Non-Technical Issues Influencing Information Assurance
October 21, 1999
0830-1000

Chair:
Paul Byron Pattak
President
The Byron Group, Ltd.

Panelists:
William Bruck, Ph.D.
Author

Donald M. Le Vine, Ph.D.
Senior Scientist
TRW

Stevan Mitchell, Esq.
Senior Trial Attorney
Department of Justice

Addison Slayton, Jr.
Former Director
Virginia Department of Emergency Services

Session Abstract:
Much of the work being done today by both industry and government to provide information assurance focuses on complex technical issues and solutions -- including hardware, software, processes and systems integration. All of these are important, but they must be done within a context of equally-important non-technical issues. Too many organizations spend resources on technical solutions without having first examined the non-technical issues which frame their environment.

Information assurance problems occur within the framework of ***social***, ***cultural***, ***political***, ***legal***, ***economic*** and ***organizational*** dynamics and each of these has a significant impact on the ability of an enterprise to protect its information systems and their contents. The panel believes that many of these items should be analyzed *before* technical decisions are made and resources committed to purely technical solutions.

The following illustrates some of the relevant points from each of the six areas to be examined by the panel.

- ***Social*** issues include our system of values and beliefs and who we are as a people.
- ***Cultural*** issues include behavior, tolerance, expressions, language, customs and rituals.

- ***Political*** issues include the formal mechanisms for adjudication of resource allocation conflicts and formal mechanisms for the redress of problems.
- ***Legal*** issues include the formal adjudication of disputes and the codification of social, cultural and political beliefs.
- ***Economic*** issues include market forces, competition, regulation and decisions based on self-interest.
- ***Organizational*** issues include human behavior as well as organizational behaviors and organizational cultures.

The Chair and the panelists all have broad experience in dealing with industry, government and academia, and can address multiple viewpoints. As all these parties contemplate partnerships to solve information assurance challenges, a keen awareness and understanding of these viewpoints and how they incorporate the non-technical issues will be critical to success.

The intent of this thought-provoking panel is to get the audience thinking about the relevant non-technical issues from a strategic point of view, and as a prelude to making decisions about the resulting technical solutions.

Questions to be posed include:

- Are non-technical issues gaining importance in an ever-increasing technical world?
- Why is it so important to review the non-technical issues prior to considering technical solutions?
- How do the non-technical issues relate to each other, and to technical issues?
- How can analysis of the non-technical issues improve decision-making for technical solutions?
- What are some of the ways to examine the non-technical issues?
- And many more…

Brief Summary of Panelist's Topics:

Paul Byron Pattak will present the panel ***overview*** and address the ***economic*** issues, specifically the need to understand the differences between how industry and government view the need to spend resources on information assurance. Mr. Pattak will also talk about how economic trends influence perceptions on the value of information, and consequently how resource decisions are made to support information assurance. Mr. Pattak was a Senior Consultant to the President's Commission on Critical Infrastructure Protection (PCCIP).

William Bruck, Ph.D., will draw upon his many years of experience as an educator, author and consultant to address the effects ***organizational*** issues have on technical solutions and vice versa. Oftentimes in his career, he has had to deal with the problems resulting from implementing technical solutions without factoring in either organizational dynamics or any human factors. Dr. Bruck has written extensively on solutions to these

problems, and how to prevent many of them in the first place. Dr. Bruck is also the author of seven books on software and information systems.

Donald M. Le Vine, Ph.D. has spent many years studying the ***social*** and ***cultural*** aspects of infrastructure assurance, and how they influence technical decisions. He has also conducted extensive studies on possible methodologies for compiling and presenting non-technical issues for incorporation into technical decisions. Dr. Le Vine's research on infrastructure inter-connections and inter-dependencies has broad applicability throughout the infrastructure assurance area and can be adapted by all types and sizes of organizations. He is a theoretical physicist who has worked closely with leading scientists and engineers from all over the country.

Stevan Mitchell, Esq. served as a Commissioner on the President's Commission on Critical Infrastructure Protection (PCCIP), representing the Department of Justice. He oversaw the development of the PCCIP's legal recommendations. Mr. Mitchell will address ***legal*** issues that are relevant to technical solutions, in particular the issue of privacy which has been getting much media attention of late. Privacy and other issues examined by Mr. Mitchell and the PCCIP Legal Team are examined in more detail in the 14 volumes of the *Legal Foundations* series of reports that can be found on the Internet at *www.ciao.ncr.gov*.

Addison Slayton, Jr. recently retired as Director of the Virginia Department of Emergency Management (DEM). During a long and distinguished career in law enforcement, Mr. Slayton worked at the highest levels of state government in Virginia and ably served several governors of both parties. Mr. Slayton will address how ***political*** issues are never far from the surface of significant public policy debates and decision-making processes on matters dealing with security, emergency management, infrastructure protection and re-constitution. As Director of the Virginia DEM, Mr. Slayton was active in the National Emergency Management Association (comprised of the state emergency management directors), and was involved in dealings with Congress, and several Executive Branch agencies such as Defense, Energy, FEMA and many others.

Audience to Attract:

This panel is designed for those individuals who are looking to better understand the impact non-technical issues have on the decision-making process for technical solutions, and ultimately to make better decisions on those technical solutions.. As a result of attending, they will better understand the non-technical issues themselves, how they are inter-connected, and what the impact of each can be on their organization. The insights gained from attending this panel session will also prepare them to deal more effectively with external entities from these non-technical areas which may be influencing their organization. The panel will also present thought-provoking viewpoints which the attendees are unlikely to hear elsewhere in the conference.

NON-TECHNICAL ISSUES INFLUENCING INFORMATION ASSURANCE

PAUL BYRON PATTAK

22nd National Information Systems Security Conference
Arlington, Virginia
October 22, 1999

© 1999 - The Byron Group, Ltd.

OUTLINE

- Why Be Concerned About Non-technical Issues?
- Effect Of Information Systems On Our World
- Six Non-technical Issues Which Influence Information Assurance
- Conclusions

© 1999 - The Byron Group, Ltd.

WHY BE CONCERNED ABOUT NON-TECHNICAL ISSUES?

- They Drive Both Internal And External Policy
- They Represent What We Think And Feel
- They Frame Our Environment And Define Many Of Our Operating Parameters
- They, More Than Technology, Define Who We Are And What We Feel Is Important

© 1999 - The Byron Group, Ltd.

BEFORE INFORMATION SYSTEMS

- Enterprises Were Relatively Autonomous
- Inter-connections Were Fewer, And Dependencies Fewer Still
- Domain Areas Were More Clearly Defined, E.G. Banks Were Banks, The Phone Company Stood Alone, Etc.
- Public And Private Sectors Had Areas Of Interests Which Did Not Generally Overlap
- Physical And Geographic Boundaries Defined The World
- We Understood The World We Were In

© 1999 - The Byron Group, Ltd.

