Risk-informed Decision Making for Homeland Security

June 28, 2006

Dr. John Cummings
Senior Manager
Advanced Concepts Group (ACG)

What kind of "problem" is Homeland Security anyway?

Political Posturing Should Not Trump Real National Security Issues

War on Terrorism: Security costs weigh heavily at local level

"Homeland Security" Threatens Constitution

Problems Plague 'No-Fly' List, TSA Considers Changes

Exposed by Katrina, FEMA's flaws were years in making

Port Problems Said To Dwarf New Fears

GAO cites lingering problems with student visa system

Border Security: Different Names, Same Problems

The Bird Flu Game: Who's on First?

Mass Transit: Challenges in Securing Transit Systems

Easy Targets: infrastructure

Electricity Grids Left Wide Open to Hackers

ACG Advanced Concepts Group

Sandia National Laboratories

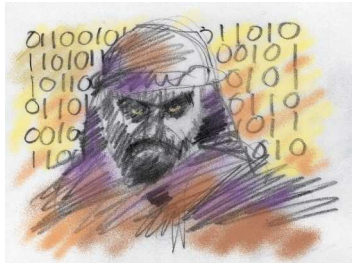# What is a "wicked" problem? (Not tame)

- Every one is essentially unique.

- No definitive formulation – no "point" solution.

- No exhaustively describable set of potential solutions.

- No immediate and no ultimate test of a solution.

- Every one is a symptom of another problem.

- Development of a "solution" itself changes the conditions of the problem

The term "wicked problems" characterizes the types of problems that we often must work on: highly complex, highly dynamic, and involving not only technology but political, social, and economic considerations. The opposite of "wicked" is "tame" (not "easy").

Rittel and Weber, 1973

Advanced Concepts Group approach to "wicked" problems

- *Formulate the mess:* understand the context and essence.

- Derive *system solutions* within the economic, social, and political constraints.

- Identify needed *advances in science and technology*.

- Catalyze solutions by focusing on *goals*

What are the concerns?

When will the attack occur?

What should be protected and how?

What is the method of attack?

What is the target?

What is needed to respond and recover?

Who is planning the attack and why?

WHO WILL CARRY OUT THE ATTACK?

What is the wicked problem?

We must help the nation understand the risks from terrorism, develop actionable intelligence about the threats, make true risk-based investment decisions, and dynamically manage those risks.

There is a clear need for tools and environments for analysis and decision making in high-consequence situations.

What are some of the elements of the "solution"?
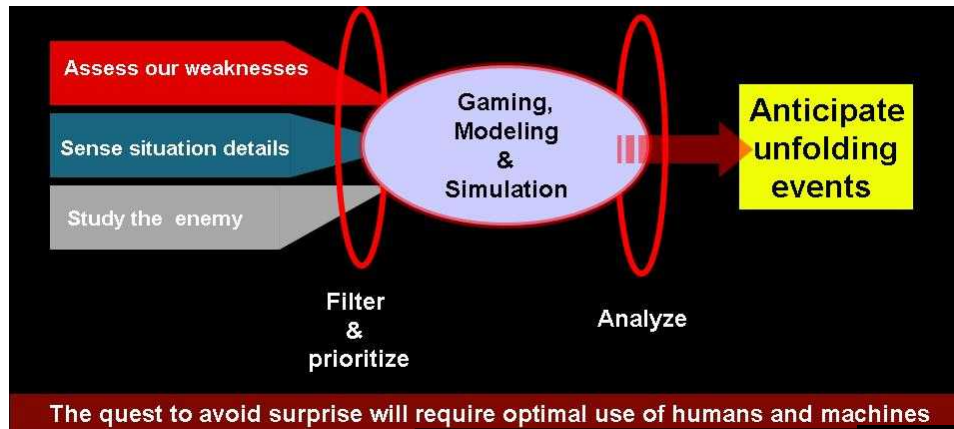
Full context understanding of the problems:

– **Facts and science-based understanding**

– **Threats, vulnerabilities, and consequences**

– **Scientific risk-assessment & management**

– **Uncertainties**

– **Effective understanding of the social and political systems**

Real decision / action support:

– **Capability to prioritize**

– **Methodologies for rolling out decisions that manage the "wickedness" of the problem**

– **The ability to make decisions be understood, accepted, acted upon, …**
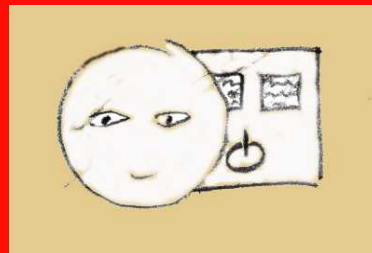
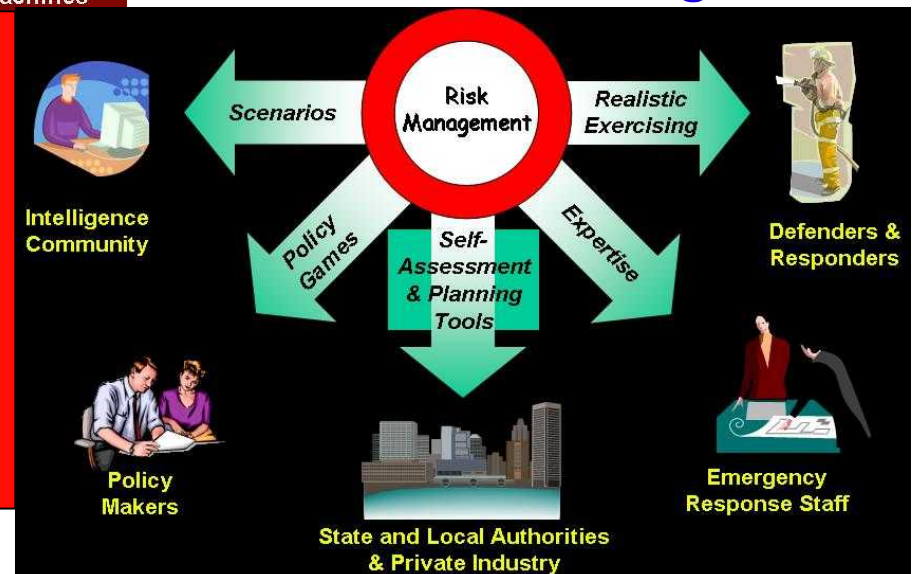# What are some specific approaches for the "solution"?

