



LAWRENCE  
LIVERMORE  
NATIONAL  
LABORATORY

# Adversary Modeling for Allocation of Effort Across Countermeasures

J. F. Lathrop

July 17, 2006

Military Applications Society Conference  
Mystic, CT, United States  
July 24, 2006 through July 26, 2006

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.



# **Adversary Modeling For Allocation of Effort Across Countermeasures**

**John Lathrop, Ph.D.  
Lawrence Livermore National Laboratory**

**July 26, 2006**

**Military Applications Society Conference  
Mystic, Connecticut**

This work was performed under the auspices of the U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

# What We Are Trying to Capture

---



**Allocation of effort across countermeasures.**

**So seek “cost – effectiveness” of CMs.**

**But what is “effectiveness”? = Reduction of Risk**

**But:**

**As implement a countermeasure,**

**population of adversaries adapts (maybe):**

- changes targets**
- changes weapon**
- changes tactics**

**What does not change?: - Adversary values**

**- Adversary decision behavior**



# And Another Thing to Capture

---



**“Countermeasures” covers:**

- Prevention**
- Hardening**
- Detection**
- Response**

# And Another Thing to Capture

---



**But really:**

**“Countermeasures” covers:**

- **Reduce Adversary Incentives to Attack**
- **Prevention**
- **Hardening**
- **Detection**
- **Response:**
  - **Response Effectiveness**
  - **Response Resilience**
- **Societal Expectations**
- **National Political/Operational Reactions/Costs**
- **Ultimate Societal Values, e.g., “England’s Finest Hour”**

# And Another Thing to Capture

---



“Countermeasures” covers:

- Reduce Adversary Incentives to Attack
- Prevention
- Hardening
- Detection
- Response:
  - Response Effectiveness
  - Response Resilience
- Societal Expectations
- National Political/Operational Reactions/Costs
- Ultimate Societal Values, e.g., “England’s Finest Hour”

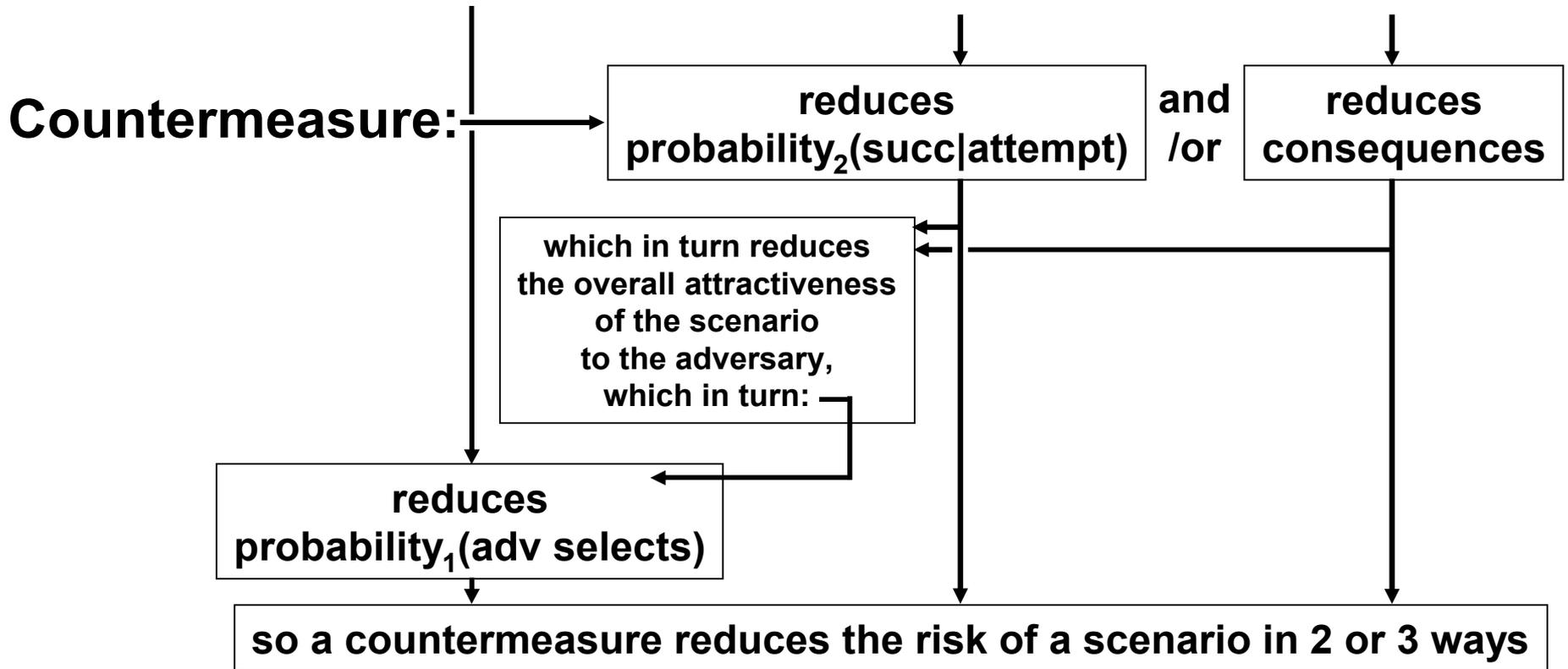
**So there’s much more to the strategy.**

**So “cost – effectiveness”  
must be based on a “yardstick”  
that applies consistently  
across those CM effects/types**

# How Countermeasures Reduce Risk



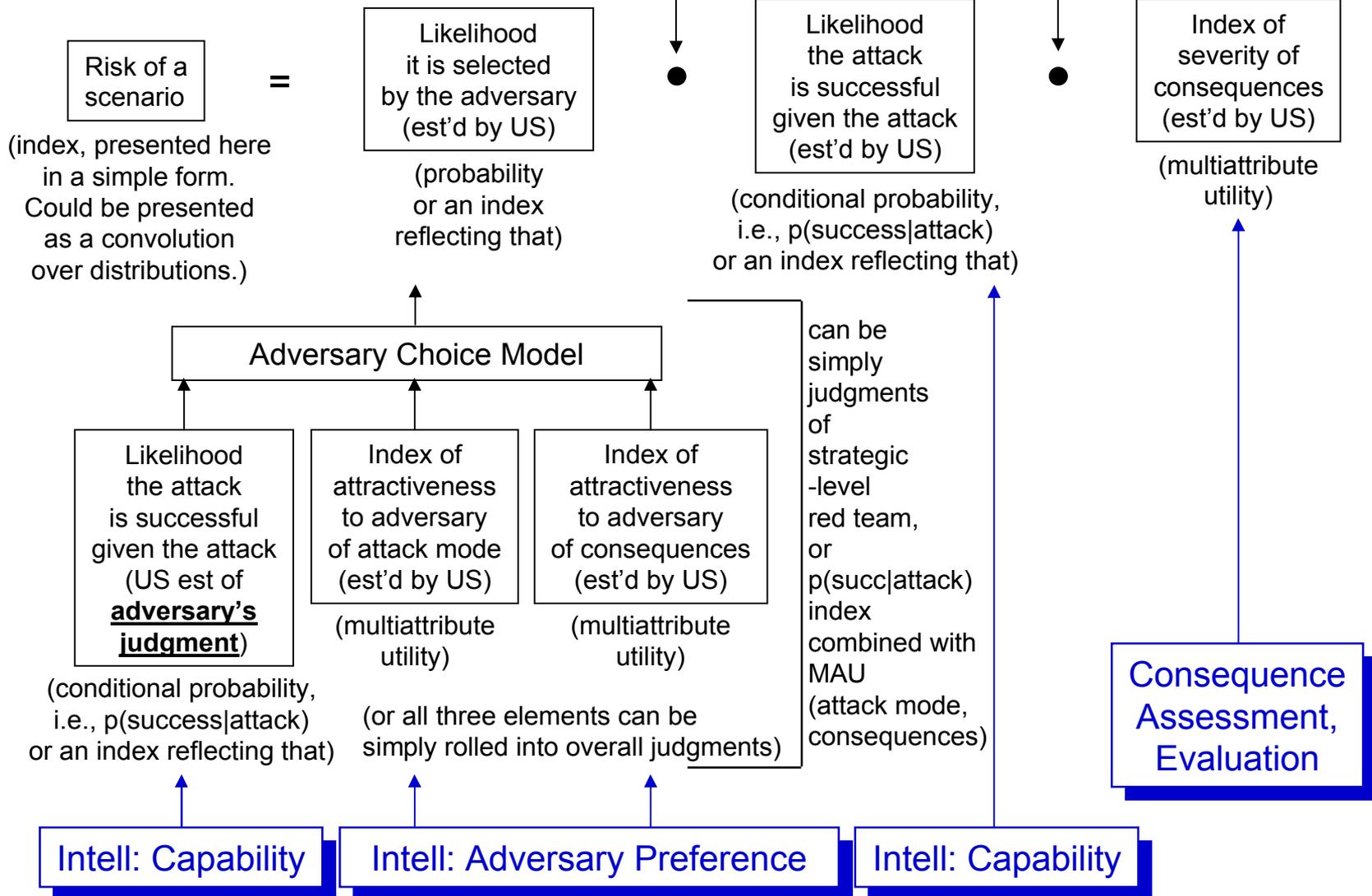
$$R(\text{scenario}) = \text{probability}_1(\text{adv selects}) \bullet \text{probability}_2(\text{succ|att}) \bullet U(\text{conseq's})$$



though that benefit is “capped” by the fact that the adversary can choose a different scenario, that was previously less attractive to him

