



# Critical Asset & Portfolio Risk Analysis

## State of Practice and Challenges

Bilal M. Ayyub, PhD, PE

Professor and Director

Center for Technology and Systems Management

University of Maryland, College Park



**The Infrastructure Security Partnership (TISP) Congress**  
**Crystal Gateway Marriott, Arlington, VA**  
**March 28, 2007**





# Outline

- Risk Analysis & Management
- Critical Asset and Portfolio Risk Analysis
- Challenges
- Selected References





# Terminology and Risk Fundamentals

**Risk**: The potential for loss or harm to systems due to the likelihood of an unwanted event and its adverse consequences.

- Potential means likelihood relating to vulnerability, consequences, and hazard rates
- Losses depend consequences and hazard rates
- Event(s) are defined by scenarios

Risk is an aggregate of (Hazard and scenarios, Consequences, Vulnerability, Threat rate)





# Risk Assessment and Management

1. What could happen? (hazards)
2. How can it happen? (scenarios & vulnerabilities)
3. How likely is it to happen? (probabilities)
4. What are the consequences if it happens? (impacts)
5. What can be done to reduce the risks in a cost effective manner?
6. What effect will these actions have on subsequent risks and options?

**Risk Assessment**

**Risk Management**





## **CAPRA**: **C**ritical **A**sset and **P**ortfolio (*including regional*) **R**isk **A**nalysis

CAPRA is a methodology and a process that can be used

- To quantitatively assess risks
- For a single asset, a portfolio of assets, or a region
- Due to natural hazards or human-caused hazards





# CAPRA attributes

- **Analytic** – breaks risk down into its contributing components
- **Transparent** – all assumptions and analytical steps are clearly and explicitly identifies
- **Quantitative** – defines and quantifies these components using meaningful metrics/units (e.g., \$)
- **Probabilistic** – uses probability theory to measure likelihood/chance





# CAPRA attributes

- **Defensible** – all assumptions are supported by data and our credible expert judgment
- **Consistent** with existing practices of probabilistic risk analysis (PRA) used in many other fields and DHS practices including RAMCAP™
- **Adapted** to the unique nature of human-caused hazards such as dynamic and gaming





# What decisions would CAPRA results inform?

## At the asset level:

- Prioritizing hazards, critical elements and potential consequences
- Identifying potential actions to limit risks
- Computing benefit/cost ratios for these actions
- Providing information for assessing capabilities, readiness, and grant funding opportunities







# What decisions would CAPRA results inform?

## At the asset-portfolio level:

- Prioritizing (in tiers) assets, hazards and potential consequences
- Providing a framework to examine interdependence
- Identifying potential portfolio-level actions to limit risks
- Computing benefit/cost ratios for these actions
- Providing information for assessing capabilities, readiness, and grant funding opportunities





# What decisions would CAPRA results inform?

## At the regional level:

- Screening hazards based on their regional impacts
- For each hazard applicable to a region, providing
  - Losses by hazard intensity (accounting for physical vulnerabilities and existing mitigation measures)
  - Security vulnerabilities
  - Conditional risk profiles (without the hazard rates)
  - Regional risk profiles
- Developing HIRA reports





# What decisions would CAPRA results inform?

At the regional level (cont.):

- Prioritizing (in tiers) hazards and potential consequences
- Providing a framework to examine interdependence
- Identifying potential region-level actions
- Computing benefit/cost ratios for these actions
- Providing information for assessing capabilities, readiness, and grant funding opportunities