Analyze Threats

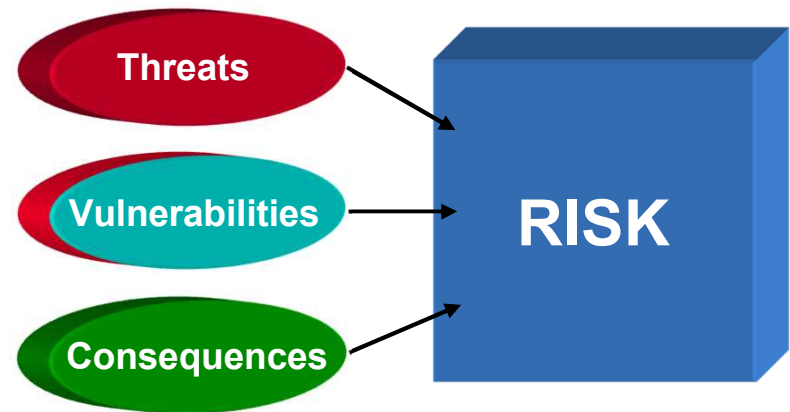**Assess & Manage Risks**

Enhance Decision Making

We need a systems approach that leverages the strengths of both people and machines in tight collaboration
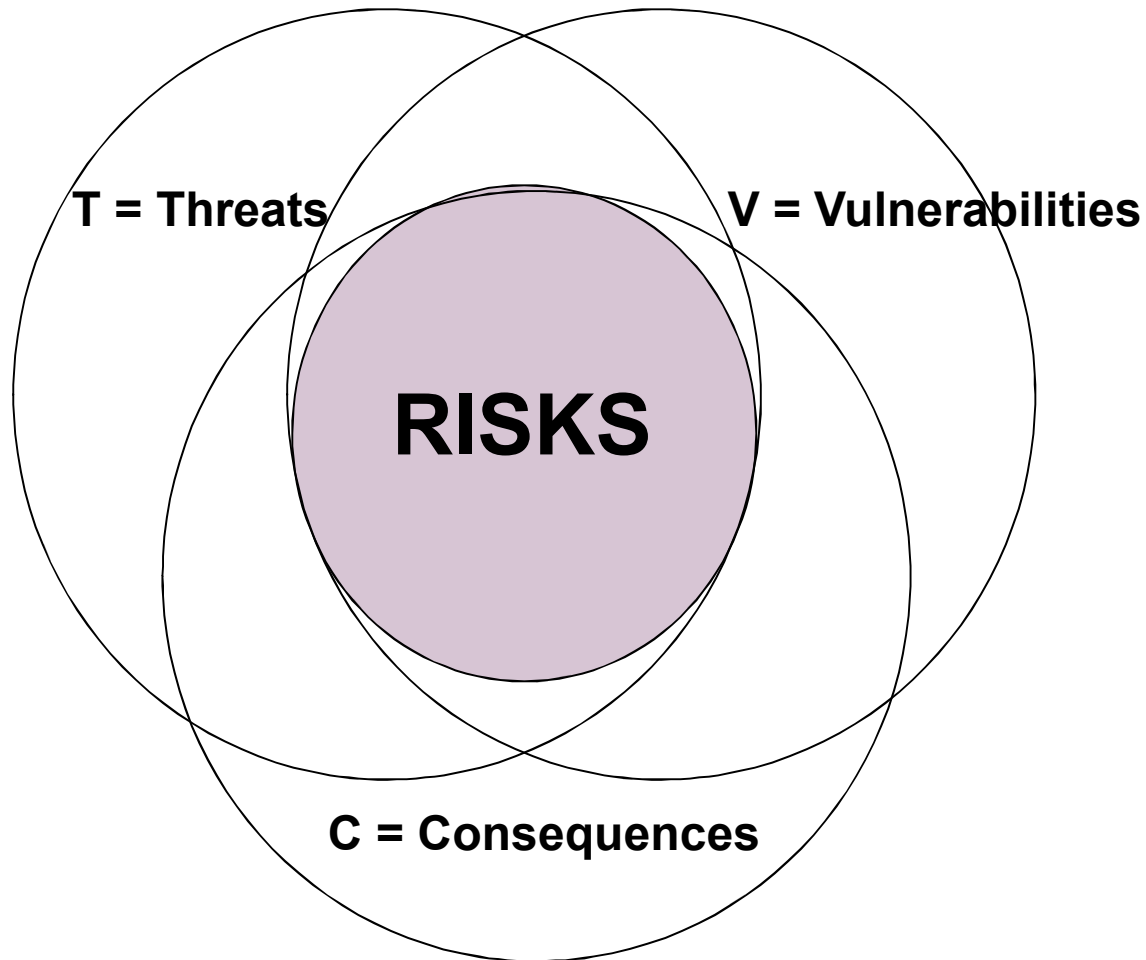
Appropriate Methods for Analyzing Risk are Goal and Problem Dependent