TODAY

- **Inter-connections And Dependencies Have Flourished**
- **Their Full Extent Is Unknown**
- **Traditional Boundaries And Parameters Have Changed, E.G. Fedex Considers Itself An "It Company" Not A Delivery Service**
- **When 95% Of DoD Communications In U.S. Are Carried Over Public Telephone Network, Public And Private Interests Have Fused**
- **We Do Not Understand The World We Are In**
- ***Distance and Time Are Irrelevant***

© 1999 - The Byron Group, Ltd.

THE CONSEQUENCES

- **Less Autonomy, Assurance, Control**
  - **Proliferation Of Interconnections**
  - **Globalization Of Infrastructures**
  - **Growing Probability Malfunctioning Anywhere Within An Infrastructure (Or Even An Enterprise) Will Have (Inter)national Impact**

© 1999 - The Byron Group, Ltd.

THE CONSEQUENCES (cont.)

- **Inadequate Hierarchy Of Values**
  - **Unprecedented Circumstance**
  - **Implications Not Well Understood**
  - **Impact Of New Tensions Not Clear**

© 1999 - The Byron Group, Ltd.

THE CONSEQUENCES (cont.)

- **Division Of Responsibilities Needs Revision**
  - **Society Is Increasingly Interconnected**
  - **Impact Of An Event Becoming Broader**
  - **More Difficult To Separate Vital Interests Of Governments, Private Organizations, Individuals**

© 1999 - The Byron Group, Ltd.

THE CHALLENGES

- Improving Communications
  - Greater Diversity Of People Involved
  - Increasing Fragmentation Of Interests
    - Narrowing Of Focus
    - Conflicting Perspectives

© 1999 - The Byron Group, Ltd.

THE CHALLENGES (cont.)

- **Increasing Awareness**
  - **Information Is Abstract**
  - **No Standard Of Measure**
  - **Technology Creates Barriers**
  - **Implications Not Understood**

© 1999 - The Byron Group, Ltd.

WHY NON-TECHNICAL ISSUES?

- To Improve Communications
- To Increase Awareness
- Because Information Systems And Their Impact Have Not Been Personalized, And Therefore Are Yet Really Understood

© 1999 - The Byron Group, Ltd.

THOUGHTS

- For Information Systems . . .
  Distance and Time are Irrelevant
- Proliferation Of Interconnections
- These Change How Governments, Private Organizations, Individuals Function And Interact
- We Do Not Understand The Implications Of These Changes
- Challenges Primarily Cultural, Organizational, Perceptional . . . Not Technological

© 1999 - The Byron Group, Ltd.

NON-TECHNICAL ISSUES

- Social
- Cultural
- Political
- Legal
- Economic
- Organizational

© 1999 - The Byron Group, Ltd.

SOCIAL

- Our System Of Values And Beliefs
- Society's Norms
- Collective Wisdom
- Who We Are As A People

© 1999 - The Byron Group, Ltd.

CULTURAL

- Behavior
- Tolerance
- Expressions
- Artistic Influence
- Customs And Rituals

© 1999 - The Byron Group, Ltd.

POLITICAL

- Influenced By Social And Cultural Forces
- Adjudication Of Resource Allocation
- Formal Mechanisms For Redress Of Problems
- Shifts Between Reactive And Proactive

© 1999 - The Byron Group, Ltd.

LEGAL

- Political Forces Are The Foundation
- Formal Adjudication Of Disputes
- Regulates Behavior
- Codification Of Social, Cultural And Political Beliefs
- Simultaneously Guarantees Freedoms And Imposes Constraints

© 1999 - The Byron Group, Ltd.

ECONOMIC

- Framework Created By Political System
- In U.S. Dominated By Market Forces
- Based In Most Part, On Competition
- Survival Of The Fittest
- Forces Decisions Based On Self-interest

© 1999 - The Byron Group, Ltd.

ORGANIZATIONAL

- Defined By Either Legal Or Economic Parameters
- Formal Dynamics
- Informal Dynamics (Even More Important)
- Provides Mostly Contstraints

© 1999 - The Byron Group, Ltd.

INFLUENCES ON INFO ASSURANCE

- Facilitates An Understanding Of What Is Important (Valuable)
- This Can Only Be Learned Through Analysis And Communication
- Requires Dealing With People Outside Traditional It Sphere
- Opportunity To Strengthen Relationship With Enterprise Leadership
- Allows It To Break Out Of Self-imposed Boxes

© 1999 - The Byron Group, Ltd.

HOW?

- A New Way To Look At Things
- An Approach Based On Asking The Right Questions Before Accepting Answers
- A New Means Of Understanding What Has Become A New World
- An Emphasis On Understanding And Dealing With People

© 1999 - The Byron Group, Ltd.

CONCLUSIONS

- In A Third Wave World, Information Assurance Now Protects The Most Important Non-human Elements Of The Enterprise
- Information Assurance Responsibilities Are Greater Than Ever Before
- It Is Time For Information Assurance Elements To Work Closely With Non-traditional Elements Both Inside And Outside The Enterprise

© 1999 - The Byron Group, Ltd.

CONCLUSION (cont.)

- For Information, Distance And Time Are Irrelevant
- Proliferation Of Interconnections
- These Change How Governments, Private Organizations, Individuals Function And Interact
- We Do Not Understand The Implications Of These Changes
- Challenges Primarily Human-based . . .
  Not Technological

© 1999 - The Byron Group, Ltd.

ANY QUESTIONS?

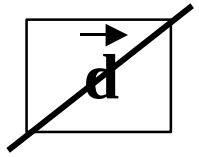
PAUL BYRON PATTAK
President
The Byron Group, Ltd
703.751.6138
pattak@tmn.com

© 1999 - The Byron Group, Ltd.

THANK YOU!

