New England Conference of Public Utilities Commissioners
necpuc

# Dependence and Interdependence in Critical Infrastructure

*Andy Bochman*
*Senior Grid Security Strategist*
*DOE / Idaho National Lab*

www.inl.gov

INL
Idaho National Laboratory

# Topics

1. Context and Orientation
2. Black Sea Regulator Cyber Training
3. Accounting for Cross-sector Dependence and Interdependencies
4. Cyber Matters in Smart cities, Megacities and Smart Rural
5. Additional Resources

# *About me*

## Work history

- USAF comms
- Cyber start-ups
- IBM Energy & Utilities
- Chertoff Group
- DOE/INL

## Current Position

Grid Security Strategist

Idaho National Lab

National & Homeland Security directorate

## Writing

- The National Security Case for Simplicity in Energy Infrastructure (CSIS)
- IoT, Automation, Autonomy and Megacities, 2025 (CSIS)
- The Mission Chief Security Officer (CXO)

## Blogs (now archived)

SGSB Smart Grid Security Blog

THE DOD ENERGY BLOG Rethinking Military Power

# *Legacy of Energy / Critical Infrastructure Security Leadership*

**Cyber-Physical Grid Protection**

**Critical Infrastructure Assessment**

**US & International Security Policy & Strategy Guidance**

**International Nuclear Cybersecurity**

**Unique capabilities for national infrastructure challenges**

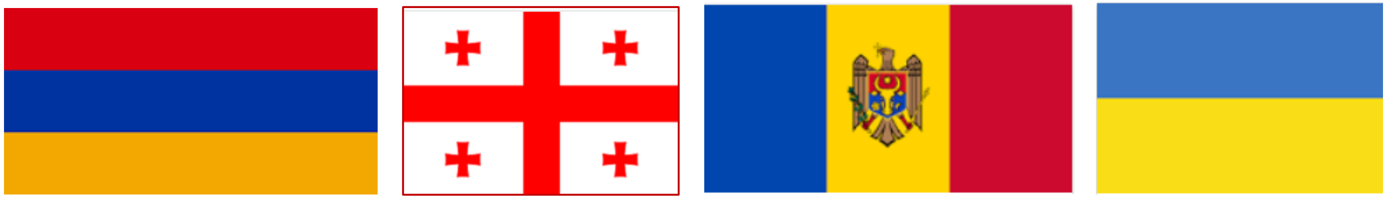
# *USAID, NARUC & USEA Black Sea Cyber Initiative*

## Regional Attack Timeline

- 2007 Estonia
- 2008 Georgia
- 2014-2017 Ukraine

## Objectives

- For Regulators : Accelerate the evolution of energy sector regulators' cyber security knowledge and catalyze the development of regionally tailored electric grid cyber oversight strategies
- For Operators : Sector-specific hands-on cyber training for grid system operators this year.



# *On Modernization (to Black Sea energy regulators)*

**What is it**

Replacing decades old electric & other critical infrastructure elements with modern highly networked digital systems

**Why is it happening … or will soon be happening**

To achieve many new capabilities and efficiencies

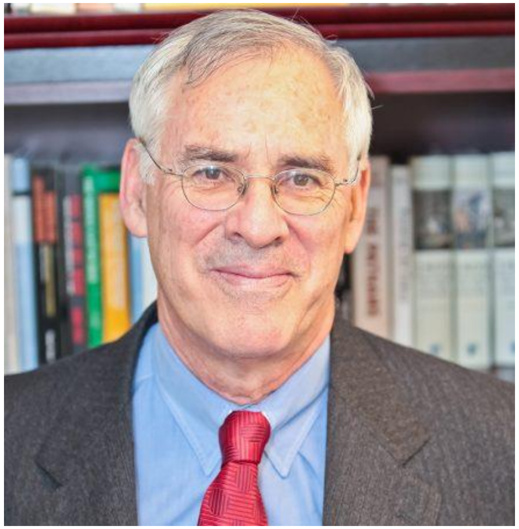
**… and from a Security Perspective?**

Greatly expands the attack surface available to cyber adversaries. These new vulnerabilities need to be recognized and mitigated, preferably before deployment

**Almost Interchangeable Terms**

Prudence, Security Effectiveness, Security Performance, ROSI

# The New Realities : Continuously Contested



Successful strategies must proceed from the premise that cyberspace is **continuously contested territory**.

*Richard Danzig*
*"Surviving on a Diet of Poisoned Fruit”*

# The New Realities : Escalating Dependence

The Wellspring of Risk is Dependence.

