

A presentation from the 2009 Topical Symposium:

Energy Security: A Global Challenge

Hosted by:
The Institute for National Strategic Studies
of
The National Defense University

29-30 September 2009

By
SCOTT PUGH



Papers presented at NDU Symposia reflect original research by members of NDU as well as other scholars and specialists in national security affairs from this country and abroad. The opinions, conclusions, and recommendations expressed or implied within are those of the authors and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUL 2009		2. REPORT TYPE		3. DATES COVERED 00-00-2009 to 00-00-2009	
4. TITLE AND SUBTITLE Secure Grid 2009. A DHS-DOE-DOD Joint Exercise				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Defense University, Institute for National Strategic Studies, 260 5th Avenue, Washington, DC, 20319				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES 2009 Topical Symposium: Energy Security: A Global Challenge, 29-30 Sep 2009, Washington DC					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 32	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

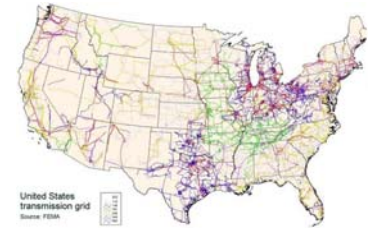
Secure Grid 2009

A DHS-DOE-DOD Joint Exercise

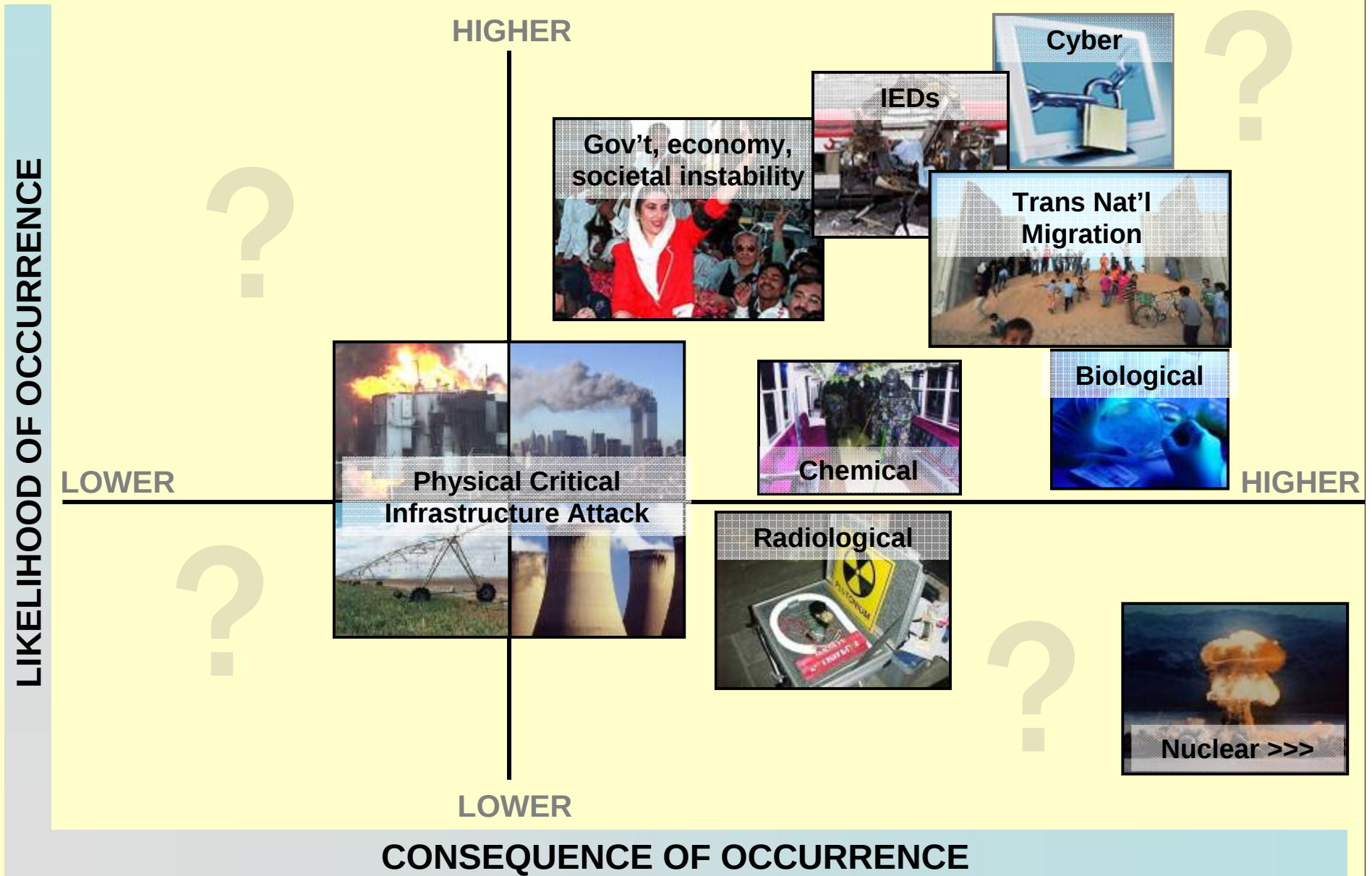
9 & 10 July 09



Hosted by National Defense University



POSSIBLE TERRORIST ROADMAP



BOMBS, BORDERS, BUGS, BUSINESS, *BODIES & BUILDINGS*

Summarizing Energy Security

Fossil Fuels

- Oil
- Coal
- Gas

Nuclear

Renewables

- Hydro
- Wind
- Solar
- Geothermal
- Ocean Energy
- Biomass
- Biofuels



**Homeland
Security**

Summarizing Energy Security

Electricity

*Fossils
Nuclear
Renewables*

Oil



**Homeland
Security**

A DOD, DOE, DHS Joint Concern

“Critical national security and Homeland defense missions are at an unacceptably high risk of extended outage from failure of the grid.”

Dependence on a vulnerable commercial power grid may be a bigger risk to DOD than dependence on oil.

*Report of the
Defense Science Board Task Force
on
DoD Energy Strategy
“More Fight – Less Fuel”*



