COMPLEXITY
and
Critical Infrastructure Vulnerabilities

Workshop I

Sponsored by:

The Cyber Conflict Studies Association
And
The Center for Technology and National Security Policy
National Defense University

Marie Stella, CISSP

June 2004
The Center for Technology and National Security Policy
The National Defense University

Opinions, conclusions, and recommendations expressed or implied within are solely those of the contributors and do not necessarily represent the views of the Department of Defense or any other agency of the Federal Government. Cleared for public release; distribution unlimited.

Portions of this book may be quoted or reprinted without permission, provided that a standard source credit line is used.

Table of Contents

Preface
Workshop Proceedings 3
Outcome of Workshop 3

Section I: Workshop Background
Introduction and Background 6
Workshop Series Objectives 8

Section II: Workshop I Concept, Goal, and Methodology
Concept 9
Goal 9
Methodology 9
The Champions 9
The Presenters 9
The Participants 11

Section III: Summary of Workshop Activities
Welcoming Remarks 12
Introduction of CCSA Objectives 13
The Ground Rules 13
Implication of Complexity on Shared Infrastructure 14
Power Grid Interconnectivity, Failures, and Regulatory Interaction 15
Impact of Sound Security Practices on Mitigating Risks from Cyber Attacks 17
A Machine Dominated Future? 20
Cascading Effects and Ubiquitous Use of Common Platforms and Protocols 22
Challenges for Securing Shared Infrastructure Against Large-Scale Cyber Attack 24
Closing remarks 25

Appendix A
Workshop Agenda 26
Attendee List 27

Appendix B (available online)
Presentation of Dr. Dejan Sobajic
Presentation of Dr. Daniel Geer

Acknowledgements

The author would like to thank the following persons who served as rapporteurs for the conference. This document is a direct result of their knowledge, understanding of complex issues, careful and unbiased capture of information, and a willingness to volunteer their time and talents to support this critical effort.

Terry Baker, Northrop Grumman Information Systems, TASC
Kyle Dunn, Potomac Institute for Public Policy
Lillian "Nicole" Noland, Northrop Grumman Information Systems, TASC
Theodore Signore, MITRE Corporation, Center for Advanced Aviation System Development

A special thanks goes to Michael Schrage, whose provocative and innovative techniques and superb knowledge of the issues, were the primary reasons for the success of the workshop.

Preface

Workshop Proceedings: The report summarizes the proceedings of the Complexity and Critical Infrastructure Vulnerabilities Workshop, held December 8, 2003, at the National Defense University (NDU), Fort Lesley J. McNair, Washington, D.C. This was the first in a planned series that will address complexity and its impact on critical infrastructure protection. The Cyber Conflict Studies Association (CCSA) and the Center for Technology and National Security Policy (CTNSP) at the National Defense University sponsored the workshops. This workshop is the first in a series of five.

The CCSA is a not-for-profit association of professionals from government, private industry, and academia, who want to promote education, research, and dialogue in the area of cyber conflict. The goals of this workshop were to educate and network and to identify issues centered on critical infrastructure protection and cyber defense that require further study.

Outcome of Workshop: Panelists and participants made recommendations in five categories:

Policy—must be resolved as a national mandate requiring action from senior leaders in national security and homeland defense

> Develop appropriate response decision-making approaches and options in the event of cyber attacks
>
> Pursue international agreements that address monitoring and isolating for cyber attacks and follow-on actions such as forensics and legal action
>
> Ensure developers and users are responsible for production and implementing of vulnerability more secure information and communications technologies
>
> Address the growing automation in the development of software code and other information technologies that limits the ability of governments or anyone else to understand how it functions
>
> Develop mechanisms for orchestrating joint government and private entities funding necessary to implement more effective cyber defense policies

Strategy—affects national planning, protection, or oversight activities

> Develop a National Cyber Red Team and strong command and control functions for Cyber Conflict. Teaming efforts should include collaborative, inter-disciplinary decision makers and members

Develop a national program, to address behaviors of complex systems and responses to serious attacks

Incorporate cyber experts in task forces and other groups addressing physical security

Develop a national capability to assure the functionality and security of code produced by whatever means

Tactics—affects operation and management of infrastructure

Develop a methodology and technology approaches to assess that when critical infrastructure(s) is (are) under cyber attack

Promote operations security strategies that include: diversity of layering, patch management; system partitioning; and other protection techniques

Research—requires further study and funding

Studies in the applications of traffic analysis and other techniques to identify internal and external threats and threat agents

Studies to understand emergent behavior and vulnerabilities of complex critical infrastructures such as the electric grid

Technical studies (and prototype development) in adaptive and self-healing systems, and other work that supports the concept of "functioning while injured"

Development of economic and risk modeling as it applies to cyber security

Studies in the behaviors of complex systems, including models from other disciplines such as the study of thermodynamics and naturally occurring robust networks

Study the implications of loss of human oversight and governmental control over automated code development and deployment within cyberspace

Education—requires a better understanding of complexity and critical infrastructure protection

Formalize and implement an educational effort to develop expertise to jointly study the area of complexity and critical infrastructure vulnerabilities/cyber defense

Establishment of programs in information security domain expertise within other critical infrastructures such as electric power

Continuous and improved Cyber conflict practitioner training that takes into account emergent social and technical issues of complex systems

Complexity and Critical Infrastructure awareness programs for public, legislatures, and other stakeholders involved in the complexity and critical infrastructure discussion

Summaries of the presentations and associated dialogue that provided the basis for these recommendations can be found in Section II.

Section I

Workshop Background

Introduction and Background: About one year ago, the Cyber Conflict Studies Association (CCSA) was formed by a group of senior cyber defense colleagues representing industry, government, and academia. The driving force behind the CCSA was recognition that the shared military/civilian infrastructure, by virtue of its complexity, interconnectivity, and reliance on information technology (IT), is becoming increasingly vulnerable to large-scale cyber attacks. Cyber tools capable of disrupting networks are not difficult to obtain, and most experts recognize that cyber conflict is the work not only of script kiddies, hackers, and hostile nation-states, but also of non-state/transnational actors, who may operate in conjunction with other forces such as organized crime. The objectives of these new threat agents may not only be web defacements, embarrassment, fraud, and business related espionage, but also political disinformation, economic and communication chaos, and disruption of military and homeland defense operations.

The impact of cyber conflicts on our complex infrastructure is unpredictable, in part because of a lack of good analytical tools and models. Enterprise designs, highly interactive mobile code, and critical reliance on network centric communications are relatively new phenomena, and their development objectives are innovation, performance, and profit, not cyber security. The nation's approach to infrastructure and information protection has focused on the physical protection of resources. Security is usually limited to redundancy of systems, backup of data drives, or some other hardware-specific solution. The cost of protecting human life and the value of structures and equipment are linked to well-established processes; risk analysis, insurance values, and manufacturing techniques that managers, engineers, financiers, and policy makers know and understand. Quantifying the costs of loss, disruption, and changes to information carried by the infrastructure is a much more abstract activity. Government efforts to foster a better understanding of cyber networks that are owned mostly by private entities were pushed into the background as a result of the September 11th attacks on the World Trade Center and the Pentagon. Since then, the emphasis has been on protecting and screening physical assets or personnel, and cyber policy has reverted to concentrating on intelligence collection, attack identification, and protecting against known vulnerabilities. In an environment where the nation's military, government, and private sector openly tout their dependence on network centric enterprises, the risks of cyber warfare must be addressed from a futuristic perspective.

To fill this apparent void, the CCSA determined that a cyber conflict framework must be established that defines and bounds the problem and assesses how serious cyber conflict could be as a coercive factor. The CCSA proposes creation of a workspace for a social-technical dialogue that addresses, at a minimum, the following questions:

- How do we define cyber conflict, and do its descriptive boundaries change situationally, depending on the adversary?
- Does cyber conflict constitute a significant form of coercive power?
- What large-scale effects can be achieved through cyber attacks?
- What factors (policies, technologies, etc.) will govern the capacity of a state or organization to deter cyber attacks?
- What thresholds for response to or use of cyber attacks might be established?
- How can states and organizations establish the most effective defenses, and how will these defenses interact with other coercive means, particularly economic and military power?
- How will establishing cyber conflict defense postures impact privacy and civil liberties?
- How should national policy and military doctrine be changed to reflect cyber conflict concerns?
- What international agreements are needed to ensure protection against interdiction and punishment of cyber attacks, while respecting the sovereignty of nation-states?

Addressing cyber conflict issues is a formidable task. It is unclear whether traditional, linear problem solving and domain-centered techniques can adequately address these complex and interconnected issues. An interdisciplinary approach is needed to understand the likely technical, operational, economic, and social impact of a cyber attack on critical, shared infrastructures. One CCSA goal is to understand and foster the establishment of effective teams and their methodologies. This requires education of leaders in the field of cyber conflict and development of metrics of the effectiveness of cyber studies. These metrics will provide the analytic data necessary to influence policy and research and product development.

The concept for the complexity workshop series was formed jointly by the CCSA and CTNSP. CTNSP has been addressing issues of information assurance as they relate to military transformation and homeland infrastructure protection and saw workshops on cyber conflict as a means to improve understanding and establish a dialogue on cyber security. The workshop leads were Col (S) Gregory Rattray, Ph.D., a founding member of the CCSA, and Marie Stella, a CCSA member and Federal Aviation Administration employee on detail to CTNSP to address cyber security issues. Mr. Michael Schrage, co-director of the MIT Media Lab's E€Markets initiative, also volunteered his time to help plan and moderate the workshops. Schrage has written and consulted extensively on the design and diffusion of digital technology and its effects on business relationships. His expertise in developing collaborative workspace and his ongoing work on the role of prototypes, simulations, and games as media for innovation, were critical to the success of the workshop effort to date.

Workshop Series Objectives: A series of workshops covering the following topics is envisaged:

I—Begin the Dialogue: to bring diverse communities together and introduce concepts and challenges of complexity and its impact on emergent issues and infrastructure vulnerabilities

II – Engage: to deepen the understanding and dialogue between the cyber defense community and developers of cyber defense applications to improve understanding of how to conduct cyber defense in complex, unpredictable environments and gain an understanding of policy needs in this area

III – Visualize: to examine approaches to visualizing complex systems, interactions of constituent parts, and how systems change with an eye to utilizing these methods within the cyber defense community. This work will add to the dialogue on technology, organizational design, and policy in the area of cyber defense

IV—Design: to examine design concepts for organizations and applications to manage missions involving complex systems and their applicability to cyber defense

V—Formulate: to review current policy constructs for cyber defense and make recommendation on national cyber defense policy

Section II

Workshop I Concept, Goal, and Methodology

Concept: The first workshop introduced the national security community to numerous issues related to protection of the infrastructure.

Goal: The aim was to raise awareness of emergent critical vulnerabilities that result from the complexity of highly interconnected, networked, and shared infrastructures.

Methodology: The workshop brought together practitioners from industry and government to discuss their perspectives on critical infrastructure protection and to lead a dialogue with participants on the concepts presented. The approach, promoted by the moderator Michael Schrage, was to create participatory panels of peer partnership between participants and speakers. This "360" learning process creates an environment in which issues and ideas flow freely. The challenge posed to presenters was to articulate their perspectives on confronting complexity and identify the two most critical issues. They were asked to link their perspectives to specific recommendations for next steps, such as areas needing further study, proposed technical or regulatory fixes, an awareness program, or a design principle that the workshop audience could use as a basis for further discussion and argument.

The presenters were asked to provide an understandable technical definition of complexity and use it to illuminate a broader discussion of the policy choices and economic trade-offs confronting public- and private sector infrastructure management. This needed to be communicated in no more than twelve minutes to allow time for audience interaction.

The presenters were asked to structure their talks to invite provocative questions and evoke constructive interactions on methods to apply complexity theory to technology adoption, organizational design, and policy.

Ultimately, the success of the workshop was predicated on the support, commitment, and collaboration of three groups: the champions, the presenters, and the participants.

The Champions: The workshop could not have happened without the support of both the Cyber Conflict Studies Association and the National Defense University. Mr. John Casciano, Maj Gen (Ret), CCSA President, provided constant support and suggestions to the workshop subcommittee. Lt Gen Michael Dunn, President of NDU, not only was instrumental in supporting CTNSP involvement in this effort, but added his own thoughts contributions on complexity and suggested follow-on activities.

The Presenters: In his welcoming remarks, Lt Gen Dunn addressed complexity and cyber conflict as they relate to civilian and military infrastructure and gave his perspective on the way ahead. The workshop leads asked Dr. Harold Morowitz, a

Robinson Professor in Biology and Natural Philosophy at George Mason University's Krasnow Institute for Advance Studies, to set the stage with a breakfast keynote address discussing the "Implication of Complexity on Shared Infrastructures." Morowitz is the author of numerous books, the former Editor-in-Chief of the journal *Complexity*, and a founding member of the Sante Fe Institute. An established authority in the area of biological networks, Morowitz is currently investigating the interface of biology and information sciences. A panel led by Dr. Dejan (Dan) Sobajic and Mr. Alan Paller followed Morowitz's talk. Sobajic, Director of Grid Reliability and Power Markets at the Electric Power Research Institute (EPRI), spoke on "Power Grid Interconnectivity, Failures and Regulatory Interaction." World-renowned in the area of neural networks, Sobajic is currently addressing reliability and security issues in the power grid and research into self-healing networks and smart grids. Mr. Paller, as Director of Research for the SANS Institute, oversees research on the top twenty Internet security threats, step-by-step security guides, and the SANS digests. Founder of the CIO Institute and Director of the Internet Storm Center, Paller led a discussion on the "Impact of Sound Security Practices on Mitigating Risks from Cyber Attacks."

Mr. Richard Clarke, founder and president of Good Harbor Consulting, presented the keynote luncheon talk entitled, "A Machine Dominated Future." Clarke is the former National Coordinator for Security Infrastructure Protection and Counter Terrorism at the National Security Council. In this role, he led U.S. government efforts on counter terrorism, cyber security, continuity of operations, domestic preparedness for weapons of mass destruction, and international organized crime. Mr. Clarke served in various leadership positions under Presidents Ronald W. Reagan, George H. W. Bush, William J. Clinton, and George W. Bush. The afternoon sessions included presentations by Dr. Daniel Geer and Dr. Gregory J. Rattray. Geer, with over twenty-five years of experience in computer science and information security, is a Principal of Geer Risk Services. Geer's former positions included leadership and technical positions at @Stake, MIT's Project Athena, and the Health Sciences Computer Facility at Harvard University. Dr. Geer has published in *RISK Digest* and *Wired Magazine* as well as well-known professional journals, and is co-author of the *Web Security Sourcebook*.[1] Geer led a panel on the "Cascading Effects and Ubiquitous Use of Common Platforms and Protocols." The second panelist Col (S) Gregory Rattray, is the Director for Cyberspace Security, Office of Defense Policy and Arms Control of the National Security Council. Rattray is responsible to the Assistant to the President for National Security Affairs for development and implementation of U.S. policy related to cyberspace security and telecommunications. Rattray was formerly the Deputy Director for Defensive Information Warfare on the Headquarters Air Force staff and has had numerous assignments in intelligence and information operations. He is the author of *Strategic Warfare in Cyberspace*.[2] Rattray led a discussion on "Challenges for Securing Shared Infrastructure against Large Scale Cyber Attack."

---

1 Aviel D. Rubin, Dan Geer, and Marcus J. Ranum, *Web Security Sourcebook: A Complete Guide to Web Security* (John Wiley & Sons, 1999)

2 Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001)

The Participants: To implement the participatory panel concept, invitations to the workshop were extended to members of the cyber defense community who have roles in researching, establishing, operating, and making policy to guide the development of our nation's cyber defense capabilities. The participants included representatives from government, the private sector, and academe. (A copy of the workshop agenda and a list of workshop participants can be found at Appendix A.)

