

# **The Role of Universities in Harmonizing the Security of Regional Cyberinfrastructure System of Systems**

**Yacov Y. Haimes**

**L. R. Quarles Professor of Systems and Information Engineering  
Founding Director, Center for Risk Management of Engineering Systems  
University of Virginia**

**[haimes@virginia.edu](mailto:haimes@virginia.edu)**

**November 4, 2009**

# **What Do We Mean by Cyberinfrastructure System of Systems?**

**Cyberinfrastructure system of systems connotes  
complex, large-scale cyber networks of  
hardware,  
software,  
organizational policies,  
procedures, and  
regulations  
associated with the Internet and the people who  
use it.**

# *Regional Cyberinfrastructure System of Systems*

**Future secure regional cyberinfrastructure systems ought to involve the development of:**

- **commonly accepted policies,**
- **effective systems integration of all of its elements,**
- **national legal dimensions,**
- **comprehensive risk modeling assessment, management, and communication, and**
- **technological solutions and standards.**

# Motivation

- **This presentation is motivated by a set of principal deficiencies surrounding the current state of security of cyberinfrastructure and information assurance.**

- **Universities can play a pivotal role in harmonizing the intricate requisite partnership between the states and the private sector in the protection of critical cyberinfrastructure.**

# Current Principal Deficiencies

- **Separation of policy development from technology solutions development, thereby reducing the integrated value that can be achieved through integration;**
- **Educational, training, and experience gaps among the collaborating professionals in state and local government and small private sector enterprises.**

# Principal Deficiencies (Cont'd)

- **Insufficient organizational interfaces among regional partners and shared understanding of cyber security requirements;**
- **Compartmentalized development in software engineering which compromises infrastructure cyber security throughout the system's life cycle;**

# Principal Deficiencies (Cont'd)

- **Insufficient funds allocated for the security of cyberinfrastructure and information assurance--an unjustified oversight by the leadership in the private and public sectors; and**
- **Inattention to *extreme events*, which results in misallocation of resources to address the full set of sources of risk to system development and operation.**

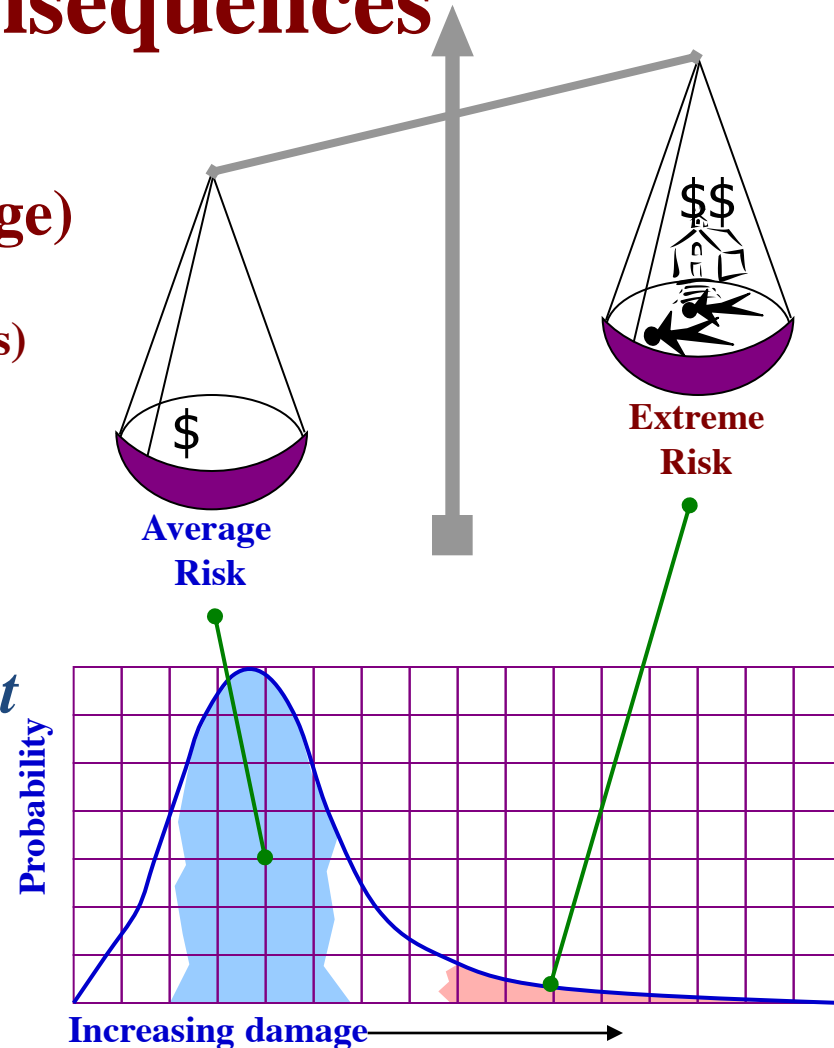
# Risk of Low Probability and Extreme Consequences

