TARGETED AND VULNERABLE:

CYBER THREATS AND SEVERE IMPACTS TO THE GRID

Presentation
For
International Society of Military Law and the Law of War

by

Roland L. Trope
Trope and Schramm LLP

DISCLAIMER:

VIEWS EXPRESSED ARE SOLELY THOSE OF THE SPEAKER,

AND HAVE NOT BEEN REVIEWED OR APPROVED BY,

AND SHOULD NOT BE ATTRIBUTED TO –

THE U.S. MILITARY ACADEMY,

THE DEPARTMENT OF THE ARMY

THE DEPARTMENT OF DEFENSE, OR

THE U.S. GOVERNMENT.

High Impact, Low Frequency Event
The Netherlands, February 1953

High Impact, Low Frequency Event
Japan 2011

OVERVIEW

1. What are key parts of a nation's electric grid?

1. How might a kinetic cyberattack crash the grid?

1. Is the grid's supply chain an attack vector?

2. Should highest priority be – on defense against attacks – or on recovery from attacks?

KEY PARTS OF THE GRID

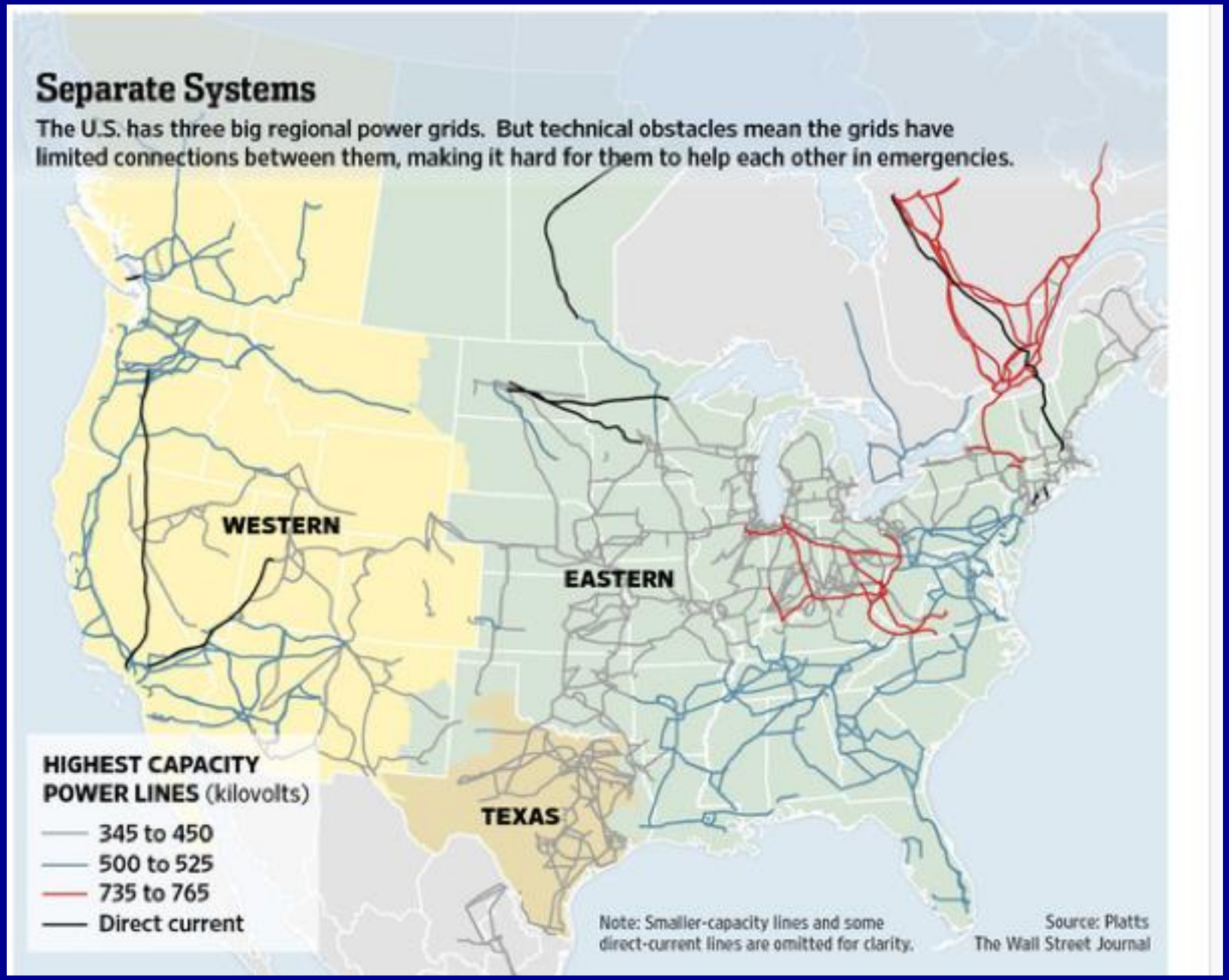
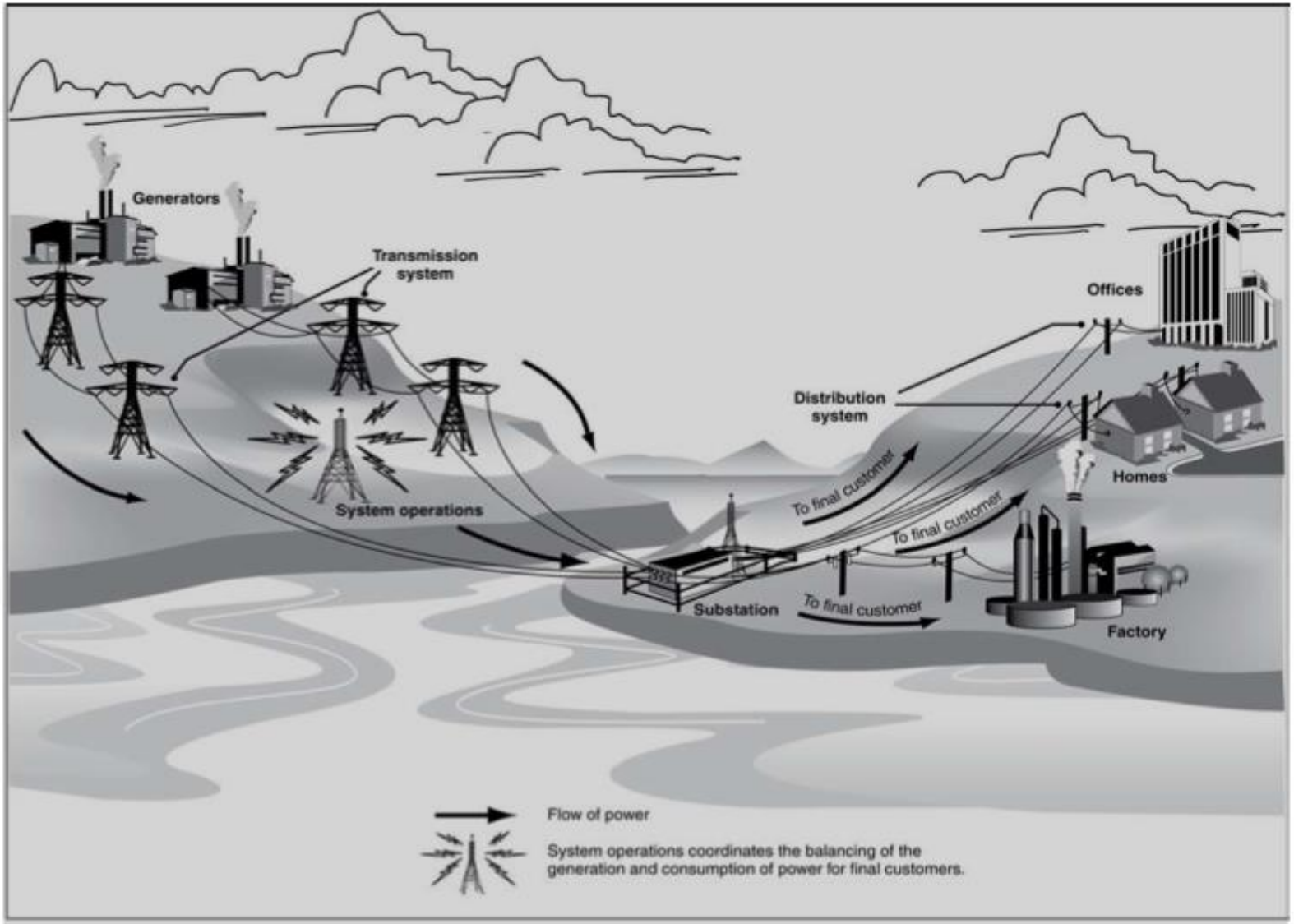
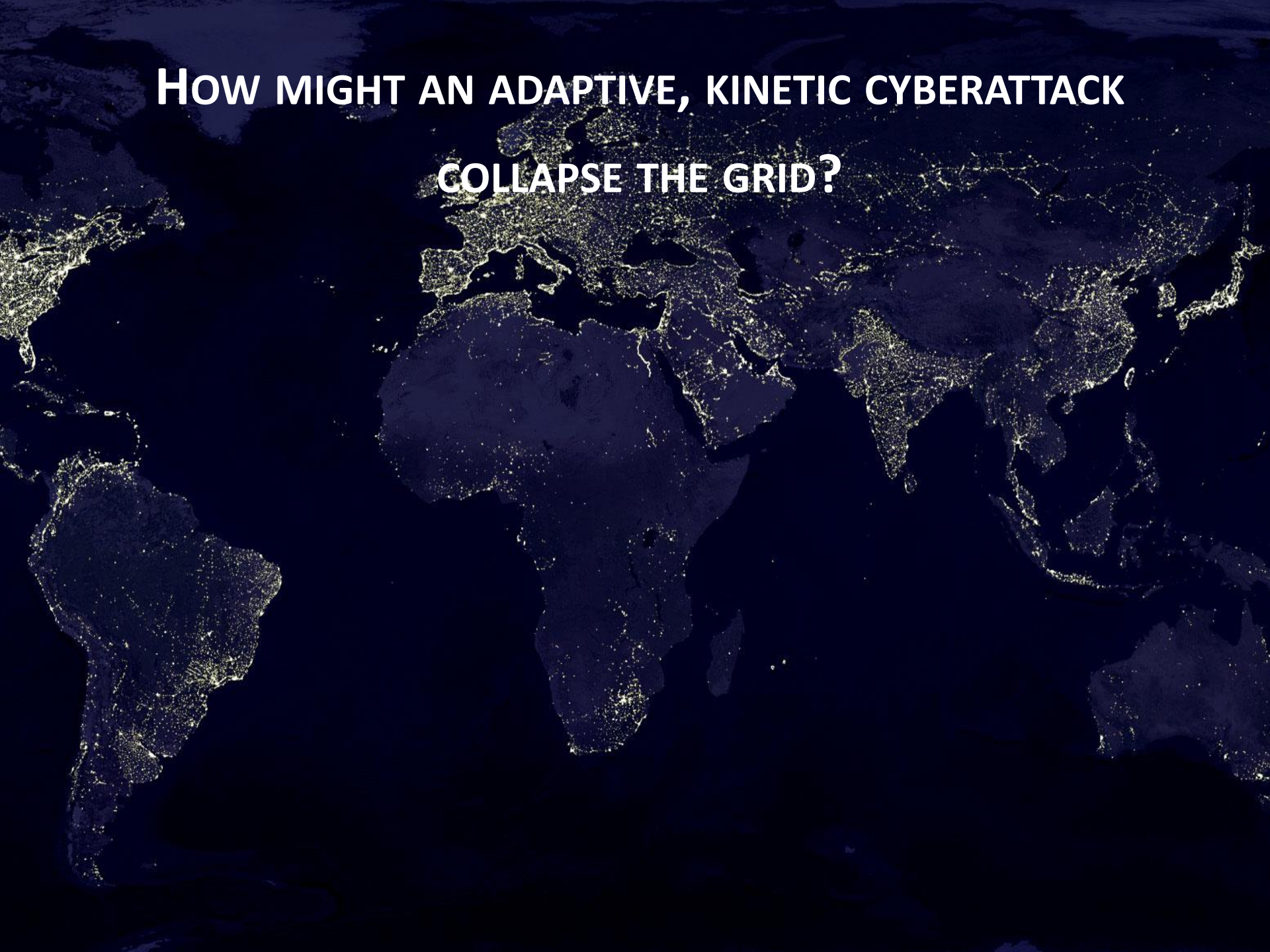