Section III

Summary of Workshop Discussions

Welcoming Remarks: Lt Gen Dunn began his welcoming remarks by emphasized the importance of the CCSA effort. Dunn noted that securing the interconnected military information technology (IT) systems that form the framework of military transformation has long been of vital importance to him. Government reform and downsizing has encouraged greater partnerships with industry and Dunn expressed his concern over the lack of understanding of the complexity of our shared infrastructure, in terms of both design and interconnectivity. Dunn pointed out that adoption of commercially used protocols, such as Internet Protocol (IP), windows platforms, and, where economically viable, using commercial networking and communication components to meet the military mission all introduce risk to these systems and, thus, to our national and homeland defense.

Drawing on his vast experience in this area, Dunn spoke of his participation in the 1997 DOD Eligible Receiver exercise focused on cyber defense. At that time, the United States did not realize how unprepared for cyber conflict we were. The U.S. government had few policies in place regarding cyber attacks then and that this problem persists. For example, there is no policy that helps determine when to categorize a cyber attack as an act of war. The United States still has few systems to detect cyber attacks. America's role in pre-emptive or defensive cyber warfare, especially as it applies to use of this shared infrastructure, is a subject of much debate as we evaluate defense and privacy issues in these challenging times. He emphasized the need for a national red team effort to address cyber conflict/defense and preparedness.

We live in a connected world and Dunn believes systems are vulnerable based on how much we use them and how critical they are. Cyber conflict is a very complex area without many experts. One of the reasons he was so supportive of the CCSA effort is that it gives NDU the opportunity to help educate civilian and military leaders on the subject and to encourage further study and work in this area. Dunn advised that the four pieces to cyber defense that should be addressed are technology, organization, policy, and law and hopes that the CCSA efforts will be instrumental in supporting that effort.

The discussion addressed concerns about the applicability of commercial off the shelf (COTS) products to DOD, especially products developed overseas. The assumption being that such products pose a greater risk of back-door installation of Trojan horses and time bombs. The attendees noted that vulnerability is a function of the inter-dependence of the systems involved. It was agreed that the current U.S. cyber policy is one of risk management, rather than anticipatory or preventive solutions.

Lt Gen Dunn left the audience with the following recommendations:

- A coherent national framework that addresses cyber conflict from a policy, legal, organizational and technical perspective must be developed
- An educational effort to develop experts in the area of complexity and critical infrastructure vulnerability issues must be formalized
- The methodology and technology to "identify when we are under attack" must be developed
- A strong command and control (C2) is needed to combat cyber attacks
- A National Red Team for Cyber Conflict issues should be established
- A policy that determines America's reaction to cyber attacks and our role in pre-emptive or defensive cyber warfare is needed

Introduction of CCSA Objectives: John Casciano, President of the CCSA, advised the audience that the CCSA was a recently-established professional association designed to support active research in the field of cyber conflict. The CCSA sponsors studies in ethics, morality, law, policy, strategy, tactics, and technologies and is seeking to increase membership and sponsors. Casciano briefly touched on the objectives and workshop agenda and that the workshop activities were a follow on to the initial CCSA conference held at the Massachusetts Institute of Technology (MIT) in the spring of 2003. Pointing out that the problems Lt Gen Dunn mentioned are real, Casciano noted that eighty to ninety percent of the critical infrastructures are owned by the private sector, and the nation needs to explore methods to improve the private/public relationship in cyber conflict and defense. Casciano suggested that the dialogue could begin around protecting the nation's economic security, which was the real potential impact of cyber attacks on the nation.

Casciano left the audience with the following recommendations:

- A private/public policy and techniques to jointly protect the infrastructure must be developed
- A dialogue must be established around the viability of the nation's economic security under cyber attack

The Ground Rules: The moderator, Michael Schrage, who played a vital role in establishing a collaborative workspace throughout the day, encouraged the participants to engage in collaborative interaction by engaging in an open if not confrontational dialogue to identify important issues quickly. Schrage pointed out that critical infrastructure protection is inherently a complex and multi-disciplinary issue and reminded the audience that the workshop goal was to produce products that would be useful to decision makers.

Schrage challenged the participants to fame their dialogue around the following questions:

- What kinds of resource will complexity provide in resolving cyber conflict issues, what will its currency be in government, and where will it be most useful in application?
- What insights from complexity can be used to support better understanding of infrastructure vulnerability?

Implication of Complexity for Shared Infrastructure: Dr. Harold Morowitz addressed the issue of whether our knowledge of biology and biochemistry was useful in protecting the critical infrastructure. Morowitz began his talk by presenting a chart of intermediary metabolism. The chart represents all known reactions among small molecules, which occur in most organisms. There are 20 million species with multiple metabolisms. These primary metabolisms are made of 300 - 400 molecules that build organisms. Focusing on the core or primary metabolism processes, Dr. Morowitz talked about the extraordinary degree of robustness of the metabolic process, universal to all organisms, that traces back 3 ½ to 4 billion years. Morowitz discussed how large changes in the environment of an organism do not adversely affect the metabolism of the organism. As an example of this robustness, he noted that bacteria are able to reproduce within a large temperature range and even when solvents replace a large percentage of their aqueous environment. Morowitz advised that two primary approaches to studying the network properties of metabolism exist. Most studies have focused on the topology of the networks, whereas studies on robustness focus on thermodynamics such as reaction rates, enzyme substrate binding, and other physical chemical features. He drew an analogy from the biological network topology approach to that of the topology of scale-free networks and the Kirchoff's law representing classical electrical networks and suggested that topology features are analogous to the Internet.

Morowitz suggests that thermodynamic features of biological networks, however, may provide a closer analog to infrastructures, which depend on mass, energy and information transfer. Metabolic networks have a core and that all reactive pathways, including the citric acid and the reductive citric acid cycle, have termini in that core. He compares this to the primary production in an economic network, where every innovation at the hierarchical level above the core is selected by its ability to reinforce the core. Morowitz talks about the multiple emergences that occur with these interactions, such as products that lead to catalytic reactions or products that result in new structures such as membranes that, in turn, lead to compartmentalization. He suggested that emergent properties of infrastructures be examined by studying the emergent properties of biochemical networks and that interdisciplinary activities between theoretical biologist and infrastructure stability experts might prove useful.

The workshop participants explored the analogy between biological network and an electric network. It was noted that a biological network has at is core the transfer of mass, energy, and information similar to infrastructure with one difference, a core property of information networks was independent agents (people). It was proposed that this feature

negates any analogy to biology. Morowitz suggested that a solution might lie in building networks to minimize the influence and actions of people and suggested this might be a path for emergent studies. A discussion followed of how the ability to control selection within networks applies to the infrastructure. Again, Morowitz pointed out the need for further study. It was noted that the biological infrastructure has existed for 3½ billion years without failure and, if possible, would be a "perfect model" for any cyber infrastructure to be built upon.

A question was posed regarding who was building software packages to emulate biological networks. Although no company came to mind, this is an area that needs further investigation. Another question was posed about how lessons from the robustness of biological metabolism and processes could be applied to information and communications infrastructures. While no conclusions were reached, group agreed this was an area warranting further study.

Morowitz left the audience with the following recommendations:

- Emergent properties of infrastructures be examined by studying the thermodynamics and emergent properties of biochemical networks
- Interdisciplinary activities between theoretical biologist and infrastructure stability experts be established
- Further studies were need regarding core differences between biological and infrastructure networks to understand role and control of non-predictive behavior

Power Grid Interconnectivity, Failures, and Regulatory Interaction: Dr. Dejan Sobajic, Director of Grid Reliability and Power Markets at the Electric Power Research Institute (EPRI), started his talk with the provocative statement that the power grid system the largest man made machine ever built. This system has been in existence for over 100 years and is composed of thousands of elements that are interconnected to 2, 3, or 4 other elements in a one to few model. The outcome of a compromise against a system's vulnerability, especially if it has a cascading effect, is an outage – simply put - the machine goes down and service is interrupted. Sobajic pointed out that the cause of these outages varies. Some are nature driven (exposure to elements – lightning, wind, rain) and others are manmade (operator error, manmade interruption).

According to Sobajic, vulnerabilities are designed into the current system. The behavior of Transmission Networks, categorized as large, non-linear, uncertain, and time dependent, is not fully understood. Additionally, the diversity of equipment installed from various international vendors often present major maintenance problems. New types of transformers are needed that can adapt or be easily repaired instead of the current scenario where spares and appropriate maintenance skills are needed for every system. Most new power grid systems receive upgrades through modem dial up, and the systems, especially those used for monitoring and control, rely heavily on the Internet. These dial-up and Internet connections introduce much vulnerability into the system and present a

target for attacks. The speed at which network attacks occur makes this a very high risk, according to Sobajic.

The power grid is a very dynamic system. Failures in the grid result from cascading events where weaknesses combine to make the system more vulnerable to unforeseen problems. Sobajic points out that light loads masks problems in the power grid. At full capacity more problems are evident and the system behaves differently than at lower capacity. He attributes this to the lack of understanding of the power grid and its complex behavior. For this same reason, Sobajic states that once vulnerabilities start to cascade, there is little intervention that can take place. Sobajic categorizes the sequences of cascading events into the following three phases:

- The Sequential Phase – Problem goes unnoticed early on, it allows for progressive weakening of the grid
- The Transition phase – Failures speed up and grid is out of balance
- The Parallel and Terminal phase – Performance failures are obvious, it is too late for human interaction and there is a loss of supply.

Sobajic reminded the participants that the existing transmission machine was not designed for today's use. The grid must absorb all energy generated or the system experiences problems. To address cascading events, Dr. Sobajic notes the following much needed requirements for avoidance:

- Development and installation of early warning systems
- Better system designs (marketing efficiency vs. failure resistance)
- Improved control and mitigation.

On preventing cascades, he recommends improved transition scheduling, near time system operations, and protection relaying.

EPRI is taking positive steps to address these problems. EPRI began an infrastructure security initiative in 2001. Techniques such as immediate replacement of failed transformers are being explored. Transformers link regional grids and their reliability are important to the system. Unfortunately, Sobajik points out, the lack of commonality in transformer equipment makes quick replacement difficult. Industry has also response to electric grid vulnerabilities by partnering in the following joint efforts:

- DOD/EPRI complex interactive networks/systems initiative (1998-2001)
- EPRI reliability initiative (1999-2002)
- EPRI infrastructure security initiative (2001-)
- DHS/EPRI/NERC North American Electricity Infrastructure Security Monitoring System

Sobajic discussed his concerns regarding the lack of qualified power engineers and advised that many programs for this discipline have been dropped from universities. He works closely with universities' power engineering programs to help initiate new

concepts for thinking about the infrastructure problems. Thinking in terms of machines is how power engineers are trained. Sobajic asked the question, "If one cannot avoid the event, can one control an event after is has started?" He questions whether a structured, power engineering discipline-method to resolving this problem will work. New approaches to resolving the power infrastructure network vulnerabilities are essential because the current process of thinking about the network as a set of machines can't continue and is only masking problems. Countermeasures aimed at preventing cascading events have not been effective and at some point the system must be capable of absorbing natural phenomena and adjusting/adapting while under attack. Sobajic proposed to the participants that out-of-the-box thinking, such as looking at biological models, might be necessary.

The workshop participants explored several concepts regarding power infrastructure protection with Sobajic. The question was asked if cascading events might be avoided by design. Sobajic stated that market efficiencies make this difficult as it is at odds with implementing failure resistance. Market driven systems are inherently steady state, are more difficult to control and thus more susceptible to unplanned events. To date, this approach has not been successful in the power grid operation. The lack of research in this area was a topic of interest and Sobajic concluded the discussion by stating that funding in R&D for the power industry has been decreasing and that collaborative research with other infrastructures domains may provide an economy of scale, but even more so, establish a dialogue with policy makers about complexity of systems and the need to support research. He notes the most complex systems equal the most dangerous systems and posed the question, "Can a system threaten you even if you are capable of understanding it?"

Sobajic left the audience with the following recommendations:

- Research needs to be performed in understanding the behavior of complex systems, especially the power grid
- Funding of research is essential to understand the network and cascading events. Multi-discipline collaboration should be investigated
- Shift thinking about the power grid as a machine to that of a network, and increased education and training in power grid design and maintenance

Impact of Sound Security Practices on Mitigating Risks from Cyber Attacks: Mr. Alan Paller, Director of Research for the SANS Institute, began his presentation by posing the following questions:

- What are the elements of the problem in cyber security?
- Where does heterogeneity fit?

To help participants in addressing those questions, Paller talked about the current status of worms, viruses, and other attacks against the Internet and IT systems. The problem was framed by providing the following data about recent attacks:

The Slammer worm (Jan. 25, 2003) was the most destructive worm to date. It was the fastest computer worm in history and infected more than ninety percent of vulnerable hosts in 10 minutes; it was 100 times faster than code red. This worm proved to many Chief Information Officers (CIOs) that systems thought to be immune to Internet attacks were indeed interconnected when it brought down a range of systems including the Seattle 911 system, Bank of America ATMs, and Continental Airlines routing information system. (The worm spread via Microsoft SQL Servers that exploited MS/SQL server's vulnerabilities.)

The Slapper Worm (Sept.13-17, 2002) took over 29,000 LINUX machines. (Linux Slapper Worm is a family of worms that use an Open SSL buffer overflow exploits to run a shell on a remote computer.) Seven days later, on Sept. 20, 2002, 330 Slapper victim systems attacked the U.S. intelligence agency web site.

Paller proposed that one aspect of the success of the Slammer worm is that technologists "lied" to their management and indicated that their systems were not susceptible, i.e., not directly connected to the Internet. Interestingly, Paller pointed out, the Slapper worm affected 29,000 systems and only 1 percent of the machines infected (335) had sufficient firepower to disable a U.S. intelligence agency's machines for more than 24 hours. The moral is that damage to the infrastructure does not always require a large number of processors in the infrastructure to be involved or a significant number of processors to be compromised.

Paller claimed that it is the system vendors that make systems vulnerable, and this situation could and should be fixed. To explain this further, the following example was provided: a federal government CIO purchased an Oracle system and wanted it delivered to certain specifications with known system vulnerabilities turned off. Additionally, she wanted to make sure that any patches that came out would not override these configurations. At first Oracle did not want to do this but eventually gave in and they are now offering this option in their sales package.

Customer demand does not always win out, especially against vendors with extremely large customer bases. In their initial efforts into concepts of self-healing networks, the NSA came up with an idea of compartmentalized LINUX SE. The idea was originally offered to Microsoft for NT, but they said it was too late to get it into the system.

Paller stated the greatest threat to the infrastructure today is the threat of compromise of financial information and extortion and cited some basic facts about threats to the Internet:

> Illegal exploitation of Internet and attached business applications is not preventable by law enforcement. The state of forensics is not sufficient to locate offending parties. Law enforcement agencies advise paying extortion fees, because they cannot protect a business from an Internet-based extortion. To prove his point, Paller quoted Pat Morrissey, former Chief of Cyber Crime Investigations for the U.S. Secret Service as saying: "Any criminal organization

> that is not using this technique [Internet extortion] should be sued for malpractice!"

Remote maintenance and control operations, which use IP protocols, are subject to being hacked with root access compromised. Paller provided data from a report by FBI agent E. Brent Rasmussen demonstrating root access to the control system of the Shasta Lake/Sacramento Dam and every other dam in the northern part of California. The Shasta dam incident provides an interesting example, because as a security mechanism, Dam security personnel wanted "backup controls" in order to prevent terrorist attacks. Those very same backup controls were more susceptible to attack (less-well protected) than the main system and became targets for terrorist attack.

Paller warns that the policy of connecting administrative computers on the same networks as systems that have critical functions – like control systems for dams – not only demonstrates weak security policy but can also put lives at risk.

The mantra for the talk was "vendors increase risk to the Internet by delivering bad software." Hackers then exploit these deficiencies to the point that hacker sites exist on the Internet where all necessary technology is available for an exploitation of the software vulnerability. Hacker sites compete on ease of use. To support this statement further, Paller provided a demonstration of how to use existing hacker sites. Very little knowledge of the Internet nor an understanding of the software was required: The only necessary skill was the ability to operate a mouse.