- **Goal**
  - **Prioritization**
  - **Assessment**
  - **Management**

- **Problem Characteristics**
  - **Size**
  - **Heterogeneity**
  - **Availability and Quality of Data**
  - **Nature and Level of Uncertainty**
  - **Threat source**
    - **Nature**
    - **Adversary**

Risk = T × V × C

T = Threats

V = Vulnerabilities

RISKS

C = Consequences

Risk-Informed Decision Making

Deliberation (environment): qualitative factors and processes
- politics
- ethical
- legal
- social

Threats
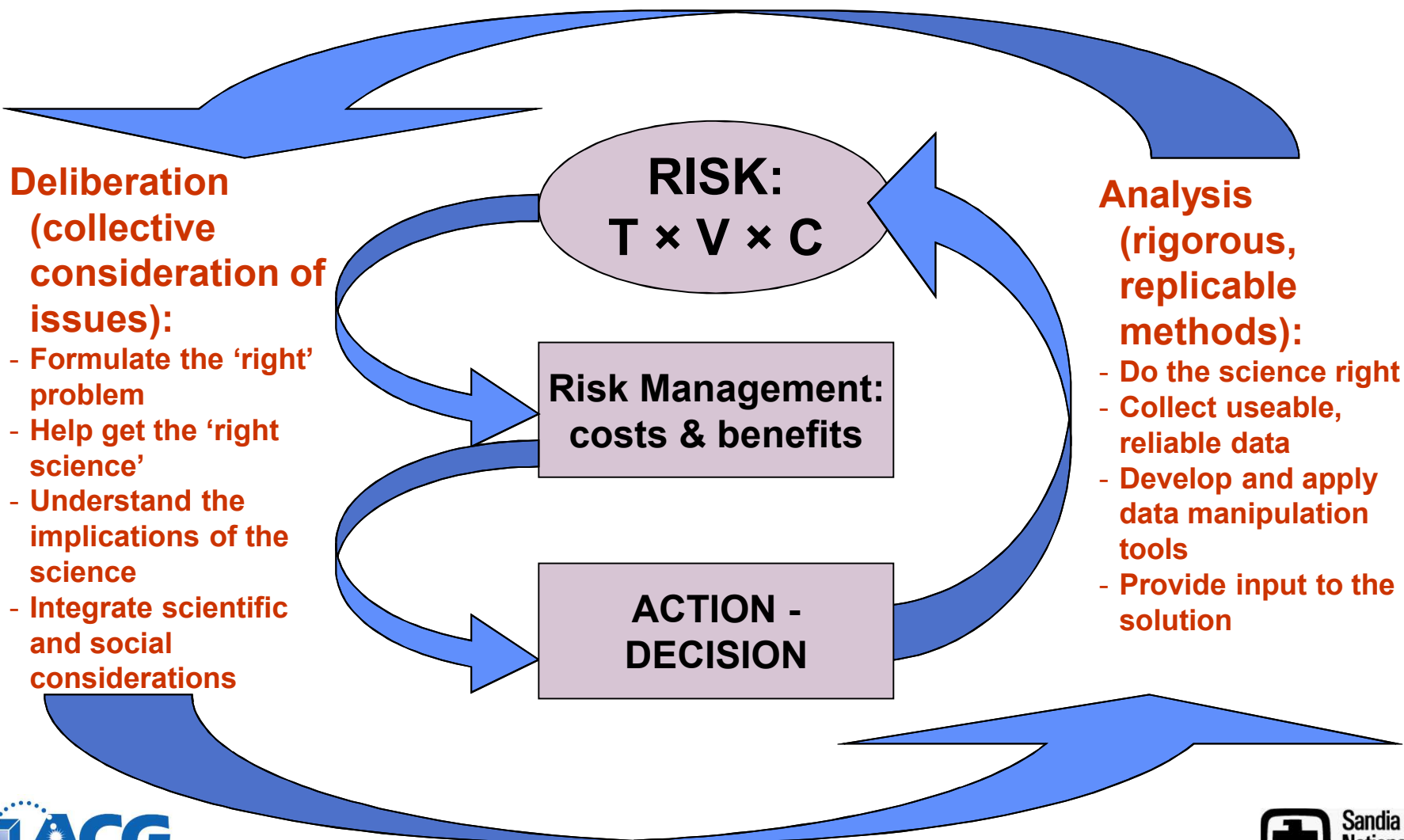
Vulnerabilities

RISKS

Consequences

Risk Management: costs & benefits ACTION - DECISION

Analysis (tools): quantitative factors and processes
- facts
- statistics
- calculations
- simulations

ACG Advanced Concepts Group

Sandia National Laboratories

Risk-Informed Decision Making

Deliberation (collective consideration of issues):
- Formulate the 'right' problem
- Help get the 'right science'
- Understand the implications of the science
- Integrate scientific and social considerations