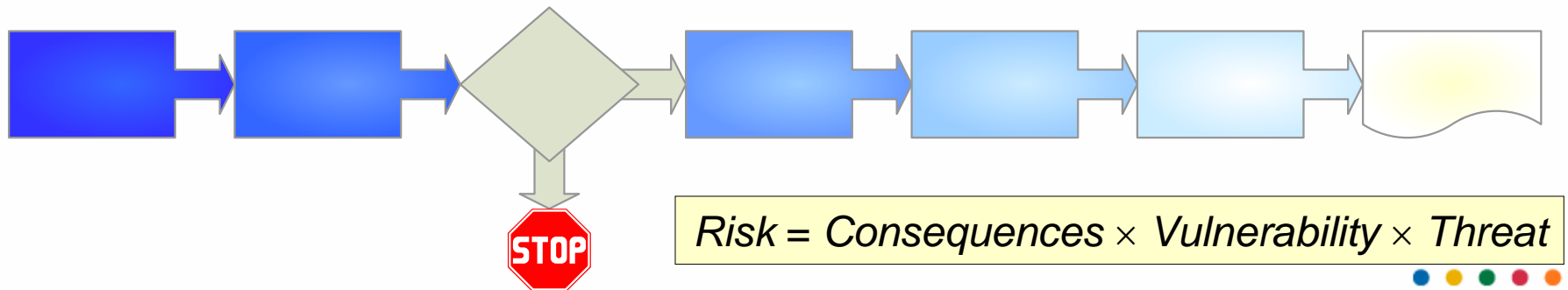


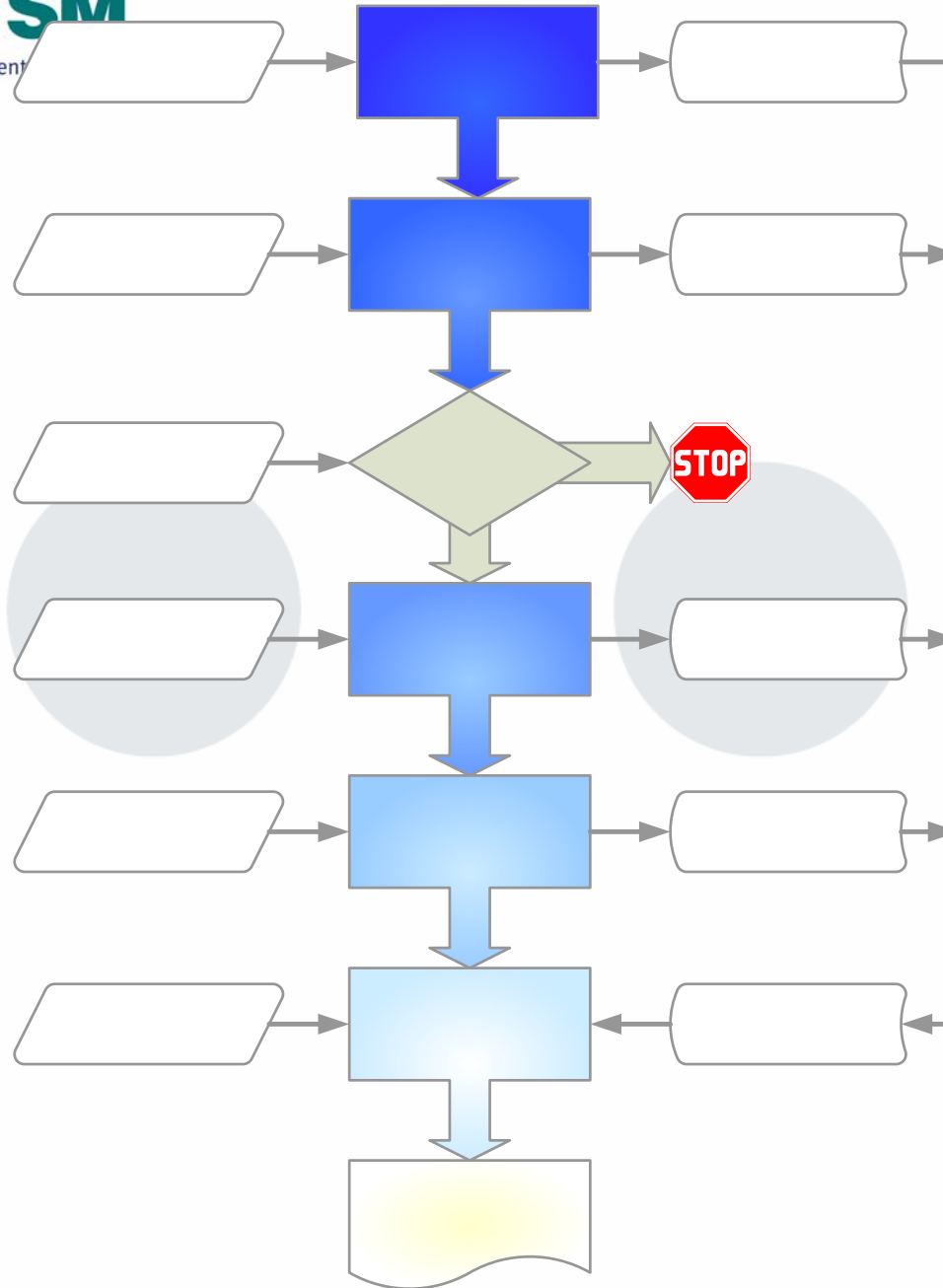


# CAPRA Overview

## Five phases:

1. Scenario identification
2. Consequence and criticality assessment
3. Security vulnerability assessment
4. Threat likelihood assessment
5. Benefit-cost analysis





Facility