*Dan Geer*
*"A Rubicon"*

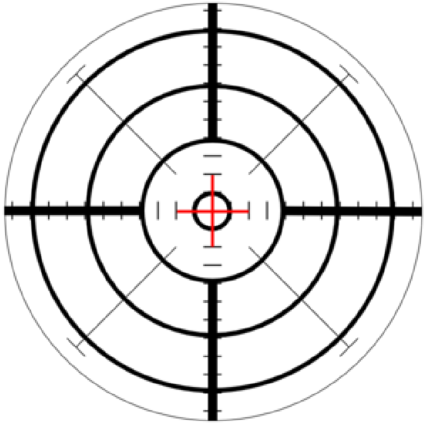
# Geer also said re: interdependencies …

**“It’s like roping all the amateur mountaineers together.”**

Source: “Climbing the North Face of the Uxbridge Road” M. Python

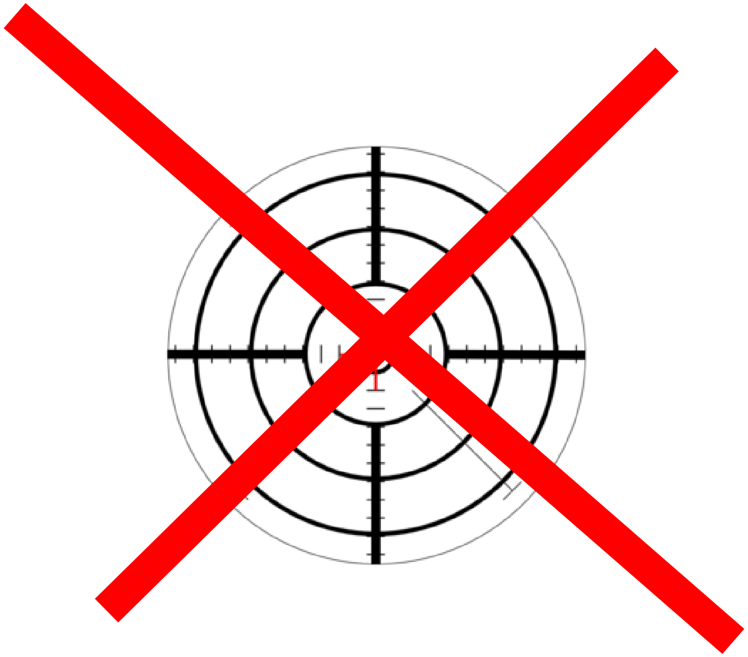
# *The New Realities: Shortest Form*

**If targeted, you will be compromised.**

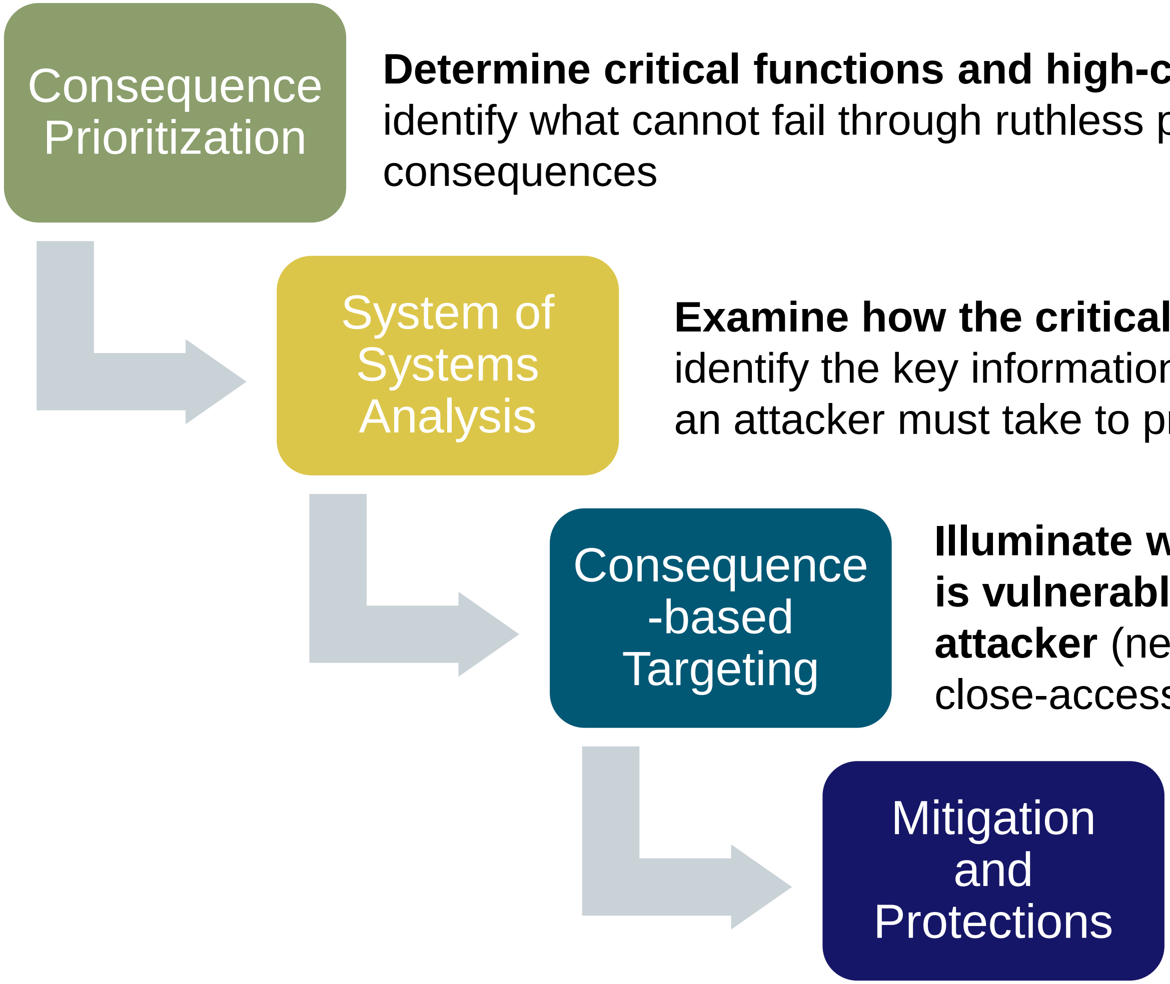


# *Unless …*

**You Take the Targets off the Table**



# CCE – A 4-Step Process



Consequence Prioritization