RISK: T × V × C

Risk Management: costs & benefits

ACTION - DECISION

Analysis (rigorous, replicable methods):
- Do the science right
- Collect useable, reliable data
- Develop and apply data manipulation tools
- Provide input to the solution

Implications

- **This formulation means that one cannot arrive at a definition of threat, vulnerability, OR consequence without both analysis and deliberation**

- **This has huge organizational implications**

- **The seam between analysis and deliberation is currently very rocky**

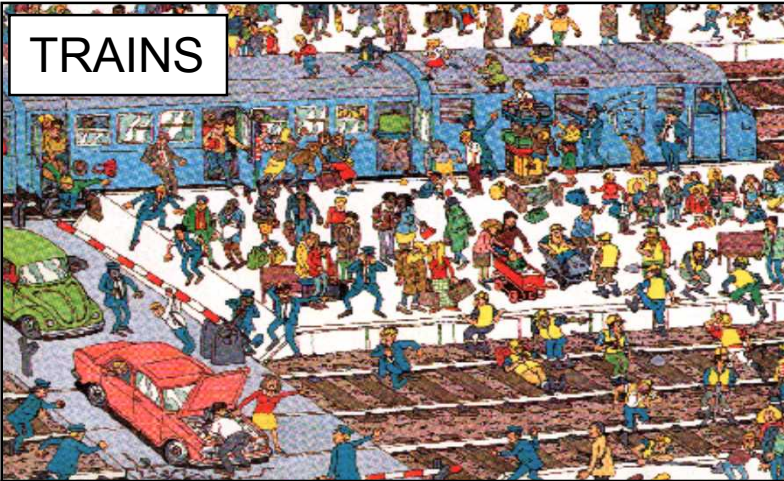- **There may be opportunities for technology to leverage the deliberative portion**
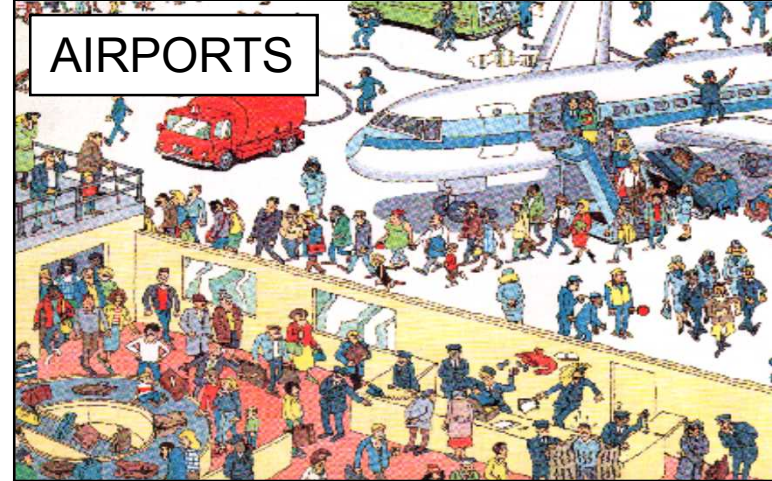
Threat Perspective

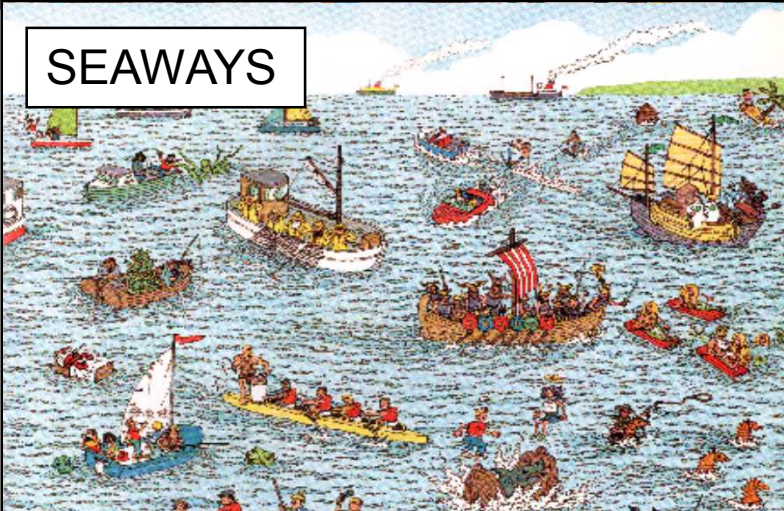# The Problem Of Finding Terrorists Is Akin To Finding Waldo In A World Of Everyday Activity

TRAINS

AIRPORTS

SEAWAYS

PUBLIC PLACES

Sparse real data among much noise

We Make Risk-Based Assessments and Decisions Every Day, Using Existing Capabilities

- …based primarily on available knowledge/judgment.
- The threat, vulnerability and consequence risk elements are not fully integrated.
- Formal risk models exist that can be applied <u>today</u> to integrate all risk elements.
- Computer-based analysis tools need to play a larger role.
- We can benefit from early application of such models.

> **What's the threat level? How should we respond?**
>
> ## Is the Risk Acceptable?
>
> **What's the target? What R&D investments?**

Humans Make Risk Acceptance Decisions Based on Available Information

Applying Risk Equation To Parse/Quantify The Terrorist Threat Results In Identified Actionable Risk Factors

Risk = Probability of attack x Consequence

Risk = function (Threat, Vulnerability, Consequence)

Target

Risk = fn [(Source, Who, Motivation/Intent, Capability, Imminence), (Hardness), (damage)]

target

Risk = fn **[(**Credibility, Person/Group ID, (doctrine, actions/tactics, location, target), weapon, urgency**), (**security/response**), (**overall impact**)]**

An integrated risk assessment is <u>much</u> greater than the sum of the pieces.