THE MODERN INFRASTRUCTURE: RESPONDING TO THE CHALLENGES

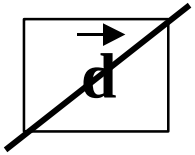
22nd National Information Systems Security Conference
Arlington, Virginia
October 21, 1999



DONALD M Le VINE

SUMMARY

- **INFORMATION SYSTEMS ARE ESSENTIAL FOR MODERN INFRASTRUCTURES**
- **THESE INTRODUCE UNPRECEDENTED CIRCUMSTANCE: *DISTANCE IS IRRELEVANT***
- **THIS FOSTERS PROLIFERATION OF INTERCONNECTIONS**
- **THESE CHANGE HOW GOVERNMENTS, PRIVATE ORGANIZATIONS, INDIVIDUALS FUNCTION, INTERACT**
- **WE DO NOT UNDERSTAND IMPLICATIONS OF CHANGES**
- **HOWEVER, THEIR IMPACT WILL BE PROFOUND**
  - » **<u>NOT</u> BECAUSE OF TECHNOLOGICAL INNOVATION OR VULNERABILITIES INFORMATION SYSTEMS FACILITATE**
  - » **<u>BUT</u>, BECAUSE OF CULTURAL, ORGANIZATIONAL, PERCEPTIONAL CHANGES THEY NECESSITATE**



THE MODERN INFRASTRUCTURE

I. **THE CHALLENGES -- DISTANCE IS IRRELEVANT**

II. THE DYNAMICS -- BASIS FOR RESPONDING

III. THE RESPONSE -- A METHODOLOGY

AN INFRASTRUCTURE

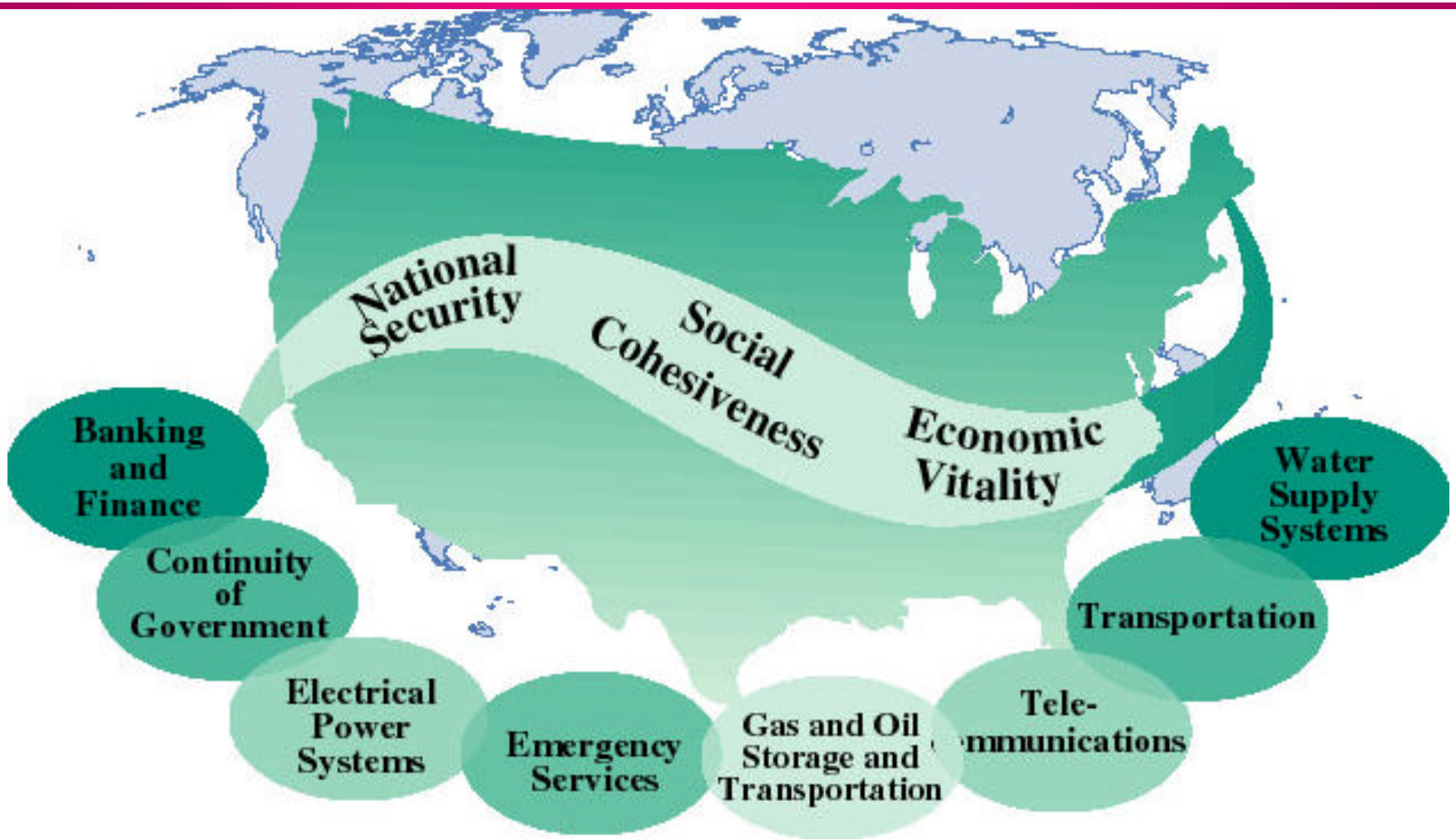
THE ROADS, FINANCIAL NETWORKS, LAWS, TELECOMMUNICATIONS, EMERGENCY SERVICES, PEOPLE, MANUFACTURING FACILITIES, ELECTRICAL POWER SYSTEMS, …, ENABLING ELEMENTS OF SOCIETY TO:

- **FUNCTION,**
- **INTERACT WITH ONE ANOTHER,**
- **ENSURE NATIONAL SECURITY, SOCIAL COHESIVENESS, ECONOMIC VITALITY.**

AN INFRASTRUCTURE -- ITS COMPONENTS

- ***PARTICIPANTS***
  - **PEOPLE**
  - **ORGANIZATIONS**
  - **ALLIANCES**
  - **SEGMENTS**
- ***INTERCONNECTIONS***
  - **INTERRELATIONSHIPS AMONG *PARTICIPANTS***
- ***FRAMEWORK***
  - **VALUES, LAWS, CULTURE SHAPING HOW *PARTICIPANTS* INTERACT**

PREVIOUS INFRASTRUCTURE



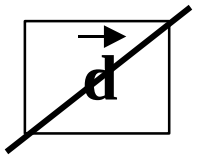
. . . Autonomous, few interconnections, well-defined

WHAT IS DIFFERENT

- **EMERGENCE OF INFORMATION SYSTEMS**
  - » **INTEGRAL TO INFRASTRUCTURE**
  - » **A PRIMARY CATALYST FOR GROWTH, NOT MERELY AN ASSET**

- **PROLIFERATION OF INTERCONNECTIONS**
  - » **EXPAND EXISTING RELATIONSHIPS**
  - » **CREATE CONNECTIONS CONSIDERED IMPLAUSIBLE OR IMPOSSIBLE**