**Determine critical functions and high-consequence events**; identify what cannot fail through ruthless prioritization based on the consequences

System of Systems Analysis

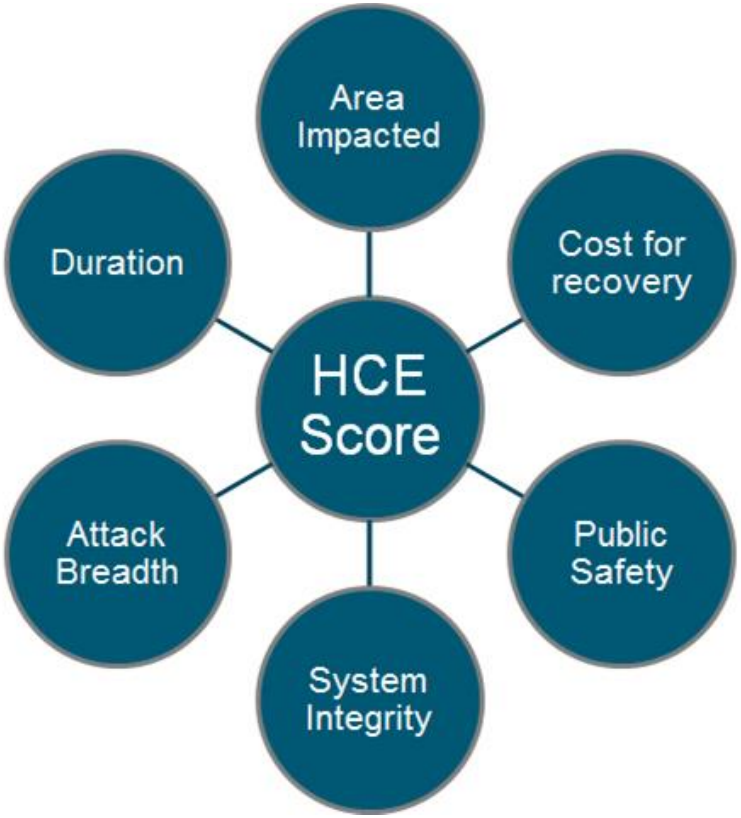
**Examine how the critical function is achieved**; identify the key information, access, and actions an attacker must take to produce an effect

Consequence-based Targeting

**Illuminate where the control system is vulnerable by thinking like an attacker** (networks, supply chain, close-access attacks)