Terrorist Threat Attack Risk Equation, Including Risk Factor Scoring Scheme

Total Risk (R) = R_{SC} x R_{IG} x R_D x R_{AT} x R_L x R_T x R_W x R_U x R_{TSR} x R_C

Where:

Risk from Source Credibility (R_{SC})

Risk from Individual or Group (R_{IG})

Risk from Doctrine (R_D)

Risk from observed Actions/Tactics (R_{AT})

Risk from Location (R_L)

Risk from Target (R_T)

Risk from Weapon (R_W)

Risk from assessed Urgency (R_U)

Risk from possible Target/Security Response (R_{TSR})

Risk from Consequence of a successful attack (R_C)

Scoring Scheme	
Score	Threat level
10	Likely a serious threat
1	Moderate threat or neutral
.1	Likely not a threat
0	False positive—NOT a threat

Each Risk Factor Is Evaluated and Scored Using a Separate Lexicon; The Absence of Information Results in a Neutral Score… NOT 0 risk!

ACG Advanced Concepts Group

Sandia National Laboratories

Vulnerability Perspective

Engineered Security: Risk Equation

- Process for risk and resource management using a suite of tools and information

- Based on the risk equation:

Probability of Attack

Probability of Adversary Success

Consequences

System Risk

$$R = P_A * [1 - P_E] * C$$

$$P_I \qquad P_N$$
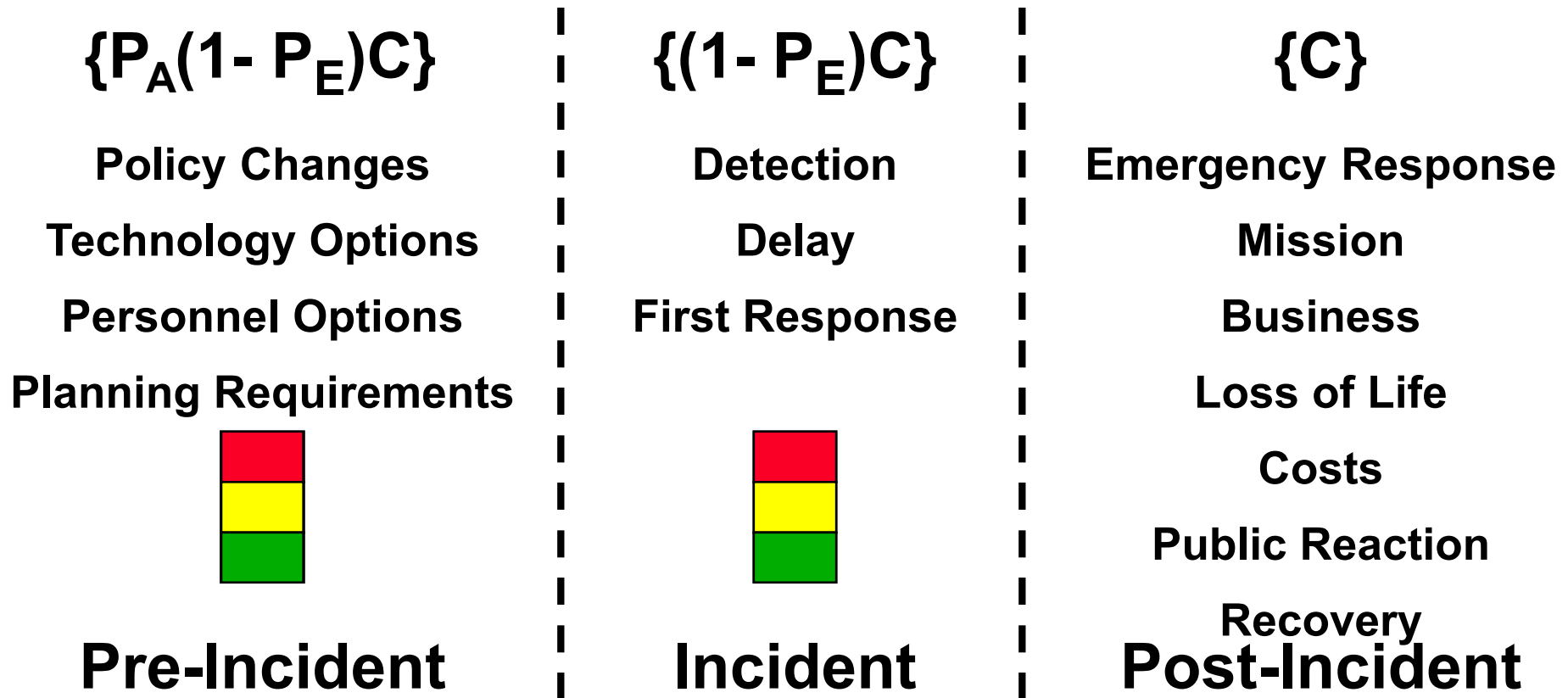
Probability of Interruption   *Probability of Neutralization*

- Integrates many components into a single, consistent, approach for determining risk and making decisions