Paller suggested that a possible mitigation is to promote diversity in "layers" to limit damage. Further work in defining the term layer might be performed. One simple method to provide diversity of layers is the simple policy of implementing diversity of operating systems to avoid cascading vulnerabilities introduced by use common operating system (OS) for an entire enterprise. For example, an enterprise can use a firewall that has a different OS than the platform(s) it is protecting. Another example would be to add an extra layer between Windows boxes and Linux boxes.

Based on available cyber protection techniques, Paller suggested a first place to start limiting the vulnerabilities of an enterprise is in the firewalls, which can be misconfigured and have their own vulnerabilities.

The workshop participants commented that the computer industry has vulnerabilities due to the fact that it hasn't used paradigms of other industries, which have to model and reduce risk, e.g., the nuclear power industry. A suggestion was made that private industry must catch up to DOD in traffic analysis in order to reduce infrastructure risk. Traffic analysis does not involve any assumptions about insider or outsider threats, as do many of the solutions for risk reduction in the computer industry today.

Paller left the audience with the following recommendations:

- We must promote a security strategy of diversity "in layers"

- Don't try to "fix everything" at first. Pick the most critical vulnerabilities and allow those to be your first target
- We need vendor-delivered system vulnerabilities wiped out
- A patch cannot solve all vulnerabilities; they must be solved *by design*
- Partitioning is needed—multiple tasks should not be assigned to single systems (a firewall should just be a firewall)

A Machine-Dominated Future? Mr. Richard Clarke, President of Good Harbor Consulting and former Presidential Special Advisor on Cyberspace Security, began his presentation by reminding attendees that authors of books and Hollywood scripts have always been concerned about the infrastructure failing due to its complexity. He used the following three examples from popular culture:

- Terminator 3: cell phones, ATMs, radio stations do not work and the DOD controls the civilian critical infrastructure
- Matrix Reloaded: nobody really cares about this infrastructure until it stops working/man's dependence on machines
- Deutsch's *A Subway Named Mobius*: people have forgotten how to add, subtract, and multiply

Clarke posited a future wherein machines are at a best a ubiquitous necessity and at worst, control mankind; he posed the question, "Where are we in the march towards a machine world?" Society has been taken over by cyber devices to an extent that we are not aware of. The idea of complexity has emerged more and more over recent years. Around the world last year, people created 5 billion megabytes of info equaling ½ million Libraries of Congress per year. Clarke pointed out that today we can not insure that data is not corrupted and cited the following statistics to support his view. Last year 114,000 virus incidents happened. The damages from Trojans and viruses cost $45 billion last year and cost $38 billion for the month of August this year. This year over $126 billion in losses occurred due to worms and viruses. There has been a 400 percent increase in damages this year to vulnerabilities in software. There are 10 coding errors in every 1000 lines of code. Unless we begin to fix these vulnerabilities, we cannot even attempt to catch up.

The cause of the problem, Clarke stated, is that humans make too many mistakes. Software vulnerabilities are a result of the inability of humans to write code well. To reduce software errors, research and development projects have been proposed to have software write software. Products are available today that claim to check software for errors. Clarke posed the following questions to the participants:

- Is this the path we want to be on?
- Should we put the brakes on computer technology?
- What will our dependencies be like in ten years with respect to software and global controls?

Clarke predicted that in five years there will be software running and that humans have had no direct involvement in coding, checking, and operations and maintenance. He reminded the participants that Bill Joy, the former CEO of Sun Microsystems, predicted three years ago that humans would lose control to machines since, to get better, we'll put machines in charge of certain functions. Mr. Joy suggested that at some point we must "put the brakes on," or else in ten to twenty years we could lose control to computers to a point where all software is written by machines, being checked by machines, machines talking to machines! Clarke asserted that Mr. Joy's warning was unheeded, and pointed out that this year we had several interruptions in operations due to computer issues (pipelines, power grid, airlines, trains). Participants were asked what they thought systems would be like in ten years. Clarke proposed a dialogue on the future of computer technology to answer the question, "Are we in danger of losing control?"

Clarke asked the rhetorical question, "Is the U.S. government doing enough to protect U.S. citizens and businesses?" He suggested that the Federal Government utilize cyber capabilities offensively as well as defensively and pointed out that the terrorists know how to use the Internet to communicate and raise money. Al Qaeda, for example, has a disturbing number of people with graduate degrees in Computer Science, many of them obtained in some of the best U.S. schools. The September 11th attacks demolished infrastructure and sent the economy into a tailspin (ripple effect and interdependencies evident). Other examples of events affecting the U.S. economy were the Anthrax mailings and the Washington Metropolitan area sniper attacks, which not only caused loss of life but immense economic damage based on building and business closures, police activities, and clean-up. Even after September 11th, Clarke pointed out, we still have folks in the intelligence community who are not focused on these problems. Al-Qaeda isn't the only organization that wants to cripple the U.S. economy. Chinese Generals have publicly stated that, if a conflict arose with U.S., they would use cyber attacks to attack the civilian infrastructure. He asked, "Why aren't we heeding these warnings?"

Clarke advised that protection of the infrastructure is dependent on obscurity of interconnections. Knowledge of the machinery is power. Collaboration between government and industry is needed if the predominantly privately owned infrastructure is to be protected. Assurance of privacy of information regarding infrastructure topology and design, system breaches, vulnerabilities and other issues are paramount for private industry to trust the government. Clarke pointed out that it is necessary to get the private sector to understand their own infrastructure. On closing, Clarke repeated the warning of John Casciano that "the civilian economy is the target."

Clarke left the audience with the following recommendations:

- The U.S. government needs to be doing much more than it is vis-à-vis offensive or defensive proactive infrastructure defense
- The government will need to keep more information secret to limit "danger" to infrastructure

- We cannot underestimate our enemy or the ripple effect on the U.S. infrastructure and economy of an adverse action in one area
- People do not understand the issues involving critical infrastructure, so they do not spend money on protecting it.

Cascading Effects and Ubiquitous Use of Common Platforms and Protocols: Dr. Daniel Geer, Principal, Geer Risk Services, discussed the health of our ubiquitous Internet and IT systems: the prognosis was poor and, more importantly, poorly understood. Geer addressed the risks and vulnerabilities of our cyber infrastructure, which permeates all aspects of the society. He began by discussing the impact of a computing infrastructure monoculture, especially where that monoculture is complex and already shown to be permeated with security faults. For example, if the source of security faults is in any way related to complexity, then it is necessary to note that Microsoft XP represents a new high water mark in complexity at over forty million lines of code. Not only has Microsoft's code size grown over the past twelve years, but so has the installed base of system vulnerabilities. Geer illustrated all these points with available data noting that there is not nearly enough data to perform detailed analysis.

Geer pointed out that vulnerabilities represent a good example of emergent problems. A combination of two vulnerabilities, which independently are annoying, can together be devastating. For instance, had anyone opportunistically mounted a computer attack combining the NIMBA worm and the emergency 911 (E911) vulnerability, the result would have disabled the entire 911 service a week after September 11th – clearly an example of avoiding a collapse of public confidence by nothing more than blind luck. Having survived a virus or worm attack, computer users should not be complacent, Geer points out, because most worms and viruses can re-infect the same or different systems at later dates. This is partially the result of incomplete patching of systems. He walked the audience through a series of statistics on the state of the cyber infrastructure that was frightening and demanded a call for action. The following is an overview of the statistical analysis presented on cyber vulnerabilities:

- Best practices do not get rid of twenty percent of the worst risks
- Patching is not one hundred percent effective, and one must assume that old worms/viruses will re-infect computers at later dates
- Access control fails to scale. These systems cannot support large systems effectively and present management and maintenance resource overload
- Reverse engineering of patches issued by a vendor can be used to generate an exploit heretofore unavailable to the hacker
- Patches that go up on the Internet are essentially advertisements for how many people are vulnerable, leading to a footrace between the customers and the bad guys
- The bundling of patches under one name that covers multiple exploits is misleading. This strategy, driven by cost and convenience, delays installation of patches as they are developed and can prevent the installation when the title of the patch does not match the user function and installation is ignored

Geer compared the computer worm/virus environment to a worst-case disease epidemic, where the infection period is long (and the disease can stay dormant for long periods of time) and the effects of the disease are quick and often lethal. One solution is to segment or quarantine networks based on traffic analysis. Another solution might be to have ISPs egress filter all traffic to minimize spread of worms, etc. However, the price of safety may be the loss of privacy, and that this is a dialogue that must be surfaced and addressed; until it is confronted directly it will limit the solution space to wishful thinking.

Geer predicted that the future of network designs is changing. This is a security-cognizant future, where systems are interconnected via loose interfaces with small modules, which are very different from a large, complex system. This future, with more and smaller computers networked together, will require different countermeasures than today.

Geer pointed out that security risks are addressed in terms of best practices, guidance, and other qualitative processes that are very subjective. The industry must incorporate sound measurement as part of cyber conflict reporting if the infrastructure is to be successfully protected. There is a great need for a cyber risk model. He suggested that the cyber world look at other bodies of developed, quantitative knowledge, such as public health, portfolio management, the insurance industry, and accelerated failure time testers to see how risk is handled in these environments. A sound risk model will not only predicate changes to cyber security policy but will support the work of quality practitioners and researchers. The lack of sound measurement techniques and reporting and an accepted risk model has a negative effect on funding of research and security product development. Today industry is driven by demands for reliability over security because a sound case cannot be made for the latter. Geer pointed out the need for more qualified people in the field. Without measurement and trained practitioners, the charlatans win.

Geer ended his talk by advising the participants that if all the code attacks to date have been conducted on known vulnerabilities, it is safe to assume that someone has a reserve of vulnerabilities that are yet to be acted upon. The lack of quality assurance in the development and management of code, off-shore development of software and software maintenance, and the problems of human error, should be of concern to all those concerned about infrastructure protection.

The workshop participants engaged in a healthy discussion regarding the implications of Geer's statistics and about the use of patching as immunization. A discussion of a policy that requires mandatory patching and methods to implement it took place and is definitely an issue that needs further study.

Geer left the audience with the following recommendations:

- Quantitative cyber risk techniques must be developed
- The price of security is privacy just as the price of privacy is security, and subsequent work is needed in addressing privacy policy and legal issues

- Techniques for protecting critical infrastructure such as quarantines, filtering of data, mandatory patching must be addressed and, if viable, effectively mandated
- Training and an increase in competent practitioners is needed

Challenges for Securing Shared Infrastructure Against Large Scale Cyber Attack: Col (S) Gregory Rattray, Ph.D., began his talk statement that securing government and private sector shared infrastructure against a large-scale cyber campaign will prove extremely challenging. Rattray posited that adversaries who use cyber conflict as a method for political or economic coercion will not necessarily use types of attacks we are witness day-to-day, either in form or magnitude of intended effect. In particular, a cyber conflict could occur over long time periods, rather than the minutes or hours characterizing the problematic period of most disruptive cyber events today. One part of a better understanding of how the nation's cyberspace will stand up to a series of large-scale attacks is deeper insight into the complexity of the infrastructure and all the actors who contribute to its vulnerabilities, are responsible for protection and might be attackers. Rattray stated that complexity sciences can provide the following insights regarding cyber conflicts and suggested the following:

- Environment opaqueness (uncertainty concerning which elements are of most dire interest for both defenders and attackers)
- Nonlinearity of effects (loss of specific functionality and associated, yet unknown, cascades effects or the ability of the system to adapt and minimize disruptions)

Rattray suggested that answers to the following might help us understand the value of such fundamental questions:

- What sorts of systems are inherently adaptive and/or recover easily?
- How does sophistication of human operators play into this?

Today, Rattray pointed out, defenders often lack the ability to predict if a system will fail totally or partially as a result of some perturbation. In general, penetration testing indicates that sophisticated attackers can generally find ways to enter systems due to the inherent multiple vulnerabilities in interconnected systems. Rattray believes concerns about insider attacks should be increasing technologies and operational approaches to identify such behavior require more attention.

Rattray pointed out that there is a need for more creative defensive techniques. Improved technological countermeasures alone will not provide comprehensive solutions. New ideas and research is needed to develop networks addressing, controls and edge systems that can adapt under attack, increasing the challenge for attackers to target and disrupt critical functionality. Rattray suggested research and field-testing of network topology changes that support a more defensive posture, when an attack is in progress. Other research might include the capability to clean up a network by sweeping for security flaws to improve confidence in its security and ability to resist attack before an

organization enters a period where network and system confidentiality and reliability is at a premium. For example, such a sweep might occur prior to a period of active field operations for a military unit or during conduct of an extremely sensitive test for an R&D laboratory.

Rattray suggests that a better understanding of combined cyber and physical attacks and what, if any, is the role and effect of the cyber-dimension in physical attacks. Cyber expertise will be increasingly important as part of efforts used to prevent physical attacks and limit their consequences.

Rattray recognized positive ongoing efforts in the infrastructure protection arena. The consolidation of the functions to secure the cyber infrastructure protection functions under the Department of Homeland Security was an important step to improving protection strategies. The State Department has international outreach programs on Critical Infrastructure Protection focusing on actions to improve cooperation in warning and protection against cyber threats.

Rattray calls for a much-needed change in the cyber defense mindset. Network operators and the senior management of most organizations that rely on information and communications infrastructures must understand the fundamental vulnerability of these technologies systems. It must be assumed that sophisticated adversaries can infiltrate and create the capacity for disruption of most systems and networks given motivation and time. Therefore, we need to be capable of "functioning while under attack." Col. Rattray finally proposed that understanding the effectiveness of practices of organizations to protect, defend and recover from cyber attacks and sharing these techniques within government and industry is essential for improved defense.

Closing Remarks: John Casciano ended the conference by summarizing the goals and mission statement for the newly formed CCSA. Casciano advised that there would be four additional workshop on the area of critical infrastructure protection as well as two conferences this year. The organization is forming committees in research, membership, publication, programs, and finance and looking for volunteers to support these activities. Success of the workshop efforts and the Association as a whole rely on the participation of members. He also noted that NDU had offered their widely distributed and recognized *Defense Horizons* publication series as an outlet for CCSA publications. The workshop ended with Mr. Casciano reminding everyone that the nuclear age began with much scholarly input into the management of the science. The same should be possible for Cyber Conflict Infrastructure Challenges.

Appendix A

Workshop Agenda

10:00 - 10:30 Registration

10:30 - 10:40 NDU Welcome—Lt Gen Michael Dunn

10:40 - 10:50 Introduction of CCSA objectives and workshop agenda—Major General John Casciano

10:50 - 11:15 Implication of Complexity on Shared Infrastructure*s*—Dr. Harold Morowitz

11:15 - 12:30 Panel Discussion and Key Issue Identification

- Power Grid Interconnectivity, Failures and Regulatory Interaction*s*—Dr. Dejan Sobajic
- Impact of Sound Security Practices on Mitigating Risks from Cyber Attacks—Mr. Alan Paller

12:30 - 13:00 Break and buffet lunch

13:00 - 13:30 Luncheon Speaker: A Machine Dominated Future?–Mr. Richard Clarke

13:30 – 15:30 Panel Discussion and Key Issue Identification led by Mr. Michael Schrage

- Cascading Effects and Ubiquitous Use of Common Platforms and Protocols – Dr. Daniel Geer
- Challenges for Securing Shared Infrastructure Against Large Scale Cyber Attack – Dr. Gregory Rattray

15:30 - 15:45 Summary of issues and future activities – Major General John Casciano

Attendee List

Speakers:

Mr. Richard Clarke
Good Harbor Consulting

Lt Gen Michael Dunn
National Defense University

Dr. Daniel Geer
Geer Risk Services

Dr. Harold Morowitz
Kranow Institute, George Mason University

Mr. Alan Paller
SANS Institute

Col (S)Gregory Rattray, Ph.D
National Security Council

Mr. Michael Schrage
MIT Media Lab

Dr. Daniel Sobajic
Electric Power Research Institute

Participants:

Mr. Terry Baker
Northrop Grumman Information Systems, TASC

Dr. Hans Binnendijk
Center For Technology and National Security Policy, NDU

Major General John Casciano
GrayStarVision, LLC

Mr. Andrew Cutts
Institute for Security Technology Studies. Dartmouth College

Dr. Paul Davis
Industrial College of the Armed Forces/NDU

Mr. Matt DeVost
Terrorism Research Center

Mr. David Dittrich
University of Washington

Mr. James Downey
Terrorist Threat Integration Center

Mr. Kyle Dunn
The Potomac Institute

Mr. Brian Dunphy
Symantec Corp.