Separate Systems
The U.S. has three big regional power grids. But technical obstacles mean the grids have limited connections between them, making it hard for them to help each other in emergencies.
WESTERN
EASTERN
TEXAS
HIGHEST CAPACITY POWER LINES (kilovolts)
345 to 450
500 to 525
735 to 765
Direct current
Note: Smaller-capacity lines and some direct-current lines are omitted for clarity.
Source: Platts
The Wall Street Journal

Figure 1: Functions of the Electricity Industry



Source: GAO analysis.

How might an adaptive, kinetic cyberattack collapse the grid?



TIMELINE – Experience of Interconnected Widespread Outages

EVENTS IN U.S.

AUG 14:
Blackout in Midwest/Northeast U.S. & Ontario, Canada
50 Million customers lose power

OCT 30:
Hurricane Sandy
> 5 Million lose power

2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013

30 JUN:
Disruption of natural natural gas supply from Indonesia leads to automatic disconnection of power to 30% of Singapore

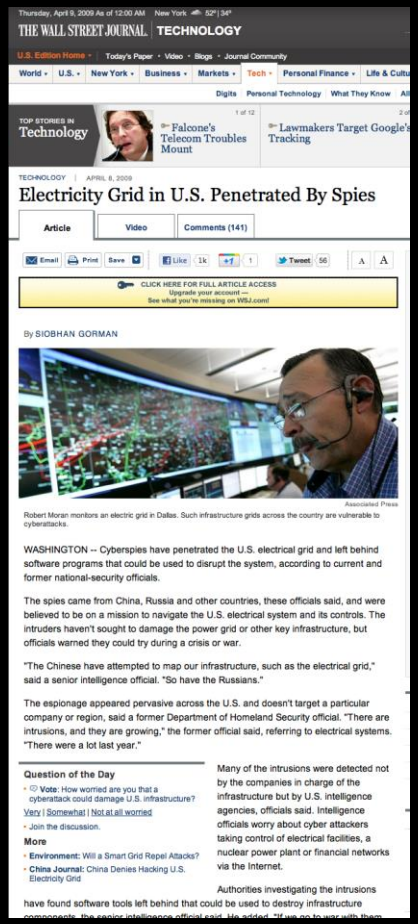
In Brazil power outage to 60 million customers

JUL 31:
Largest blackout in history collapses India's interconnected northern grids
½ Billion people lose power

EVENTS OVERSEAS

July 31, 2012
India's Northeastern Grid Collapse

Warnings



Thursday, April 9, 2009 As of 12:00 AM New York 52° | 34°

THE WALL STREET JOURNAL. | TECHNOLOGY

U.S. Edition Home • Today's Paper • Video • Blogs • Journal Community

World • U.S. • New York • Business • Markets • Tech • Personal Finance • Life & Cultu

Digits | Personal Technology | What They Know | All

TOP STORIES IN Technology

1 of 12

Falcone's Telecom Troubles Mount

Lawmakers Target Google's Tracking

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

Article | Video | Comments (141)

Email | Print | Save | Like 1k | +1 1 | Tweet 56 | A A

CLICK HERE FOR FULL ARTICLE ACCESS
Upgrade your account --
See what you're missing on WSJ.com!

By SIOBHAN GORMAN

Associated Press

Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks.

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.

"The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians."

The espionage appeared pervasive across the U.S. and doesn't target a particular company or region, said a former Department of Homeland Security official. "There are intrusions, and they are growing," the former official said, referring to electrical systems. "There were a lot last year."

Question of the Day

- Vote: How worried are you that a cyberattack could damage U.S. infrastructure?

Very | Somewhat | Not at all worried

- Join the discussion.

More

- Environment: Will a Smart Grid Repel Attacks?
- China Journal: China Denies Hacking U.S. Electricity Grid

Many of the intrusions were detected not by the companies in charge of the infrastructure but by U.S. intelligence agencies, officials said. Intelligence officials worry about cyber attackers taking control of electrical facilities, a nuclear power plant or financial networks via the Internet.

Authorities investigating the intrusions have found software tools left behind that could be used to destroy infrastructure

"We know that cyberintruders have probed our electrical grid."

President Obama 5/29/2009

TIMELINE – Escalating Threats to Critical Infrastructure

EVENTS IN U.S.

Assault rifle attack damages Metcalf substation transformers near Silicon Valley

Iranian cyberattacks on Citigroup, Wells Fargo, Bank of America, and U.S. Bank

China's "Comment Group" penetrates Diablo Canyon nuclear plant

2009 | 2010 | 2011 | 2012 | 2013 | 2014

Stuxnet damages Iranian uranium enrichment centrifuges

Iranian cyberattacks on Aramco, wipe out hard drives on 55,000 PCs – ¾'s of Aramco's corporate PCs

EVENTS OVERSEAS

April 16, 2013 Assault-Rifle Attack on Metcalf Substation Transformers

THE WALL STREET JOURNAL.