Risk Management Process

$$Risk = P_A * [1 - P_E] * C$$
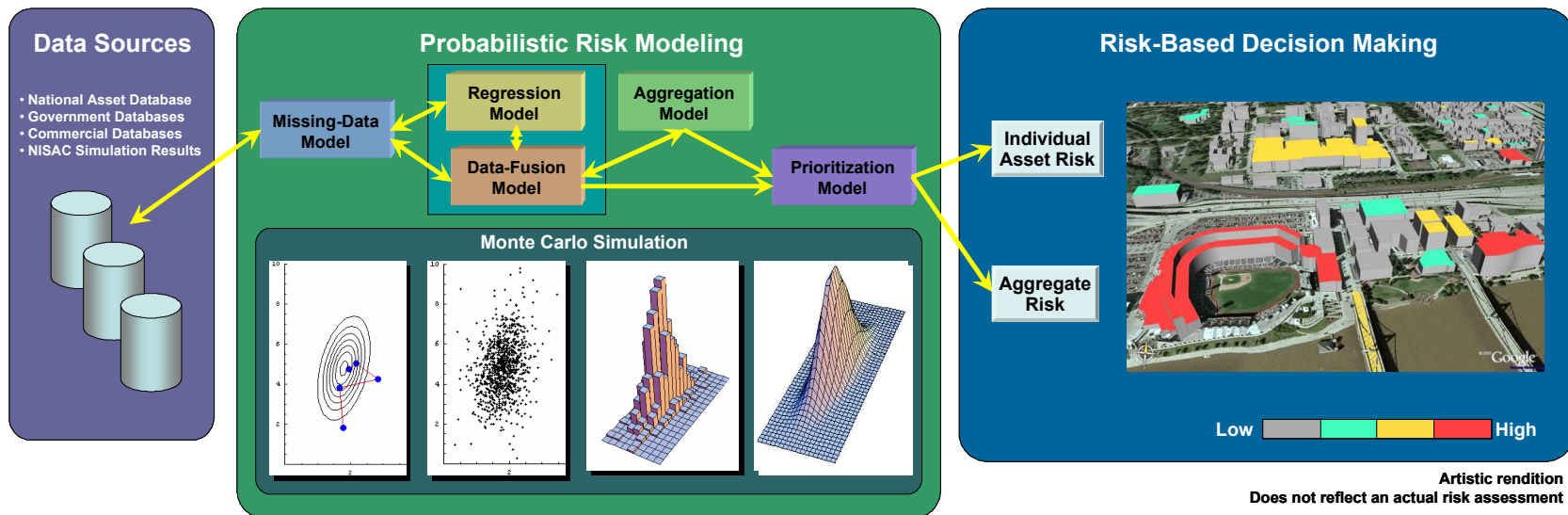
Characterize Assets — Context

Determine Consequences C — Prioritized Targets

Define Threats P_A — Protection Goals

Define Safeguards P_E — Protection System

Analyze System R — RISKS

Change (×6)

Risks Acceptable? — Y → End Until Change

N

CHECK YOUR ASSUMPTIONS

RAM Timeline Factors

$\{P_A(1- P_E)C\}$	$\{(1- P_E)C\}$	$\{C\}$
Policy Changes	Detection	Emergency Response
Technology Options	Delay	Mission
Personnel Options	First Response	Business
Planning Requirements		Loss of Life
		Costs
		Public Reaction
		Recovery
Pre-Incident	**Incident**	**Post-Incident**

Return to Pre-Incident Based on C
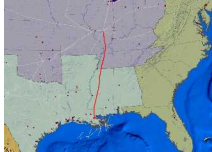
Consequence Perspective

Methodology for Asset Prioritization

$$R = \sum_T P(T) \times P(V|T) \times \int_C P(C|T,V)U(C)$$

What are the consequences of infrastructure disruptions in the Gulf Coast region?

Crude Oil Pipeline Disruptions

- *Fuel Price Increases (vary by region)*
- *Refinery Crude Oil Shortages (vary by region)*
  - ▶ *Increased Imports*

- *Depletion of Fuel Stores (limited to 3 regions)*
- *Fuel Price increases in all regions*
  - ▶ *more than doubles in 1 region*

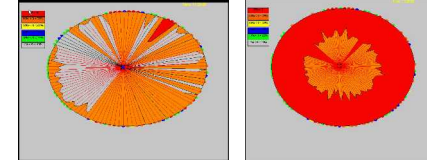## Refined Product Pipeline Disruption

- *Depletion of Fuel Stores (limited to 2 regions)*
- *Retail Fuel Shortage in 1 region*
- *Prices double in 2 regions*
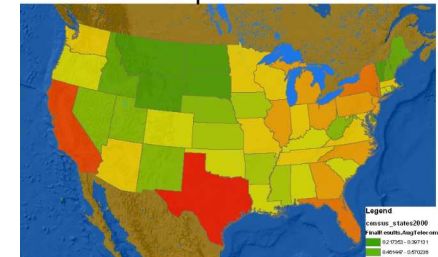- *Prices increase in all regions*