Ms. Kathy Emmons
Information Resource Management College/NDU

Mr. Michael Farmer PNNL

Mr. Geoff French
General Dynamics Corp

Maj Teresa Hall
Department of Defense

Mr. James A. Holtzclaw
Northrop Grumman IT TASC

Dr. Stuart Johnson
Center For Technology and National Security Policy, NDU

Mr. Paul Kozemchak
DARPA

Lt Col Fred Krawchuk
U.S. Army

Dr. Daniel Kuehl
Information Resource Management College, NDU

Mr. Steven Lemon
Terrorist Threat Integration Center

Mr. Brett Lovgren
SAIC

Mr. William Lucyshyn
University of Maryland

Dr. Chester Maciag
AFRL/IFGB

Dr. Douglas Maughan
Department of Homeland Defense

Mr. John McCarthy
Critical Infrastructure Protection Program, George Mason University

Mr. Bruce McDonald
Institute for Defense Analysis

James Mulvenon
Rand Corporation

Mr. Gary Nelson
Private Consultant

Ms. Lillian Noland
Northrop Grumman IT TASC

Mr. Dan Owen
Independent Consultant

Mr. John Owen
Department of Defense

Mr. Brian Peretti
U.S. Dept. Of Treasury/NSC

Mr. Will Roger
Computer and Communications Industry Assoc.

Ms. T. Irene Sanders
Washington Center for Complexity and Public Policy

Mr. Robert Schmidt
Institute for
Security

Mr. Theordore Signoret
CAASD/MITRE Corp.

Mr. Stuart Starr
MITRE Corporation

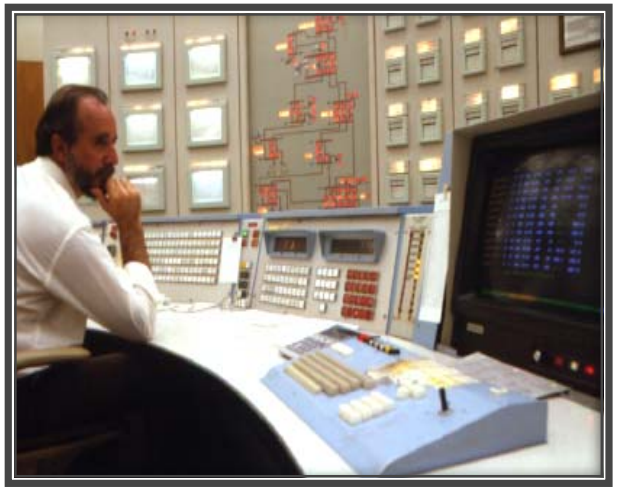
Ms. Marie Stella
Federal Aviation Administration/CTNSP

Mr. Michael Tanji
Department of Defense

Major William Thomas
Air Force Institute For National Security
Studies

Dr. J. Kenneth Williams
Zel Technology

Mr. John Woodward
The MITRE Corporation



Network Events in Electric Transmission Grids

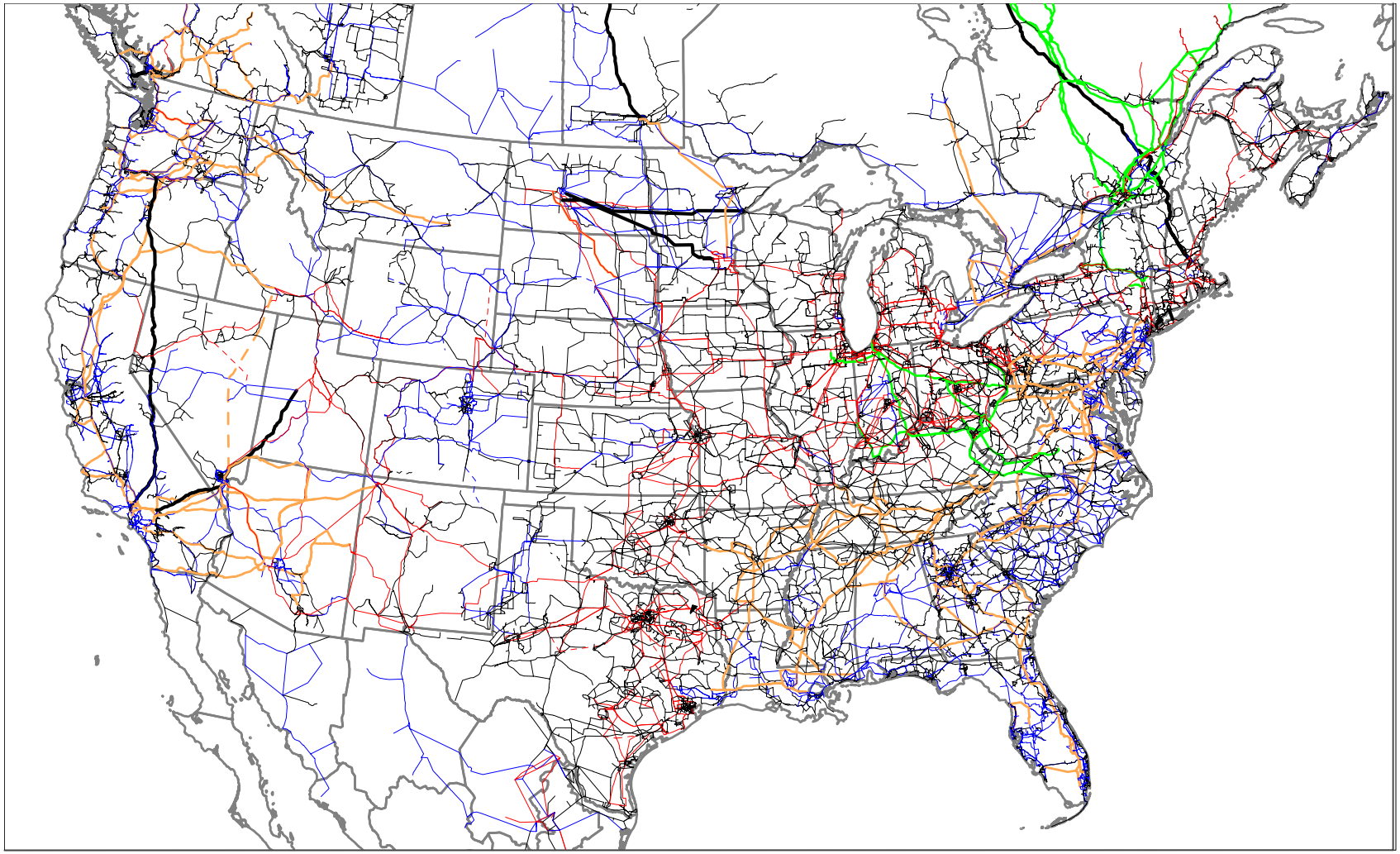
Dejan J. Sobajic

EPRI

December 8, 2003

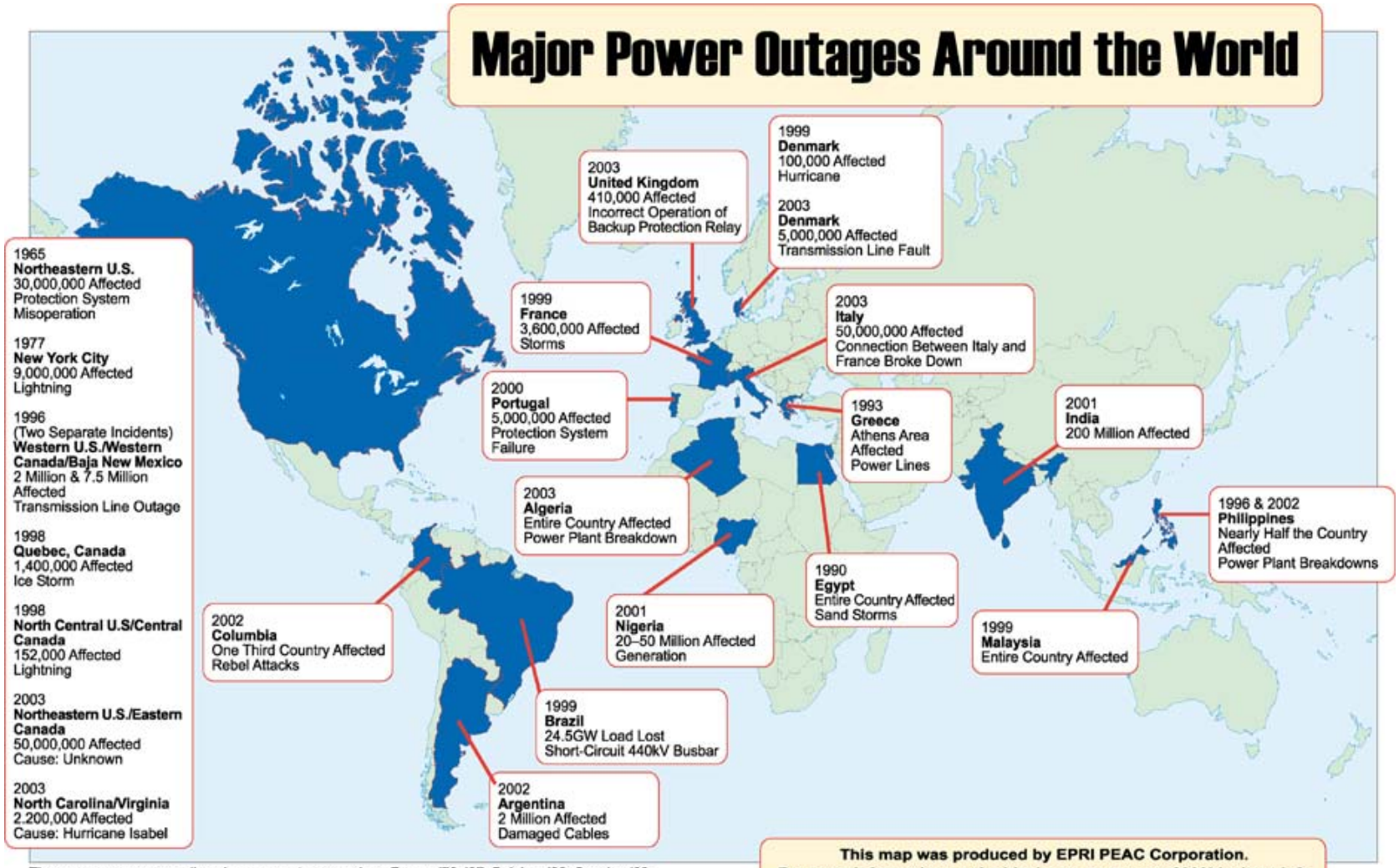
North American Electric Grid

Largest Machine Ever Built!



EPRI

Vulnerabilities of Electricity Grid: Examples



There are numerous small-scale power outages such as France '78, '87; Belgium '82; Sweden '83; Italy '89, '93, '94; Netherlands '97; and Chicago '99 that are not shown on the map.

Vulnerabilities of Electricity Grid:
Industry Response

- **DOD/EPRI Complex Interactive Networks/Systems Initiative (1998 – 2001)**
- **EPRI Reliability Initiative (1999 – 2002)**
- **EPRI Infrastructure Security Initiative (started in 2001, Phase Zero completed)**
- **DHS/EPRI/NERC North American Electricity Infrastructure Security Monitoring System (started in 2003)**

How Networks Fall Apart?

- Cascading Events (CE)
  - Unnoticed early on
    - Progressive weakening of the Grid
    - Sequential Phase
  - Then things speed up
    - Grid is out of balance
    - Transition Phase
  - When obvious it's too late for human actions
    - Loss of supply
    - Parallel & Terminal Phase

Transmission Networks are:

- Large
- Nonlinear
- Uncertain
- Time-dependent. and
- Not Fully Understood

On Cascading Events

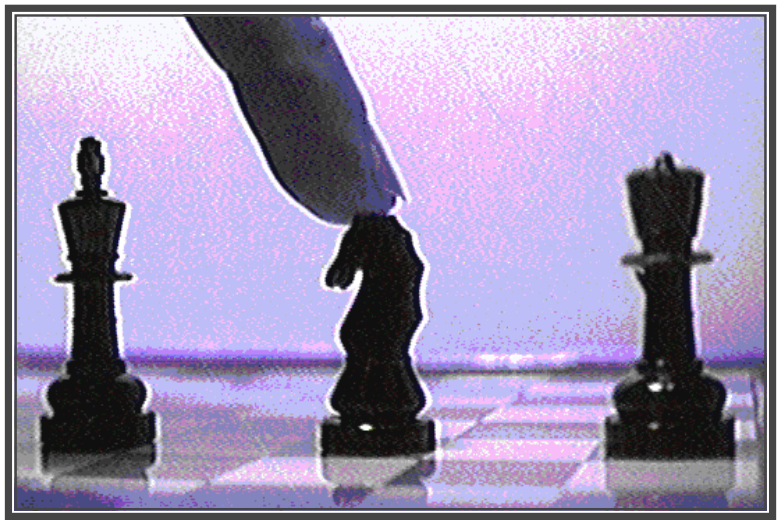
- Early CE Warning Systems badly needed
- Avoid CE by design?
  - Market efficiency vs. failure resistance
- Avoid CE through Control & Mitigation?
  - Italians tried but it didn't work

Monitoring Interconnected Transmission Networks requires:

- Real-time hardware/software
- Communications
- Accurate measurements
- Well trained people

Preventing cascades
Today's Technology

- Transaction Scheduling
  - "contract path"
- Near Real-Time System Operations
- Protection Relaying
  - Automatic & fast
  - Pre-programmed
  - Market-insensitive

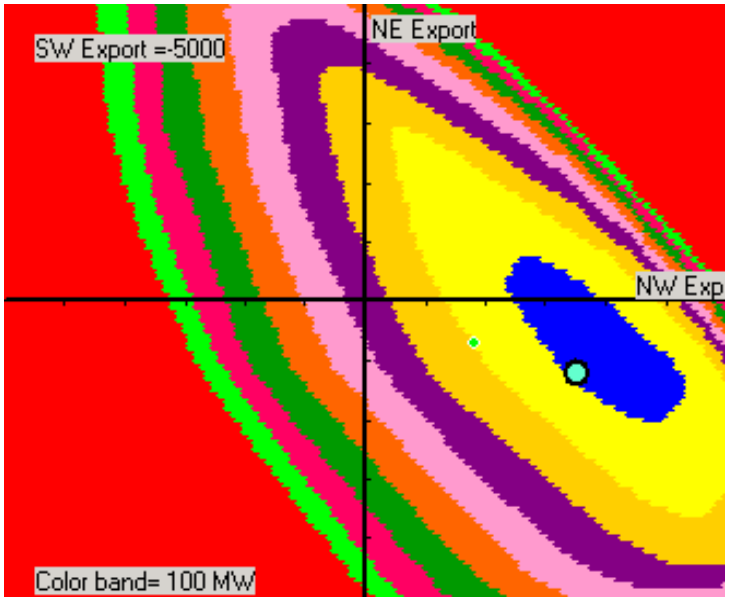


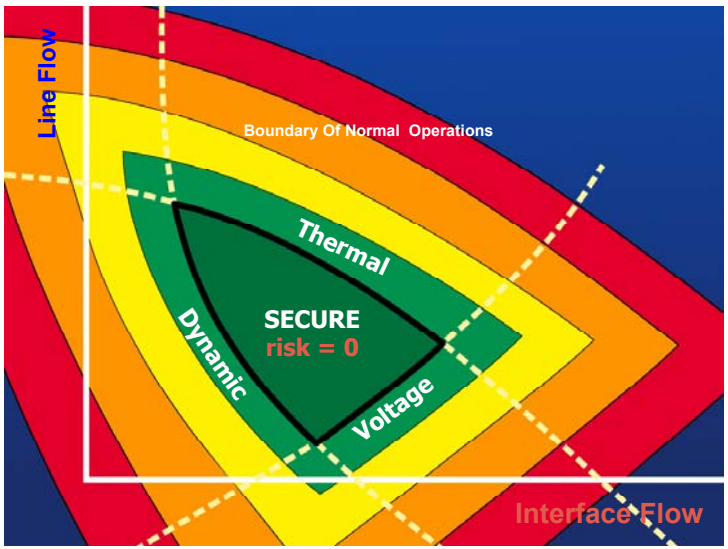
On Interconnectedness:

- US ITN was built to provide reserve not enable commerce
- How would TN look like were it built for commerce?
- Is US TN going to become a limiting factor for growing economy? How soon?