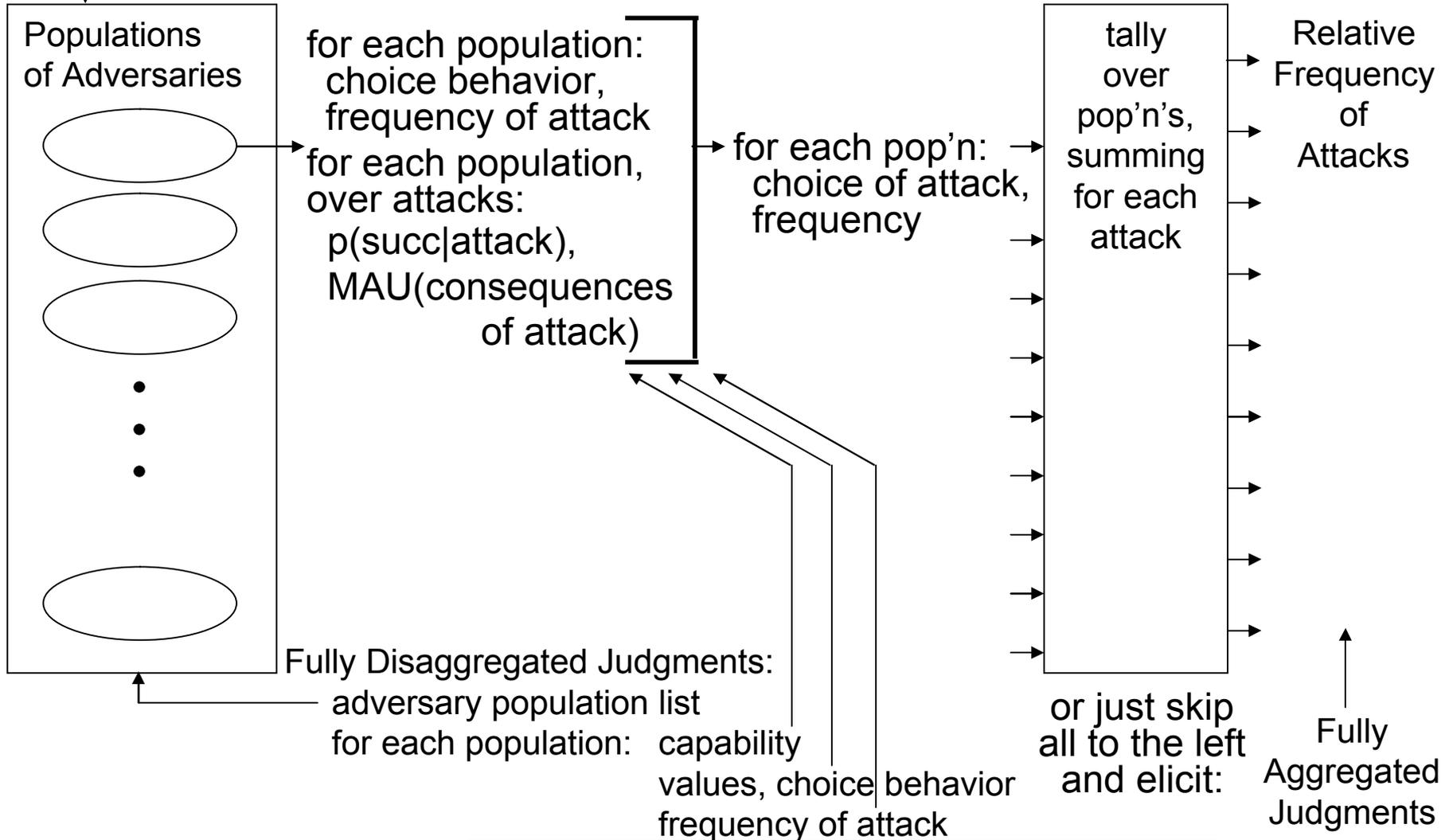
Operator that combines the indices in a metrically appropriate way.  
 If indices are probabilities, this would be a multiplication.  
 If the indices are more general indices, this would be a table relating two index values to a single combined index value.

As before. If likelihood index is a probability and severity a utility, this would be a multiplication.



# An Inference Structure

↙ A list? Or: Agent-Based Modeling. Talking with John Hiles, NPS



**Basic Principle: Push as far to the left as you can.**

# Model Requirements

---



**Must evaluate CMs in the context of a Game Against the Adversary:**

**Capture that:**

- the adversary shifts his attacks in response to CMs  
(else will overestimate risk reduction of a CM)
- the adversary has preferences and chooses  
(account for his values, his choice behavior)
- $MAU_{adv} \neq MAU_{us}$ , predictive vs evaluative, respectively
- $p_{adv}(succ|attack) \neq p_{us}(success|attack)$ ,  
predictive vs evaluative, respectively

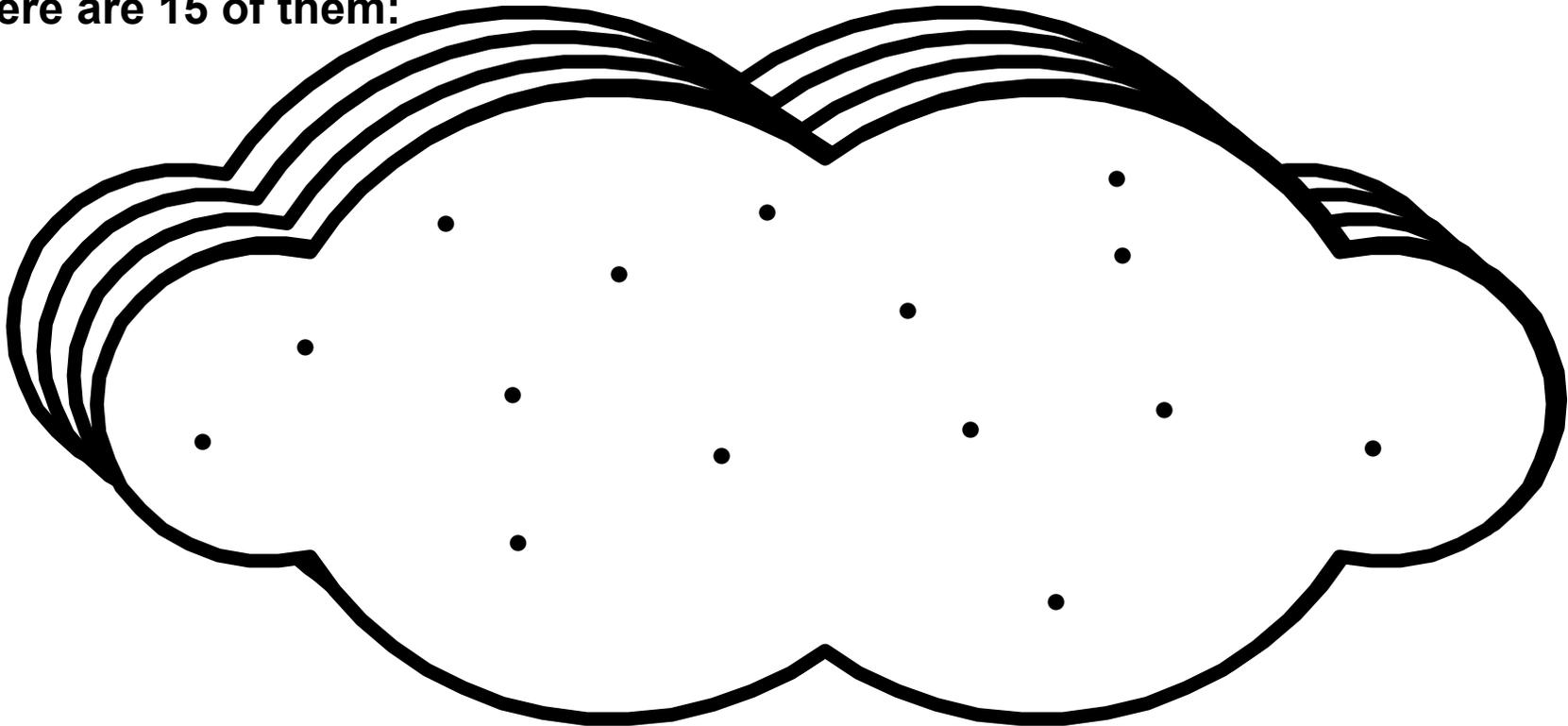
**Can do that with MAU modeling,**

**not counting on adversary actually behaving strictly that way,  
but using MAU as a noisy predictive guide.**

**So in fact: MAU plus probabilistic choice model.**

# Model Requirements: Address Problem: Coverage of Scenario Space

Any finite list of scenarios only addresses a small part of the scenario space.  
Here are 15 of them:

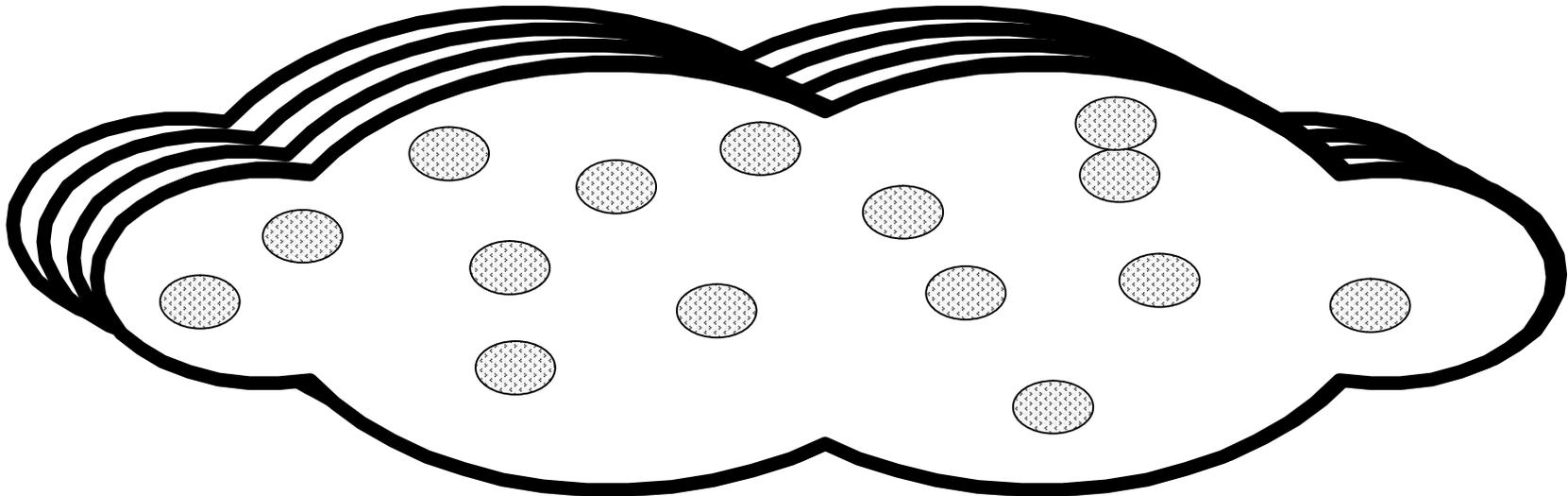


Call them “Design Basis Threats.” Still the same problem.