- ✷ ***DISTANCE IS IRRELEVANT***



THE CONSEQUENCES

- **GREATER UNCERTAINTY**
  - **LOSE OF AUTONOMY, ASSURANCE, CONTROL**
  - **CURRENT EXPERIENCES, INSIGHTS, SKILLS MAY NOT SUFFICE IN FUTURE**
- **NEW TENSIONS**
  - **INTEGRATING INFORMATION INTO HIERARCHY OF VALUES**
  - **ACCOMMODATING RAPID CHANGE**
- **CONFLICTING RESPONSIBILITIES**
  - **CURRENT DIVISION BASED UPON COMPETING, BUT SEPARABLE INTERESTS**
  - **FUTURE INVOLVES COMPETING, BUT <u>IN</u>SEPARABLE INTERESTS**

THE CHALLENGES

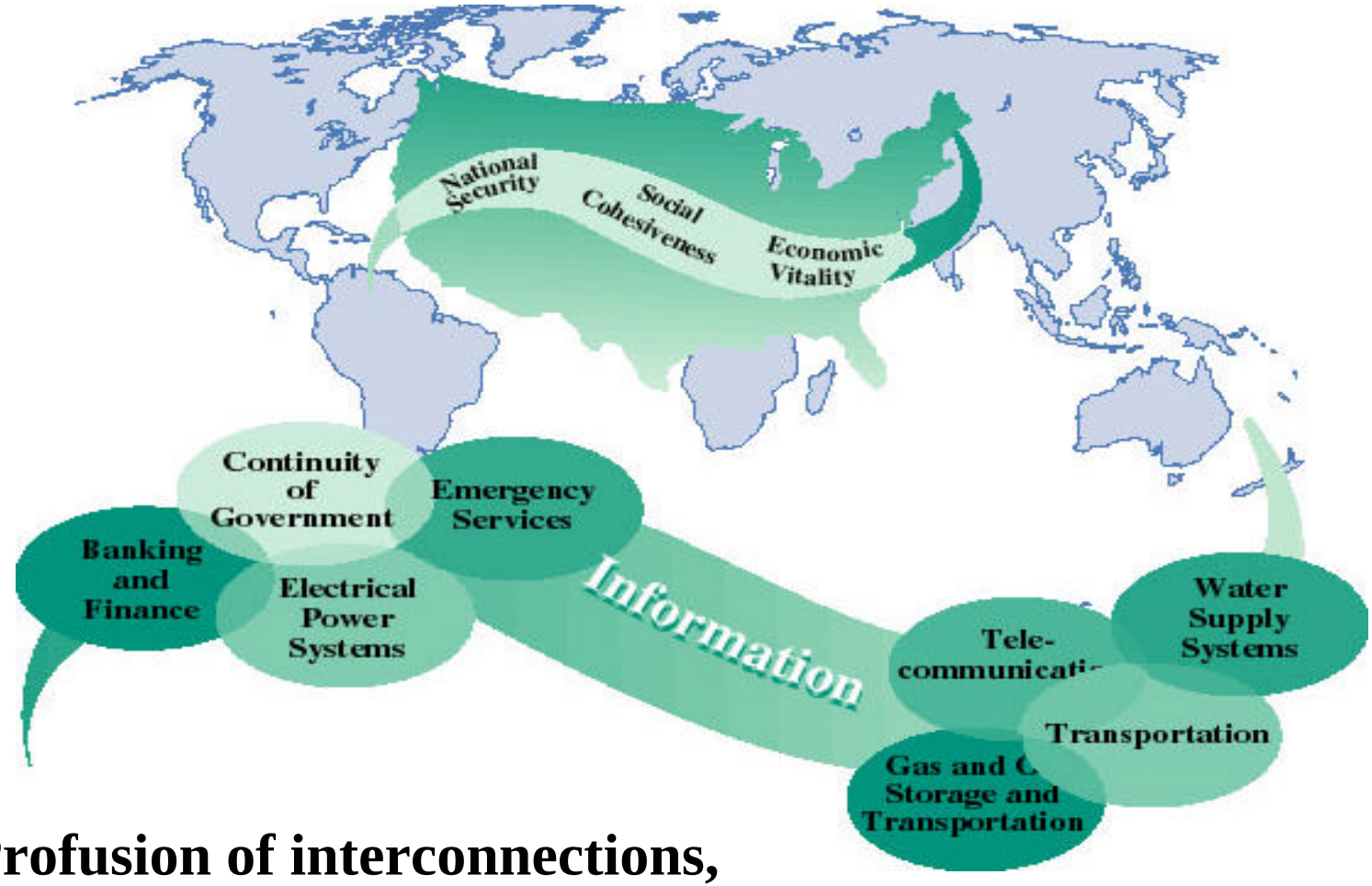
- **IMPROVING COMMUNICATIONS**
  - **WIDER SPECTRUM OF PEOPLE, IDEAS, INTERESTS**
  - **FRAGMENTATION OF FOCUS**
  - **BROADER PERSPECTIVE NECESSARY**
- **INCREASING AWARENESS**
  - **INFORMATION IS ABSTRACT**
  - **NO STANDARD OF MEASURE**
  - **POTENTIAL STIGMA**

. . . INFORMATION SYSTEMS AND THEIR IMPACT HAVE NOT BEEN PERSONALIZED

THE CHALLENGES

- **IMPROVING COMMUNICATIONS**
- **INCREASING AWARENESS**
- **EVOLVING FRAMEWORK**
  - **ADAPT CULTURAL, POLITICAL, LEGAL, ECONOMIC STRUCTURES**
  - **ADJUST ROLES OF GOVERNMENT, PRIVATE INDUSTRY, CITIZENS**
  - **INTEGRATE INFORMATION INTO HIERARCHY OF VALUES**
- **FINDING A CATALYST**
  - **HISTORICALLY: PRESERVATION OF HUMAN LIFE**
  - **THE FUTURE: COMPLEXITY?**

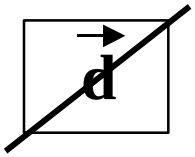
SUMMARY
THE MODERN INFRASTRUCTURE



. . . Profusion of interconnections,
interdependence, complexity, overlapping capabilities

SUMMARY

- **INFORMATION SYSTEMS ESSENTIAL FOR MODERN INFRASTRUCTURES**
- **THESE INTRODUCE UNPRECEDENTED CIRCUMSTANCE: *DISTANCE IS IRRELEVANT***
- **THIS FOSTERS PROLIFERATION OF INTERCONNECTIONS**
- **THESE CHANGE HOW GOVERNMENTS, PRIVATE ORGANIZATIONS, INDIVIDUALS FUNCTION, INTERACT**
- **WE DO NOT UNDERSTAND IMPLICATIONS OF CHANGES**
- **HOWEVER, THEIR IMPACT WILL BE PROFOUND**
  - » **<u>NOT</u> BECAUSE OF TECHNOLOGICAL INNOVATION OR VULNERABILITIES INFORMATION SYSTEMS FACILITATE**
  - » **<u>BUT</u>, BECAUSE OF CULTURAL, ORGANIZATIONAL, PERCEPTIONAL CHANGES THEY NECESSITATE**