Maximum  
Physical  
Mitigation





## Benefit-Cost Analysis

**Benefit = (Risk Before) – (Risk After)**

$$\text{B/C Ratio} = \frac{\text{Benefit}}{\text{Cost}}$$

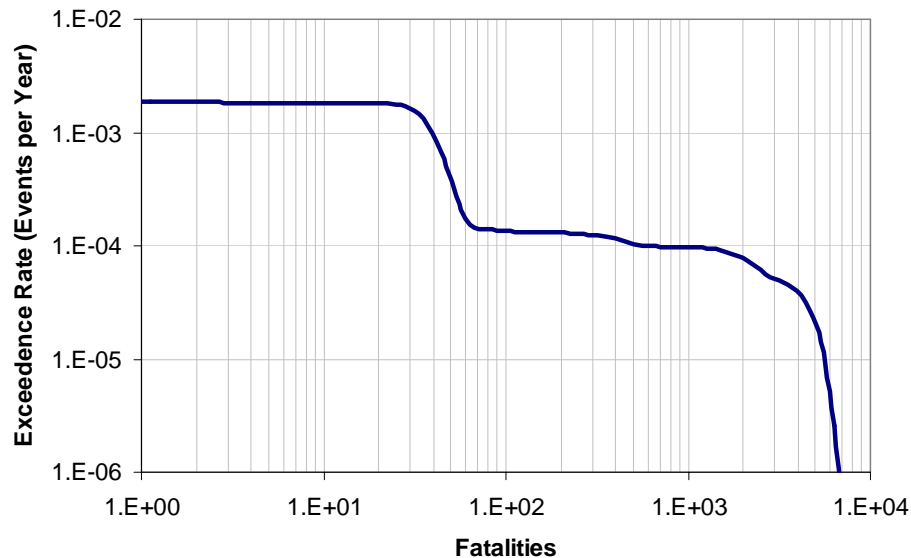




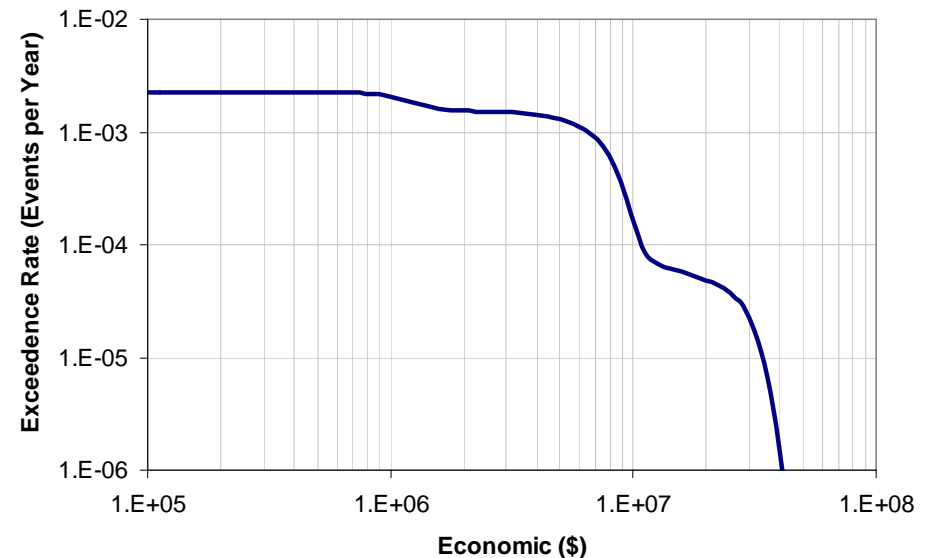
# Case Study: Explosive Attack Against Sport Center