How do you establish preparedness for scenarios “not on the list”?

# Model Requirements: Address Problem: Coverage of Scenario Space

You can “genericize” each scenario, to “smear it out” over more space:



But then each scenario is too unspecified to calculate consequences.

Once you make a scenario specific enough to calculate consequences, it covers very little scenario space.

Shifting from scenarios to countermeasures does not solve the problem: Measuring countermeasure effectiveness still requires calculating consequences of scenarios, without, then with, the countermeasure.

# The Challenge, Basic Approach

---



The analysis structure is not the challenge – that is “easily” sketched.

The challenge and the approach:

- the information exists in experts’ heads;
- the challenge is in getting it out of those heads, and
- that challenge is met by structuring the problem, developing the models and coefficients, then expertly eliciting them.

And so, key line of investigation is:

What information can be elicited how from whom,

- on:
- adversary MAU attributes
  - adversary perceived probabilities
  - adversary choice behavior

(how identify alternatives, list them, choose among them)

# And So We Can Now Name The Approach:

---



## MARS / NEXIIS

### The Model / The Program

#### **MARS: Modeling the Adversary for Responsive Strategy**

Mars = the Roman god of war

#### **NEXIIS: National Enterprise**

#### **(X)Crossing Intelligence with Infrastructure Systems**

Nexus = a means of connection, a link or tie,  
a place where two systems interlace into a single system

# Overall Structure of MARS



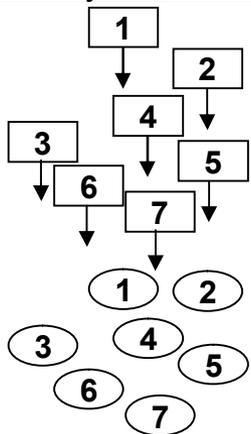
## Adversary Model Inputs

goals, values,  
choice behavior,  
information,  
capabilities

(after countermeasures)



## Adversary Model Loaders



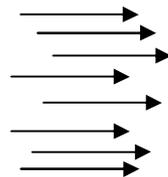
## Adversaries

each a  
choosing/acting  
agent,  
with goals, values,  
choice behavior,  
information,  
capabilities

(after countermeasures)

## Possible Attacks

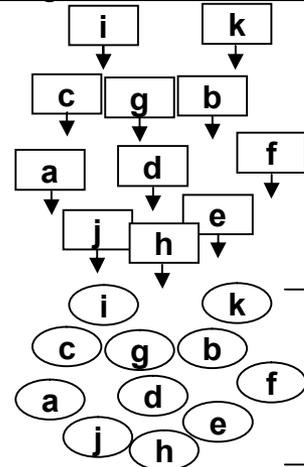
each with an  
adversary –  
target pair,  
probability  
per year



Target Model Inputs  
 $p(\text{consequences}|\text{attack})\text{s}$   
(after countermeasures)  
over ranges of  
capabilities, attacks



## Target Model Loaders



Targets  
each with  
 $p(\text{consequences}|\text{attack})\text{s}$   
(after countermeasures)  
over ranges of  
capabilities, attacks

probability  
distribution  
over  
consequences,  
 $p$  per year

Model  
runs  
over  
uncertainties

Output:  
single  
numeraire:  
subjective  
expected  
multiattribute  
utility  
(of consequences  
to the US,  
values of the US)  
for the  
Input Data Set

# Inputs – Outputs Structure

## Adversary Model Inputs

goals, values,  
choice behavior,  
information,  
capabilities  
(after countermeasures)

The bulk of the adversary models built up over time into a database. Gradually build up a “stable” of perhaps 20 adversary groups, improving the model for each group as data becomes available.

## Countermeasure Evaluation:

Load adversary choice/capability implications of the countermeasure. Assume goals, values, choice behavior unchanged by countermeasure. Then run MARS, compare output to baseline output.

Target Model Inputs  
p(consequences|attack)s  
(after countermeasures)  
over ranges of  
capabilities, attacks

The bulk of the target models built up over time into a database. Gradually build up a “stable” of very many targets, starting with generic target type groups, then getting more specific over time, improving the model for each target/group as data becomes available.

## Countermeasure Evaluation:

Load target p(consequences|attack)s implications of the countermeasure. Then run MARS, compare output to baseline output.

Output:  
single numeraire:  
subjective expected  
multiattribute utility  
(of consequences to the US,  
values of the US)  
for the  
Input Data Set

The output numeraire, subjective expected multiattribute utility (SEMAU) provides a metrically valid “yardstick” for measuring the benefits of any countermeasure, comparable across countermeasures.

## Countermeasure evaluated by:

- loading adversary choice/behavior implications of the countermeasure
- loading target p(consequences|attack)s implications of the countermeasure
- running MARS with those loaded datasets, calculate SEMAU
- compare that with the baseline SEMAU.

# Details of MARS

---



After loading countermeasure implications (for adversary models, for target models):

Each Adversary Model conducts several steps in each run of the overall model:

- Adversary:
- acquires any incremental information being considered (once acquired, assume it stays)
  - acquires any incremental capability being considered (once acquired, assume it stays)
  - acquires a target-attack choice set, or modifications of its baseline choice set
  - chooses a target-attack from that set
  - launches that attack, at some probability per year based on propensity to attack per year

For that same run of the overall model, the attacked Target Model generates a consequence vector based on its loaded  $p(\text{consequences} \mid \text{attack, adversary capabilities, countermeasure})$ .

Still being considered: How best to model the several uncertainties involved in the above steps.

A “baseline” way to handle all of those uncertainties:

For any given countermeasure (loading its implications into the adversary and target models): the MARS model is run many times, in a monte carlo fashion,

where the runs vary in instantiations of:

- a probabilistic increment-in-information model
- a probabilistic increment-in-capability model
- a probabilistic choice model, covering:
  - acquisition of a choice set of target-attacks
  - choosing from among that set
  - choosing to actually launch that attack
- $p(\text{consequences} \mid \text{attack, adversary capabilities, countermeasure})$  of the attacked target.

All runs can be normalized to a background propensity to attack per year.

# Another Mode of MARS: Emergent Threat Time Series

---



**MARS can just as easily be run with a fixed baseline set of countermeasures, re-arranging the monte carlo calling program to run a series of time series where at each time step the “dice is rolled” on:**

- does each adversary group acquire an increment of information (which then stays acquired)**
- does each adversary group acquire an increment of capability (which then stays acquired)**

**In that mode, MARS can paint out a “growth in risk over time” curve for any given set of inputs re**

- probability an increment in information**
- probability an increment in capability**  
**will be acquired per time period (and once acquired, stays).**

# Improvement Over: “Scenarios”



The MARS model is an improvement over the use of “scenarios.”

“Scenarios,” in fact, do not exist. They are a construct.

What exists, actually, in the real world, is what is shown on Slide 9:

- a population of adversary groups
- a population of targets
- information on adversary choice, capability, success and consequences

Like any good model, MARS structurally mimics reality.

Because of that, MARS cannot even represent a “scenario,” since no such thing exists in reality.

If you still want to “risk prioritize” scenarios, it’s a stretch, but you can do it with MARS, in the following steps:

- make the (bold) assumption that the “risk” of a scenario is the difference between the overall risk faced by the US (SEMAU) in the baseline minus the overall risk faced by the US (SEMAU) in a world where all consequences of that scenario are zeroed out.
- run MARS in those two modes (baseline and consequences zeroed)
- define the “risk” as the difference in those two runs in SEMAU.

# Improvement Over: “Vulnerability Assessment”



**MARS is an improvement over the use of “Vulnerability Assessments.”**

**VAs can misallocate resources by assessing the vulnerabilities of targets, and prioritizing countermeasures based on:**

- ease of attacking that target and**
- the consequences of such an attack.**

**Two problems with that:**

- because no thought is given to adversary choice, VAs can recommend countermeasures (primarily hardening) for cases that may be quite unlikely to be chosen by adversaries.**
- effectiveness of countermeasures are over-estimated, since implicitly, VAs assume that the countermeasure reduces overall risk by reducing probability times consequence of that attack-target pair. But in fact the adversary is apt to simply go elsewhere to attack.**

**MARS evaluates countermeasures based on the strategic logic of Slide 9, and so avoids both of those problems.**

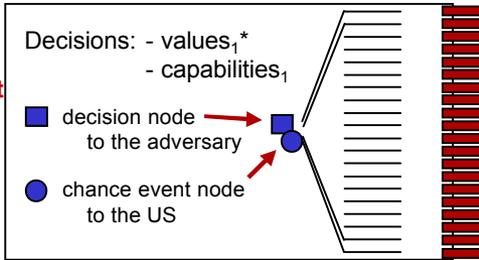
# Restructuring MARS into Lists



\*MAU<sub>adv</sub>(CEIFUD<sup>1</sup>, embarrass USG, attack attributes, p<sub>adv</sub>(success))

<sup>1</sup>Casualties, Economic Loss, Icons, Fear-Uncertainty-Doubt

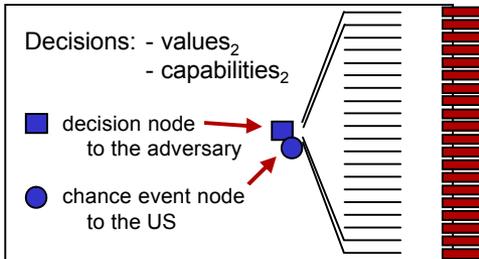
Adversary Group 1



20 attacks (target-weapons-tactics)