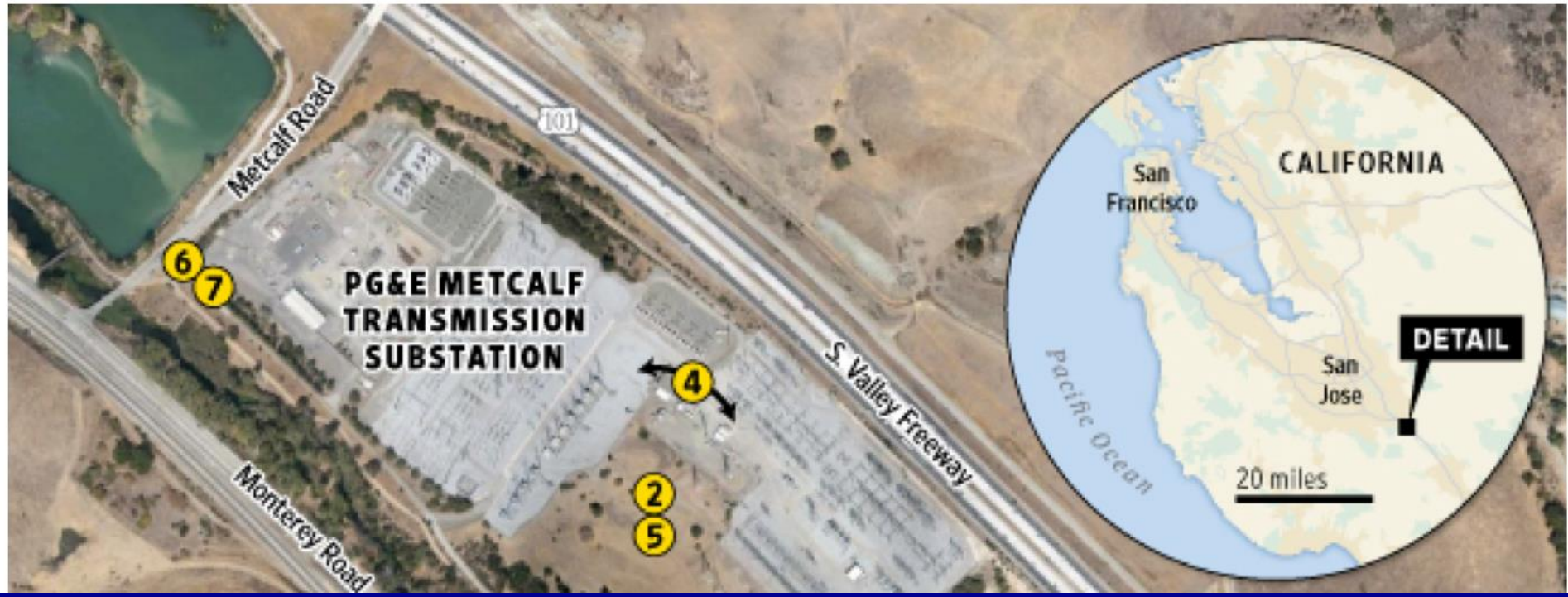
U.S. NEWS

Assault on California Power Station Raises Alarm on Potential for Terrorism

April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid

By REBECCA SMITH

Updated Feb. 18, 2014 3:50 p.m. ET



STATE OF CALIFORNIA EDMUND G. BROWN JR., *Govern*

PUBLIC UTILITIES COMMISSION
505 VAN NESS AVENUE
SAN FRANCISCO, CA 94102-3298

March 10, 2014

Mr. Patrick M. Hogan
Vice President Asset Management, Electric Operations
Pacific Gas & Electric
245 Market Street, #1064 (N10A)
San Francisco, CA 94105

Re: Substation Security

Mr. Hogan:

On April 16, 2013 PG&E's Metcalf Substation was attacked by gunfire, raising concerns about critical infrastructure in California. Continuous electric service is critical for business and public convenience. Therefore, it is imperative that the delivery of electric service be interfered with as little as possible.

Safety and Enforcement Division (SED) hereby directs you and your company to examine your company's security programs and make any necessary changes to minimize the likelihood of a physical or cyber attack on your company's substations. Some revisions may include, but are not limited:

National Research Council 2012 Report

"greatest vulnerability in the event of a terrorist attack on the power system will likely be securing needed replacement of high-voltage transformers."