Mitigation and Protections

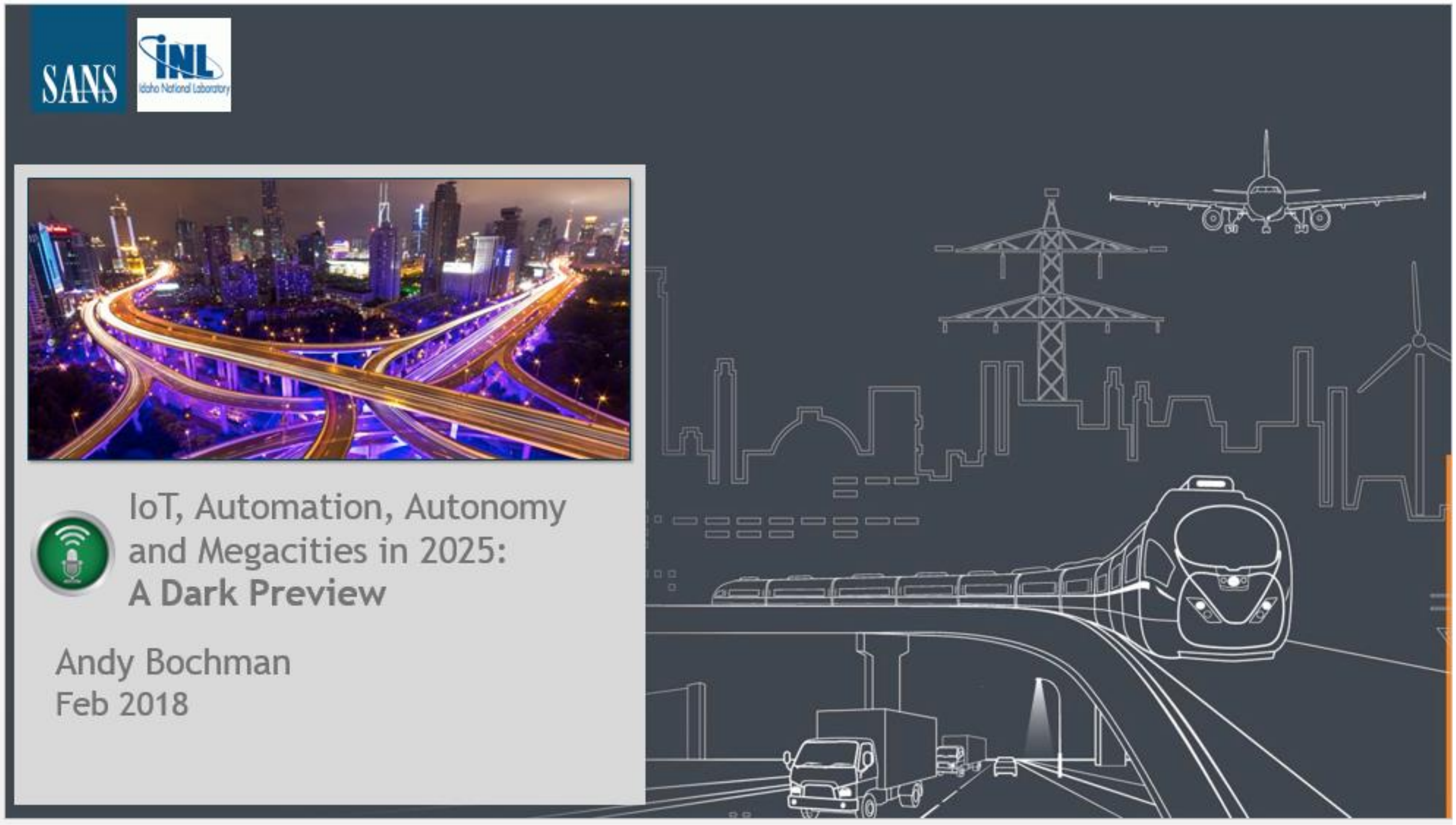
**Engineer-out the cyber-risk;** interrupt the attacker’s progress with simple and complex engineering controls



Certain attackers will find ways to create high consequence events.

# *Interdependencies*

# *Megacities & Interdependencies*



IoT, Automation, Autonomy and Megacities in 2025:
**A Dark Preview**

Andy Bochman
Feb 2018

# *Smart Rural & Interdependencies*

## Business Driver

"One tethered, autonomous aerostat flying at 250 meters can provide as much coverage as 20 or 30 cell towers"

## Need a Plan B

"In the rare occasion that weather conditions are too severe for flight, the system will reel the aerostat back in until it's time to fly again. (*During these times, residents would have to rely on landlines or other forms of communication to contact emergency services, if they were needed*.)"

## Cyber Vector

"A fleet of *SuperTowers* around the country could be monitored remotely from a single network operating center."

https://spectrum.ieee.org/tech-talk/telecom/wireless/soaring-supertowers-to-bring-mobile-broadband-to-rural-areas

# Cautionary Observations

What must we understand while building out future infrastructures

### Cell overload

Technologies implemented to digitize infrastructures have outpaced cell networks

### Restoration overload

Large deployments of things can quickly stakeholder’s ability outpace to restore them with widespeard common failures