THE MODERN INFRASTRUCTURE

I. THE CHALLENGES -- DISTANCE IS IRRELEVANT

II. THE DYNAMICS -- BASIS FOR RESPONDING

III. THE RESPONSE -- A METHODOLOGY

WHERE WE ARE

- VARYING LEVELS OF AWARENESS
- NO VIGOROUS CHAMPION
  - » CAN THE GOVERNMENT LEAD?
  - » ORGANIZATIONS UNSURE OF WHAT IS NEEDED
- APPROACHES PREDOMINATELY REACTIVE
  - » VARIATIONS OF THE PAST
- FOCUS ON TECHNOLOGY
- MINIMAL EXPERIENCE COLLABORATING
- LITTLE NATIONAL PERSPECTIVE

- CAN RESPOND TO AN OKLAHOMA CITY DISASTER; <u>CANNOT</u> FOR ELECTRONIC COUNTERPART

WHAT NEEDS TO BE DONE

- **IMMEDIATE**
  - **PROVIDE EMERGENCY RESPONSE**
  - **IMPLEMENT POLICIES, PROCEDURES**
  - **INCREASE EDUCATION AND AWARENESS**
- **SYSTEMIC**
  - **EXPLORE IMPLICATIONS OF *DISTANCE IS IRRELEVANT***
  - **EVOLVE FRAMEWORK**
  - **CREATE LONG TERM CONTEXT FOR PRESERVING NATIONAL SECURITY, SOCIAL COHESIVENESS, ECONOMIC VITALITY**

HOW WE GET THERE

TWO COMPLEMENTARY APPROACHES

- **REACTIVE**
  - SHORT TERM
  - FOCUSSED
  - CONVENTIONAL
  - TECHNOLOGY DRIVEN
  - IMPLEMENT SOLUTIONS
- **ARCHITECTURAL**
  - LONG TERM
  - BROAD PERSPECTIVE
  - HIGH RISK
  - TECHNOLOGY IN A SUPPORT ROLE
  - SHAPE SOLUTIONS

WHO MUST BE INVOLVED

- **SINCE CHALLENGES PRIMARILY CULTURAL, ORGANIZATIONAL, PERCEPTIONAL**
  - **NON-TECHNOLOGISTS *AND* TECHNOLOGISTS**
  - **GOVERNMENT *AND* PRIVATE INDUSTRY**
  - **ORGANIZATIONS *AND* INDIVIDUAL CITIZENS**