Wall Street Journal
March 13, 2014

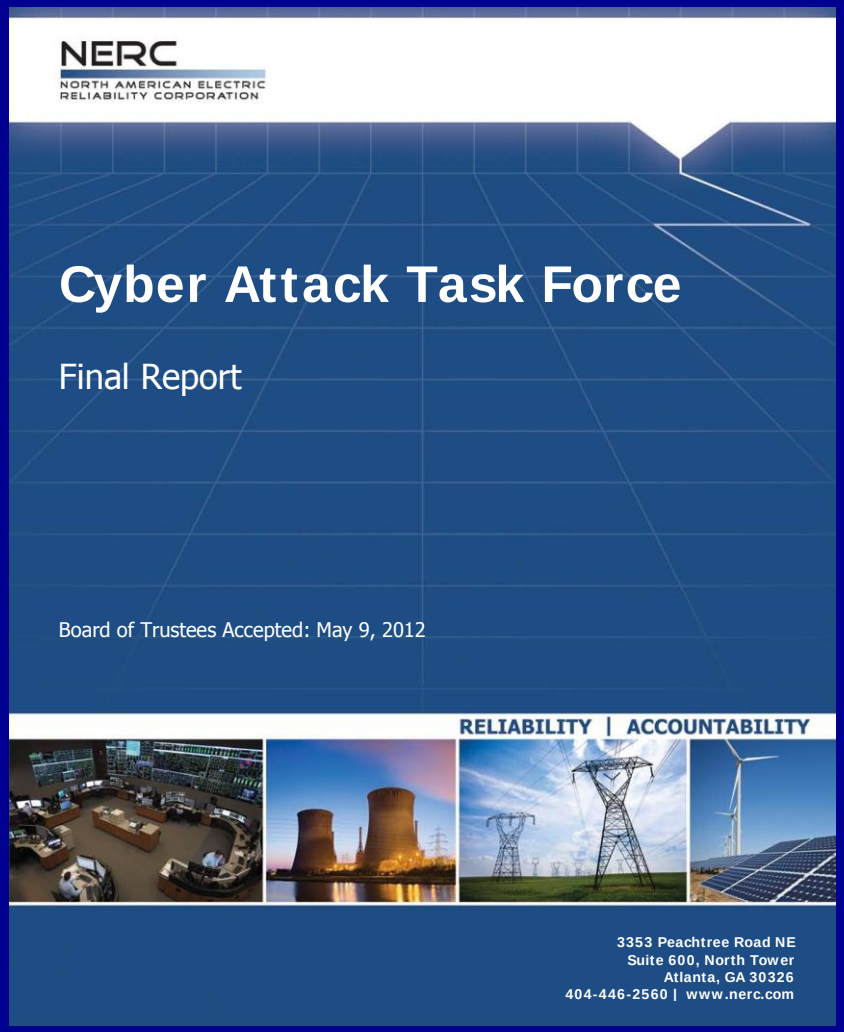
Power Grid Vulnerable To Sabotage

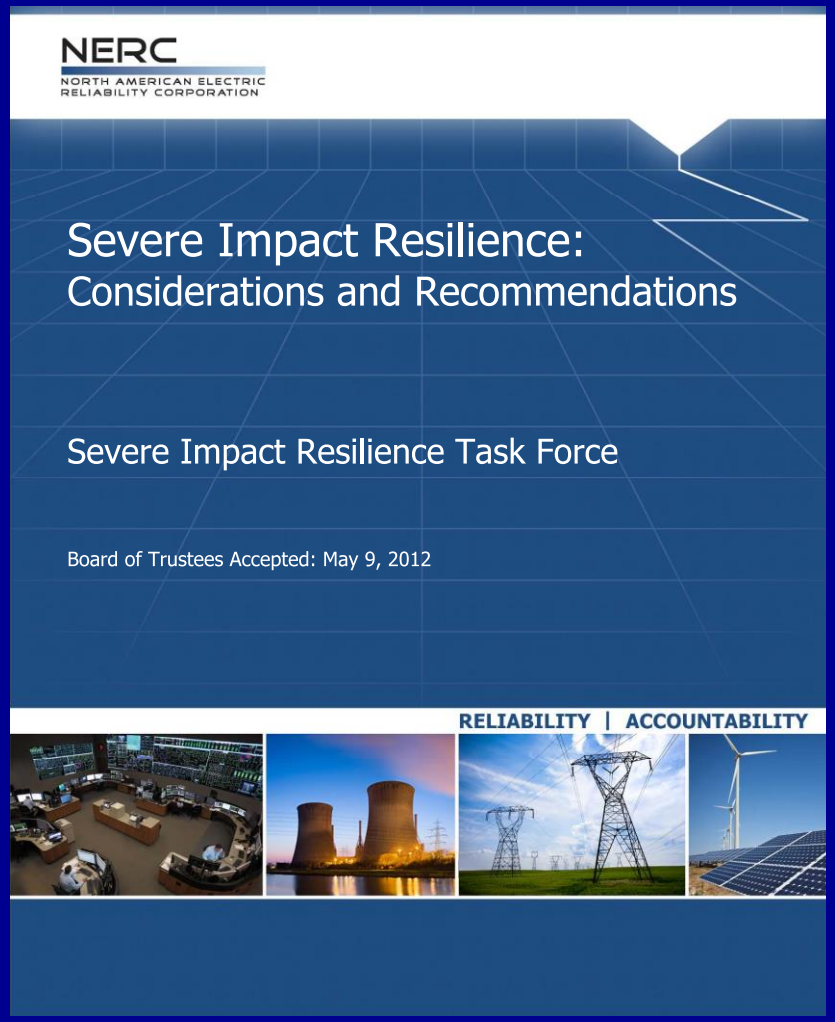
By Rebecca Smith

The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day, according to a previously unreported federal analysis.