Preventing cascades
Tomorrow's Technology

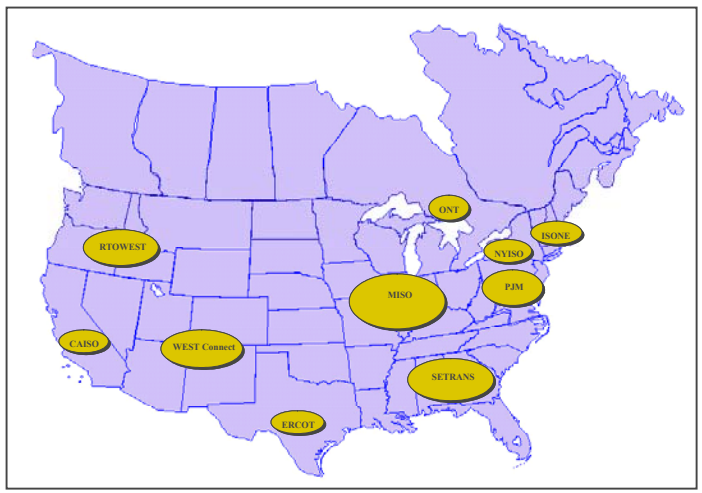
- Transaction Scheduling
  - "flow-based"
- TRUE Real-Time System Operations
- Protection Relaying
  - Automatic & fast
  - Adaptive Islanding
    - What happens with interconnectivity?
    - Adaptive Interconnectivity
  - Self-Healing





Policy Issues

- Investments in US Transmission Network are insufficient
  - As a corollary, reliability R&D dollars are unacceptably low
- Business practices need to take into account physical realities of the Grid
- Generation & Transmission extension planning has to be integrated
- Incomplete markets don't work
  - Demand response must be deployed beyond an emergency measure



Conclusion

- Cascading events may be triggered in many different ways.
- Deeper understanding of CE is a necessity
- Keeping the lights on !
  - Is an enormous undertaking
- Requiring a collaborative workshop including
  - Industry
  - Government
  - Academia
  - International “point–of –view”

Infrastructure Security Initiative:
Phase 1 -- Major Project Activities

- **Recovery Transformer**
  - Build and Test Prototype Hardware at Manufacturer Sites
- **Vulnerability Assessment**
  - Develop Methodology & Software to Evaluate Gas and Electric Grid Interactions/Vulnerabilities
- **Secure Communications**
  - Develop & Demonstrate Cyber Tools to Secure Communication Networks
- **Red Team Attacks**
  - Document Lessons-Learned from Cyber Attacks on Host Utility Systems
- **Immediate Countermeasures**

  (Response to 8/14/03 NE Blackout)
  - Document Lessons-Learned from International & Domestic Utility Attacks

Crude Propagation Model

"Domino Effect"

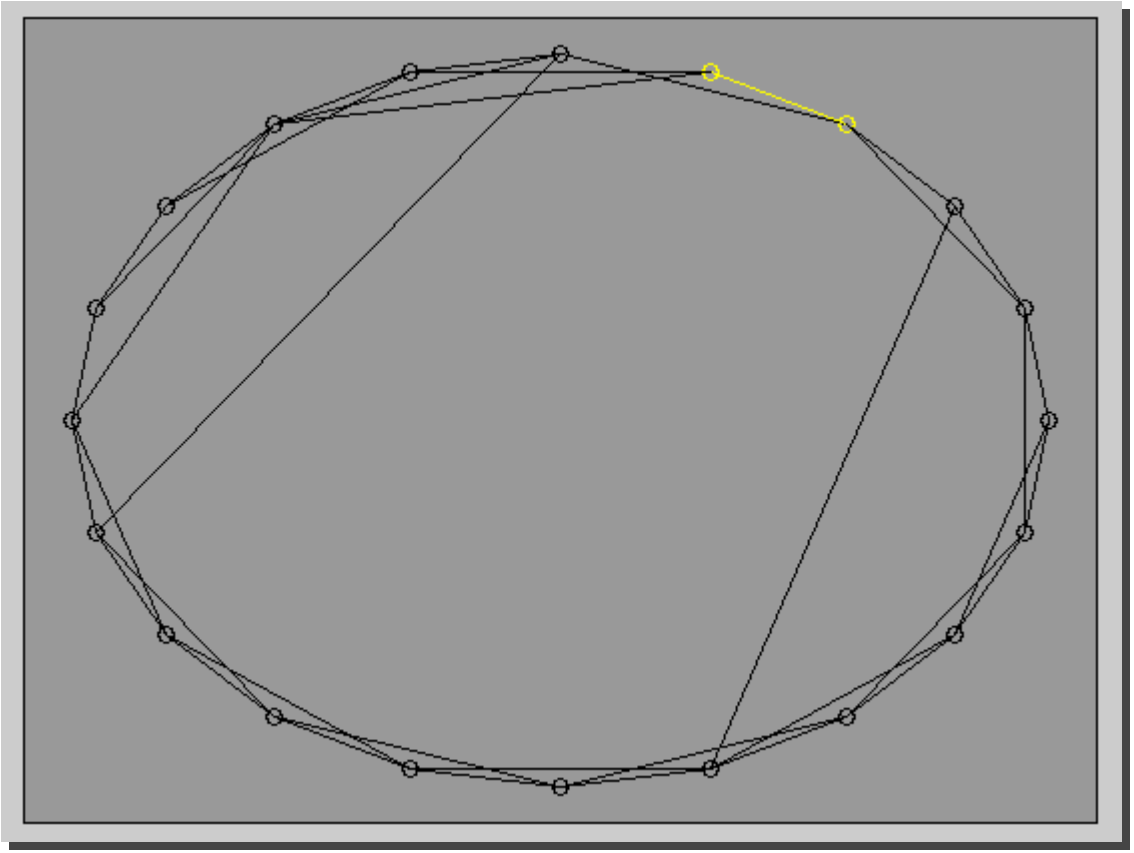
Circuit Breaker Action
$\Leftrightarrow$ virus spreading

1) Lightening strikes a line.

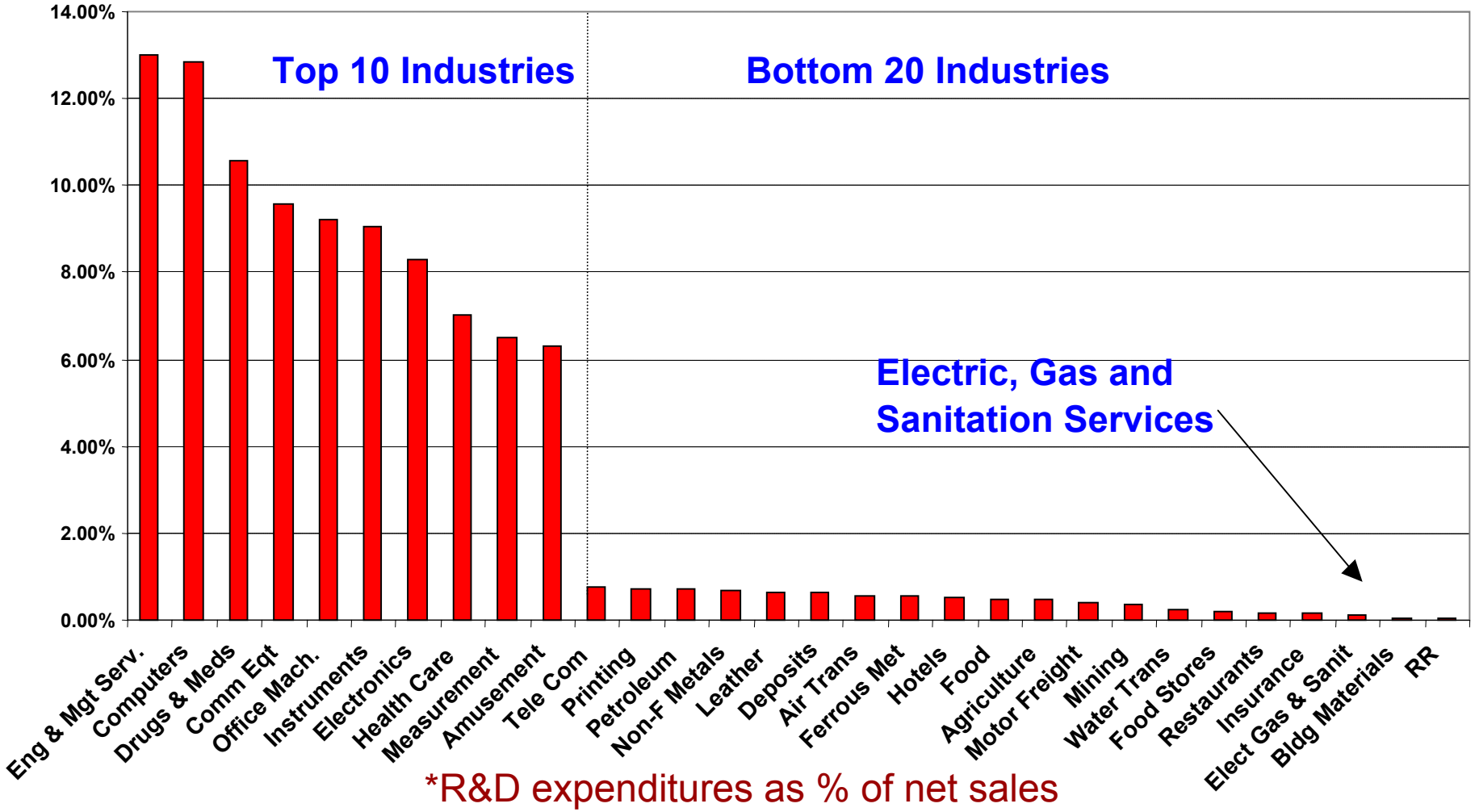
2) Induced transient trips breakers at neighboring busses with probability $0 \leq q \leq 1$.

3) Continue until cascade stops.

4) Blackout size $\propto$ number of busses affected.