. . . SOCIETY

REVENGE OF THE NON-NERD

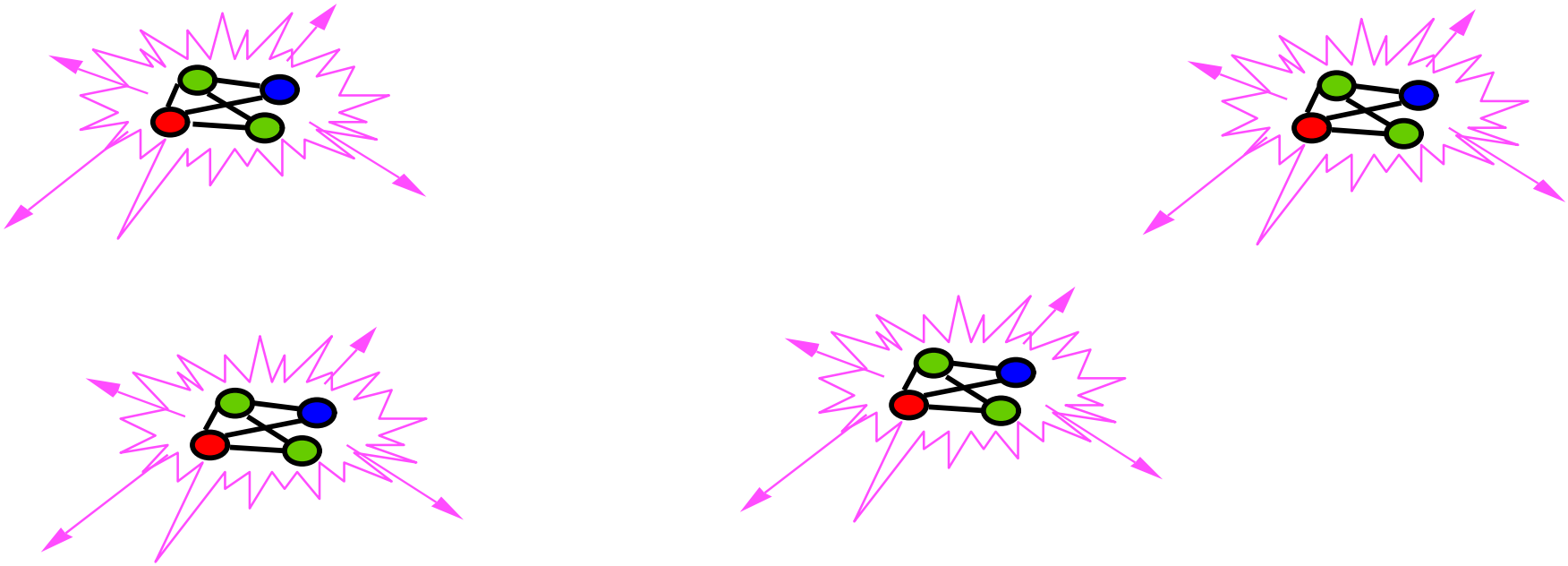
THE MODERN INFRASTRUCTURE

I. THE CHALLENGES -- DISTANCE IS IRRELEVANT

II. THE DYNAMICS -- BASIS FOR RESPONDING

III. THE RESPONSE -- A METHODOLOGY

ASSUMPTIONS -- PARTICIPANTS

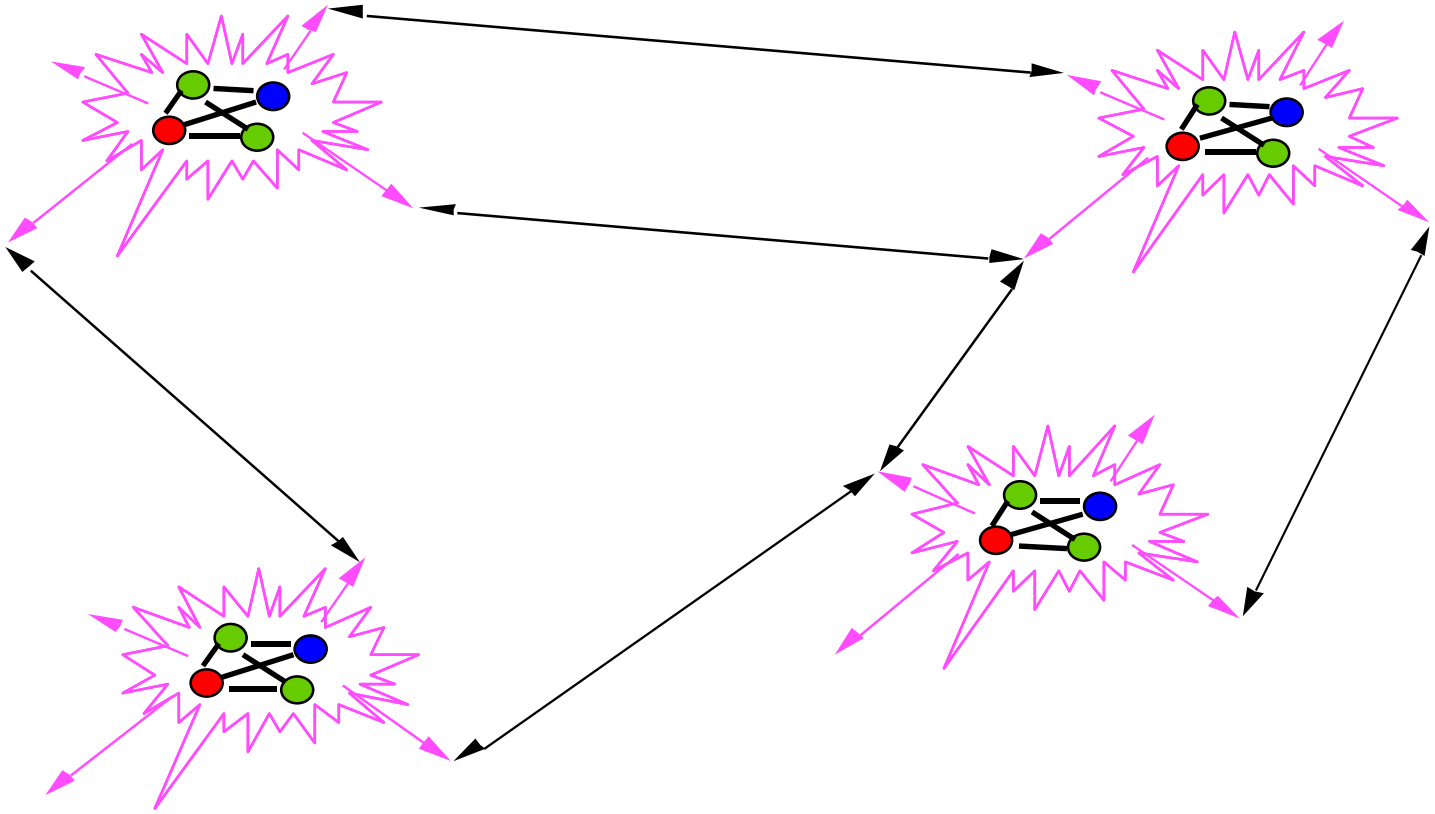


* COMPETENT
* MOTIVATED
* COMPETITIVE
* PROTECTIVE
* FOCUSSED

– – – – – – – – – – – – –

PRESUME INFRASTRUCTURE WILL BE AVAILABLE

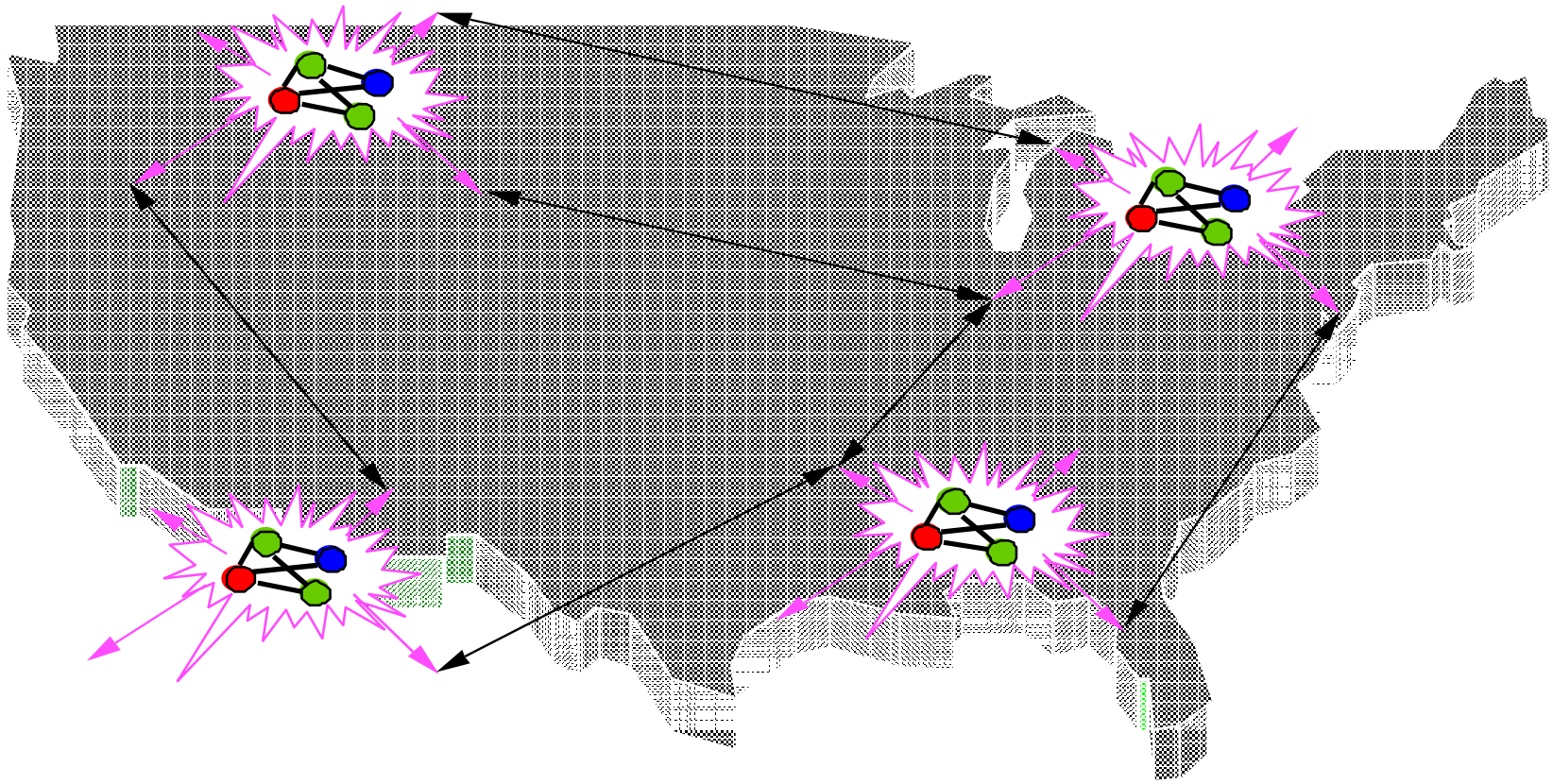
ASSUMPTIONS -- INTERCONNECTIONS



* PROLIFERATING
* REVOLUTIONARY
* COMPLICATED

NO PROPONENT

ASSUMPTIONS -- FRAMEWORK



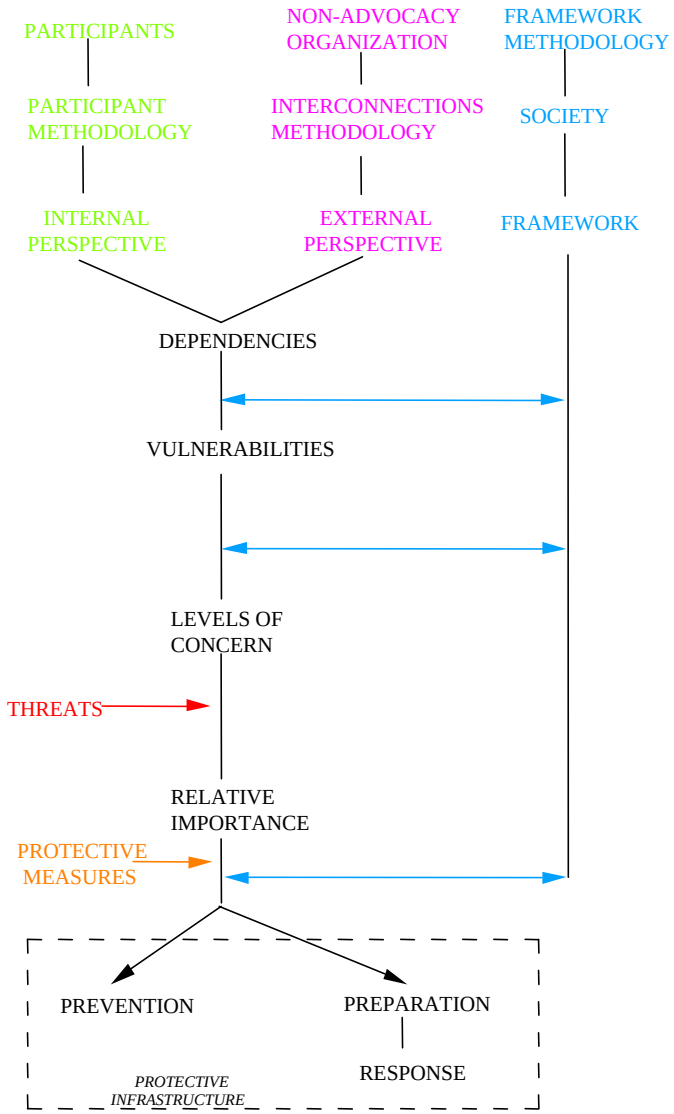
* UNPRECEDENTED CIRCUMSTANCES
* GROWING DIVERSITY OF PERSPECTIVES
* INCREASING INTERDEPENDENCE

– – – APPROPRIATE STRUCTURE NOT OBVIOUS

METHODOLOGY -- OVERALL

- IDENTIFY PARTICIPANTS
- ASSESS INTERCONNECTIONS
  - DETERMINE INTERDEPENDENCIES
  - HIGHLIGHT VULNERABILITIES
  - OVERLAY THREATS
  - ORDER RELATIVE LEVELS OF IMPORTANCE
  - SUGGEST, EVALUATE, PRIORITIZE PROTECTIVE MEASURES
- EVOLVE FRAMEWORK
- IMPLEMENT PROTECTIVE INFRASTRUCTURE

METHODOLOGY -- OVERALL



DONALD M. Le VINE
TRW, INC
ONE FEDERAL SYSTEMS PARK DRIVE
FAIRFAX, VA 22033
703/968-2539
DONALD.M.LEVINE@TRW.COM

Critical Infrastructure Protection and Privacy: *What's the Deal?*

(a post-PCCIP perspective)

22nd National Information Systems Security Conference
Arlington, Virginia
October 21, 1999

Stevan D. Mitchell
Trial Attorney, U.S. Department of Justice
Former Member, President's Commission on Critical Infrastructure Protection
(202) 514-1026, stevan.mitchell@usdoj.gov

President's Commission on Critical Infrastructure Protection

- ✓ PCCIP Report: *Critical Foundations* (1997)
- ✓ Recognized increasing risk to critical infrastructures; physical and "cyber"
  - increased dependency, vulnerability, *inter*dependency
- ✓ Recommended modest "starter" measures
  - Partnership to perform shared functions
    - information sharing; public and private
    - shared policy formulation
  - Enhance government's ability to prevent, respond
  - Enhance private sector's ability to manage risk

Electronic Privacy Information Center

