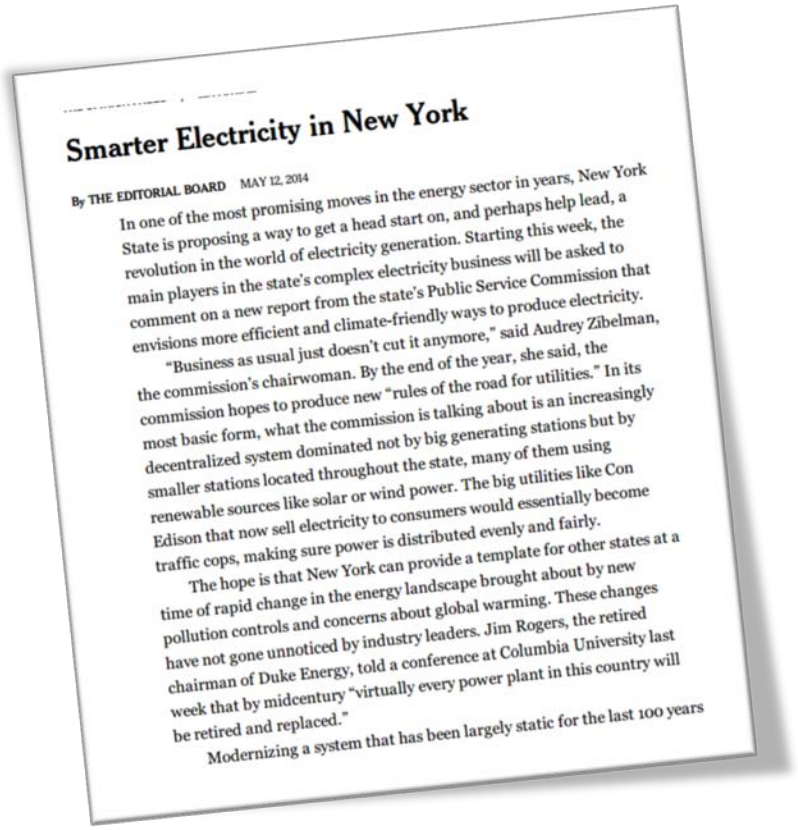
HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

Cybersecurity and Electric Power: An Interdisciplinary Public Policy Challenge

HEPG: Session Three
June 13, 2014

Professor Venkatesh Narayanamurti
Benjamin Peirce Professor of Technology and Public Policy and Professor of Physics
Faculty Chair and Director, Science, Technology, and Public Policy Program

The Security Paradox: Physical Security and Cybersecurity



Smarter Electricity in New York

By THE EDITORIAL BOARD MAY 12, 2014

In one of the most promising moves in the energy sector in years, New York State is proposing a way to get a head start on, and perhaps help lead, a revolution in the world of electricity generation. Starting this week, the main players in the state's complex electricity business will be asked to comment on a new report from the state's Public Service Commission that envisions more efficient and climate-friendly ways to produce electricity.

"Business as usual just doesn't cut it anymore," said Audrey Zibelman, the commission's chairwoman. By the end of the year, she said, the commission hopes to produce new "rules of the road for utilities." In its most basic form, what the commission is talking about is an increasingly decentralized system dominated not by big generating stations but by smaller stations located throughout the state, many of them using renewable sources like solar or wind power. The big utilities like Con Edison that now sell electricity to consumers would essentially become traffic cops, making sure power is distributed evenly and fairly.

The hope is that New York can provide a template for other states at a time of rapid change in the energy landscape brought about by new pollution controls and concerns about global warming. These changes have not gone unnoticed by industry leaders. Jim Rogers, the retired chairman of Duke Energy, told a conference at Columbia University last week that by midcentury "virtually every power plant in this country will be retired and replaced."

Modernizing a system that has been largely static for the last 100 years

Editorial, *New York Times*, May 12, 2014

- Improving Physical Security May Undermine Cybersecurity
  - Decentralization of Physical Assets, May Increase the Attack Surface for Cyber Attacks and Exploits
  - Governing Emerging Technologies: How Do we Capture the Benefits of Decentralization, while Managing the Risks of Increased Reliance on Information and Communication Technologies (ICTs)?

Reconciling Cybersecurity and Markets: Learning from Hurricane Sandy

- Secure, Affordable, Reliable, Innovative, and Profitable: Tensions and Trade-Offs
  - Cybersecurity and Commerce are Not Always Perfectly Compatible
  - How Do We Shape Markets to Provide Multiple, at Times Conflicting and Competing Values?

The Christian Science Monitor - CSMonitor.com

4 ways to get phone service the next time a hurricane Sandy calls

In the aftermath of a disaster such as superstorm Sandy, two-way communication is essential. People need to be able to receive news and updates, and to request assistance and provide status updates to loved ones.

Yet after hurricane Sandy, large portions of New York, New Jersey, and other areas lost their communication systems – their mobile phone network, cable TV, and Internet. Some sought out the last few pay phones as the only equipment that worked.