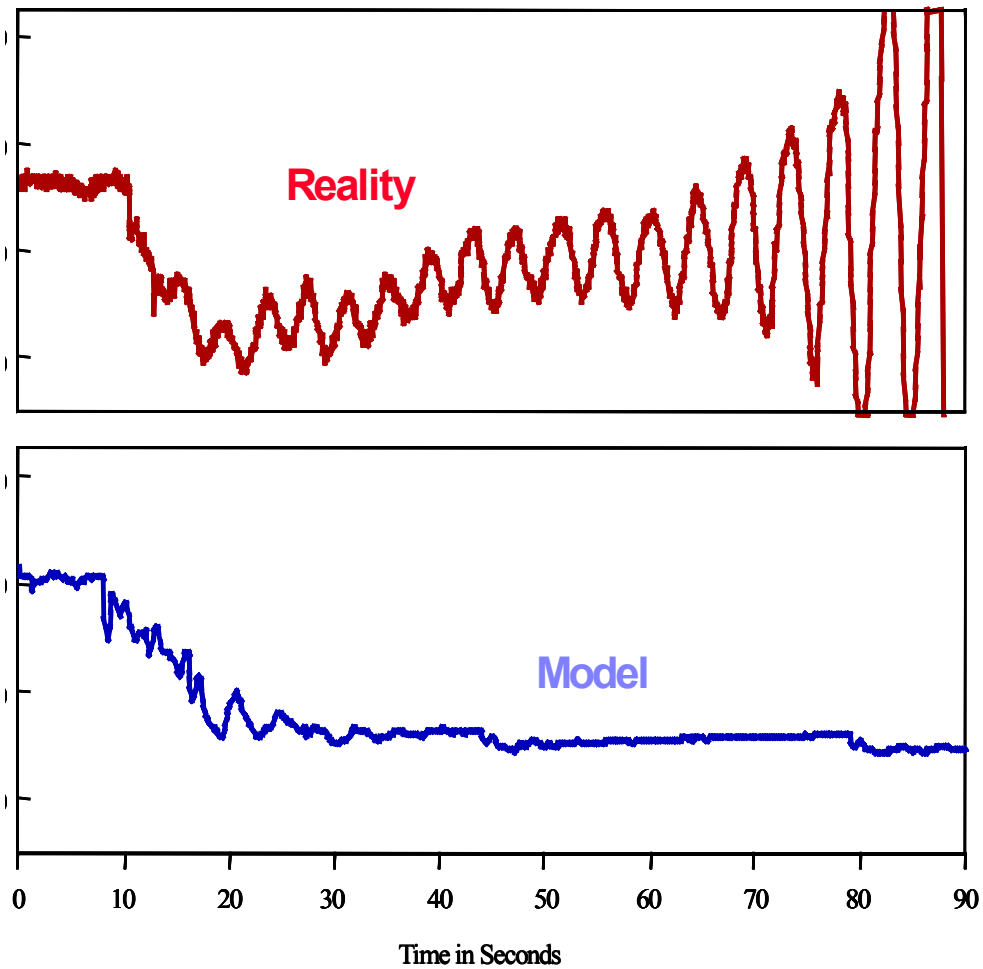


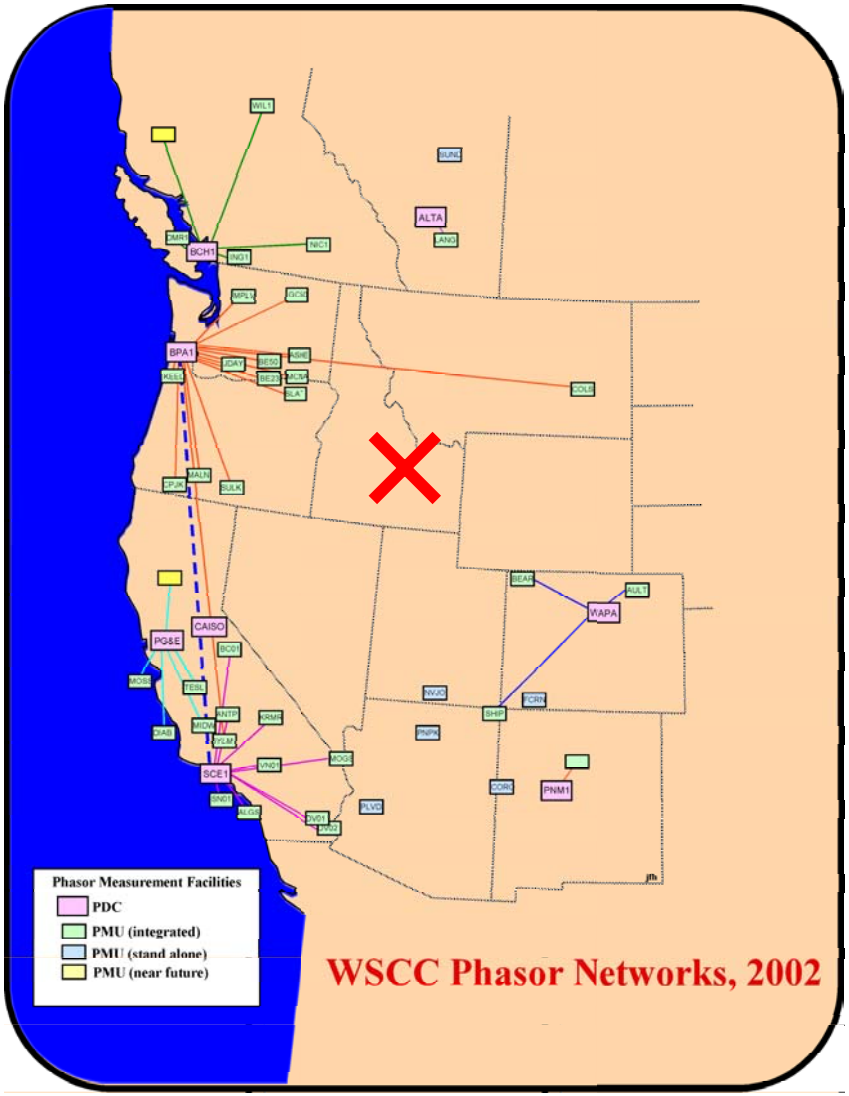
R&D Expenditures*



*R&D expenditures as % of net sales

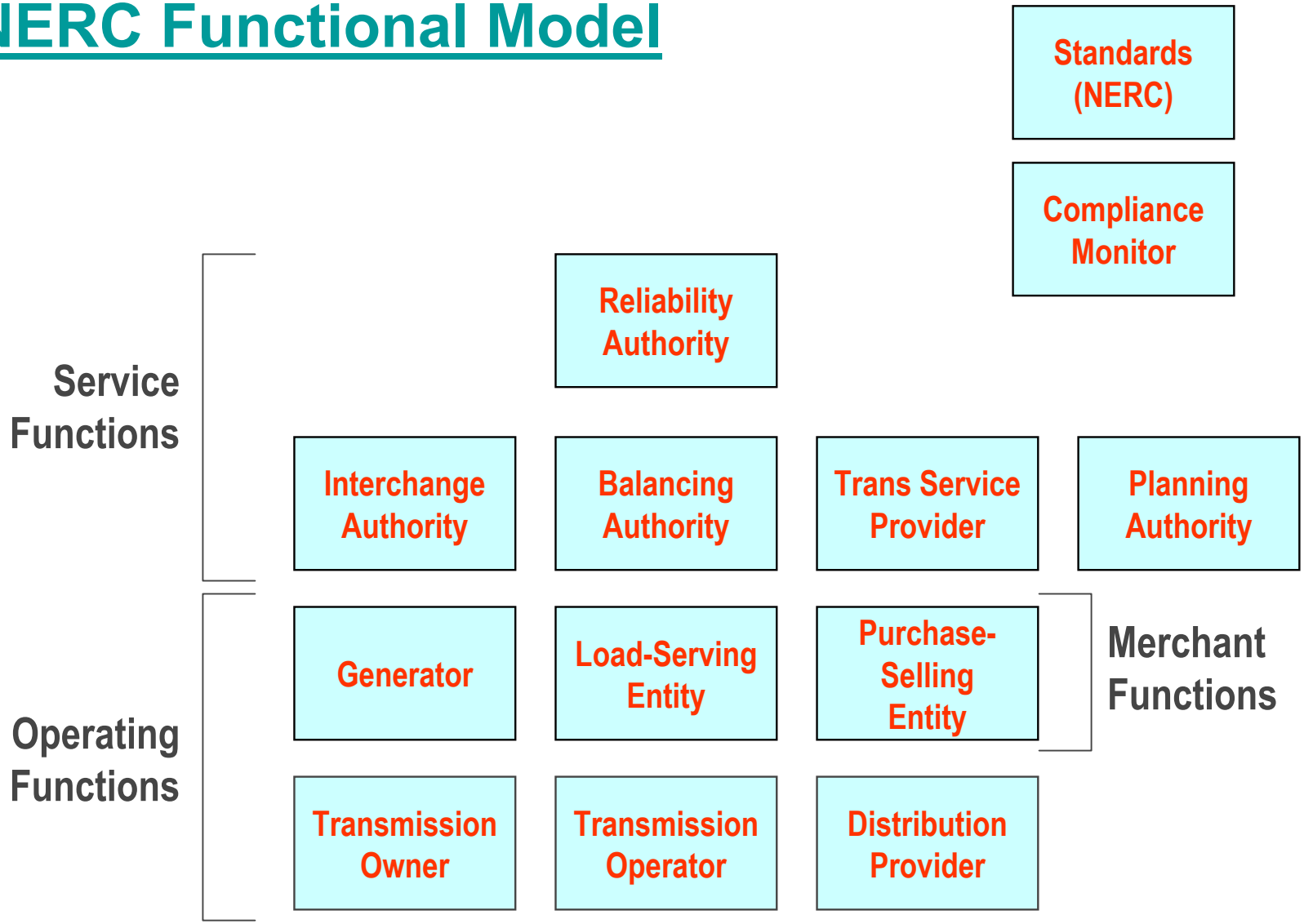
Modeling Failures May Spell Future Troubles!



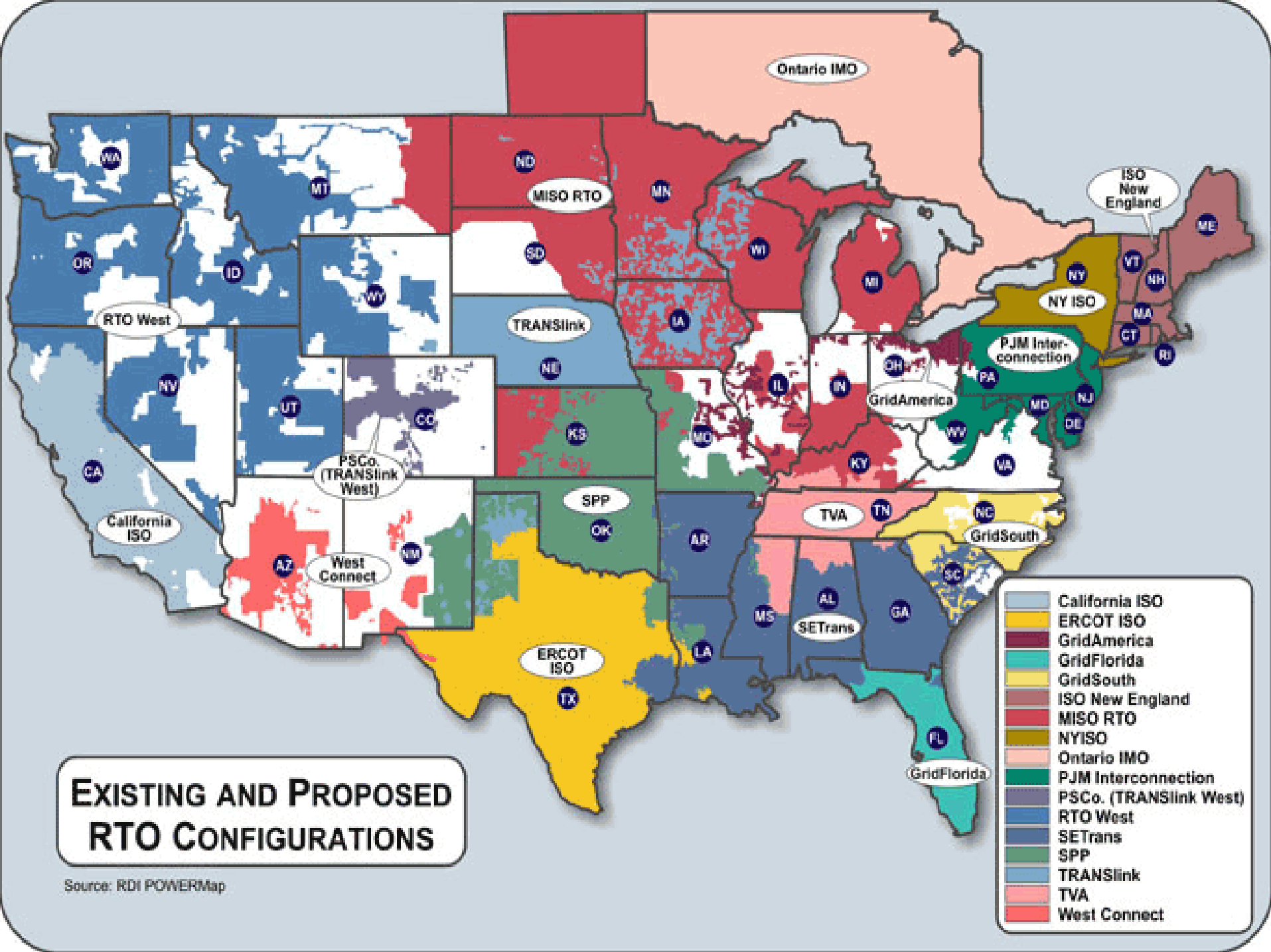


Provided by Dr. John Hauer, PNNL

NERC Functional Model



return



Existing and Proposed RTO Configurations

Source: RDI POWERMap

RTO Characteristics & Minimal Functions

Characteristics

- Independence
- Scope and Regional Configuration
- Operational Authority
- Short Term Reliability

Minimal Functions

- Tariff Administration
- Congestion Management
- Parallel Path Flow
- Ancillary Services
- OASIS and TTC/ATC
- Market Monitoring
- Planning and Expansion
- Interregional Coordination

Approved RTOs

- **PJM (RT01-2-000)**
- **MISO (RT01-87-000)**

Independent System Operators

Key Objectives

- Enhance interregional reliability through coordinated operations and planning.
- Facilitate broader competitive markets.
- Improve flow of information to market participants and the public.

Existing ISOs	**- CAISO**	**- PJM**
	- ISONE	**- MISO**
	- NYISO	**- ERCOT**
	- IMO (Canada)	

The August 14 Blackout

from the US-Canada Interim Report

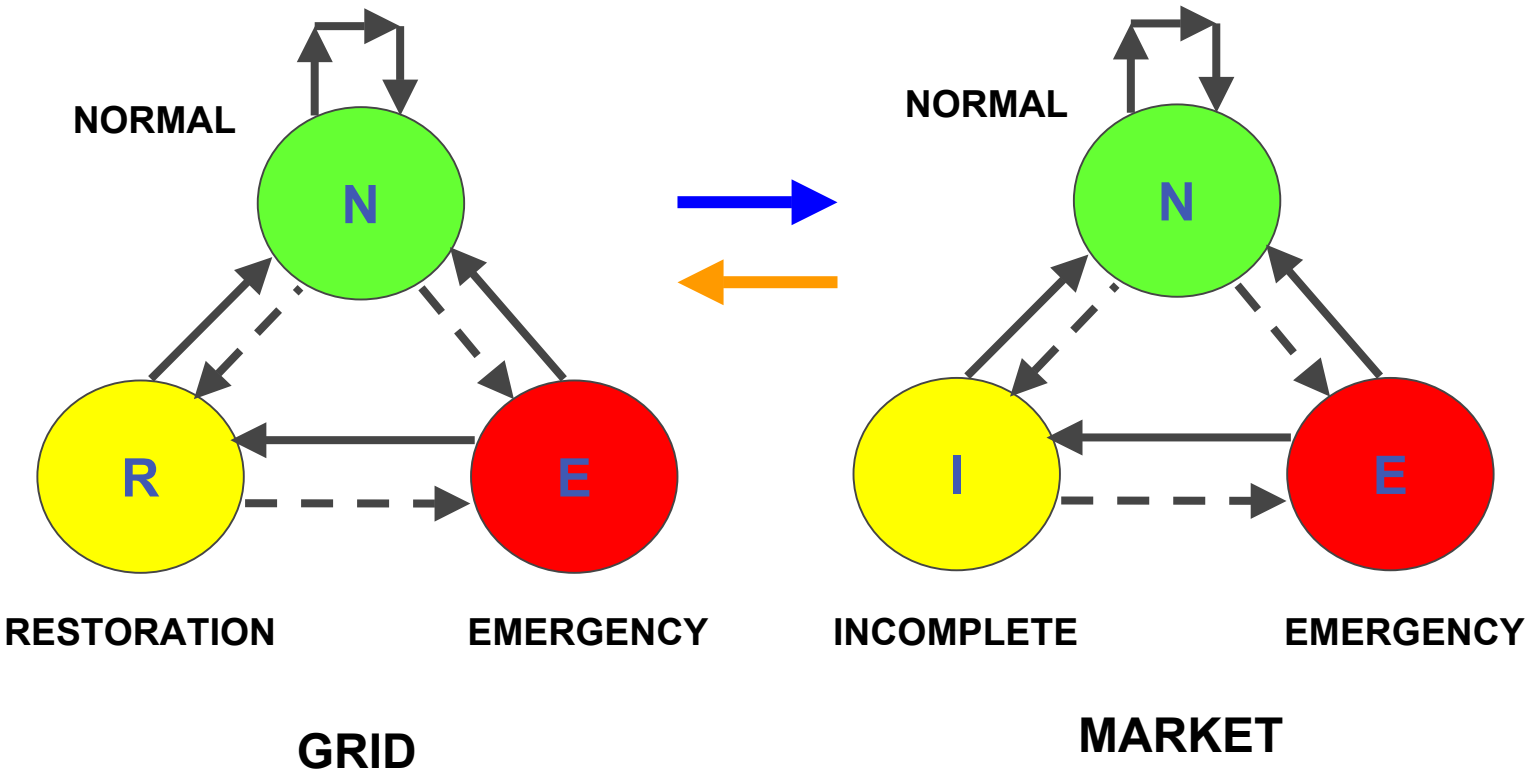
Causes or contributing factors

- Inadequate vegetation management
- Failure to ensure operation within secure limits
- Failure to identify emergency conditions and communicate that status to neighboring systems
- Inadequate operator training
- Inadequate regional-scale visibility over the power system.

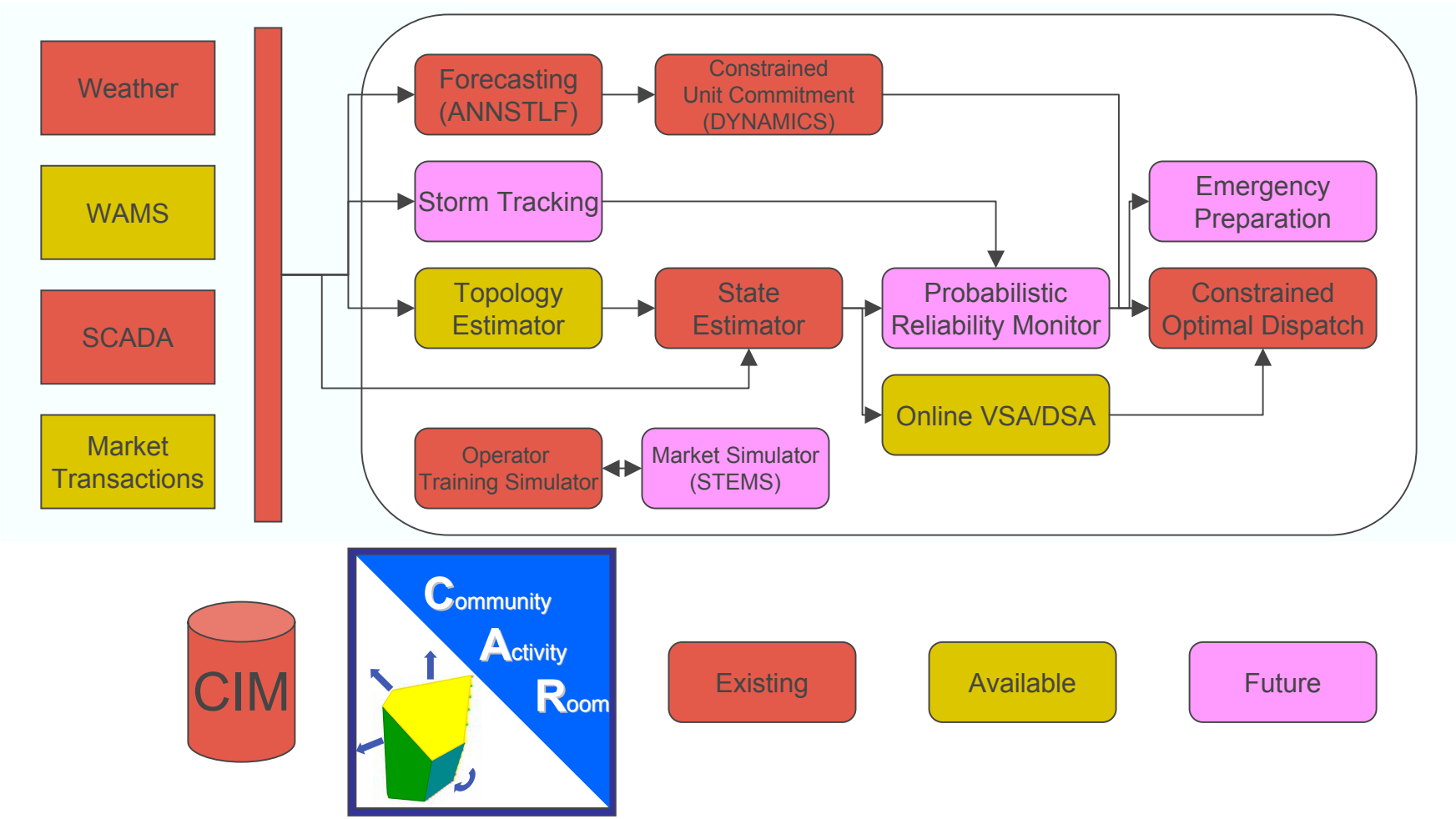
New causal features of the August 14 blackout

- Inadequate interregional visibility over the power system
- Dysfunction of a control area's SCADA/EMS system and
- Lack of adequate backup capability to that system.