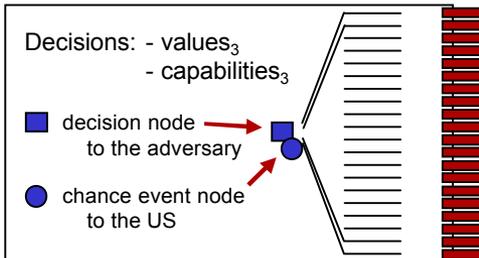
for each attack:  
p(consequences | attack, capability, CM)  
(CM = countermeasure)

Adversary Group 2



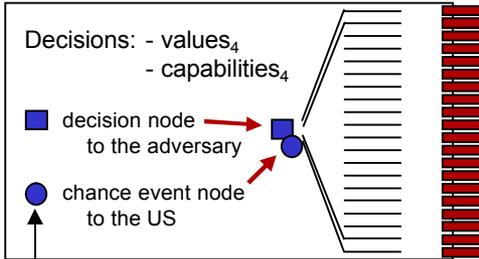
The same 20 attacks for each attack:  
p(consequences | attack, capability, CM)

Adversary Group 3

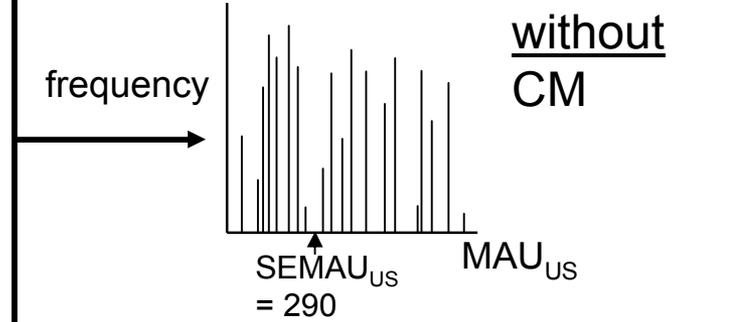
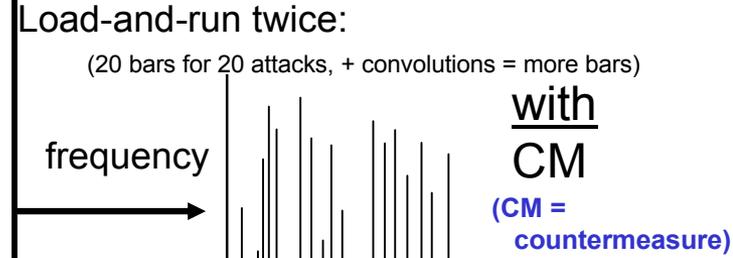


The same 20 attacks for each attack:  
p(consequences | attack, capability, CM)

Adversary Group 20



The same 20 attacks for each attack:  
p(consequences | attack, capability, CM)



So CM is "worth" 290 → 320 SEMAU, equivalent to "\$20B" (\$ as relative scale, metric = cardinal)

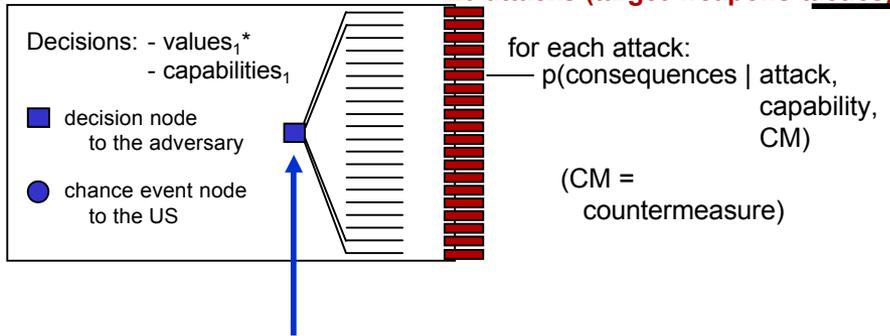
As a first approx: 
$$\text{Our } p_{US}(\text{adv will choose } i) = \frac{\text{MAU}_{adv}(\text{attack } 1)}{\sum_{i=1, n_i} \text{MAU}_{adv}(\text{attack } i)}$$

“Scenario Generator”

# List-Wise MARS, detail 1

\*MAU<sub>adv</sub>(CEIFUD, embarrass USG, attack attributes, p<sub>adv</sub>(success))

Adversary Group 1



The goal of the decision model is to “automate” IC judgments

As a first approx:

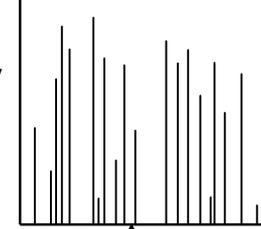
$$p_{US}(\text{adv will choose } i) = \frac{\text{MAU}_{\text{adv}}(\text{attack } 1)}{\sum_{i=1, n_i} \text{MAU}_{\text{adv}}(\text{attack } i)}$$

This approximation “behaves well,” but is decision-process nonsensical.

Load-and-run twice:

(20 bars for 20 attacks, + convolutions = more bars)

frequency



with  
CM

(CM = countermeasure)

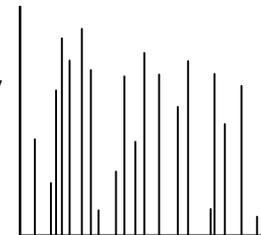
SEMAU<sub>US</sub>  
= 320

MAU<sub>US</sub>

(MAU = multiattribute utility)

(SEMAU = subjective expected MAU)

frequency



without  
CM

SEMAU<sub>US</sub>  
= 290

MAU<sub>US</sub>

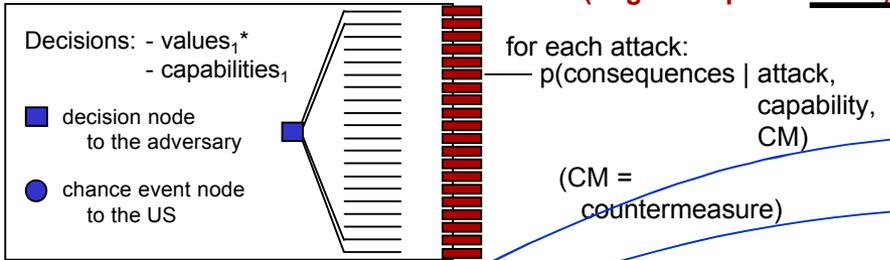
So CM is “worth”  
290 → 320 SEMAU,  
equivalent to “\$20B”  
(\$ as relative scale,  
metric = cardinal)

# List-Wise MARS, detail 2

\*MAU<sub>adv</sub>(CEIFUD, embarrass USG, attack attributes, p<sub>adv</sub>(success))

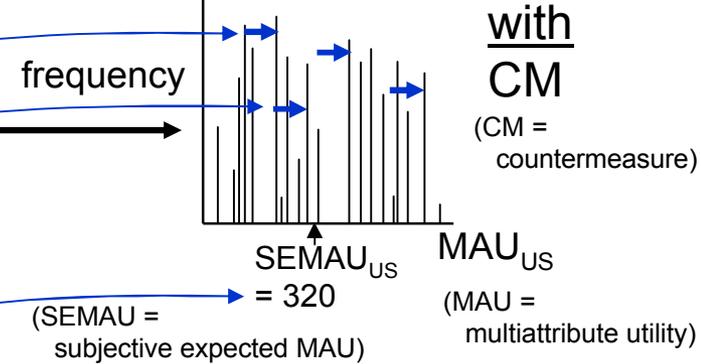
20 attacks (target-weapons-tactics)

Adversary Group 1



Load-and-run twice:

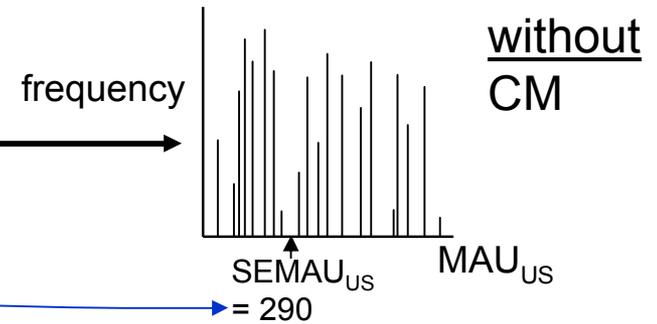
(20 bars for 20 attacks, + convolutions = more bars)



Can run “contrasts” to show how a CM reduces risk.

Can take derivatives and draw conclusions:

- characterize best directions for CM improvements
- demonstrate effectiveness of resilience



So CM is “worth” 290 → 320 SEMAU, equivalent to “\$20B” (\$ as relative scale, metric = cardinal)

# Adversary Decision Modeling



From before: Can predict adversary choice with MAU modeling, not counting on adversary actually behaving strictly that way, but using MAU as a noisy predictive guide.

So in fact: MAU plus probabilistic choice model.

Simply take past work in sensitivity analysis over weights, and re-apply to propagate weight uncertainty into choice uncertainty.

But a problem:

What about an adversary that chooses based on dreams/visions?

Shouldn't go full LaPlacian (equal probability of all alternatives), but could go to a mix of decision models, one of which is LaPlacian.

Will use both standard and unique MAU elicitation, and SP elicitation, tools, based on broad experience.