- **EPIC Report: *Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructure Protection* (Nov. 1998)**
  - **“These proposals are more of a threat to our system of ordered liberty than any single attack on our infrastructure could ever be."**
  - **"Openness, not secrecy, remains the key to a nation's security and its future prosperity."**

PCCIP's "Privacy Commissioner"

- ✓ PCCIP, Department of Justice concerned about privacy implications from the outset
  - Commissioners included 1 representative from each of 10 federal agencies
  - Each also hired additional representative from outside federal government
- ✓ DOJ recruited privacy, consumer protection specialist as full time Commissioner
  - Respected by, maintained contact with privacy and consumer communities
  - Saw that recommendations could be implemented in "privacy neutral" ways

Employee Privacy

- (EPIC Report, p. 20) [Commission recommended Fed. & state laws be amended to] “balance employers' needs against individual interests in privacy.'"
- Called recommendation "frightening" b/c companies increasingly monitor employee communications
  - *Macworld* survey: 22 % of large companies engage in searches of employee computer files, voice mail, e-mail, etc.
  - Only 1/3 informed employees that surveillance was occurring
- (PCCIP Report, p. 87) “Attorney General convene … professionals … from law … labor … management … and the privacy community to explore existing laws and recommend measures to balance employers’ needs against individual interests in privacy.”

Polygraph Protection Act

- (EPIC Report, p. 21) PCCIP recommended "Congress amend the Employee Polygraph Protection Act to include information security personnel in the category of professions which can be required to be subjected to polygraph tests"
- PCCIP recommended that existing exemption in law and Department of Labor regulations be extended to include certain information security personnel
  - Exemption allows employers whose employees provide physical security services to public utilities (armored car services, alarm installation) to polygraph *own employees* under strict rules and restrictions
- Why shouldn't federal law treat firewall installers the same as burglar alarm installers?