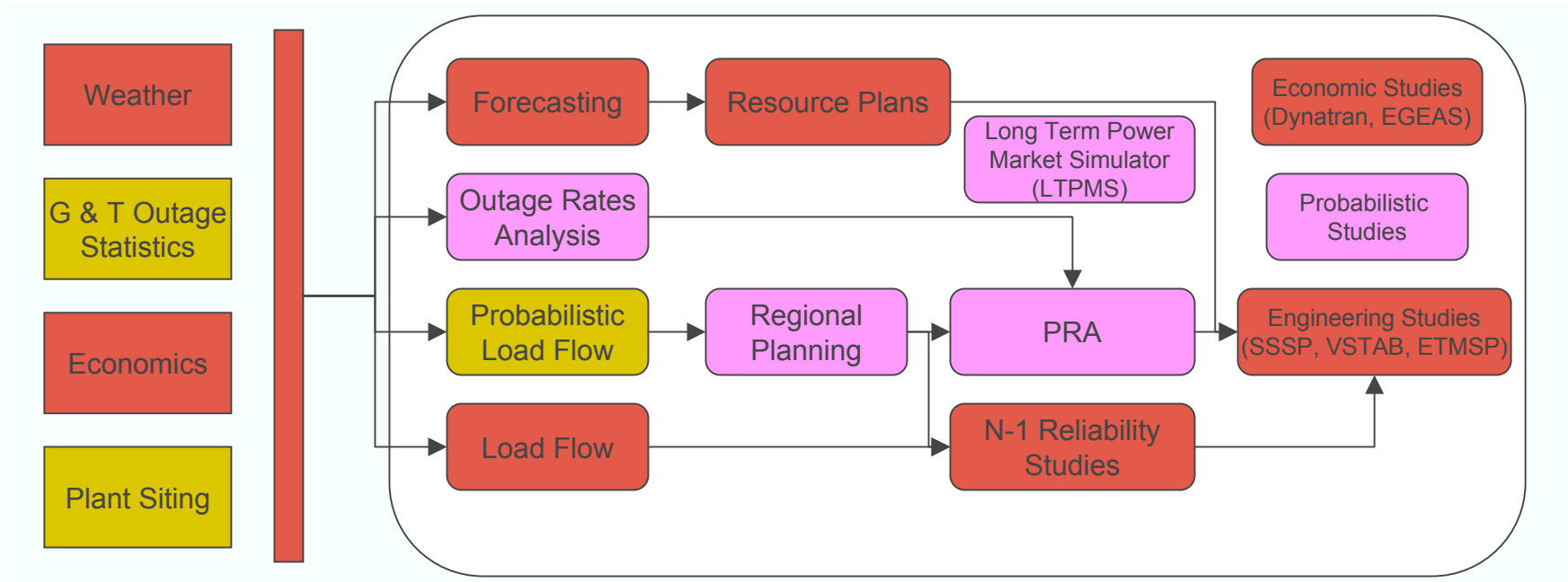
Framework for Market/Grid Operations & Analysis



Architecture of Future Operation



Architecture of Future Planning



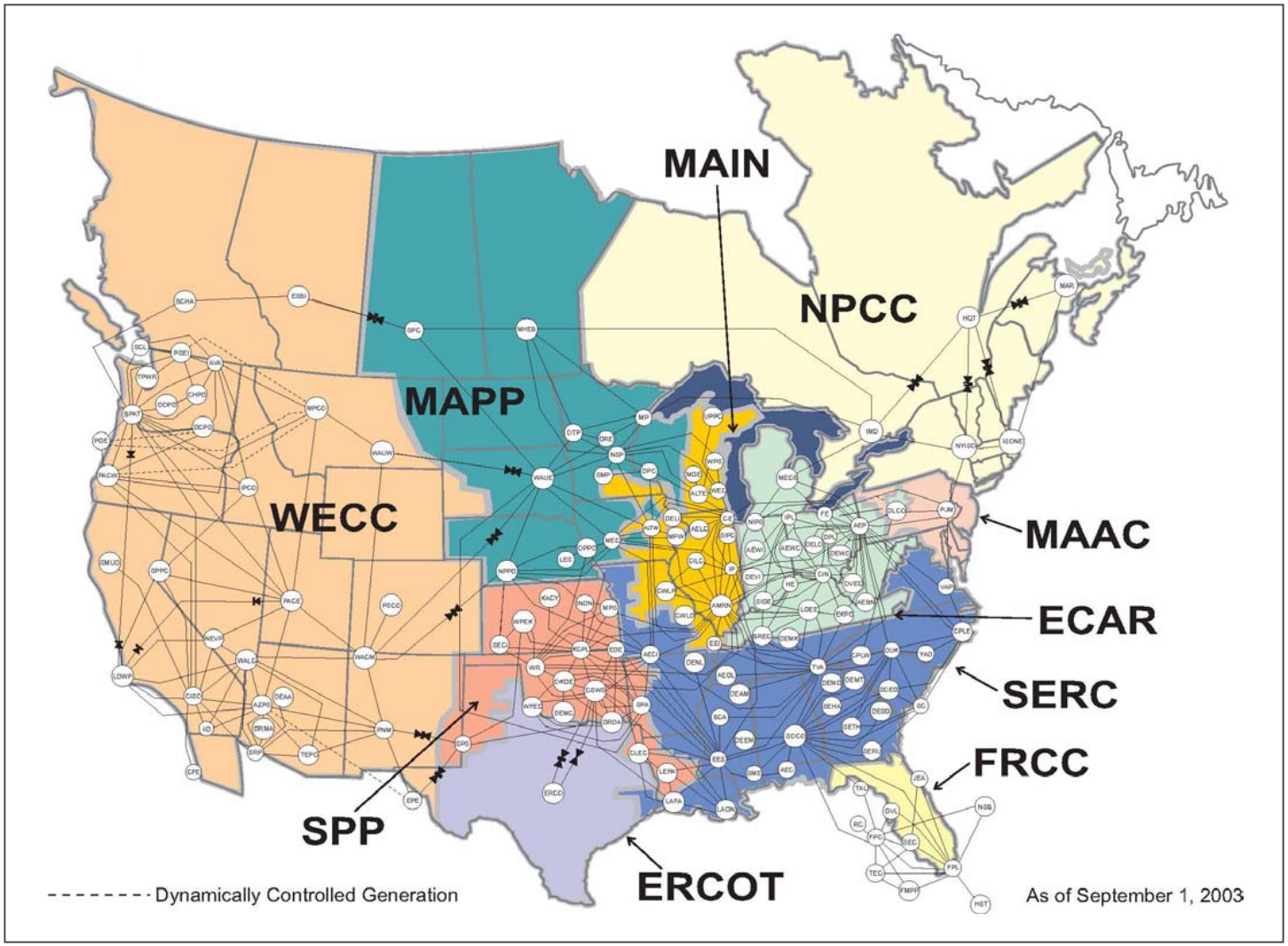
Existing

Available

Future

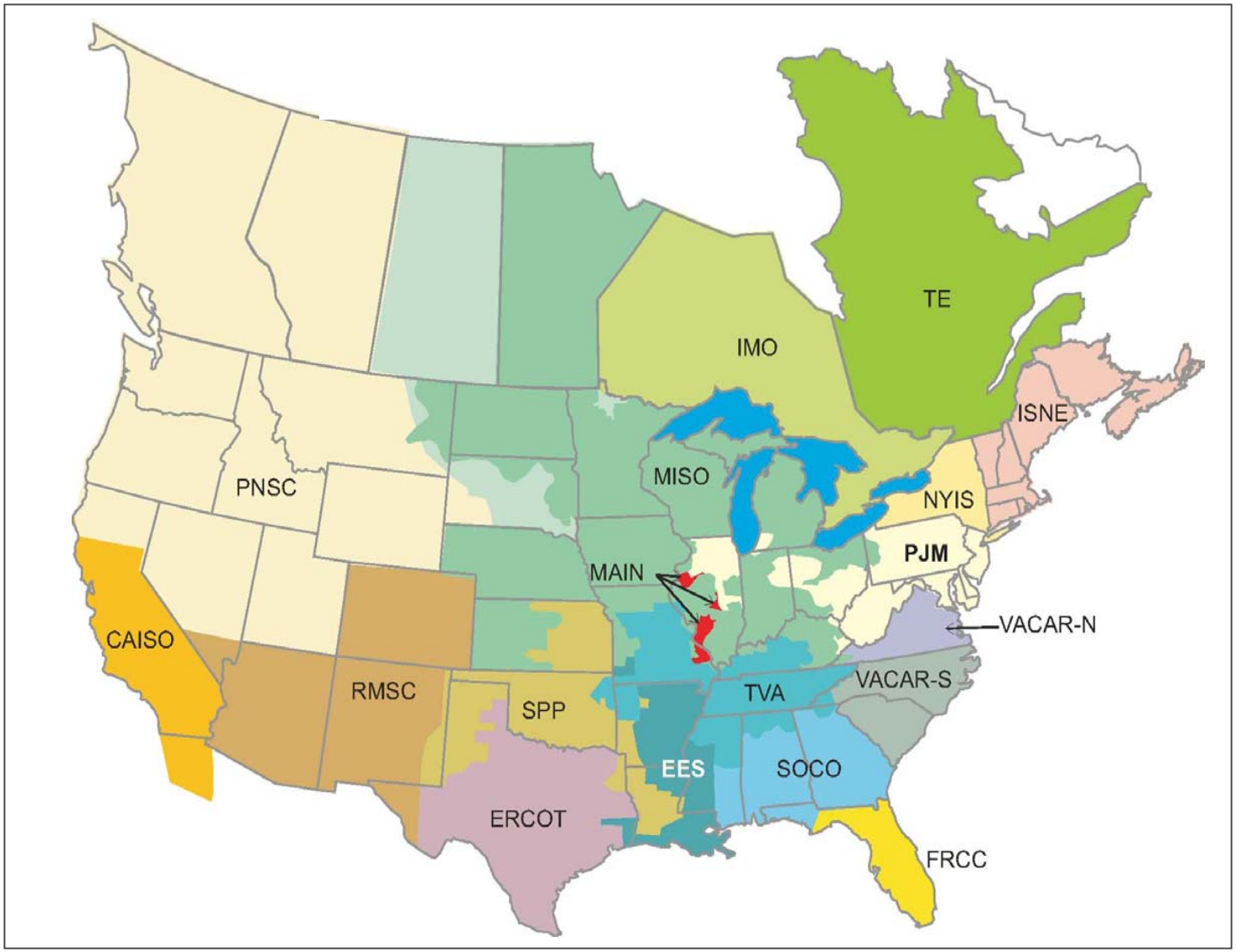
Who are our clients?

NERC Control Areas



Who are our clients?

Reliability Coordinators & ISOs

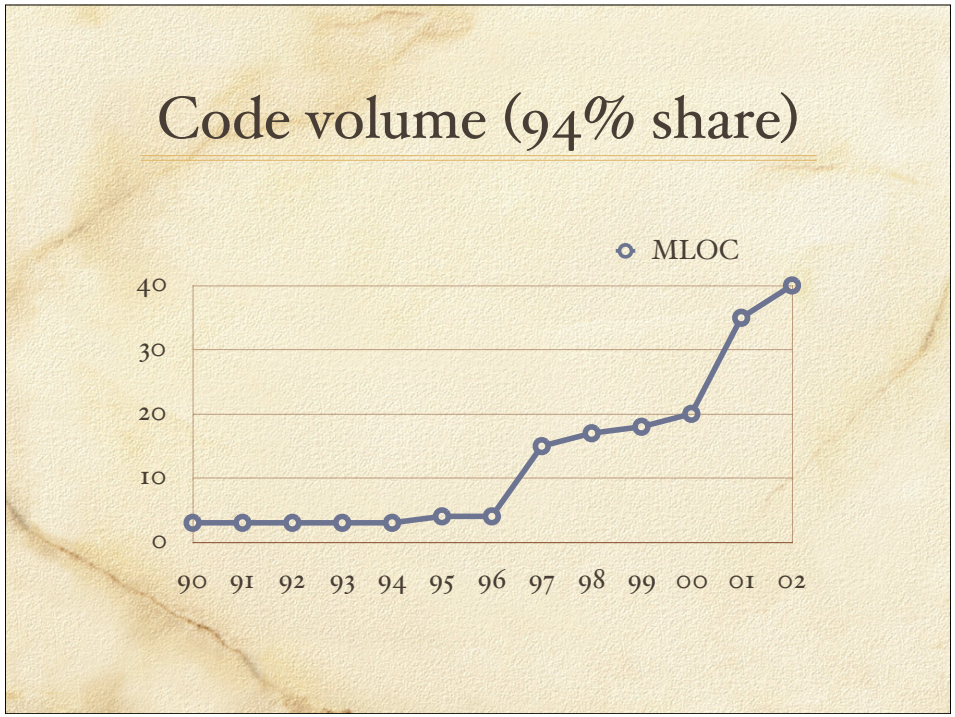


Cascade, Monoculture, Policy

Daniel E. Geer, Jr., Sc.D.