- Risk Assessment
  - Considering all security threat scenarios

Fatality Loss-Exceedence Curves



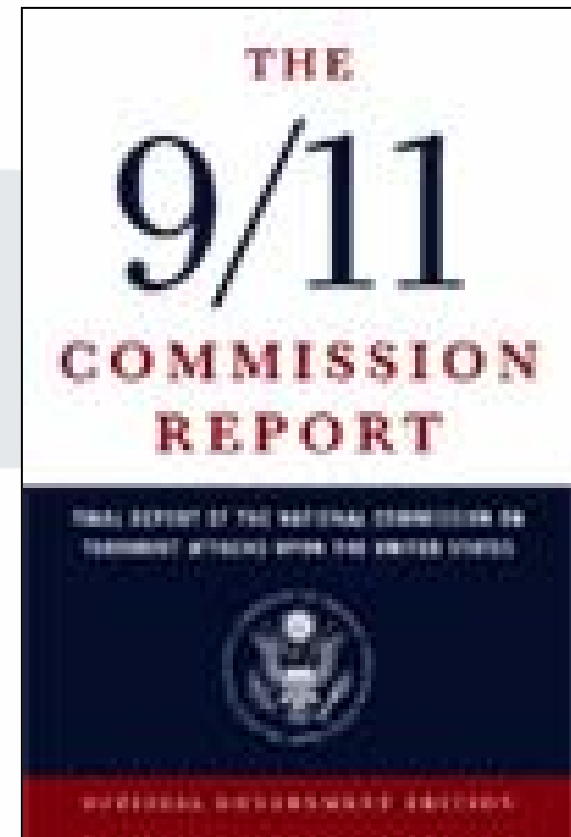
Economic Loss-Exceedence Curves





# Challenges: Scenario Identification

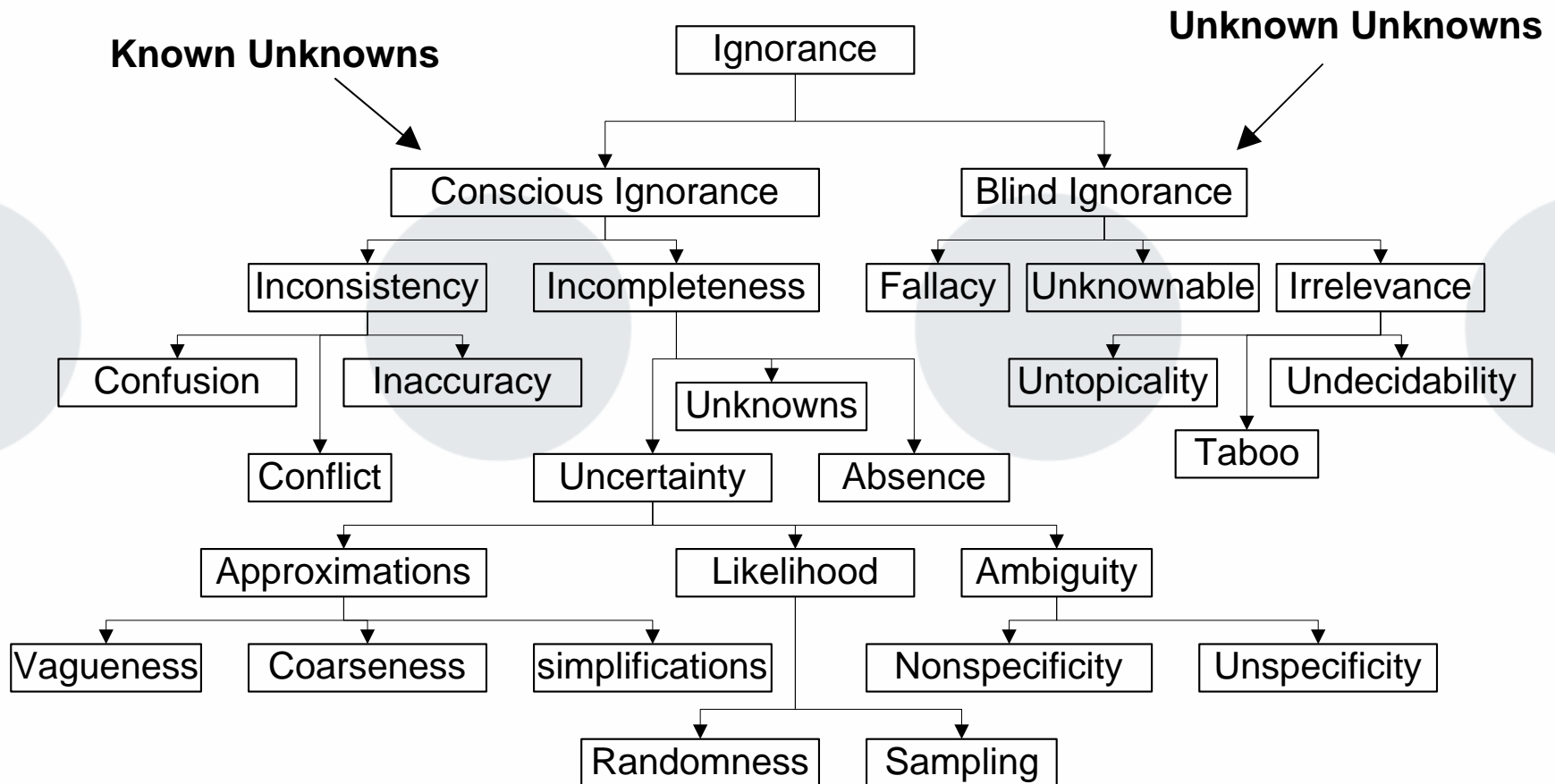
- “We believe the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management”  
Page 339
- Open World Assumption,  
“Unknown Unknowns”