# First Step: Objectives Hierarchies

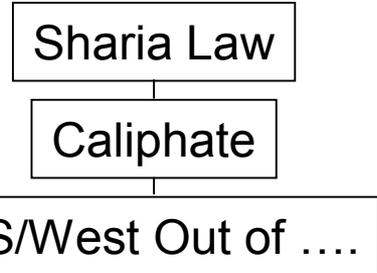


**Fundamental US objective: pursue policies with minimum impediment**

## Adversary Objectives Hierarchies

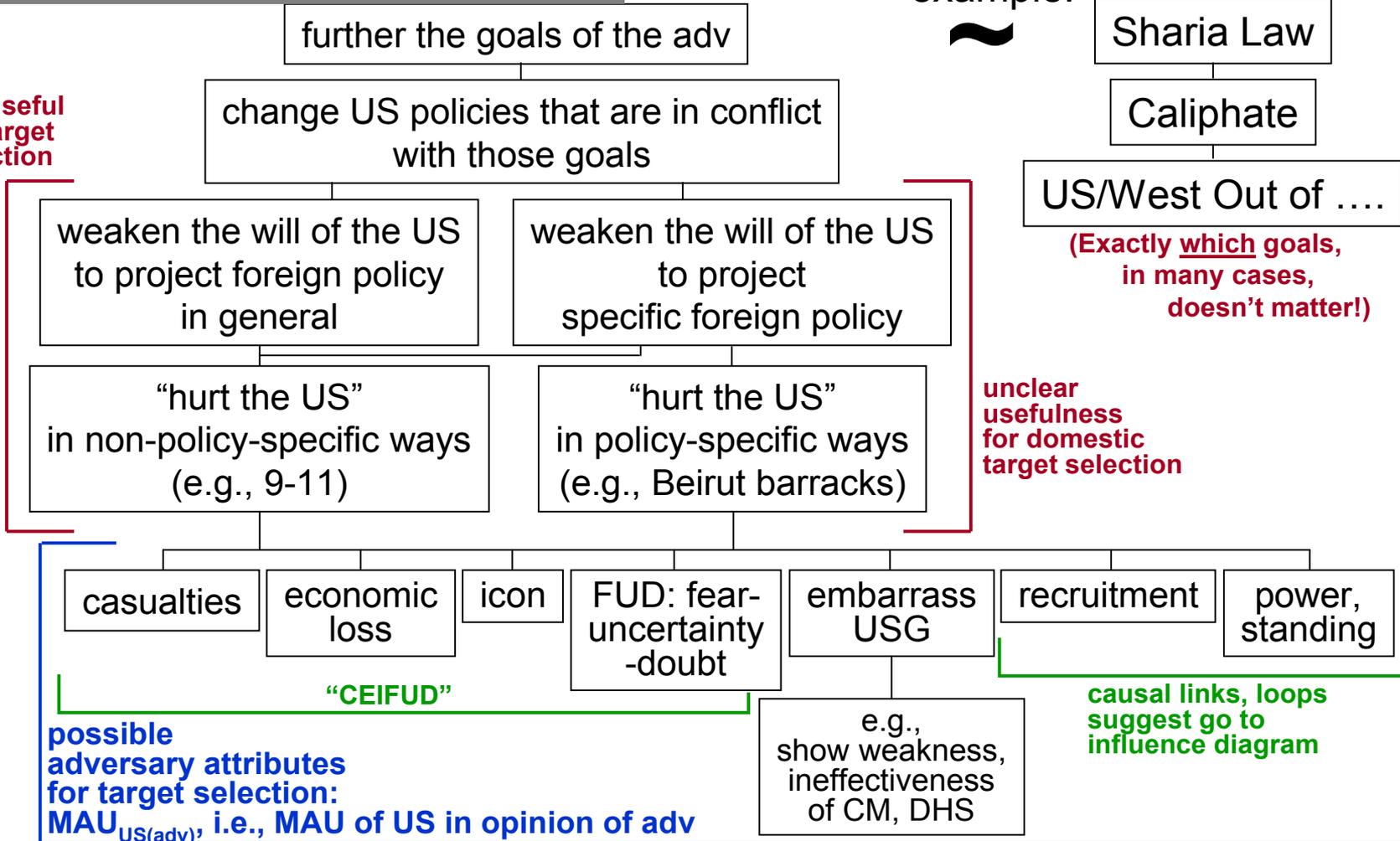
not useful for target selection

example:



(Exactly which goals, in many cases, doesn't matter!)

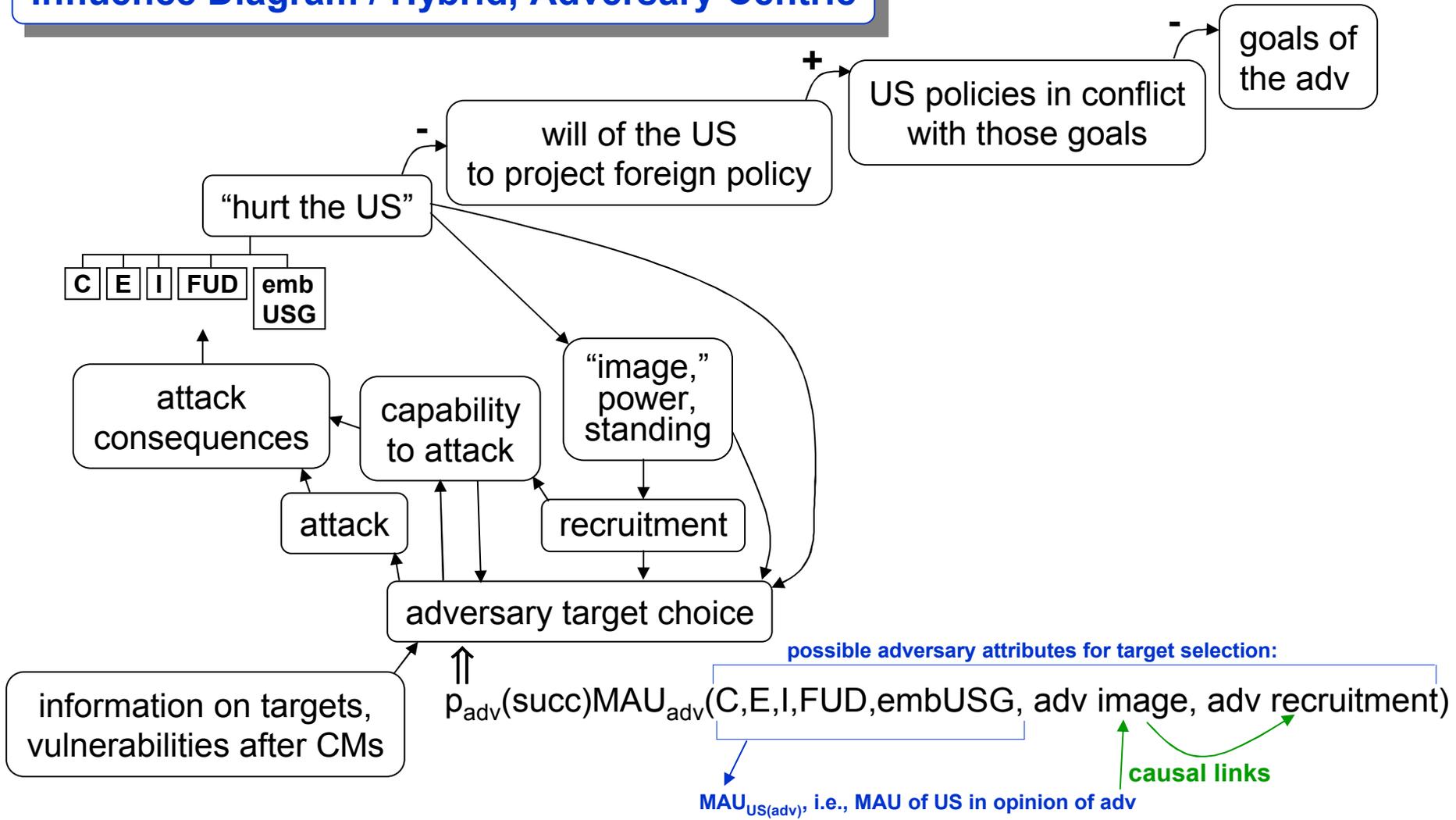
unclear usefulness for domestic target selection