**Risk =  $f$  (Probability, Damage)**

or

**Risk =  $f$  (Likelihood, Consequences)**

*The fallacy of the expected value of risk as the sole metric for risk measurement*



# The Black Swan

**Nassim Nicholas Taleb ascribes three attributes to an extreme event:**

- (a) it is an outlier, as it lies outside the realm of regular expectation; nothing in the past can convincingly point to its possibility.**
- (b) it carries an extreme impact.**
- (c) in spite of its outlier status, human nature makes us concoct explanations for its occurrence *after the fact*, making it explainable and predictable.**

# **Role of Universities**

- **The Federal government, by necessity, makes extensive use of FFRDCs and the National Academies for technical and other science-based support (DHS relies on MITRE).**
- **State governments already have in-house technical expertise and science-based support at universities.**
- **Universities can play a pivotal role in harmonizing the intricate requisite partnership between the states and the private sector in the protection of critical cyberinfrastructure.**

# **Role of Universities, Cont'd**

- 1. Extensive research and technology-transfer programs are performed today by university faculty for the all levels of government and the private sector;**
- 2. Close relationships have been established over the years between universities state and local governments and the private sector;**
- 3. Graduate students working on such joint ventures for regional security of critical cyberinfrastructure gain valuable experience and add value to the partnership;**

**The above position universities in a natural harmonizing and supporting role.**

# *A Vision for Secure Regional Critical Cyberinfrastructure System of Systems*

**It is important to frame the security of critical cyberinfrastructure and information assurance on:**

**principles upon which the foundations of regional coordination and partnership are based.**

# Foundational Principles

**The ultimate adaptive, incremental, and sustainable security of regional cyberinfrastructure system of systems should be developed and nominally agreed upon by:**

- **users,**
- **developers,**
- **polycymakers, and**
- **other stakeholders of diverse technical and non-technical disciplines.**

# Foundational Principles (Cont'd)

The Regional Model of cyberinfrastructure system of systems ought to have a code of conduct and governance behavior including:

- (i) Reporting mechanisms for information sharing on breaches, incidents, and risks;
- (ii) Defining standards and acceptable levels of investments on cyber security resources;

# Foundational Principles (Cont'd)

- (iii) Formulating policies to prevent, mitigate, and regulate risks;**
- (iv) Addressing legal implications of consequences from cyber security incidents;**
- (v) Developing appropriate technologies and policies for their utilization, maintenance, and updating; and**
- (vi) Monitoring system intruders and adversaries.**

# How to Achieve Better Security of Cyberinfrastructure System of Systems?

**The answer is through a systems-based risk-informed decisionmaking process that is holistic, adaptive, incremental, and sustainable;**

**when we understand the complexity of the definition of the risk vector.**

# How to Achieve Better Security of Cyberinfrastructure System of Systems?

**Risk, a vector of probabilistic consequences is a function of:**

**time,  
threat (intent, capability, time, and the target)),  
states of the cyberinfrastructure,  
vulnerability and resilience  
of the system of the system, leading to a vector  
of consequences.**

**Yacov Y. Haimes, “On the Complex Definition of Risk: A Systems-Based approach,” *Risk Analysis*, 2009 December issue, pp. 1-8.**

# What is Vulnerability?

***Vulnerability*** is the manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can be ***exploited*** by an adversary to adversely affect (cause harm or damage to) that system.

**The vulnerability of a system is a vector that is a function of the specific threat and the time frame.**

# What is Resilience?

*The resilience of a system is a manifestation of the states of the system.*

*It is a vector that is time and initiating-event (threat) dependent.*

*Resilience is defined as the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable composite cost and time.*

*Resilience represents the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable cost and time.*

**Resilience cannot simply be measured in a single unit metric; its importance lies in the ultimate multidimensional outputs of the system (the consequences) for any specific inputs (threats).**

**In sum, the resilience of a system is a function of the threat, states and vulnerability of the system, and the time frame.**

# Resilience

**The question: “What is the resilience of Cyberinfrastructure X?” is unanswerable. Because the answer implicitly depends upon knowing whether it would recover following any specific attack within an acceptable time and composite cost.**

**Thus, such a question can be answerable only when the threat (initiating event) scenario (or a set of scenarios) is specifically identified.**

# Epilogue

- Universities are uniquely positioned to contribute to this effort in partnership with state and local governments and the private sector.
- **Although many such partnerships exist, they are not necessarily focused on the risks to and security of cyberinfrastructure.**
- Many of the listed existing deficiencies in the security of cyberinfrastructure can be reduced or removed altogether through the harmonizing role of universities and by serving as surrogates to the FFRDC-type support needed by the partners.