, Y, Z) = \underbrace{p(Z | X, Y) p(Y) p(X)}_{\text{prior probability densities}}$$

**Compare Models:**  
 exact solutions  
 delta sensitivity  
 training data  
 priors' validity

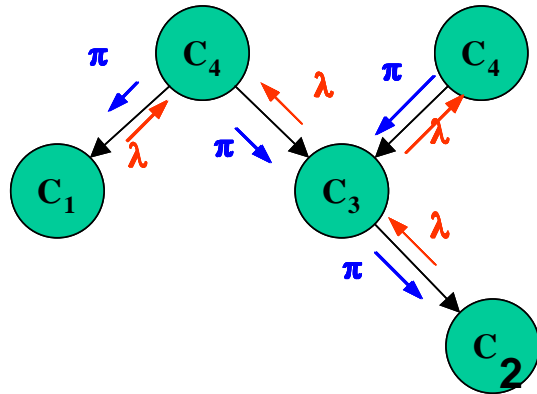
## Universal Solutions:

$$p(Z) = \sum_{X, Y} p(X, Y, Z) = \sum_{X, Y} p(Z | X, Y) p(Y) p(X)$$

- 1979: Decision Graph (Influence diagram) / Bayesian network definition (Howard & Matheson)
- 1981: First interactive universal inference algorithm solution (Shachter)
- 1984: Singly connected Bayesian networks inference algorithm solution (Pearl)
- 1988: First universal inference algorithm solution – join-tree algorithm (Lauritzen & Spiegelhalter)
- 1991: Second universal solution – symbolic probabilistic inference algorithm (D'Ambrosio)
- 1992: All exact universal decision algorithm solutions proven to be NP-hard (Cooper)
- 1997: IET trade-secret Java implementation of SPI (Takikawa & D'Ambrosio)
- 1998 – present: IET Quiddity\*Suite for additional functionality; object-orientation; robustness