# Hierarchy of Ignorance





# Consequence and Criticality Assessment

- Valuation



*"O.K., who can put a price on love? Jim?"*

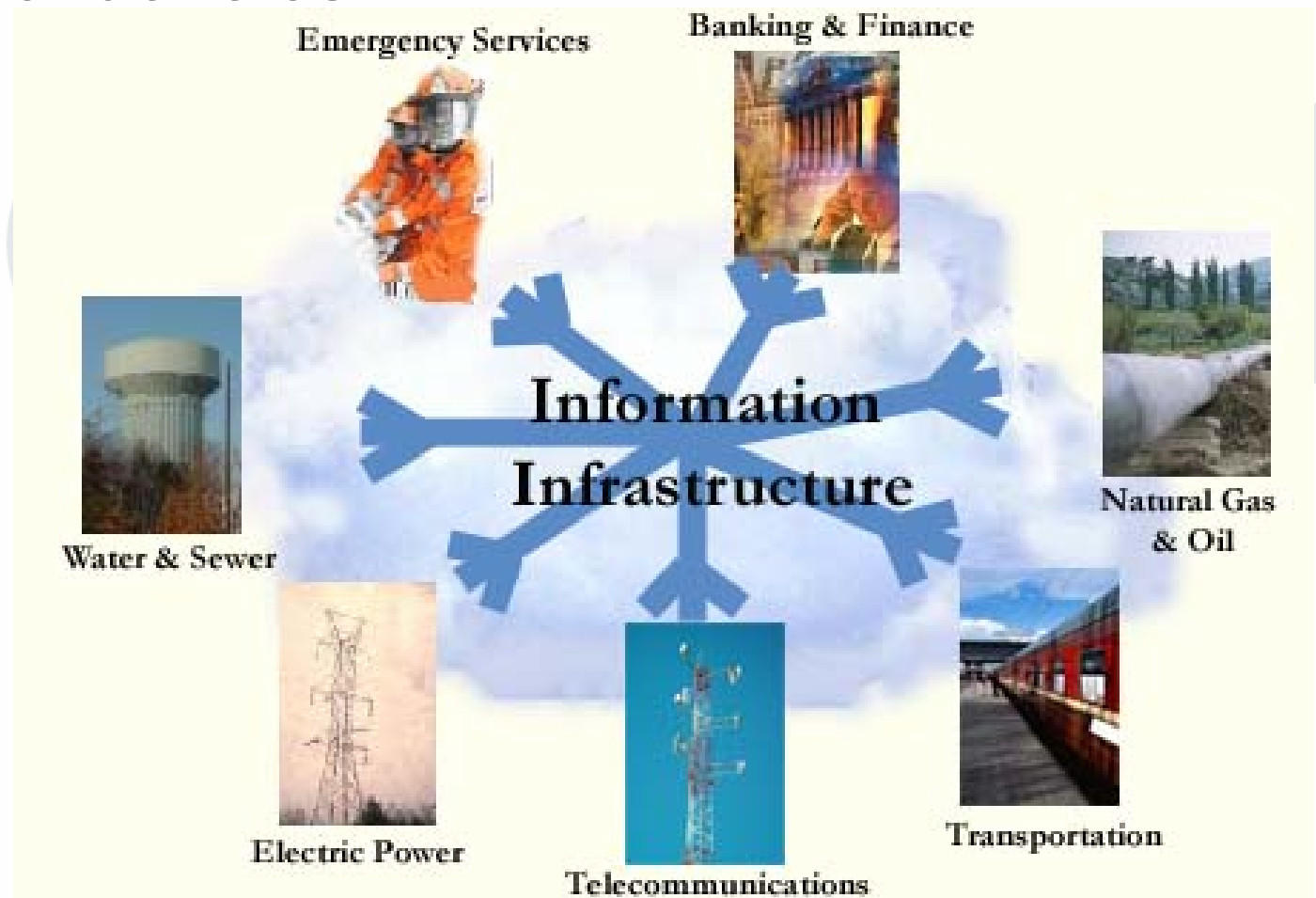
The New Yorker Collection 1991 Jack Ziegler from cartoonbank.com. All rights reserved.