### Mass cascades

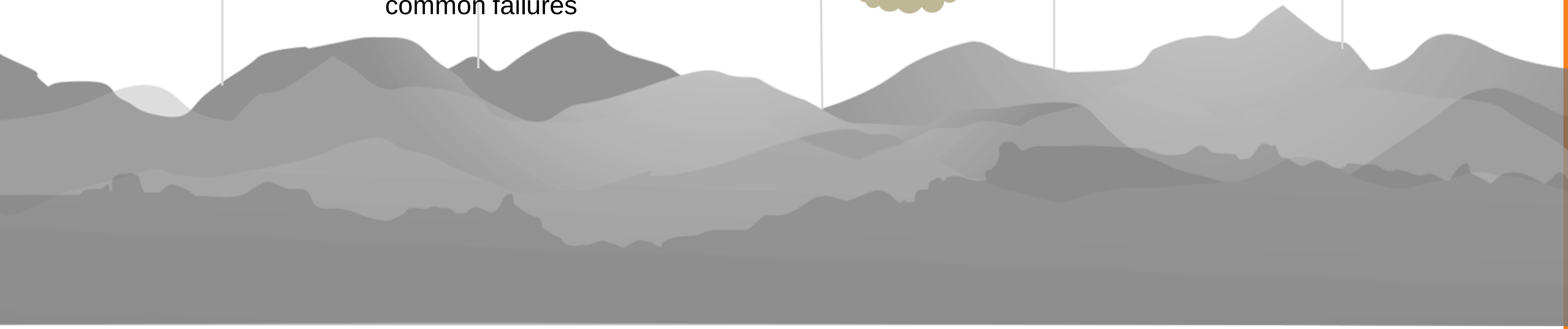
Single system disruptions can quickly cascade as large concentrations of people are impacted