Here are four ways to better prepare our phones and other devices for the next disaster:

By Tolu Odumosu and Venky Narayanamurti
posted December 3, 2012 at 9:18 am EST

1.Aim for a resilient power supply

A man works on local phone lines during the arrival of the nor'easter in Hoboken, New Jersey, Nov. 7. The winter storm dropped snow, wind, and flooding to a region still climbing out from the devastation of superstorm Sandy. (Eduardo Munoz/Reuters)

Above all, America's telecommunications system depends on the electric grid. It is possible to protect the grid by burying power lines and creating alternate lines of

T. Odumosu and V. Narayanamurti, “4 Ways to Get Phone Service the next Time A Hurricane Sandy Calls, *Christian Science Monitor*, Dec. 3., 2012

Governance Under Uncertainty: Knowledge about Cybersecurity is Limited and Provisional

Cybersecurity: What We Know

- Information and Communication Technologies (ICTs) are Central to the Provision of Electric Power
- The Electric Power Grid will Remain Vulnerable to Cyber Attack and Cyber Exploitation: Zero-Day Vulnerabilities are an Ongoing Challenge
- Cyber Attack Can Cause Physical Damage (e.g., Stuxnet)
- Malicious Actors Target the Electric Power Grid
- Our Reliance on ICTs Will Continue to Grow

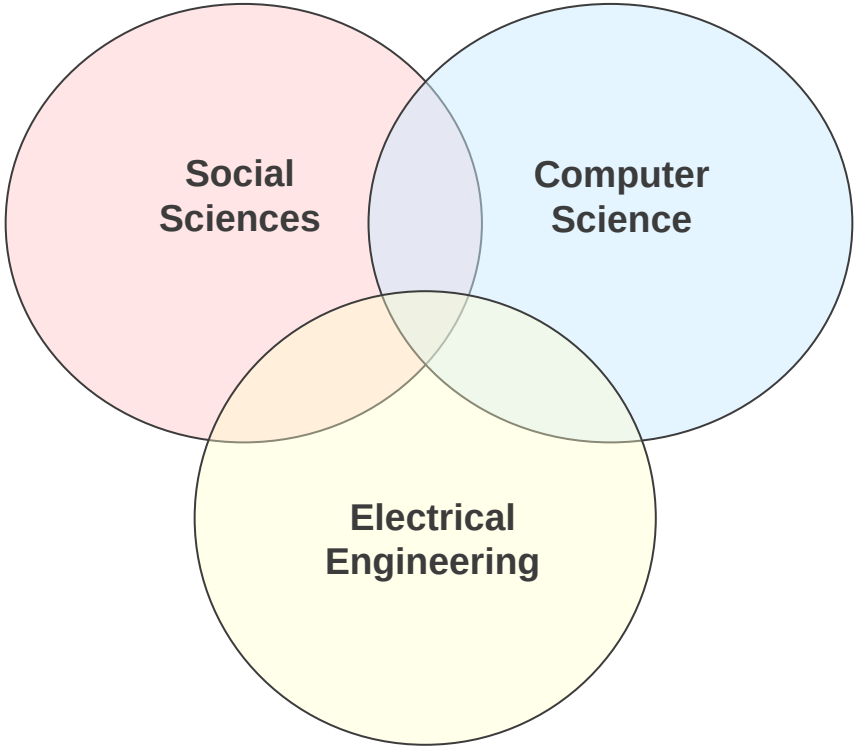
Governance Under Uncertainty: Knowledge about Cybersecurity is Limited and Provisional

Cybersecurity: What We Do Not Know

- What is the Likelihood of A Disruptive Attack (Now or in the Future)?
- What is the Upper Limit of Damage That Could be Caused by a Cyber Attack (Now or in the Future)?
- How Will the Capabilities of Different Actors (Non-State Actors) Change in the Coming Years?

How Do We Govern the Present Given an Uncertain Future?

Cybersecurity, Electric Power, and Public Policy: **The Importance of Interdisciplinary Exchange**



The Search for Metrics: Fuzzy Terminology, Conflicting Interpretations, and Setting Standards

“Every day, America’s armed forces face millions of cyber attacks”

- General Keith Alexander, Director of the National Security Agency and Commander of U.S. Cyber Command, in a 2010 testimony before the U.S. House Armed Services Subcommittee

Do non-intrusive probes count?

Do exploits that enter a system without authorized access, but leave no trace and cause no damage count as an attack?

- Cybersecurity Governance Must Confront Poor Metrics
- Confusion Around Terminology Prevents the Development of Metrics. It can Lead Different Groups to Make Wildly Different Assessments of Risk Based on the Same Information
- Collaboration of Disciplines is Key
- As Metrics Continue to Mature, Adaptive Standards are Crucial

Discovered Vulnerabilities: What Next?

How Significant are Discovered Vulnerabilities?

- ***Electrical Engineers and Computer Scientists*** Can Identify Vulnerabilities and Inform Us About Possible Power System Impacts

What Quantity of Limited Resources Should we Devote to Managing Risk from Discovered Vulnerabilities?

- ***Social Scientists*** (e.g., Political Scientists, Sociologists, Economists), Can Inform Us About Why These Vulnerabilities Matter, and How Seriously They Should be Considered

Both Questions Need Answers.
Both Sets of Disciplines Have a Key Role to Play.

Governing Emerging Technologies and Evolving Risks: A Cross-Cutting Challenge

We Need to Invest in Security, but How Aggressively and When?

- We Need **Computer Scientists** to Describe Best Practices and the Range of Different Security Options Available
- We Need **Sociologists** to Understand the Range and Hierarchy of Values to Consider, and Help Characterize the Uncertainty
- We Need **Financial Analysts and Risk Management Experts** to Help Understand How Uncertainty Impacts the Optimal Decision

Complex Questions Need Involvement from a Broad Set of Disciplines.

Conclusion: Cybersecurity, Electric Power, and Public Policy

- Cybersecurity is a Public Policy Challenge: Interdisciplinary Engagement is Crucial
- Interdisciplinary Engagement is Difficult: It Often Falls Between the Cracks of Academic Rivalries, Industry Priority, and Governmental Funding Aims
- Emerging Cyber Technologies Carry Uncertain Risks and Uncertain Benefits: Sound Governance Balances Caution and Innovation

Thank You

venky@seas.harvard.edu