# First Step: Influence Diagrams, Hybrid

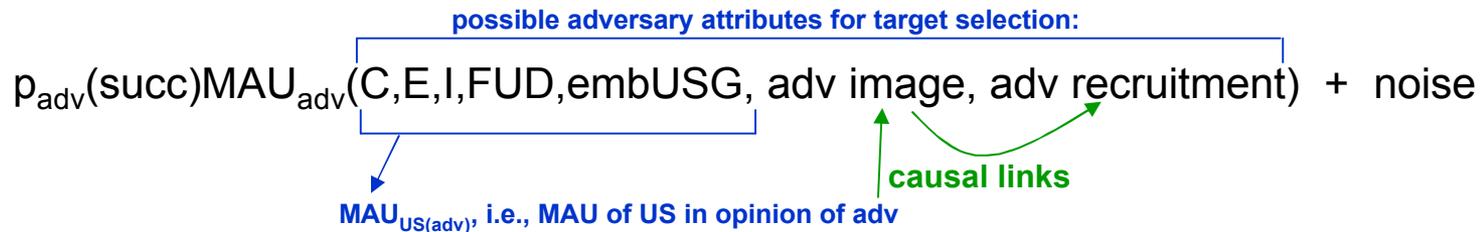


## Influence Diagram / Hybrid, Adversary-Centric

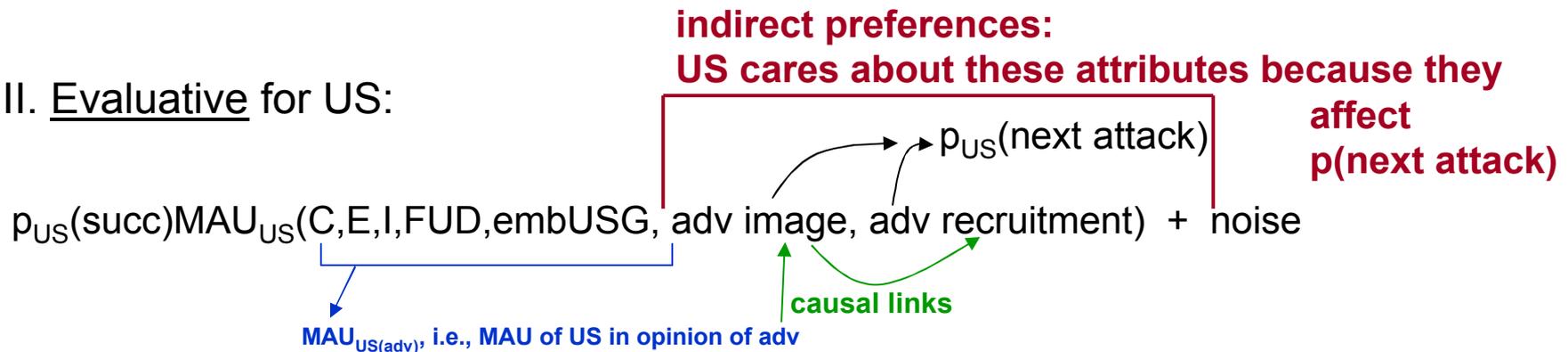


# Causal Links Among Attributes

I. From previous slide: predictive adversary choice model, for  $p_{US}(\text{attack})_s$



II. Evaluative for US:



**Causal links and indirect preferences make elicitation challenging.**

# Seeking an Elegant Rendition of Spectrum of Adversary Groups

---



**What matters to MARS/NEXIIS**

**is adversary groups with distinctly different values/decision behavior.**

**Adversary decision-behavior-distinct “agents,” “groups,”**

**perhaps let’s say 20 different ones,**

**i.e., 20 agents with distinct values/decision behavior,**

**are more stable than**

**actual adversary groups in real world (one estimate: 700+).**

**But then must treat each of those “groups”**

**with attack-generation frequencies**

**reflecting that each one represents a number of actual groups**

# Adversary Values vs Capabilities

Elicitations will find adversary group spectrum to lie somewhere on a range:

**Groups' values/decision behavior is strategically the same, (i.e., we can't tell any differences well enough to elicit them and use them reliably) so groups only strategically vary on capability.**



**Groups' values/decision behavior can be elicited as different between groups, in which case capability differences matter less, though still matter.**

**Note:**  
**Some groups may target capability increases based on their values/goals.**

# What, Information-Wise, Do Adversary Models Do, Actually?

---



- they do not add information
- they organize information into modeling-useful “objects” or agents with behavior patterns
- they help aggregate information, over time, about groups
- they help communicate information

# A Key Challenge: Attack Frequency

---



**If fit attack frequency for each group  
based on a base rate fit to the  
observed frequency of domestic terrorist attacks  
for the last five years,  
that attack frequency will be quite low.**

**But we may have a nonstationarity problem.**

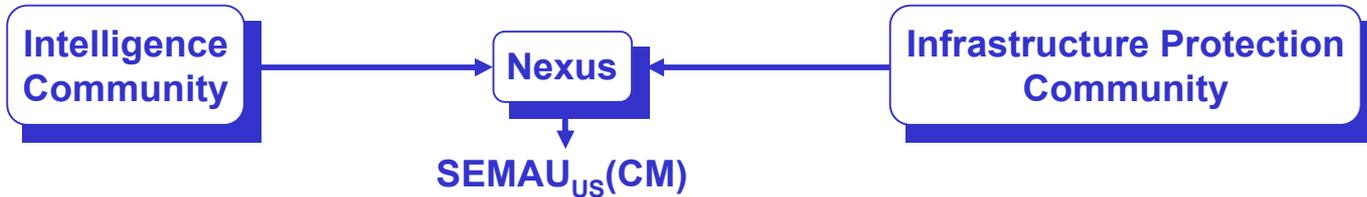
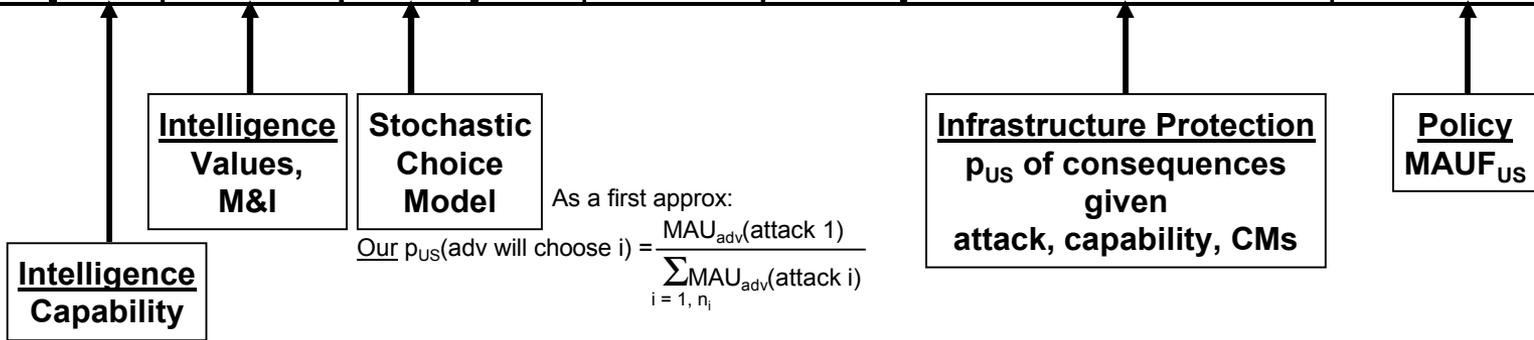
**So how do we set those frequencies?**

# Restructuring MARS into Excel



attack #	Adversary Group 1, MAUF <sup>1</sup> <sub>adv1</sub>			Adversary Group 2, MAUF <sup>1</sup> <sub>adv2</sub>			Attack (target-weapons-tactics)	
	Capability	MAU <sub>adv</sub> (attack i)	p <sub>US</sub> (attack i)	Capability	MAU <sub>adv</sub> (attack i)	p <sub>US</sub> (attack i)	p <sub>US</sub> (consequences   attack, capab'y, CM)	MAU <sub>US</sub> <sup>2</sup> (consequences)
1								
2								
3								
4								
5								
6								
7								
...								
20								

Convolved to frequency distribution over MAU<sub>US</sub>  
then Expectation = SEMAU<sub>US</sub>(CM)



## Two Different Value Models

<sup>1</sup>MAUF<sub>adv</sub> = f(consequence attributes, attack attributes, p<sup>3</sup><sub>adv</sub>(success))

<sup>2</sup>MAUF<sub>US</sub> = f(consequence attributes)

## Two Different Probabilities

<sup>3</sup>p<sub>adv</sub>(success | attack, capability, CM)

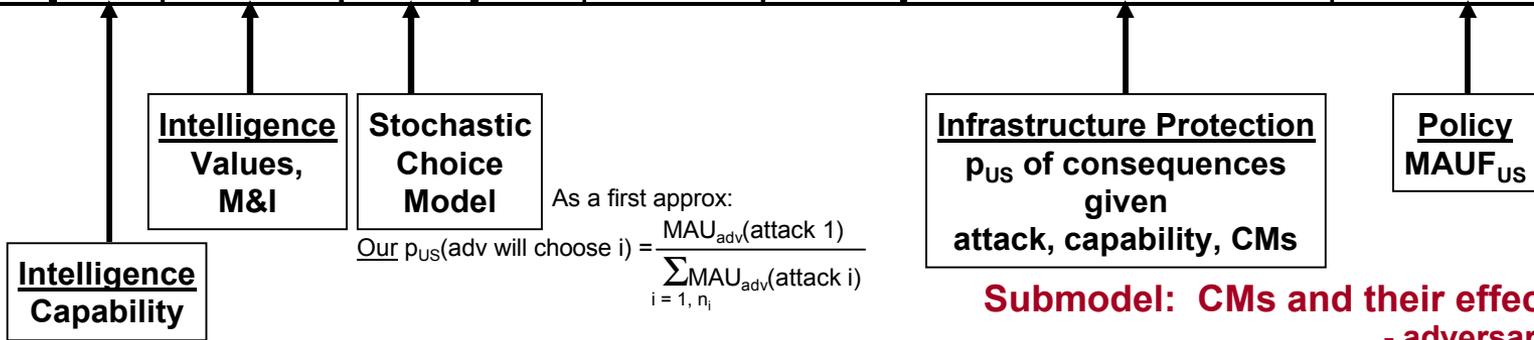
<sup>4</sup>p<sub>US</sub>(conseq's | attack, capability, CM)

# Excel-Wise MARS, detail 1



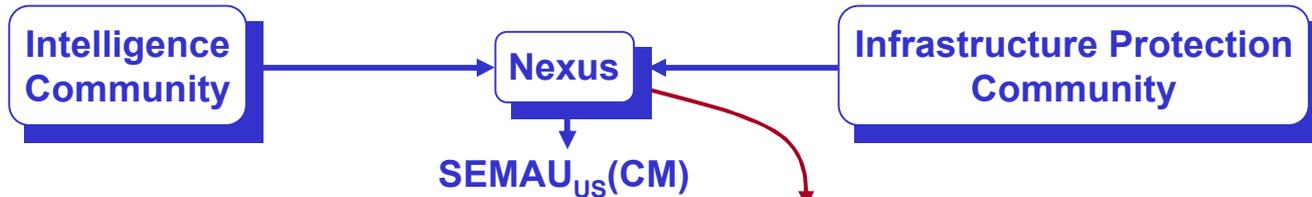
attack #	Adversary Group 1, MAUF <sup>1</sup> <sub>adv1</sub>			Adversary Group 2, MAUF <sup>1</sup> <sub>adv2</sub>			Attack (target-weapons-tactics)	
	Capability	MAU <sub>adv</sub> (attack i)	p <sub>US</sub> (attack i)	Capability	MAU <sub>adv</sub> (attack i)	p <sub>US</sub> (attack i)	p <sub>US</sub> (consequences   attack, capab'y, CM)	MAU <sub>US</sub> <sup>2</sup> (consequences)
1								
2								
3								
4								
5								
6								
7								
...								
20								