# Bayesian Network Solutions

## Join Tree

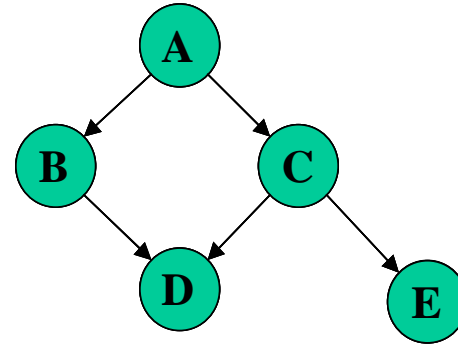


Message Passing Algorithm

Numerical Computation

Must be repeated for every query

## Symbolic Probabilistic Inference



$$P(D, E) = \sum_A \sum_B \sum_C P(A)P(B|A)P(C|A)P(D|B,C)P(E|C)$$

Symbolical mathematics to simplify the equation

Then compute numerical result

Unchanged factors can be cached

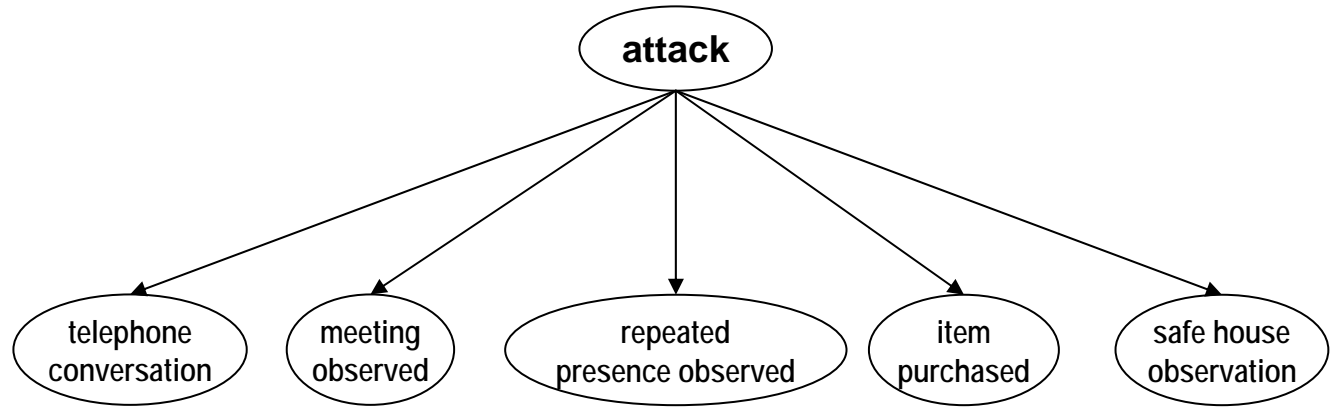
Each query is a function

Can generate extremely efficient runtime code

- Proceedings Uncertainty in Artificial Intelligence, AUAI Press
- [www.auai.org](http://www.auai.org)

# Naive Evidential Accrual

Hypothesis:



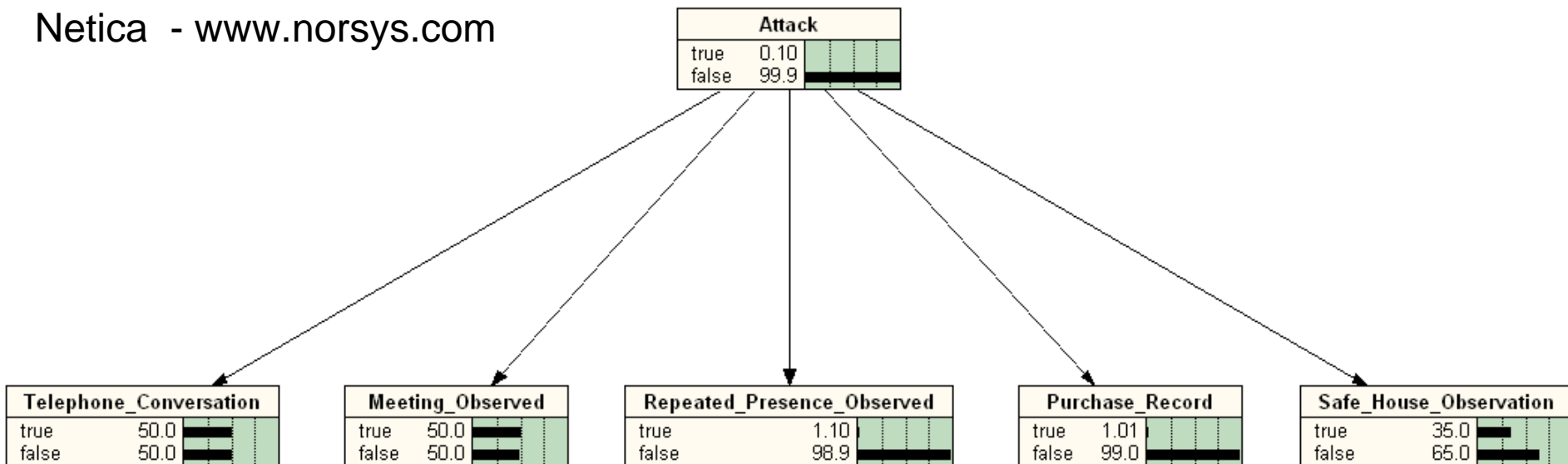
Evidence:

Prior Conditionals:

		attack	
		true	false
evidence	true	$p(t t)$	$p(t f)$
	false	$p(f t)$	$p(f f)$

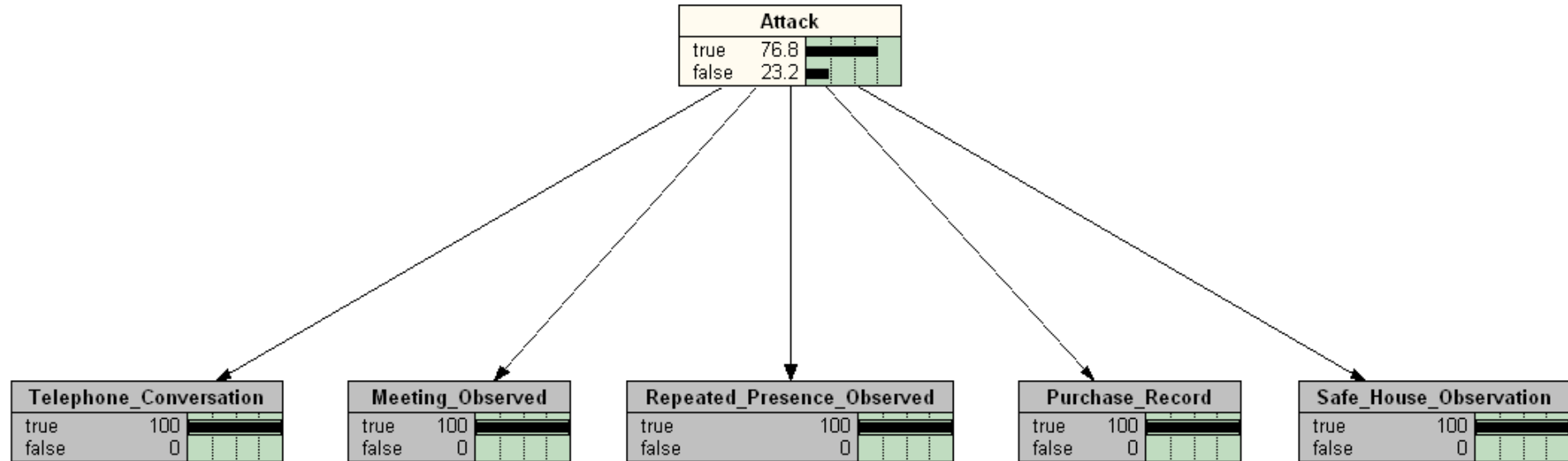
# Naive Evidential Accrual - Prior

Netica - www.norsys.com

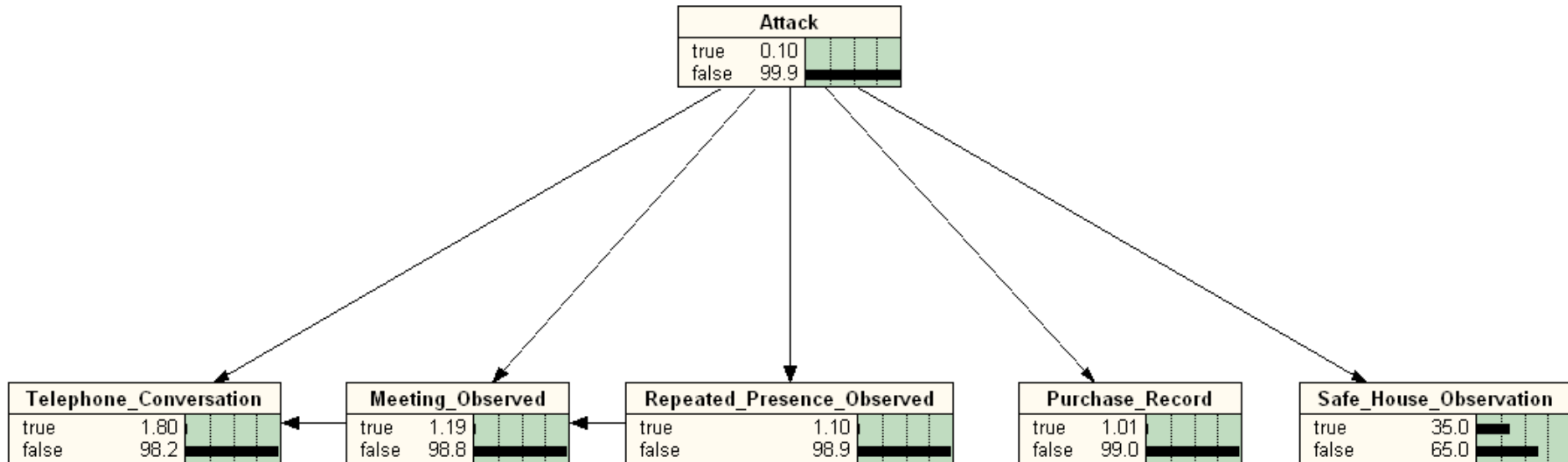


	a:=true	a:=false
$p(t:=true   a)$	.5	.5
$p(t:=false   a)$	.5	.5