Regional Power Outage

- *Short-term disruptions in multiple infrastructures within the outage area:*
  - ▶ *Water Supply*
  - ▶ *Refining*
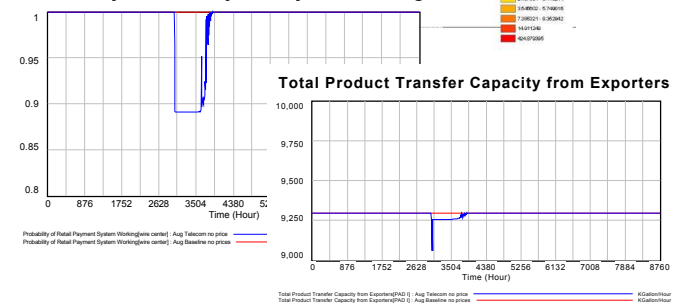 - ▶ *Banking*
- *National Economic Impacts*

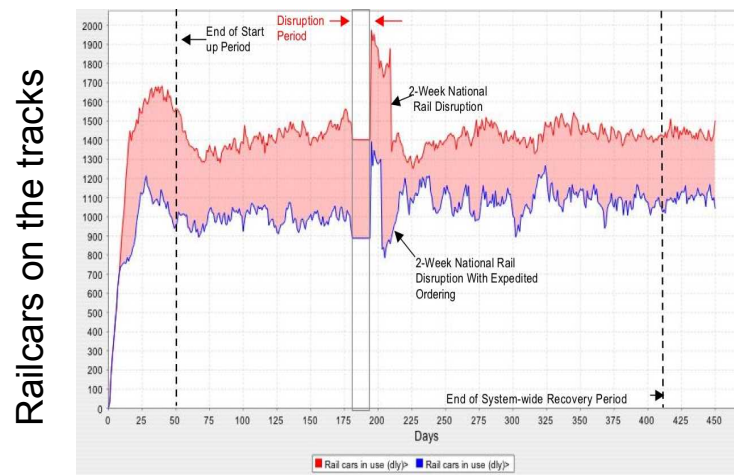## Telecommunication Assets Disruption

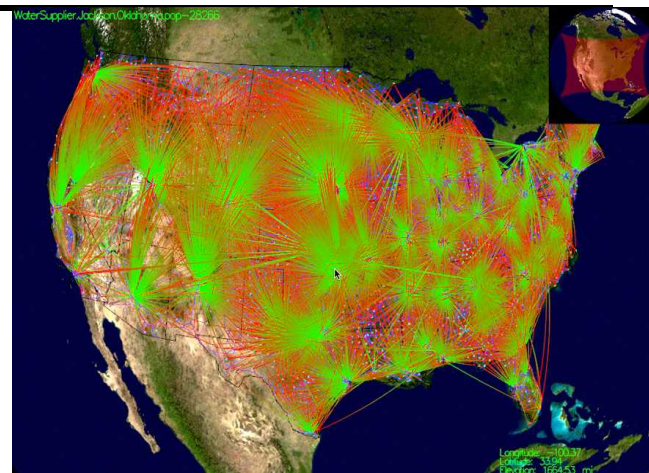Economic Impacts Distribution

Probability of Retail Payment System Working

Total Product Transfer Capacity from Exporters

Regional Analysis performed using
Petroleum System Model,
N-SMART, Port Simulators,
CIP/DSS National Interdependency Model
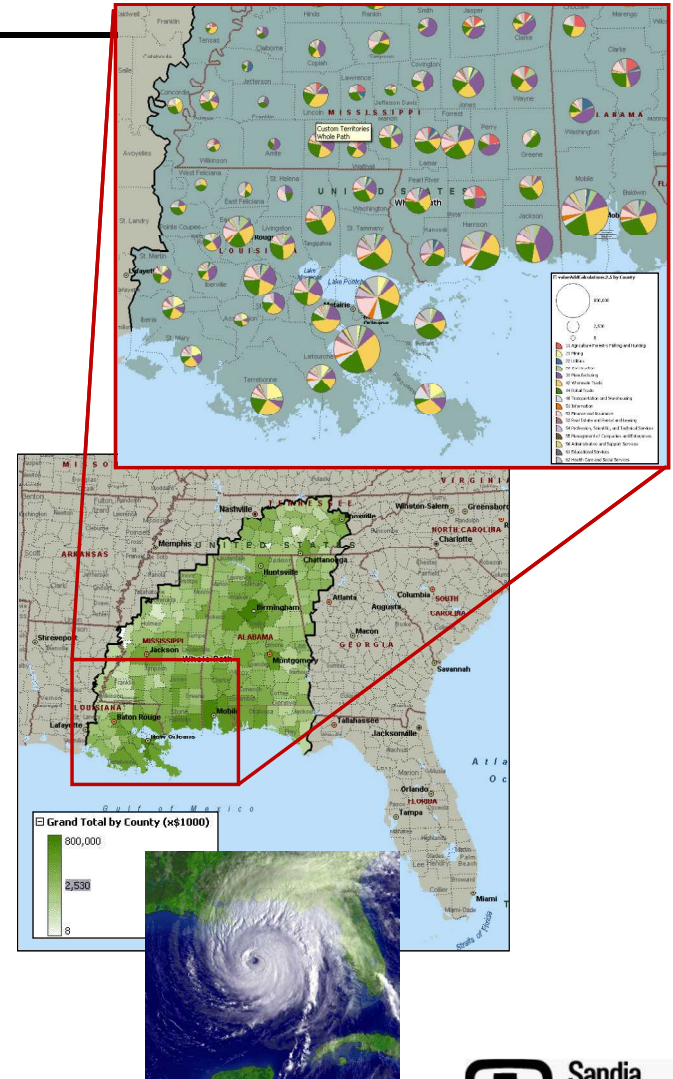
Hazardous Shipments Policy Analyses