Information Sharing

- ✓ **(EPIC Report, Preface): "The critical thrust of the PCCIP effort [is to] extend the reach of law enforcement, to limit the means of governmental accountability, and to transfer more authority to the world of classification and secrecy…. Openness, not secrecy, remains the key to a nation's security and its future prosperity"**
- ✓ **(PCCIP Report, Executive Summary): "Because it may be impossible to determine the nature of the threat until after it has materialized, [private sector] owners and operators … must focus on protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about those tools and their employment. This cooperation implies a more intimate level of mutual communication, accommodation and support than has characterized public-private sector relations in the past"**

Legal Impediments to Information Sharing

- Conclusions derived from PCCIP outreach: Public meetings in 5 U.S. cities; conferences, seminars, simulations; approximately 6000 contacts
- (PCCIP Report, p. 21): "Information sharing is the most immediate need."
- (PCCIP Report, p. 31) "We envision the creation of a trusted environment that would allow the government and the private sector to share sensitive information openly and voluntarily. Success will depend on the ability to protect as well as disseminate needed information. We propose altering several legal provisions that appear to inhibit protection and thus discourage participation"

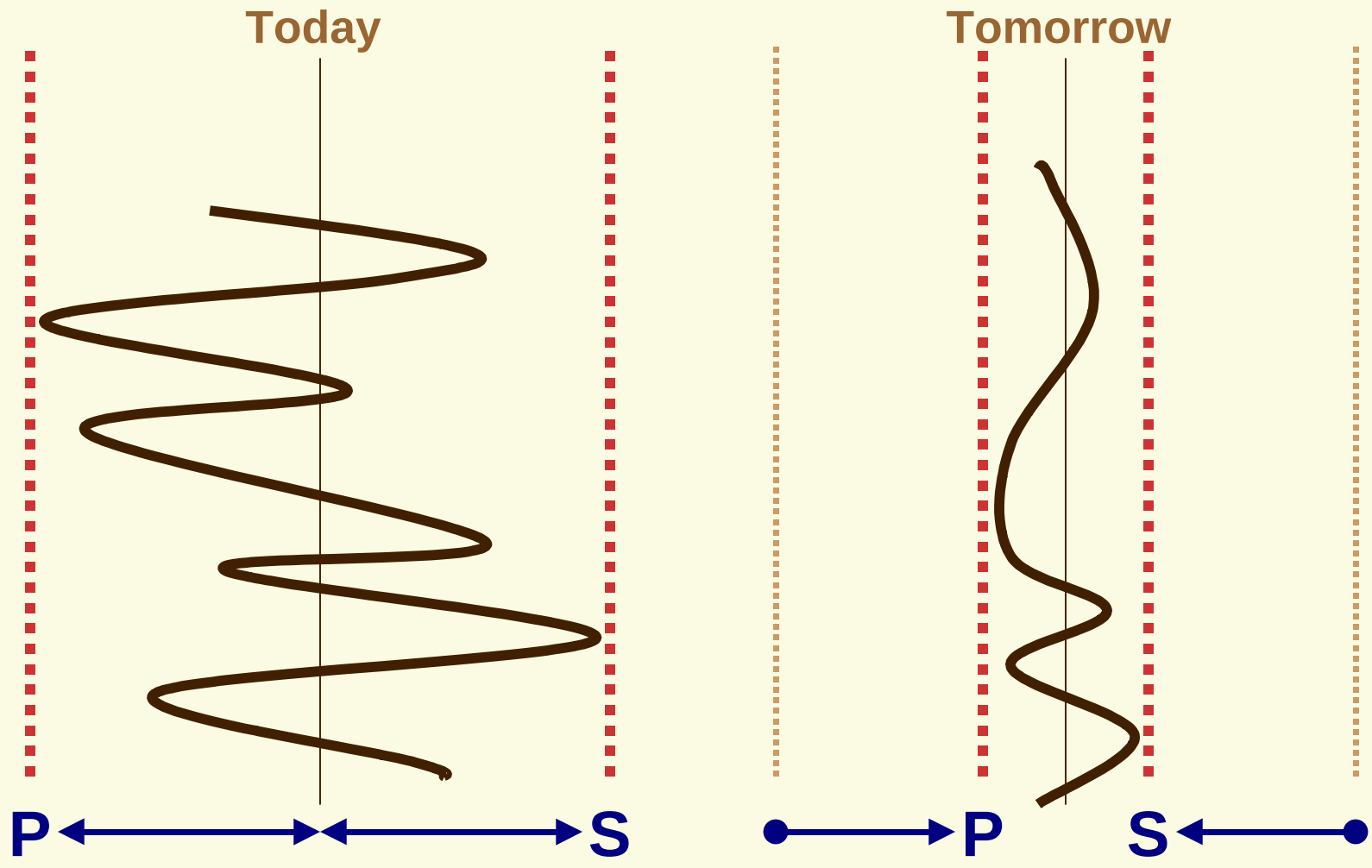
Legal Impediments to Information Sharing

- ✓ **Create trusted environment for information sharing that addresses legal impediments:**
  - **Antitrust -** The Department of Justice should "offer limited assurances ... that participation in information sharing processes will not run afoul of antitrust laws" and consider issuing guidelines (PCCIP Report, p. 32)
  - **Liability -** Federal government should "undertake a detailed study of liability issues surrounding participation in an information sharing process" (PCCIP Report, p. 32)
  - **National security -** NSC should study whether to standardize guidelines for sharing infrastructure assurance information with foreign corporations (PCCIP Report, p. 33)

Legal Impediments to Information Sharing

- **Proprietary information** - information-sharing activities should "require appropriate protection of information containing trade secrets or other … proprietary information" (PCCIP Report, p. 32)
- **Access to government information** - "Potential participants in an information sharing mechanism may require assurances that their sensitive information will remain confidential if shared with the federal government." Appropriate protection "may require inclusion of a b(3) FOIA exemption in enabling legislation." (PCCIP Report, p. 31)
- **State and local participation** - "We recommend a study group identify legal impediments to information sharing at the state level, propose solutions, and draft model legislation." (PCCIP Report, p. 33)

Privacy/security continuum



More??

- **www.pccip.gov/whatsnew.html**
  - *Legal Foundations*: 14 supplemental reports on legal recommendations:
  - Posted to PCCIP website on December 2, 1998
- **Ask me**:

Stevan D. Mitchell

U.S. Department of Justice

Computer Crime and Intellectual Property Section

(202) 514-1026

stevan.mitchell@usdoj.gov