# Consequence and Criticality Assessment

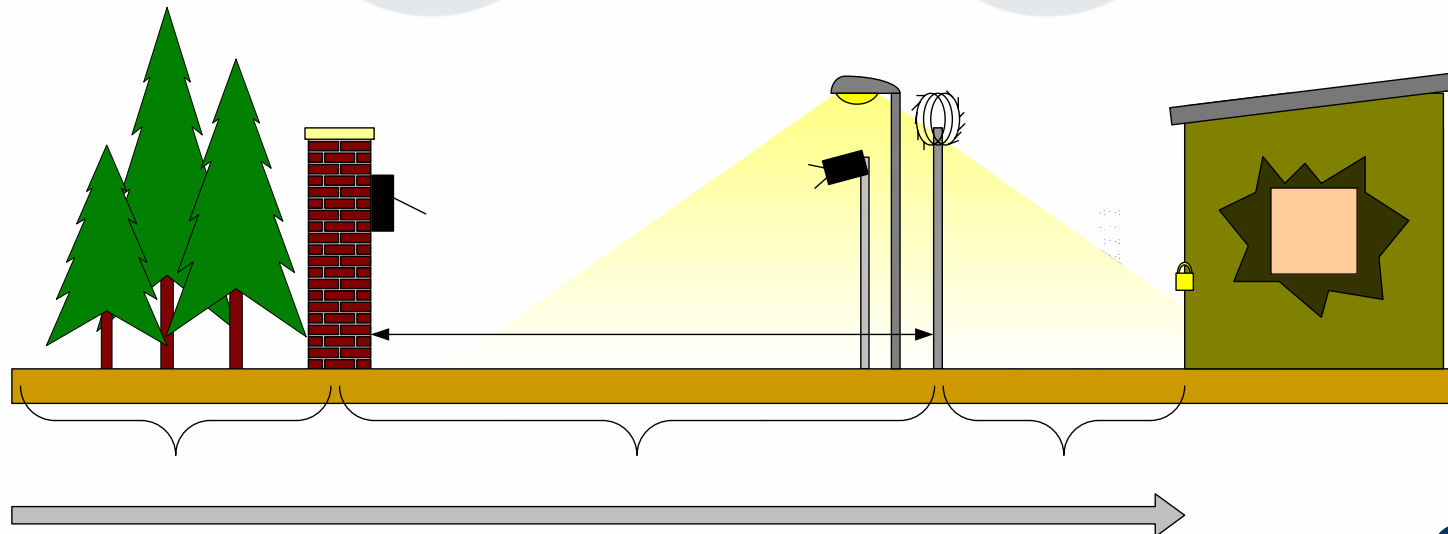
- **Interdependencies**





# Security Vulnerability

- Information sharing
- Public access
- Adverse impact on education (publications, visa policy, image, etc.)





## Threats and Their Likelihood

- Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Transmittal Letter, March 31, 2005
- “We conclude that the Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq’s weapons of mass destruction. ... On a matter of this importance, we simply cannot afford failures of this magnitude.”





# Risks

- Shifting and changing threats
- Standards (methods and features/products)
  - Would they lead to added vulnerabilities?
- All hazards
- Owner liability





# Types of Risk Analysis

- Strategic risk analysis
  - Uses a notional adversary (or postulated threat)
  - Seeks to minimize the risks associated with all that could happen
  - Leads to budgets/priorities for risk reduction
- Operational risk analysis
  - Is similar to the strategic type
  - Divides resources up among static and dynamic countermeasures and consequence mitigation strategies
- Tactical risk analysis
  - Focuses on effectively leveraging dynamic countermeasures in response to real-time risks





# Implementations of CAPRA-like Methods

- Buy-in and active participation by all stakeholders
- Too many assets and threats
- Consistency
- Stratified sampling and predictions







# Risk Communication


NOTIONAL PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI)

Government Building January 31, 2006

**NOTIONAL**

Critical Asset & Portfolio Risk Analysis (CAPRA):  
Asset Survey Report

Government Office Building



Updated January 31, 2006

**DISTRIBUTION NOTICE:** This document contains Protected Critical Infrastructure Information (PCI) in accordance with the provisions of 6 CFR part 29. It is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b)(3)). Unauthorized release may result in civil penalty or other action. It is to be safeguarded and disseminated in accordance with Protective Oil Program requirements.

Prepared by:  