The study by the Federal Energy Regulatory Commission concluded that coordinated attacks in each of the nation's three separate electric systems could cause the entire power network to collapse, people fa-

Scenario:
Severe Event Impact





NERC TASK FORCE REPORTS: Cyberattacks Can Blackout Several Regions, If Two Events Occur

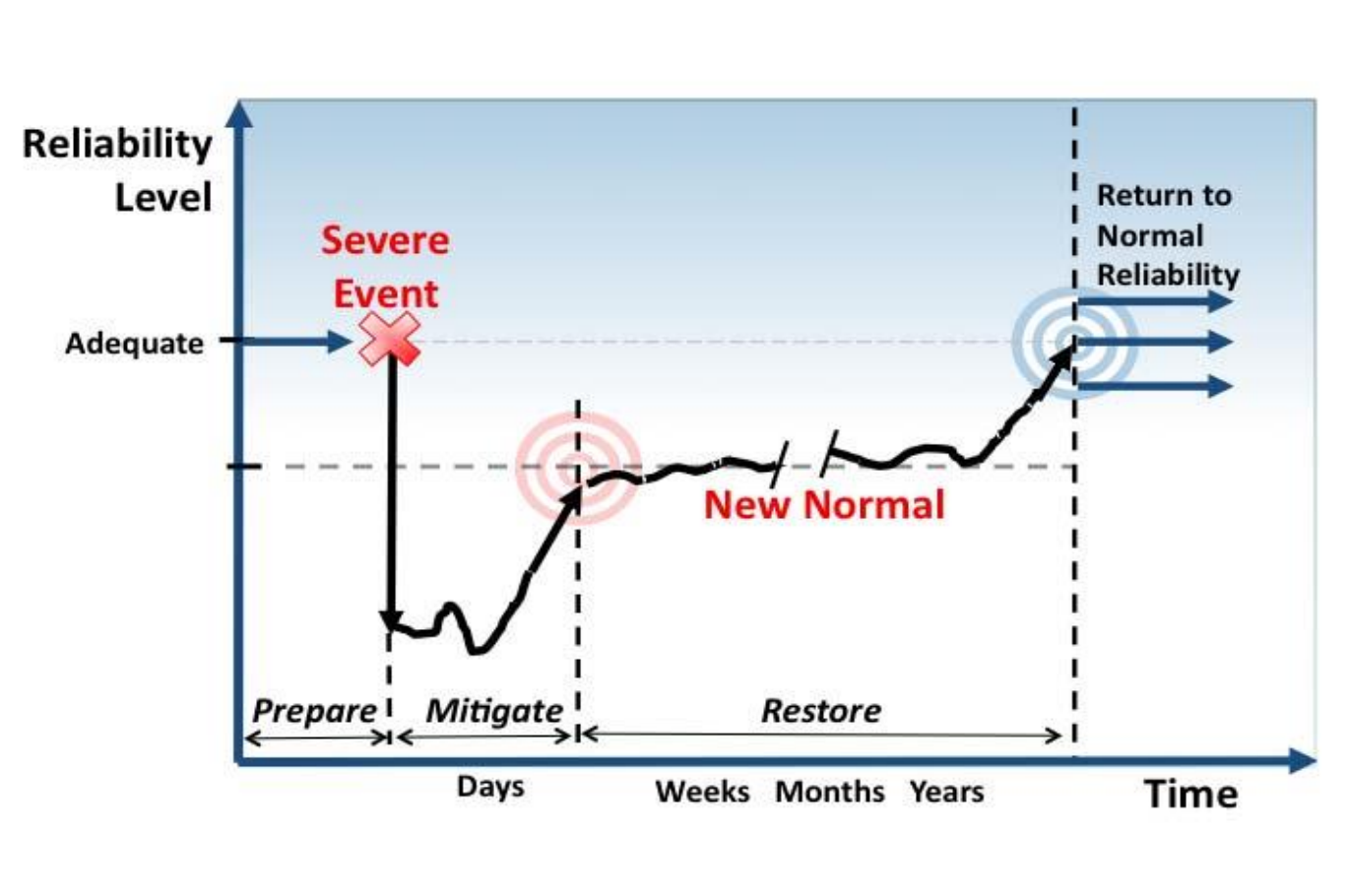
1. A compromise of situational awareness
   - False or misleading system data
   - Disorienting of operators in control rooms