# Naive Evidential Accrual - Posterior

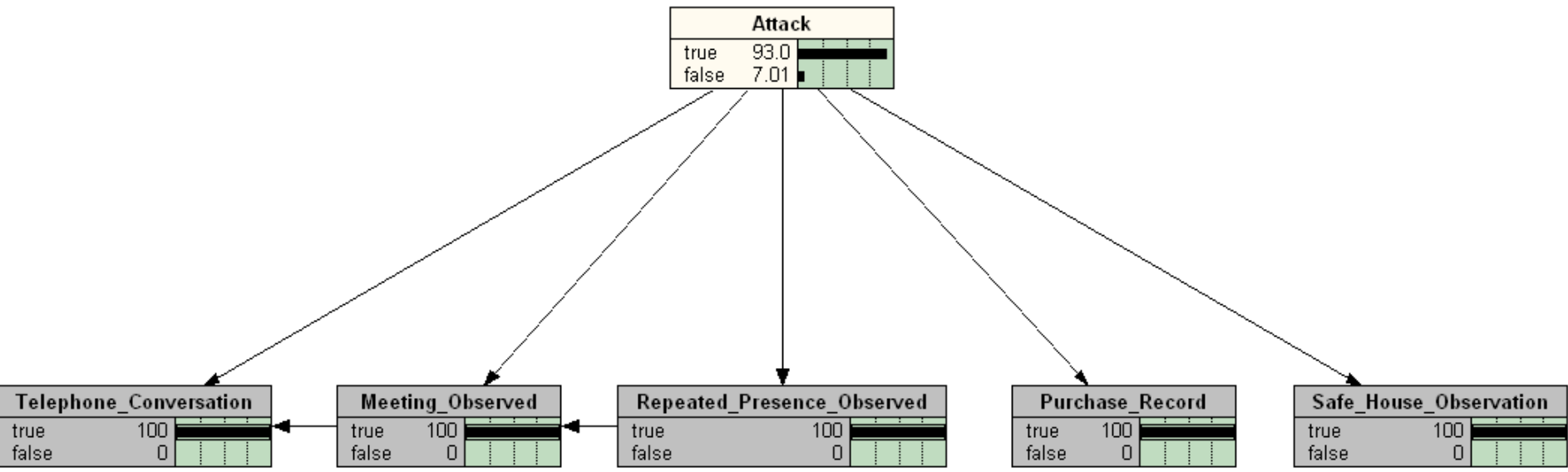


# Dependent Evidential Accrual - Prior



	a:=true m:=true	a:=true m:=false	a:=false m:=true	a:=false m:=false
$p(t:=true \mid m \ \& \ a)$	.5	.7	.7	.1
$p(t:=false \mid m \ \& \ a)$	.5	.3	.3	.9