### Software @scale

Software introduces karge-scale systemic risk. Be aware of mono-culture risk

### Complexity

Difficulties in risk detection because of complexity, opacity, and disguise

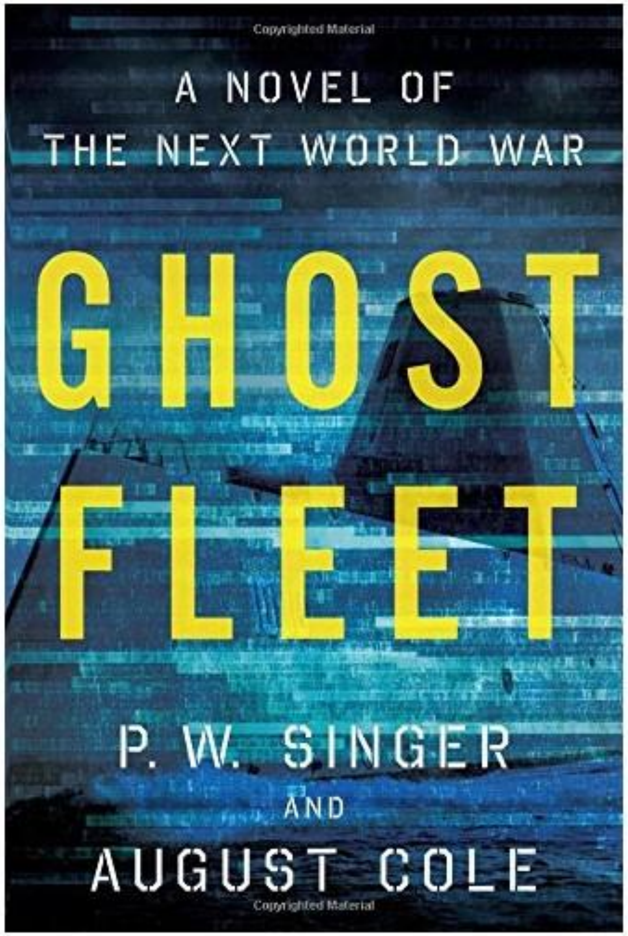


# *Additional Resources*

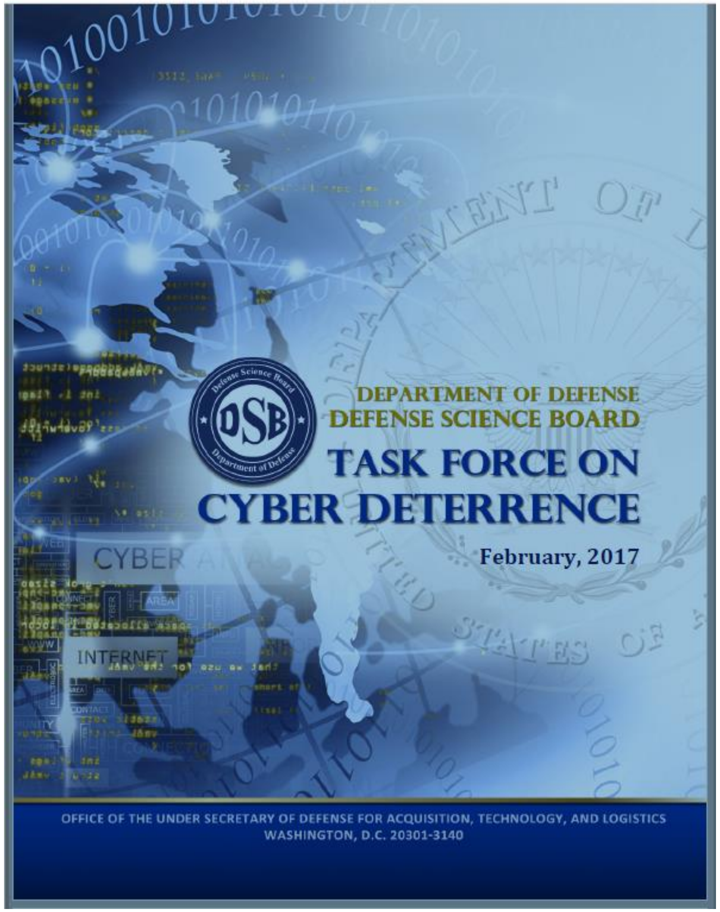
# SANS : Targeted ICS Attack

https://www.youtube.com/watch?v=_eNB1gq5gbA

# *A Narrative Backdoor*



# The Most Sobering USG Account



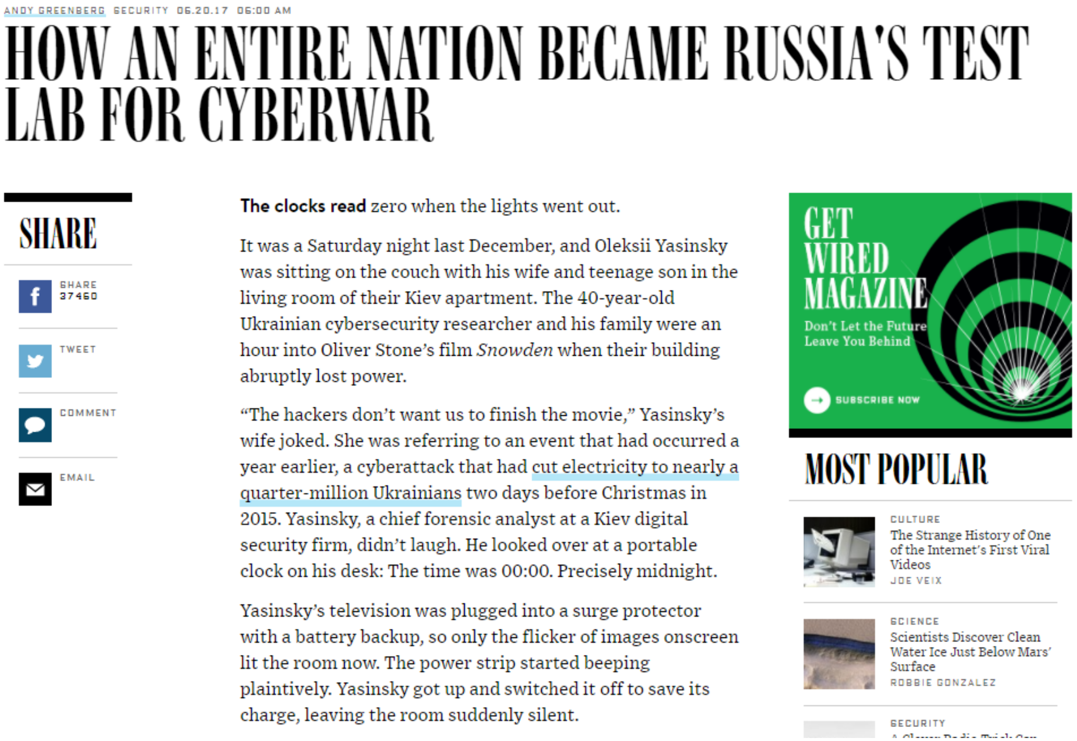
DEPARTMENT OF DEFENSE
DEFENSE SCIENCE BOARD
TASK FORCE ON
CYBER DETERRENCE
February, 2017

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
WASHINGTON, D.C. 20301-3140

Report says that the United States military is at a critical junction when it comes to the cyber security, and therefore the dependability, of some of its own most important weapon systems. The DSB recommends the urgent creation of a "**cyber-resilient** second-strike capability" to ensure the US can strike back after a massive surprise cyber attack by the most capable nation-state adversaries.

According to the DSB, the **current imbalance between adversary offensive and US defensive cyber capabilities is so great** that it “threatens to place the United States in an untenable strategic position."

# Extracting (& Sharing) Lessons from Ukraine



ANDY GREENBERG SECURITY 06.20.17 06:00 AM

## HOW AN ENTIRE NATION BECAME RUSSIA'S TEST LAB FOR CYBERWAR

SHARE

SHARE 37460

TWEET

COMMENT

EMAIL

**The clocks read** zero when the lights went out.

It was a Saturday night last December, and Oleksii Yasinsky was sitting on the couch with his wife and teenage son in the living room of their Kiev apartment. The 40-year-old Ukrainian cybersecurity researcher and his family were an hour into Oliver Stone's film *Snowden* when their building abruptly lost power.