1

Daniel E. Geer, Jr., Sc.D.
Principal, Geer Risk Services
Post Office Box 390244
Cambridge, Mass. 02139

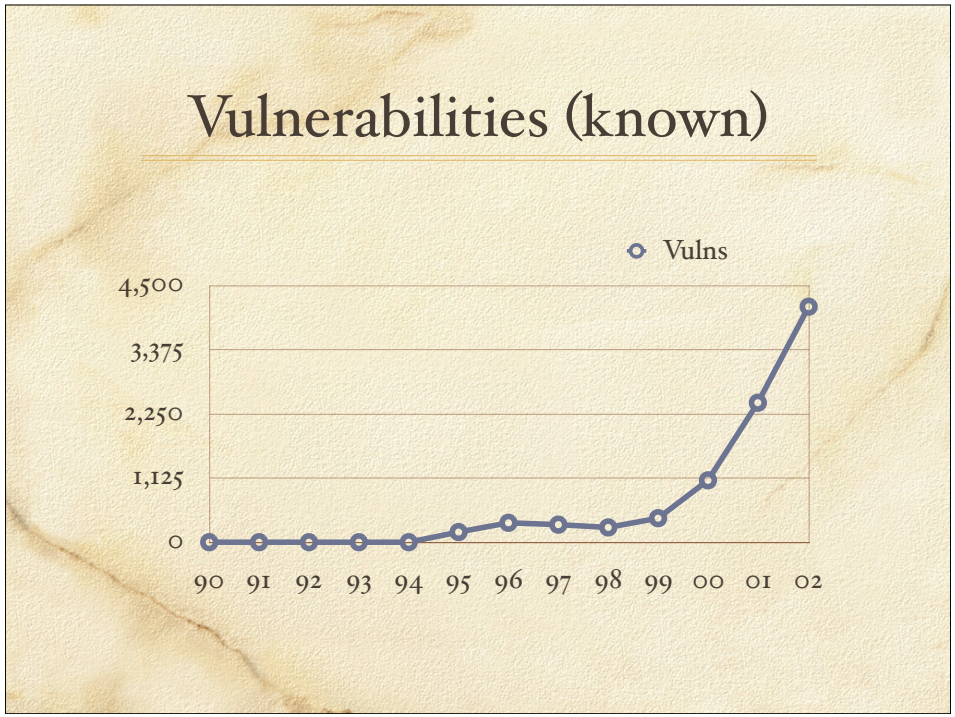


2

Windows 94% market share per IDC

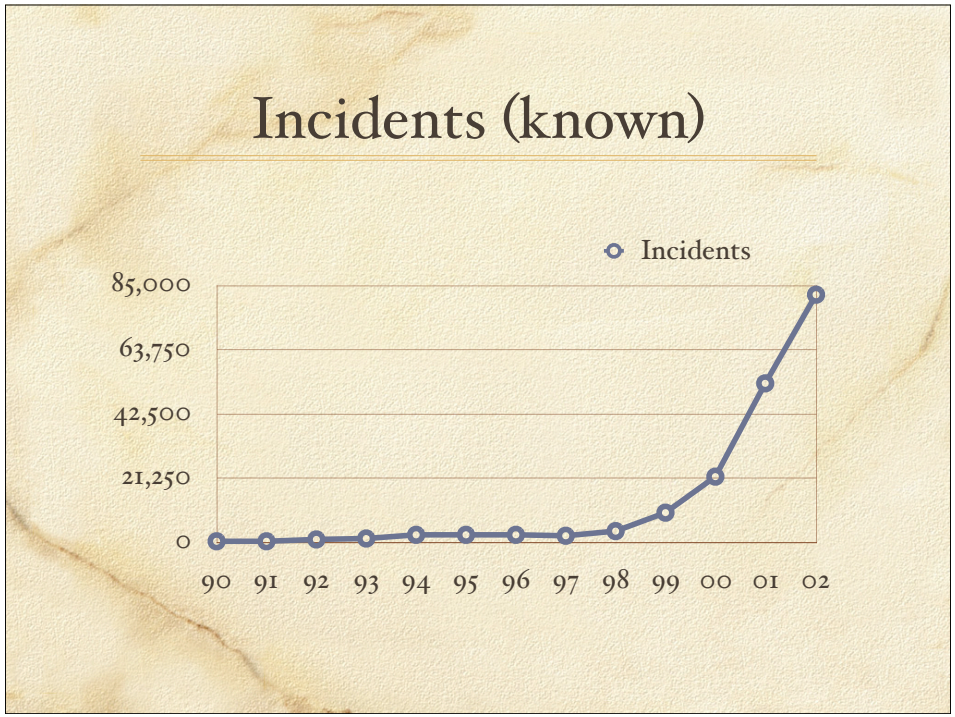
Code volume as observed:

Win 3.1	Win NT	Win 95	NT 4.0	Win 98	NT 5.0	Win 2K	Win XP
3	4	15	17	18	20	35	40
1990	1995	1997	1998	1999	2000	2001	2002

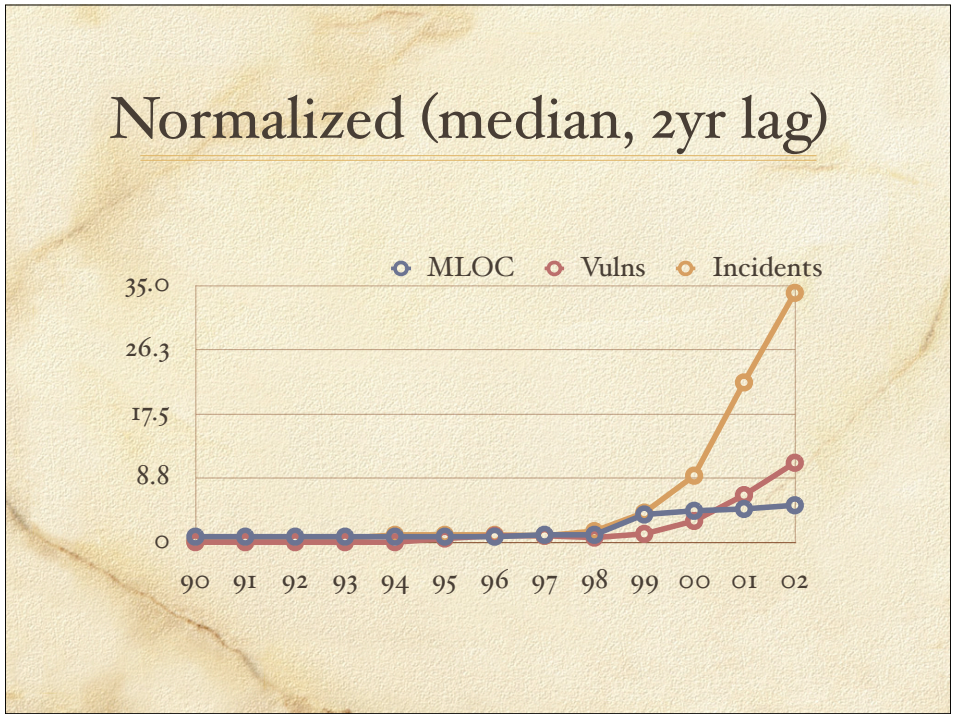


3

Public CERT data

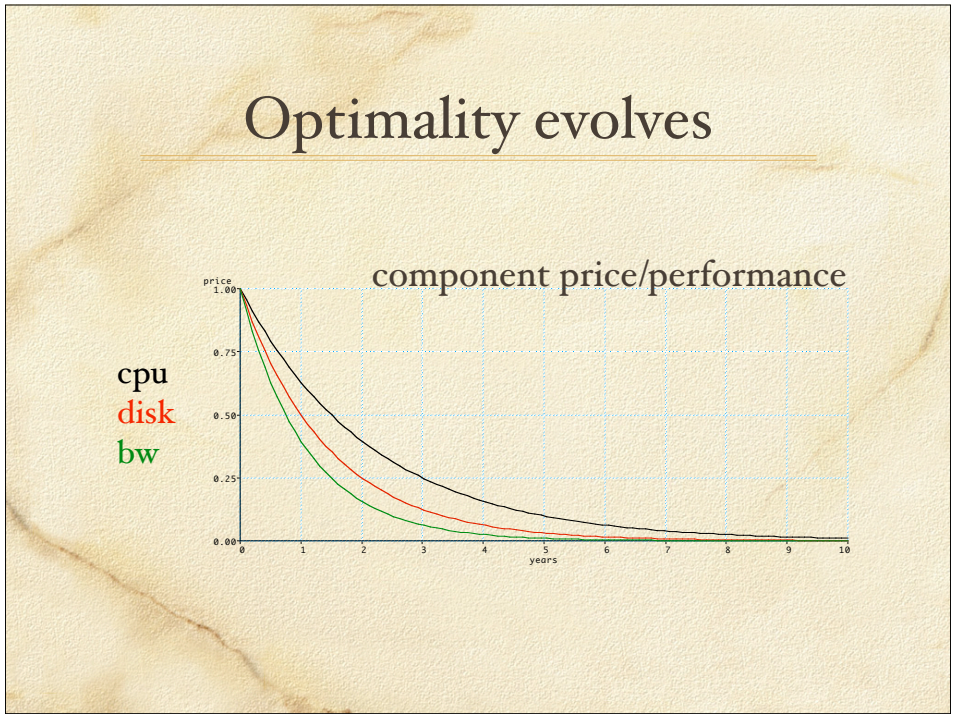


Public CERT data



Each curve is normalized against its own median over this period.

Code volume curve is shifted right two years to simulate diffusion delay.



6

Moore's Law is "cpu" curve, i.e., price/performance falls by 50% every 18 months.

Similar curves for data storage (halving at 12 months) and bandwidth (halving at 9 months). [These are lab results; market introduction is a lagged step function.]

Ten year outlook is, for constant dollars, two orders of magnitude for processing power, three orders of magnitude for data capacity, and four orders of magnitude for transmission capacity. This changes the economically optimal computing platform.

Thus do countermeasures

- WAS trust-mediated => the firewall
- IS application-mediated => the code scanner
- WILL BE data-mediated => tracking & sync

... As the threat rises the perimeter contracts

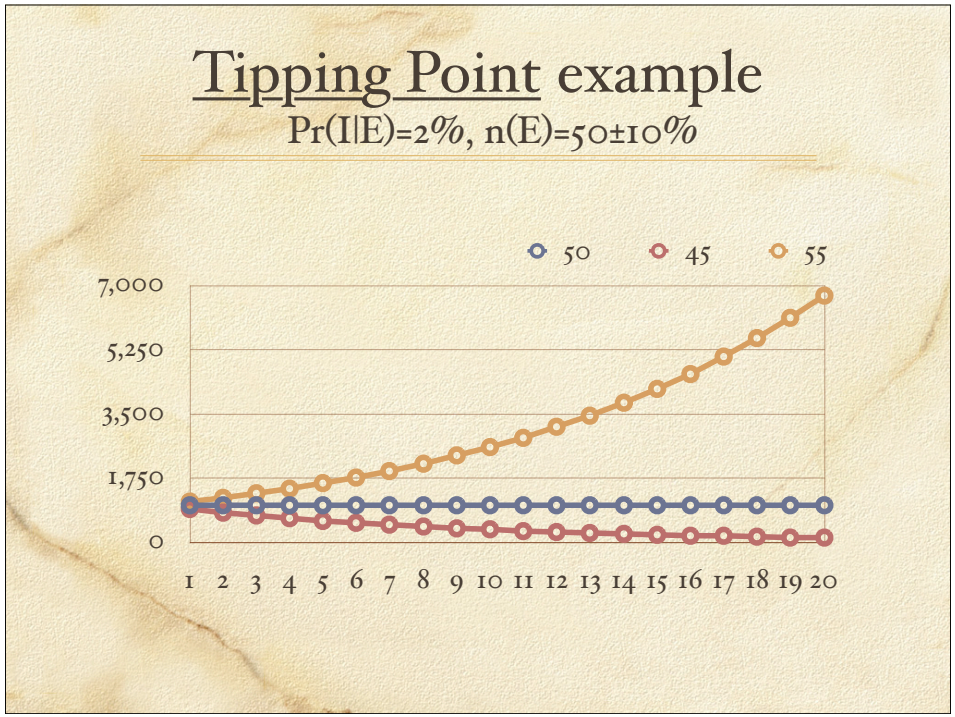
Security must be designed for what will be. Note that the change in optimality makes the question of external vs. internal attack scenarios largely moot.

Epidemics

- Characteristics of infectious processes
  - Pr(infection|exposure)
  - interval from infection to infectiousness
  - duration of infectiousness
  - interval from infection to symptoms
  - duration of acquired immunity

8

The math for modeling epidemics is well developed, as is the math for accelerated failure time testing, actuarial science, portfolio management, and others. There is no need, and no time, to invent new science before progress can be made. Steal these skills, and do so while the senior practitioners in security still include people with these sort of skills learned elsewhere. The hybrid vigor in the security field is at a maximum today before formal education begins to supply trained practitioners, rather than self-selected career changes as been the case heretofore.



This is simply the example used in Gladwell's The Tipping Point. It illustrates the chaotic nature of epidemics which is to say that small changes in initial conditions produce large changes in downstream values. This example is where the initial number of cases is 1,000, the probability of infection given exposure is 2%, the number of exposure events while infectious is 50 plus or minus 5 (10%), and the downstream shows that in only 20 days at -10% the disease will die out while in only 20 days at +10% the epidemic will be well underway.

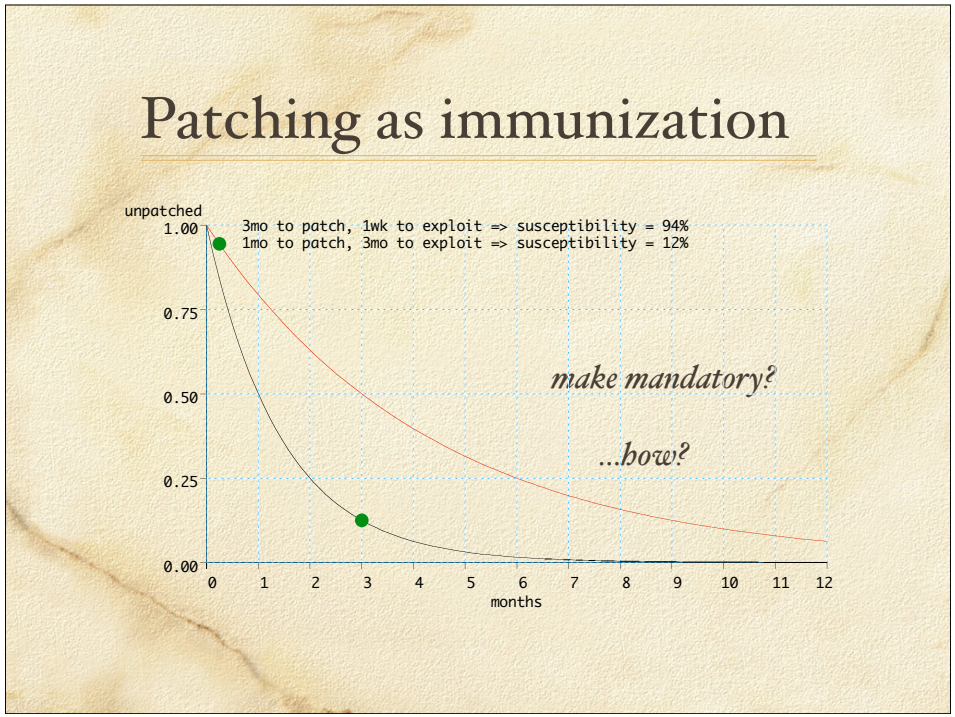
Worst case disease

- Pr(infection|exposure) = 1.0
- interval from infection to infectiousness = 0
- interval of infectiousness = open ended
- interval from infection to symptoms = indef
- duration of acquired immunity = 0 (mutates)

10

If you were designing a pessimal disease, it would be perfectly transmissable (100% chance of getting the disease once exposed and no acquired immunity), no symptomatic sign of infection, and an instantaneous conversion from pre-infection to infections (or from prey to predator, if you prefer).

The above describes worm propagation, or DDOS zombies, or the stockpiling of unannounced vulnerabilities.



11

Qualys, Inc., has data that implies patching is like radioactive decay in that 50% of the remaining unpatched systems will be patched in each succeeding “half-life.” Qualys’s figure is 30 days.

Posting a patch starts a race wherein the patch is reverse-engineered to produce exploits. The two data points are intended to bracket current reality. In the one case, if patching does have a one-month half-life while the reverse engineering interval is 90 days, then the susceptibility would be 12% at the moment of exploit. By contrast, if patching has a three-month half-life while the reverse engineering interval is one week, then the susceptibility would be 94% at the moment of exploit.

Time-to-exploit is shrinking while the time-to-patch is lengthening (if you factor in the growth of always-on, always-connected home machines) so the question becomes whether “mandatory” is a word we must use and, if so, what would it mean.

never enough time...
...so let's talk

Daniel E. Geer, Jr., Sc.D.
Principal, Geer Risk Services
Post Office Box 390244
Cambridge, Mass. 02139