# Dependent Evidential Accrual - Posterior



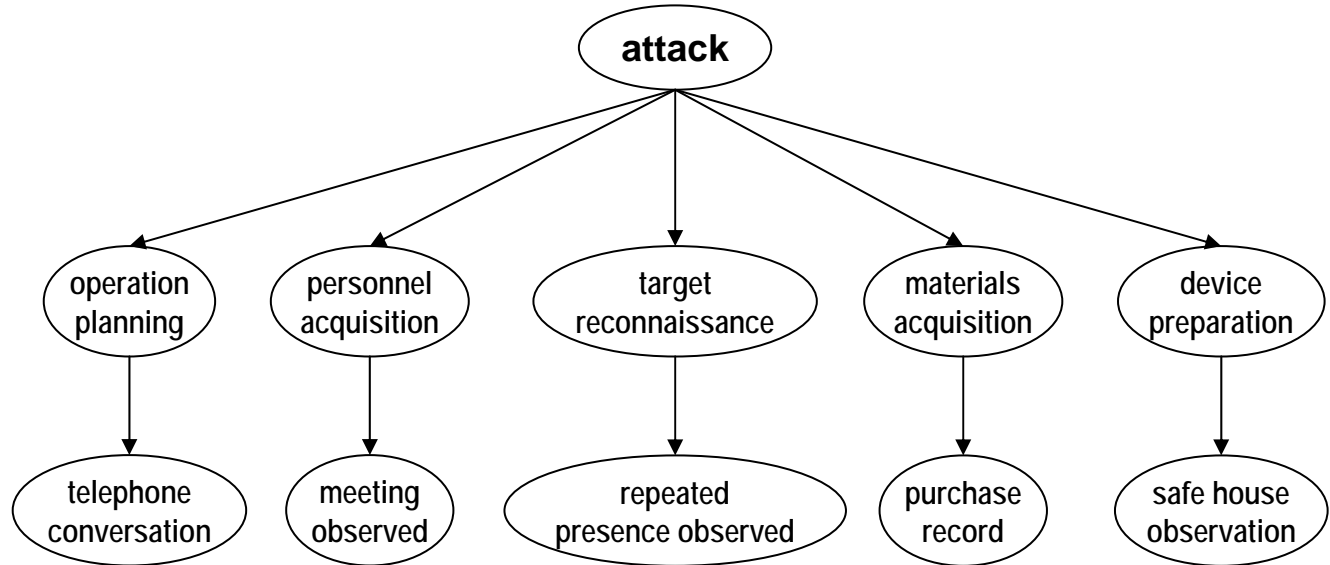
# Causal Models Intermediate Variables

---

Hypothesis:

Steps:

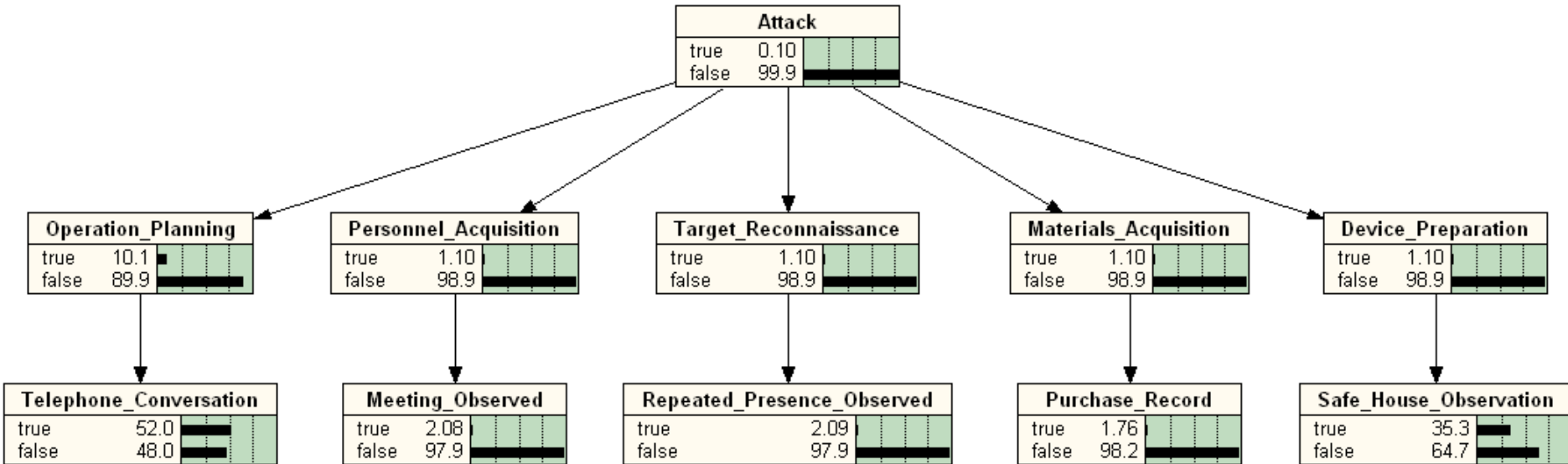
Evidence:



Prior Conditionals:  $p(\text{step} \mid \text{attack})$ ;  $p(\text{evidence} \mid \text{step})$

Result: Causal representation makes prior conditionals reasonably estimable

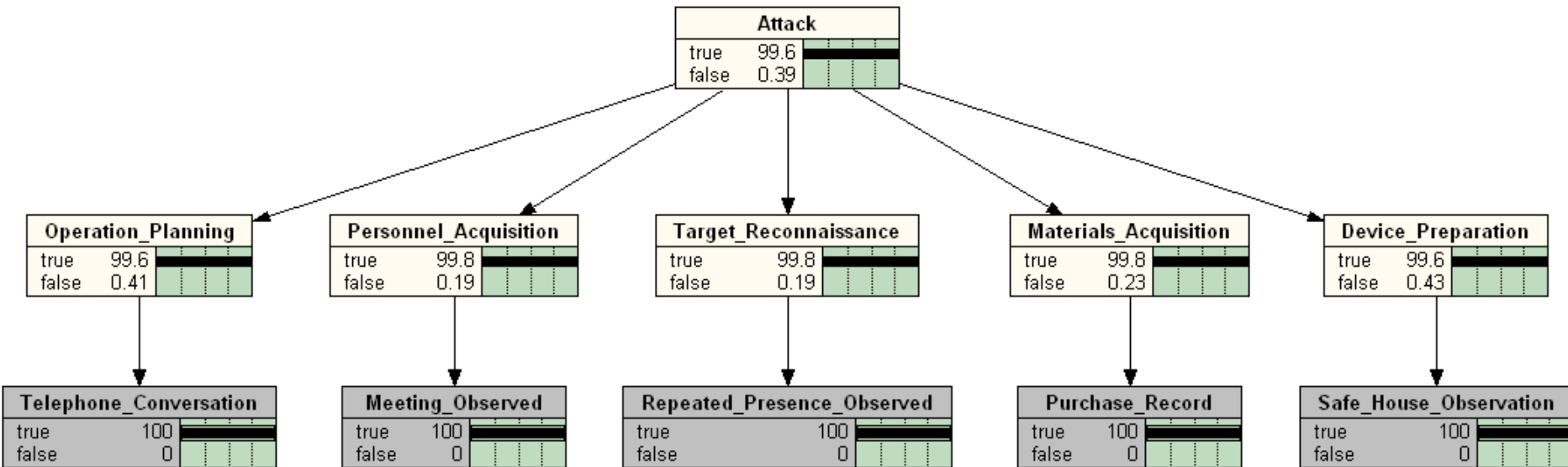
# Causal Evidential Accrual - Prior



	o:=true	o:=false
$p(t:=true   o)$	.7	.5
$p(t:=false   o)$	.3	.5

	a:=true	a:=false
$p(o:=true   a)$	.999	.1
$p(o:=false   a)$	.001	.9

# Causal Evidential Accrual - Posterior



# Counter-Terrorism Reasoning

---

- **Use causal Bayesian probabilistic modeling for rare event inductive reasoning**
  - Causality provides natural linkages for observable evidence
  - Causality constrains the sampling space
- **Develop causally structured models of variable relations that support reasoning chains**
  - Causal models have “natural” conditional priors
  - Provides platform for discussion of prior probabilities
- **Account for hypotheses completeness and credibility**
  - Models introduce credibility and context variables
  - “Forces” consideration of complementary alternative hypotheses
- **Arrival-driven automated evidence accrual**
  - Account for variables dependencies
  - Solve problem of asynchronous evidence arrival