Convolved to frequency distribution over MAU<sub>US</sub>  
then Expectation = SEMAU<sub>US</sub>(CM)



## Submodel: CMs and their effectiveness:

- adversary capabilities
- CMs
- vulnerabilities
- targets as consequence generators
- consequences



**Integrative Function: Has become a multi-Lab effort**

# Excel-Wise MARS, detail 2



attack #	Adversary Group 1, MAUF <sup>1</sup> <sub>adv1</sub>			Adversary Group 2, MAUF <sup>1</sup> <sub>adv2</sub>			Attack (target-weapons-tactics)		Pedigree	QM
	Capability	MAU <sub>adv</sub> (attack i)	p <sub>US</sub> (attack i)	Capability	MAU <sub>adv</sub> (attack i)	p <sub>US</sub> (attack i)	p <sub>US</sub> (consequences   attack, capab'y, CM)	MAU <sub>US</sub> (consequences)		
1										
2										
3										
4										
5										
6										
7										
...										
20										

Intelligence Values, M&I

Stochastic Choice Model

Infrastructure Protection  
p<sub>US</sub> of consequences given attack, capability, CMs

Policy  
MAUF<sub>US</sub>

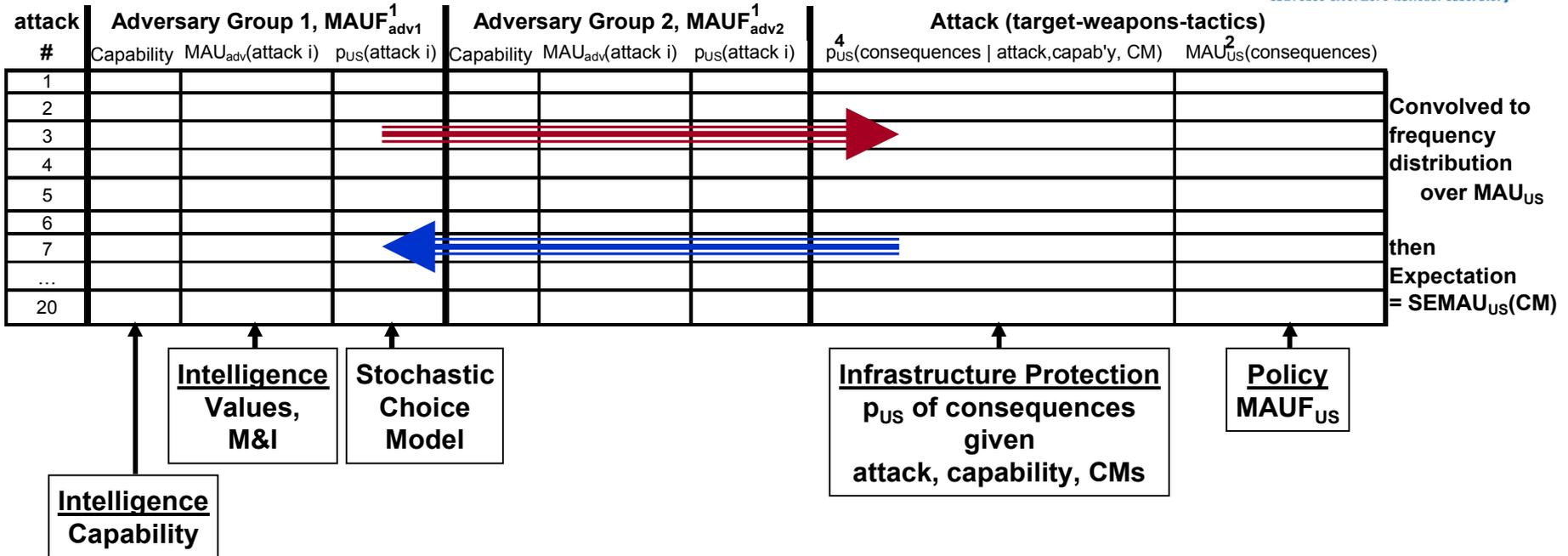
Intelligence Capability

**Integrative Function / Collective Function:**

Spreadsheet = a formally correct way to “dump in” whatever data is available, then seek more:

- enforcing consistency, pedigree, Quality Management
- building up a structured “landscape of risk”
- iterative, accumulation - of - knowledge, as data becomes available:
  - adversary models
  - infrastructure targets, vulnerabilities, p<sub>US</sub>(consequences | attack, capab'y, CM)
- project - management advantages

# Excel-Wise MARS, detail 3

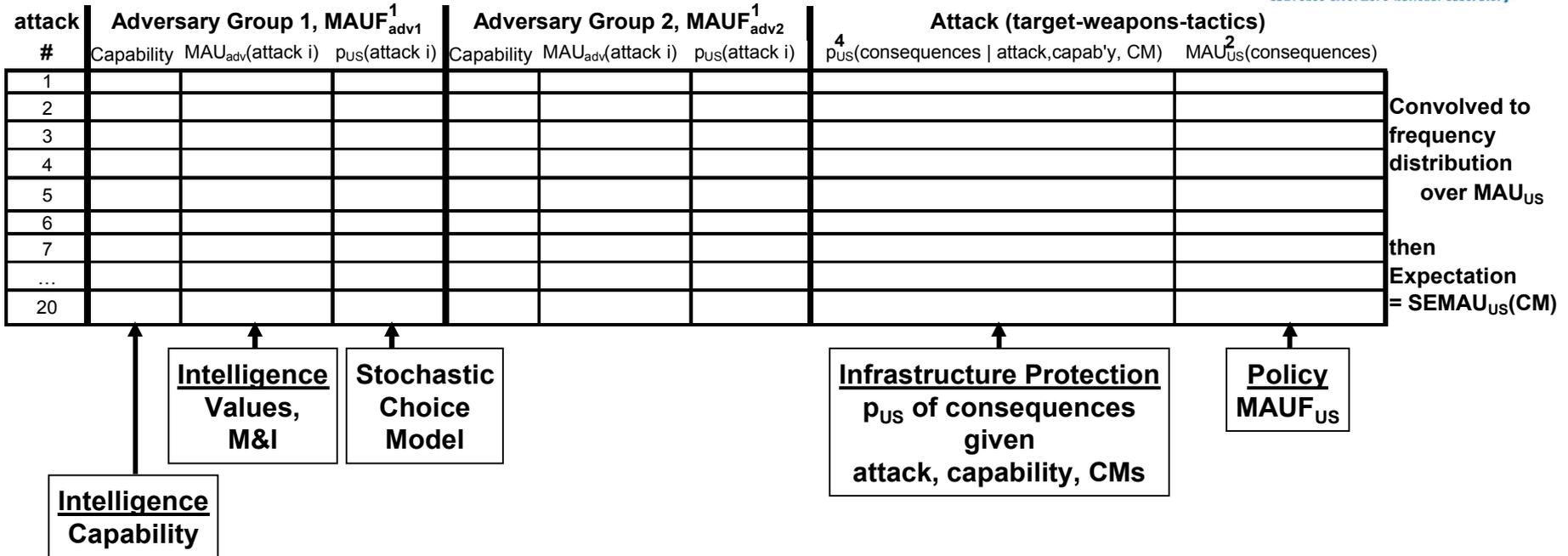


One Form of Integration: Prioritization Goes Both Ways Between IC and IP

**IC => IP: Countermeasure prioritization based on likelihood**

**IC <= IP: Prioritization of groups/attacks based on the harm they could do**

# Excel-Wise MARS, detail 4



**Two Different Value Models**

**Two Different Probabilities**

**Predictive, Evaluative**

<sup>1</sup>MAUF<sub>adv</sub> = f(cons'q attr's, attack attr's, p<sub>adv</sub>(succ))    <sup>3</sup>p<sub>adv</sub>(success | attack, capability, CM)    to predict adv choice

<sup>2</sup>MAUF<sub>US</sub> = f(cons'q attr's)    <sup>4</sup>p<sub>US</sub>(conseq's | attack, capability, CM)    to evaluate for US

**An LLNL Intelligence Working Group “Brain Trust”  
is convening often to work out four sets of issues:**

- availability of data**
- most feasible structuring of adversary decisions, values and uncertainties**
- most feasible structuring of adversary choice models**
- feasibility of elicitation tools to elicit:**
  - subjective probabilities**
  - adversary values, value tradeoffs**

**A joint-work contract is being developed with John Hiles,  
key developer of Agent-Based Modeling,  
currently a professor at the Naval Postgraduate School, Monterey.**

# Strengths

---



- **Decision analysis expertise, specifically with dual decision tree background**
- **Decision analysis expertise in elicitation of decision models, subjective probabilities**
- **That expertise and intelligence community expertise “under one roof” at LLNL**
- **Access to Capitol Area intelligence Community**
- **Access to, ongoing relationship with, John Hiles**

# And an Ending Quote

---



**"These complexities do not relieve humans from the responsibility for making decisions... aimed at navigating their organizations successfully through campaigns.... Minds must be prepared beforehand... this preparation must be predicated on the internalization of 'valid' knowledge about the conflict environment."**

**Robert C. Rubel, Naval War College Review, Spring 2006, vol. 59, no. 2**

# Appendix: Slides for Working With Intelligence / M&I Working Group

---



**Adversary Decisions:**

- What decisions? (within each group)
- Among what options?
- What can we know about them?

**Adversary Values:**

- What motivation/intent factors?
- What objectives hierarchies?
- What attributes?
- What can we know about them?