1. A bulk power system event or instability
   - Load imbalance not corrected instantly
   - Operator errors cause loss of load & generation

“Severe Event”

- Emergency situation so catastrophic that complete restoration of electric service is not possible.
- Preparedness aims at graceful degradation
- BPS operated at reduced state of reliability and supply for months or possibly years through “New Normal” period.
- May require operating “islands” of power and rolling outages

“Severe Event” and “New Normal”

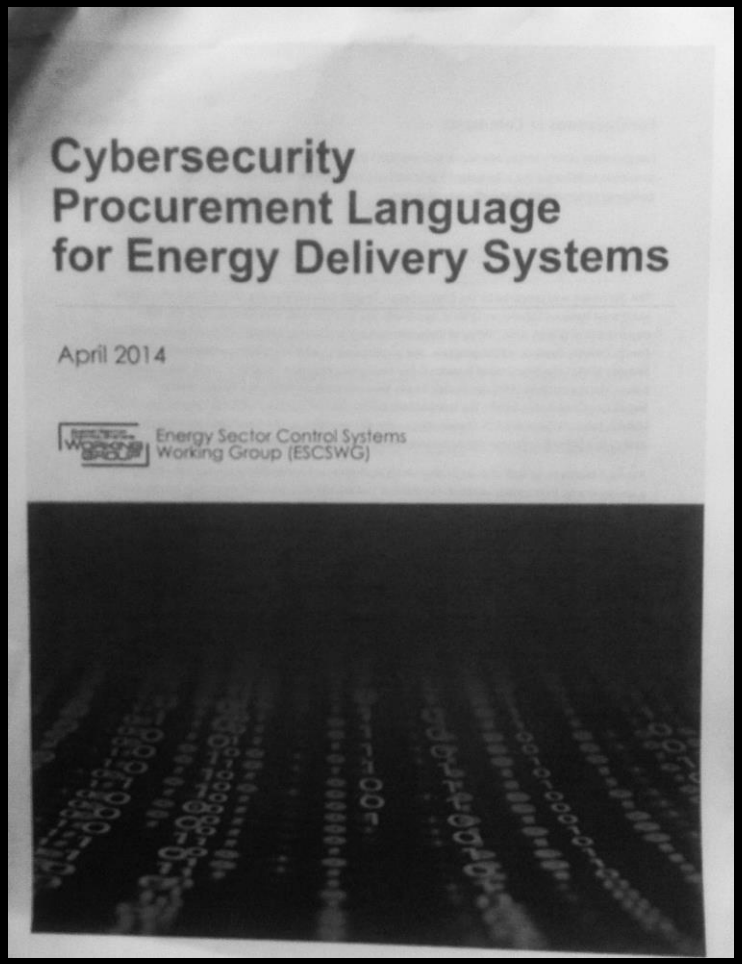


INITIAL DAYS OF CYBERATTACK

- Attack not detected
- “Islands” of electricity
- Rotating blackouts
- More than 50% of total instantaneous demand cannot be supplied in islands

Is grid’s supply chain an attack vector?

Private Sector Efforts


Cybersecurity
Procurement Language
for Energy Delivery Systems

April 2014

Energy Sector Control Systems
Working Group (ESCSWG)

Supply Chain Risk
Excess Software

Unused and unnecessary software in energy delivery systems and components

pose potential entry points for exploits

Precaution in Contract

"Supplier shall remove all software components that are not required for the operation and/or maintenance of the procured product."

Supply Chain Risk Heartbeat Signals

Heartbeat signals =

regularly repeated signals generated by hardware, software, or firmware –

indicate operation within specified limits for energy delivery system

Supply Chain Risk Heartbeat Signals

If heartbeat signal is not received in prescribed time

Indicates the component generating the signal is operating outside limits

(Stuxnet disguised these signals)

Precaution in Contract

Supplier shall identify heartbeat signals

At a minimum, a last gasp report from a dying component shall be included in network monitoring

WHAT SHOULD WE DO?

- "Hurricane Sandy" test
  - Can't be blamed for coordinated cyber attack

- Will be judged chiefly on –
  - ✓ Resilience to disruption
  - ✓ Preparedness for recovery
  - ✓ Speed and extent of restored operations

Questions?