Center for Technology and Systems Management  
Department of Civil and Environmental Engineering  
University of Maryland, College Park, MD 20742  
http://ctsm.umd.edu

**CTSM**  
Technology for Intelligent Decisions

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI) Page 1

NOTIONAL PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI)

Government Building January 31, 2006

**NOTIONAL**

The following asset information is on file with the State:

Asset Name: Government Office Building  
Address: Camp Fretwell Military Reservation, 5401 Rue Saint Lo Drive, Reisterstown, MD 21136  
Coordinates: 39-56g, 0-7m N, 76-56g, 0-7m W  
Phone: (301) 555-1212 Email: <http://www.government.state.us>  
Jurisdiction: Capital City  
Asset POC: Supervisor  
Phone: (301) 555-1234 Email: [superv@on.government.state.us](mailto:superv@on.government.state.us)

DHS Infrastructure Classification:  
15.5. Government Facilities/Other Government Facilities


**WHAT IS RISK?**  
Risk = Threat x Vulnerability x Consequence (or loss)

- Threat is the intent to cause harm or damage
- Vulnerability is an inherent weakness that can be exploited to cause harm or damage
- Consequences are effects from an event (human, economic, property losses, etc.)

The following are the key elements belonging to the asset and human-made threats considered in relation to these elements:

Key Asset Elements	Human-Made Threats
Main Building	Explosive
Computer Network	Ballistic
Broadcast Antenna	Radiofrequency
Telephone Bank	Inventory
Backup Power Generator	Chemical
Backup Water Supply	Biological
Personnel	Cyber

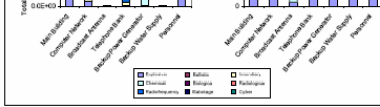
1. Risk Profiles for Previous Assessment Years



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI) Page 2

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI)

Page 3



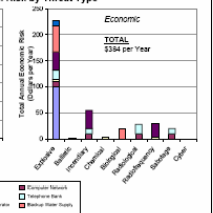
PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI) Page 3