**Uncertainties in Adversaries':**

- goals, values
- capabilities
- information
- choice behavior

(how list alternatives,  
then how choose)

# **We Can't Avoid Modeling Adversary Decision Behavior**

---



**So Key Questions:**

**What decisions does the adversary make?**

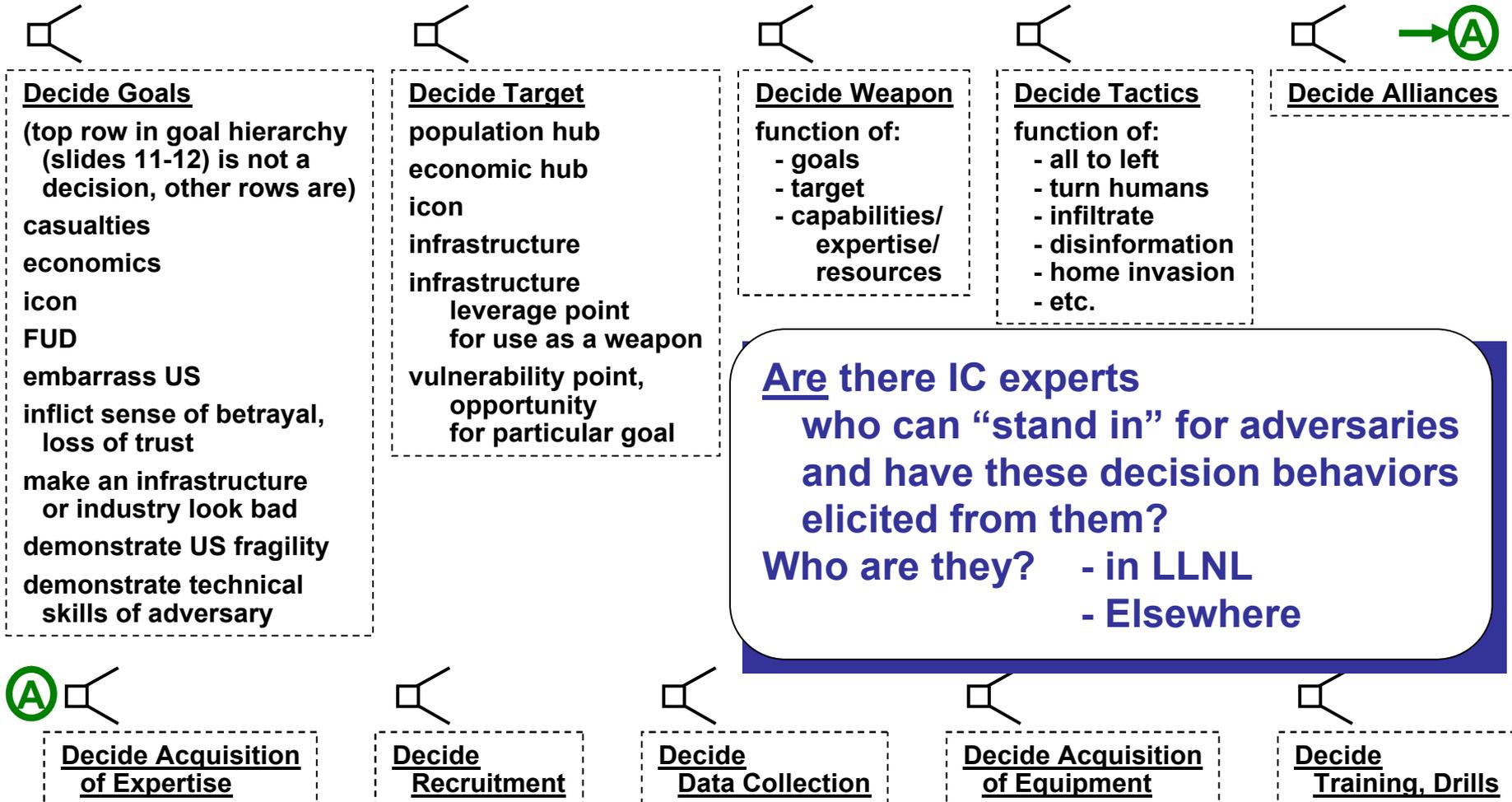
**Does one adversary (group) choose among scenarios?**

**On what attributes does he make those decisions?**

**What are the key uncertainties to capture?**

# What Decisions Does the Adversary Make?

## Highly Speculative Adversary Decision Sequence



# If the Adversary Chooses Among Scenarios: What Do Those Scenarios Look Like? HSC 15

---



- 1 Nuclear Detonation – 10-Kiloton Improvised Nuclear Device
- 2 Biological Attack – Aerosol Anthrax
- 3 Biological Disease Outbreak – Pandemic Influenza
- 4 Biological Attack – Plague
- 5 Chemical Attack – Blister Agent
- 6 Chemical Attack – Toxic Industrial Chemicals
- 7 Chemical Attack – Nerve Agent
- 8 Chemical Attack – Chlorine Tank Explosion
- 9 Natural Disaster – Major Earthquake
- 10 Natural Disaster – Major Hurricane
- 11 Radiological Attack – Radiological Dispersal Devices
- 12 Explosives Attack – Bombing Using IED
- 13 Biological Attack – Food Contamination
- 14 Biological Attack – Foreign Animal Disease (Foot & Mouth)
- 15 Cyber Attack

# If the Adversary Chooses Among Scenarios: What Do Those Scenarios Look Like? Other 44

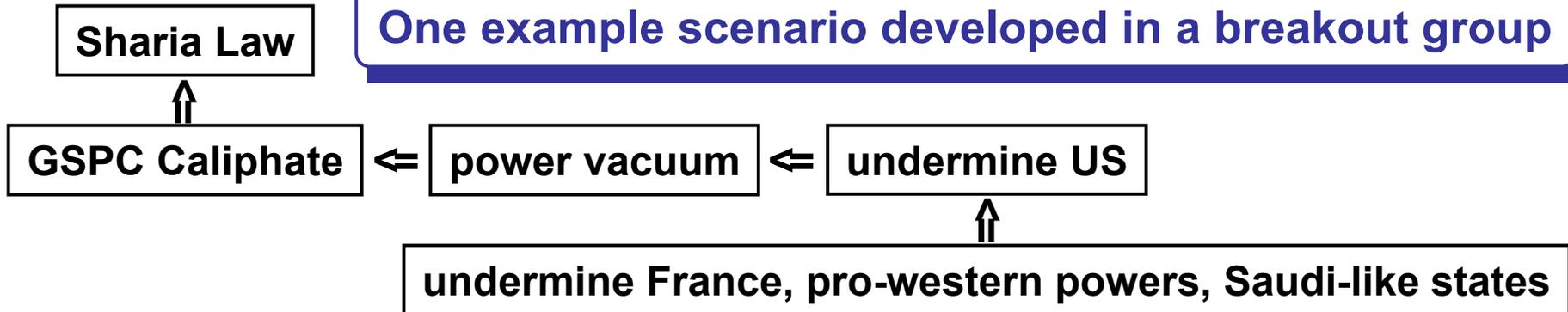


INSIDER:	Support staff (janitor, landscaper, etc) Security staff Technical or Administrative staff Executive staff	CYBER:	Infiltration of a network from outside Exfiltration of stored data Corruption of stored data Rendering stored data inaccessible Interception of data flows/communications Interruption of data flows/communications Redirection of data flows/communications Malicious (untrusted) software agents Compromised trusted software applications Local disruption of services Widespread disruption of services Compromised hardware components Compromised (hijacked) machines Networks of compromised machines
BIO:	Smallpox (contagious) Anthrax (not contagious) Foot & mouth (livestock) Pathogen in food Soybean rust (crop) Novel emerging pathogens (e.g., engineered organisms)	PHYS ASS'LT:	Small team with weapons (less than 10 people) Large team with weapons (10 or more people) Vehicle
CHEM:	Toxic Industrial Chemical (external wide area) Chemical Warfare Agent (internal to facility) Toxin in water system	EMERGING:	EMP, high-power microwave, directed energy devices
RAD/NUKE:	Source release or placement Radioactive Dispersal Device (explosive dispersal) Improvised Nuclear Device Nuclear weapon	NATURAL DISASTERS	Major storm (hurricane, set of tornados, snow/ice storm) Major earthquake
EXPLOSIVES:	Small clandestine charges Bomb on person Bomb in vehicle Projectile with charge (RPG, mortar, small rocket, MANPAD) Incendiary devices	+ OTHER EMERGENCIES:	Major wildfire Major accident (power plant, chemical plant, etc)

# Motivation & Intent Structure From CIT Monterey Workshop



One example scenario developed in a breakout group



and so how do that:

- FUD (bombs in shopping malls, MANPADs) 2, 6
  - “Crusade:” foment Christian/Moslem conflict 3, 5
  - Undermine US alliances 4, 6
  - Economic hits (price, scarcity) 1, 6
1. 3 NG pipelines from Canada
  2. bombs in many shopping malls, with webcams, spread all over US
  3. sustained attack on mosques in US
  4. UN attack (Lehay will do a note)
  5. sustained Europe attacks alternating churches and mosques
  6. sustained MANPADs on US planes in and out of Paris
  7. Info campaign: take credit for 1, 6; deception 2,3,5; blame Christian Fund’sts 4.

# Adversary Value Attributes



## Consequence Attributes

- fatalities, injuries
- economic loss
- icons
- general FUD
- get US/West out of ...
- sense of betrayal, loss of trust
- FUD due to infra as weapon
- embarrass “hi-tech” society, that “hi-tech” used against it
- Demo fragility of US society
- Make an infra look bad
- Demo tech skills of the adversary

## Attack Attributes

- violent/not
- covert/overt
- suicide/not
- attribution direct-clear/not
- turn humans
- sleepers
- any of 10 ways to use infra as a weapon

### Which of these are “capturable:”

- have some idea that adversaries value them.
- have some information such that a person/panel (IC experts) can “stand in” for an adversary and have values elicited.

**Green = attribute sets/values found in brainstorming workshop**

# And Finally: Uncertainties



## Sequence of uncertainties

standing between us and predicting adversary choice:

Our uncertainties in: - adversary values, goals

- adversary capabilities

- adversary information

- adversary choice behavior

(how assembles list of alternatives,  
how then chooses among them)

## Intrinsic noise:

Adversary is probably inherently not a fully consistent  
subjective expected multiattribute utility maximizer.

## Deliberate noise:

Adversary could transmit disinformation re intent, etc.

From whom can I “capture” these:

- have some information such that a person/panel (IC experts)  
can have subjective probabilities elicited.