"The hackers don't want us to finish the movie," Yasinsky's wife joked. She was referring to an event that had occurred a year earlier, a cyberattack that had cut electricity to nearly a quarter-million Ukrainians two days before Christmas in 2015. Yasinsky, a chief forensic analyst at a Kiev digital security firm, didn't laugh. He looked over at a portable clock on his desk: The time was 00:00. Precisely midnight.

Yasinsky's television was plugged into a surge protector with a battery backup, so only the flicker of images onscreen lit the room now. The power strip started beeping plaintively. Yasinsky got up and switched it off to save its charge, leaving the room suddenly silent.

MOST POPULAR

CULTURE
The Strange History of One of the Internet's First Viral Videos
JOE VEIX

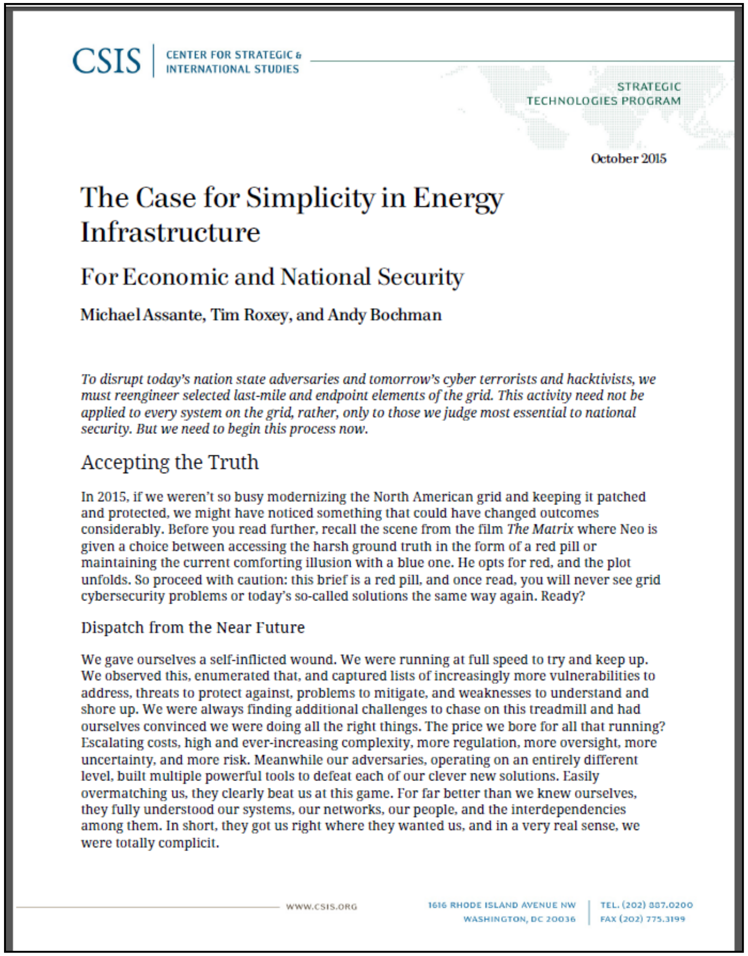
SCIENCE
Scientists Discover Clean Water Ice Just Below Mars' Surface
ROBBIE GONZALEZ

SECURITY

… and a classroom for the ROW

# Valuing Simplicity

***Tim Roxey***
***Mike Assante***
***AB***



CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

STRATEGIC
TECHNOLOGIES PROGRAM

October 2015

## The Case for Simplicity in Energy Infrastructure

### For Economic and National Security

Michael Assante, Tim Roxey, and Andy Bochman

*To disrupt today's nation state adversaries and tomorrow's cyber terrorists and hacktivists, we must reengineer selected last-mile and endpoint elements of the grid. This activity need not be applied to every system on the grid, rather, only to those we judge most essential to national security. But we need to begin this process now.*

### Accepting the Truth

In 2015, if we weren't so busy modernizing the North American grid and keeping it patched and protected, we might have noticed something that could have changed outcomes considerably. Before you read further, recall the scene from the film *The Matrix* where Neo is given a choice between accessing the harsh ground truth in the form of a red pill or maintaining the current comforting illusion with a blue one. He opts for red, and the plot unfolds. So proceed with caution: this brief is a red pill, and once read, you will never see grid cybersecurity problems or today's so-called solutions the same way again. Ready?

### Dispatch from the Near Future

We gave ourselves a self-inflicted wound. We were running at full speed to try and keep up. We observed this, enumerated that, and captured lists of increasingly more vulnerabilities to address, threats to protect against, problems to mitigate, and weaknesses to understand and shore up. We were always finding additional challenges to chase on this treadmill and had ourselves convinced we were doing all the right things. The price we bore for all that running? Escalating costs, high and ever-increasing complexity, more regulation, more oversight, more uncertainty, and more risk. Meanwhile our adversaries, operating on an entirely different level, built multiple powerful tools to defeat each of our clever new solutions. Easily overmatching us, they clearly beat us at this game. For far better than we knew ourselves, they fully understood our systems, our networks, our people, and the interdependencies among them. In short, they got us right where they wanted us, and in a very real sense, we were totally complicit.