- **Consider a policy to alter chlorine shipments**

- **Intra-and inter-firm economic impacts to 3,300 chlorine-related firms were simulated.**

- **Disruption impacts and consequence mitigation options were evaluated for effects on:**

  - **inorganic chemical, PVC, pulp and paper, and organic chemical firms production and revenue**

  - **water systems chlorine supplies**

  - **public health**

  - **national economy (GDP)**

Days

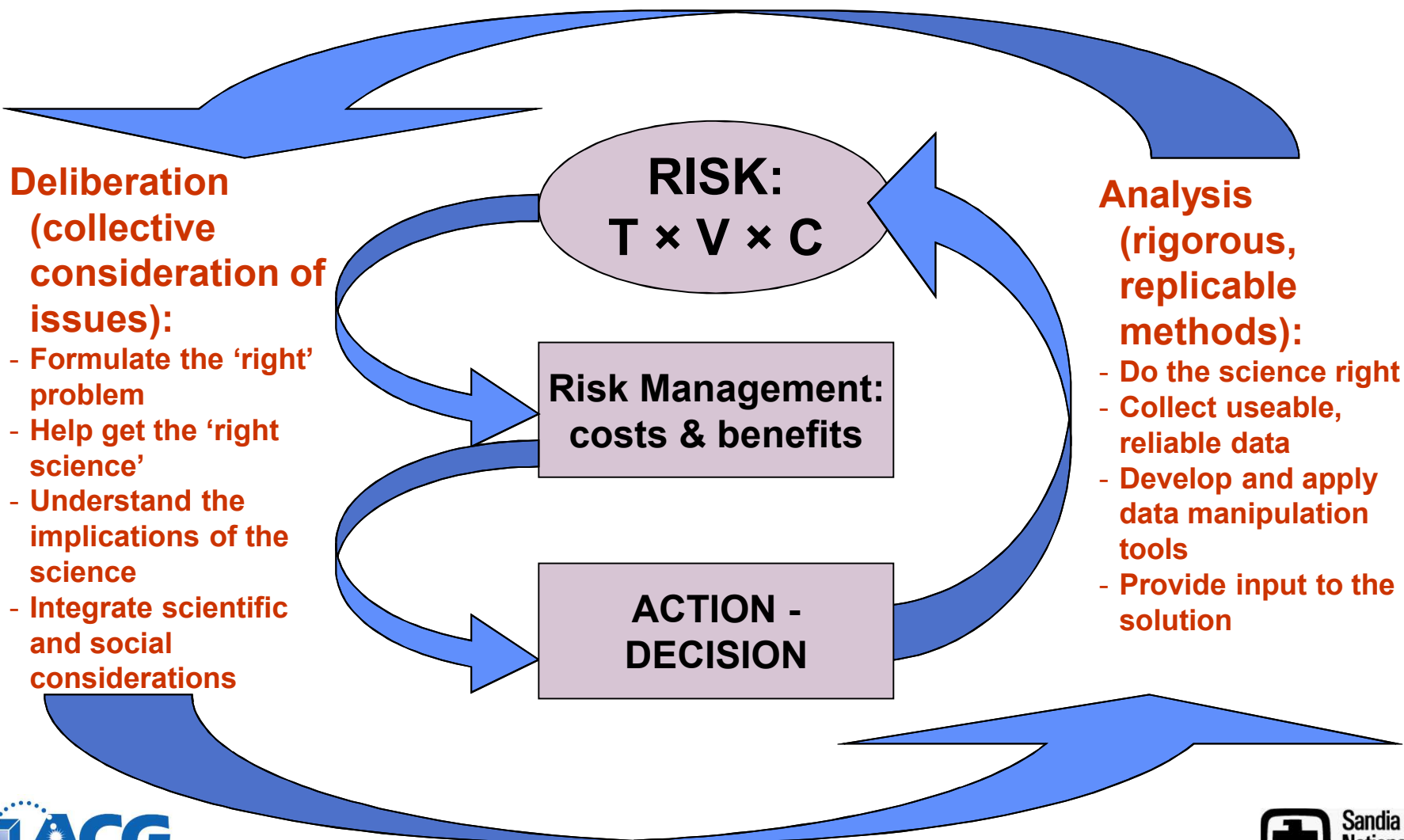# What do we need to know
when a hurricane is coming?

- **Damage areas, severity, duration, restoration maps**
- **Projected economic damage**
  - **Sectors, dollars**
  - **Direct, indirect, insured, uninsured**
  - **Economic restoration costs**
- **Affected population**
- **Affected critical infrastructures**

MANAGING RISK

Risk-Informed Decision Making

Deliberation (collective consideration of issues):
- Formulate the 'right' problem
- Help get the 'right science'
- Understand the implications of the science
- Integrate scientific and social considerations

RISK:
T × V × C

Risk Management: costs & benefits

ACTION - DECISION

Analysis (rigorous, replicable methods):
- Do the science right
- Collect useable, reliable data
- Develop and apply data manipulation tools
- Provide input to the solution

Conclusions

- **Homeland Security is a "wicked" problem**
- **Risk = T × V × C**
- **Risk-informed decision making is essential**
- **Need integrated <u>analysis and deliberation</u>**
- **Risk management:**
  - **Communication is a key element**
  - **Prevent, protect, respond, recover**
  - **Resilience (and robustness) for critical US infrastructure**