

Special Session
on
**Robust and Resilient Critical
Infrastructure Systems**

Overview, Problem Description, and Challenges

Jagdish Chandra
The Institute for Reliability and Risk Analysis
The George Washington University
October 30, 2003

Some Basic Definitions

- Infrastructures: Linked system of facilities and activities that provide the range of essential services
- Critical Infrastructures: So vital that their incapacitation or destruction would have a debilitating impact on defense or national security (Clinton, 1997)
- Robustness: Failure- resistant through design and /or construction
- Resilience: Ability to recover quickly

INTERDEPENDENCIES

- Physical Interdependency
 - Cyber Interdependency
 - Geographic Interdependency
 - Logical Interdependency
- ***Modeling and Simulation of Interdependent Infrastructures is a complex, multifaceted, and multi-disciplinary problem***

Factors: Analyses of Interdependencies

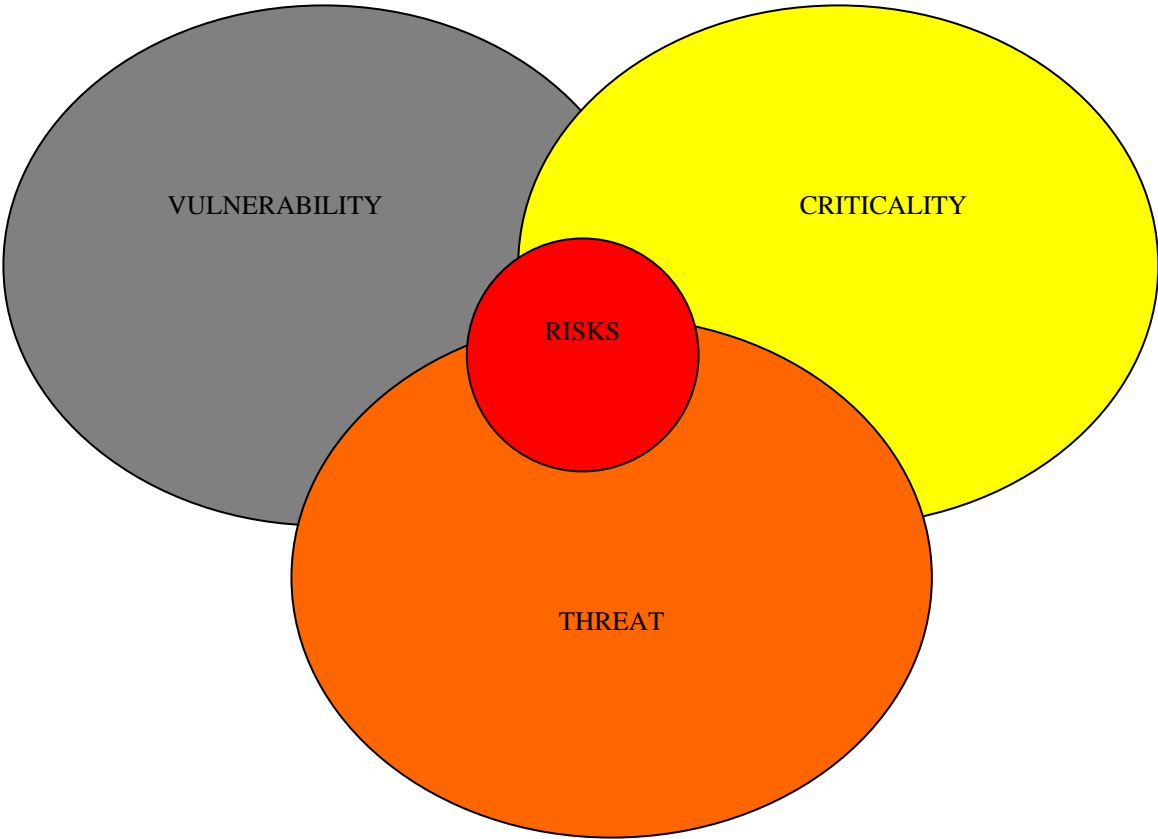
- Time Scales
- Geographic/Spatial Scales
- Higher Order Effects/ Cascading
- Human/Social/Psychological
- Operational Procedures
- Business Policies/Government Regulations
- Restoration/Recovery Procedures
- Stakeholders Concern

Network-centric Warfare

Global Economy

Communications
Sensors, Energy, Human Resources
Transportation

Networked Information Systems
(NIS)



INFRASTRUCTURE VULNERABILITIES

- Natural Hazards
- Degradation of Material and Components
- Complexity/ Interconnections
- Malevolent Acts
- ***Characterize Vulnerabilities, Role of Dependencies, and Propagation of Failures***

THREAT ANALYSIS

- Analyze data, patterns of threat scenarios and intrusion (some data-centric tools combining data-mining and adaptive case-based reasoning have been developed at FSU)
- Information fusion and management (Bayesian techniques for both cooperative and adversarial/compromised sensors/sources-GWU)
- A stochastic framework for intrusion detection (optimal filtering techniques for IDS- UW)

Fault Tolerance and Recovery in Mobile Wireless Networks



- Hybrid totally wireless networks
- Standby (backup) mobile routers are used to provide recovery and enhance reliability
- Developed distributed recovery protocols: the backup routers are scattered among the primary mobile routers (UCF)
- Using a flock-like dynamics, studying the arrangement of backups to maximize reliability (GWU)

RESILIENT INFRASTRUCTURES

- Reliable communication in a dynamic battlefield (developed fault-tolerant and distributed recovery protocols for hybrid totally mobile wireless networks-UCF)
- Robustness and Resiliency (analysis and design of strategies for optimal deployment of back-up mobile routers-GWU)

Risk Assessment and Management

- What can go wrong? What is the likelihood that it will? And, what are the consequences
- What can be done and what options we have? What are the trade-offs in terms of costs, benefits, and risks? And, how these decisions impact the future?
- ***Characterize optimal defensive strategies for sabotage risks (e.g., game theory as a paradigm for critical infrastructure protection-UW)***
- ***Risk management strategies for high consequence/low probability events***

Information Assurance of NIS

- Human introduced errors
- System probing (malicious, non-malicious)
- System penetration
- Subversion of networks
- Devise security and control mechanisms
- Misuse of policy, authority, power
- ***The interface between technology and human behavior; human factor is the Achilles heel of information security***

Networked Systems Simulation

- Modeling and simulation for resiliency designs (developed distributed modular intrusion detection system for ad hoc and hybrid totally-mobile wireless networks- UCF)
- Complex systems simulation (optimizing performance in networked systems- UW)