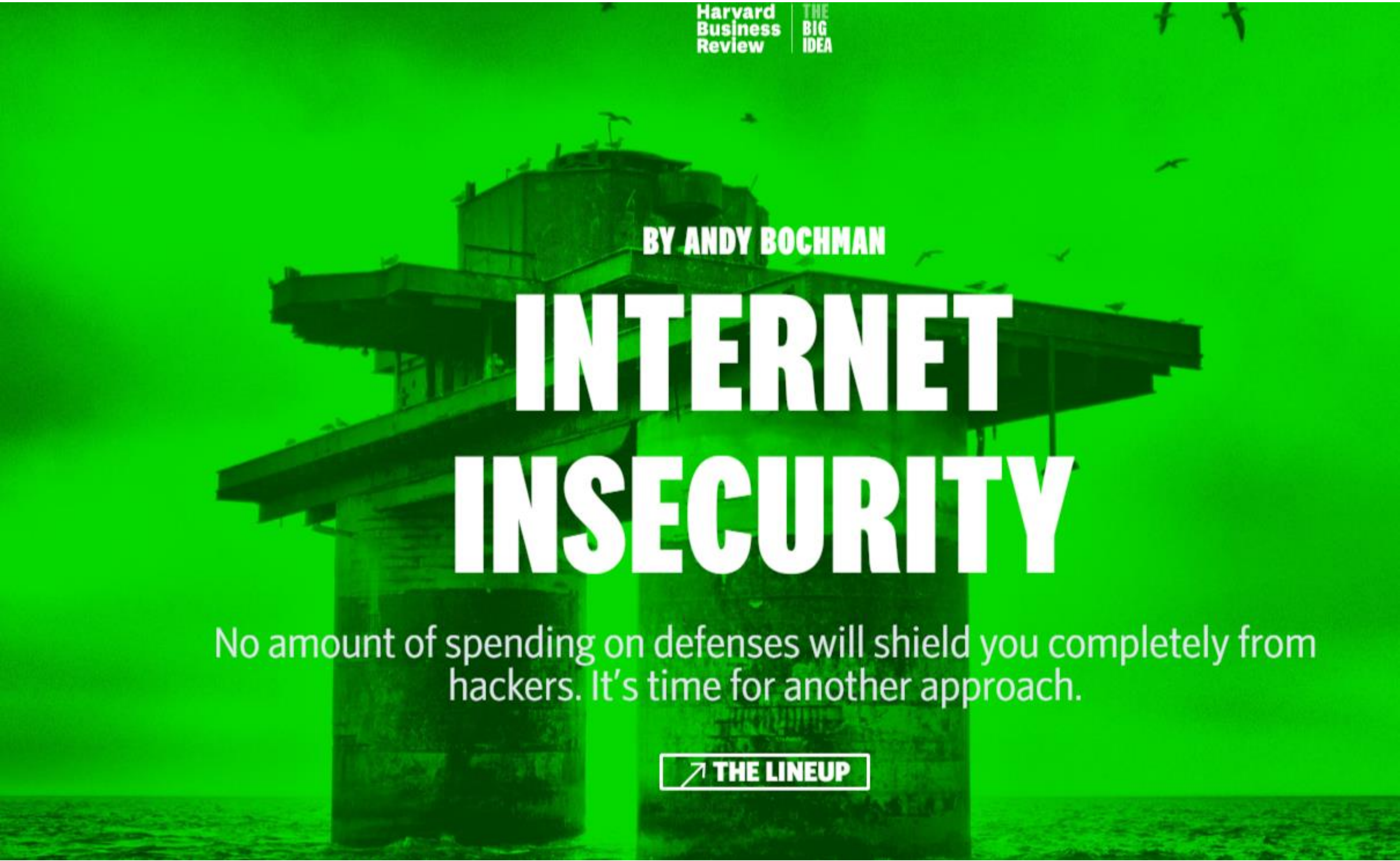
WWW.CSIS.ORG

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036

TEL. (202) 887.0200
FAX (202) 775.3199

"When considering the risks and rewards of going fully digital in the most critical of critical infrastructure systems, the optimal solution will often be a hybrid architecture where the benefits of digital are realized while the determinism of analog is drawn upon as an impermeable bulwark of cyber defense."

# Will Leave You With This …



Harvard Business Review | THE BIG IDEA

BY ANDY BOCHMAN

INTERNET INSECURITY

No amount of spending on defenses will shield you completely from hackers. It's time for another approach.

***Thanks!***
***andrew.bochman@inl.gov***
***@andybochman***