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI)

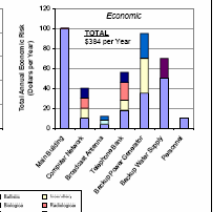
January 31, 2006

**NOTIONAL**

3. Total Risk by Threat Type



4. Total Risk by Element



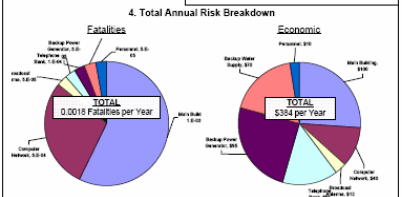
PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI) Page 3

NOTIONAL PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI)

Government Building January 31, 2006

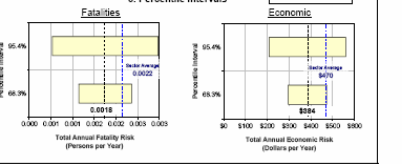
**NOTIONAL**

4. Total Annual Risk Breakdown



Dimension	Fatalities	Economic Risk	Combined
Total Risk per Year	0.0018	\$384	\$7,384
Epistemic Uncertainty	34.3%	22.9%	33.0%
95.9% Interval	0.0011 - 0.0024	\$256 - \$473	\$4,583 - \$8,834
55.4% Interval	0.0008 - 0.0030	\$209 - \$589	\$2,503 - \$72,284

5. Percentile Intervals



PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCI) Page 4

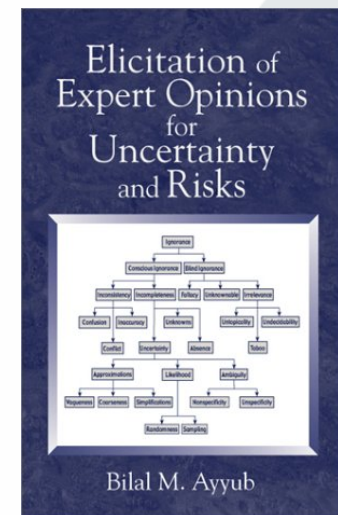
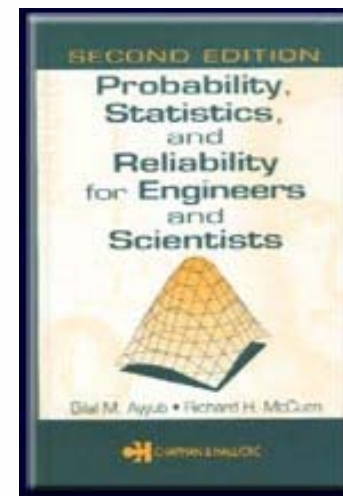
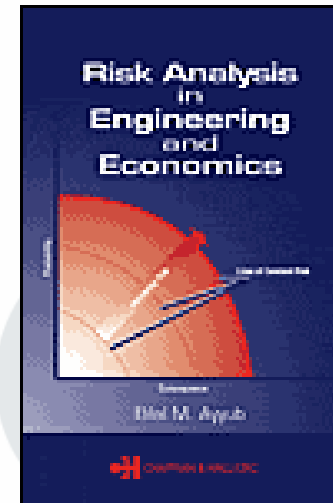
## Information security and vulnerability





# Publications

- Ayyub, B.M., and Klir, G.J., Uncertainty Analysis in Engineering and the Sciences, Chapman & Hall/CRC Press, 2006.
- Ayyub, B.M., Risk Analysis in Engineering and Economics, Chapman & Hall/CRC Press, 2003.
- Ayyub, B. M. , Elicitation of Expert Opinions for Uncertainty and Risks, CRC Press, FL, 2001.
- Ayyub, B.M., and McCuen, R., Probability, Statistics and Reliability for Engineers and Scientists, Chapman & Hall/CRC Press, 2003.





# Contact

## Professor Bilal M. Ayyub

Center for Technology and Systems Management  
Department of Civil and Environmental Engineering  
University of Maryland, College Park, MD 20742

301.405.1956 TEL

[ba@umd.edu](mailto:ba@umd.edu)

301.405.2585 FAX

<http://www.ctsm.umd.edu>