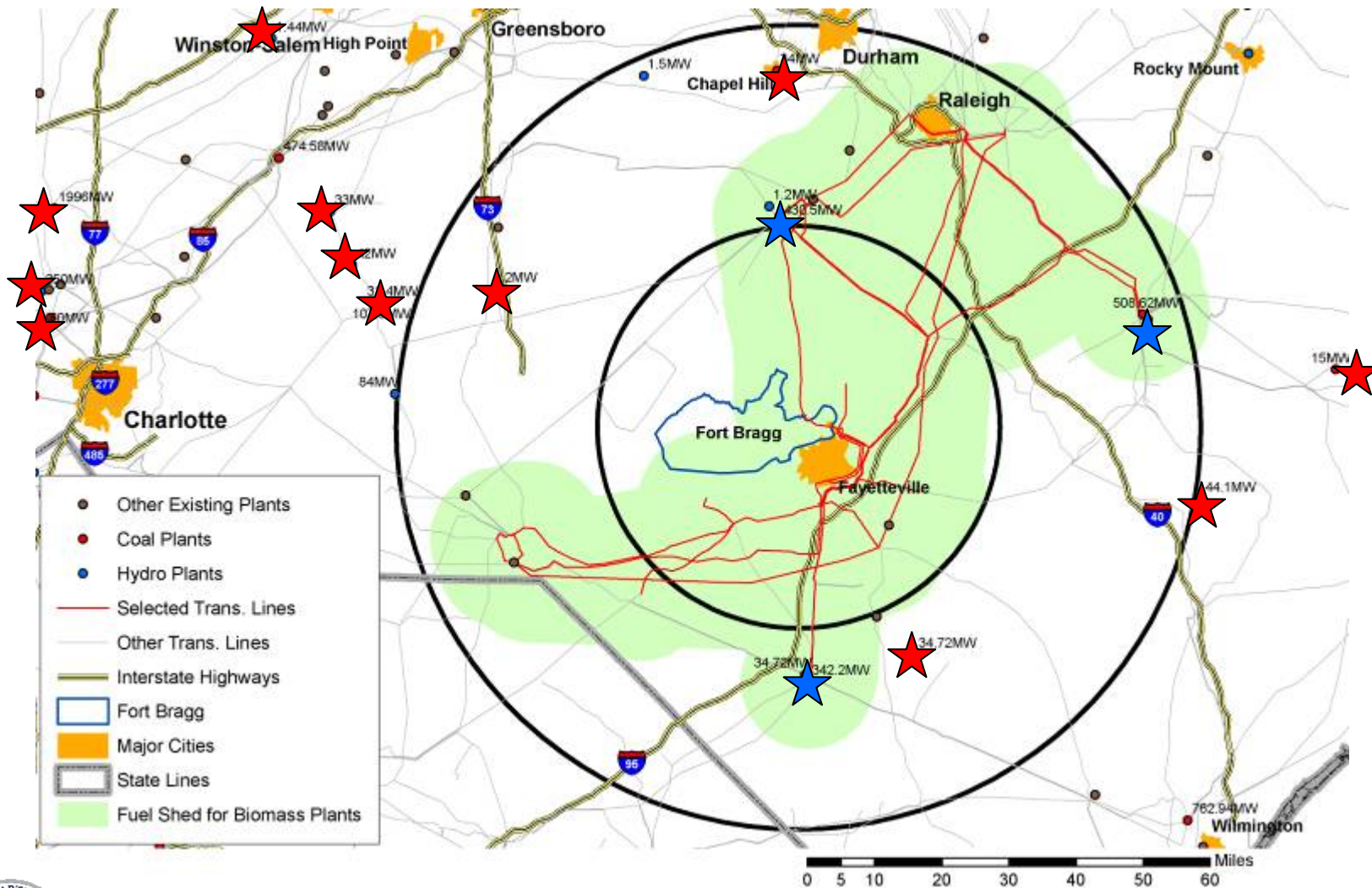
February 2008

*Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140*



**Homeland
Security**

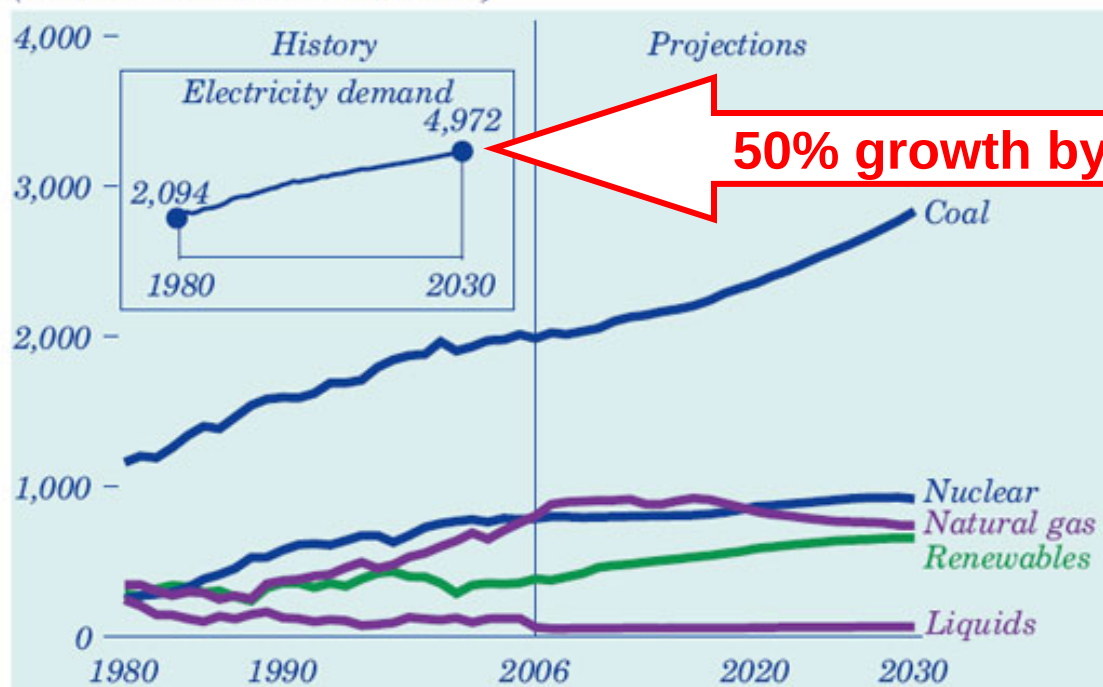
“DOD Facility Islanding”



**Homeland
Security**

Projected US Electric Demand

*Figure 7. Electricity generation by fuel, 1980-2030
(billion kilowatthours)*



US EIA AEO 2009



**Homeland
Security**

50% Electricity Demand Growth By 2030

To preserve current electric fuel supply mix:

	50	Nuclear reactors (1,000 MW)	(104 today)
	261	Coal-fired plants (600 MW)	(~ 600)
	279	Natural gas plants (400 MW)	(~ 750)
	93	Renewables (100 MW)	

Source: 2006 Annual Energy Outlook, Energy Information Administration

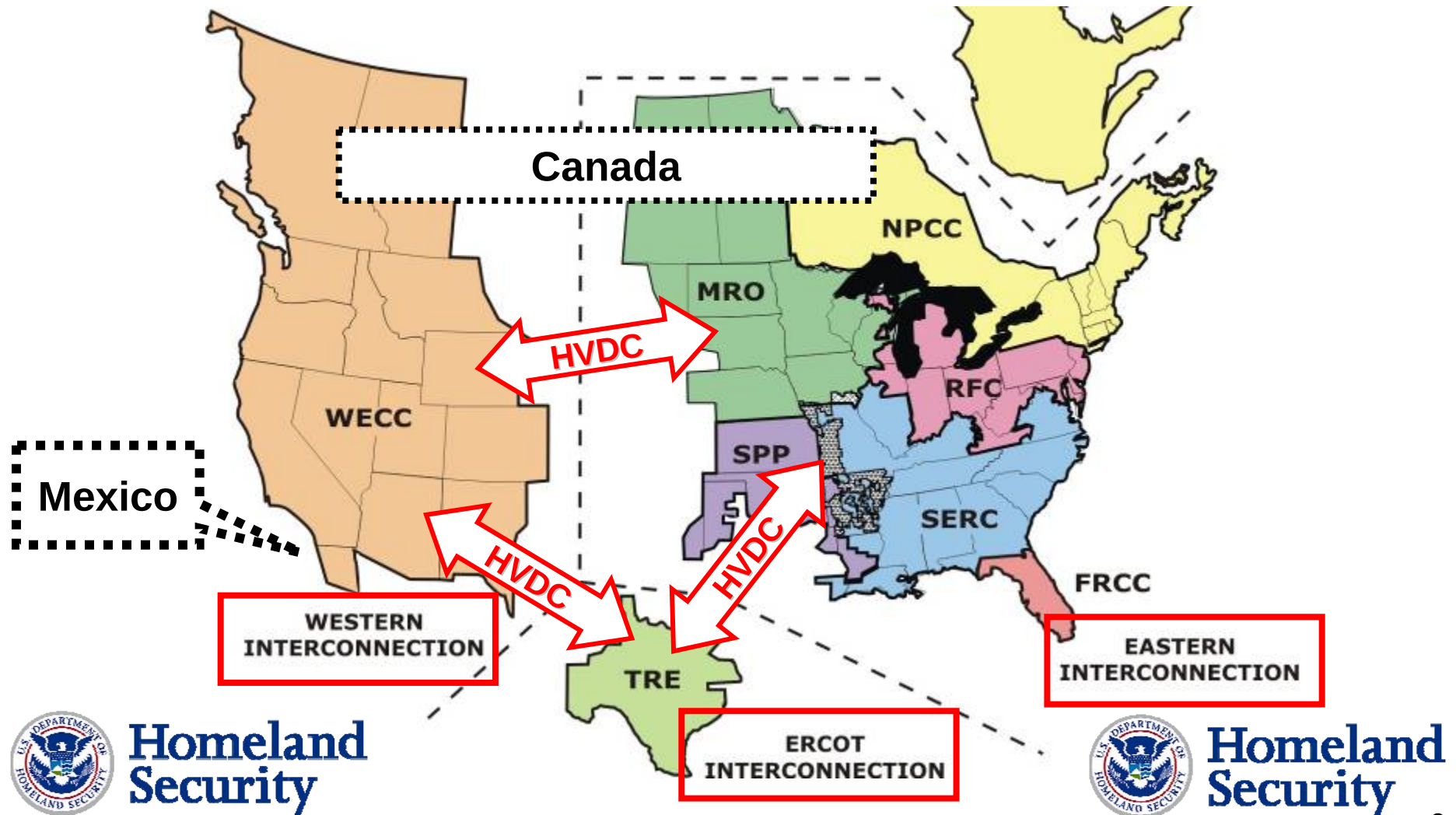
*Bigger grid needed to accommodate growth.
Smart grid needed to integrate renewables and manage demand.*



**Homeland
Security**

North American Transmission Grid

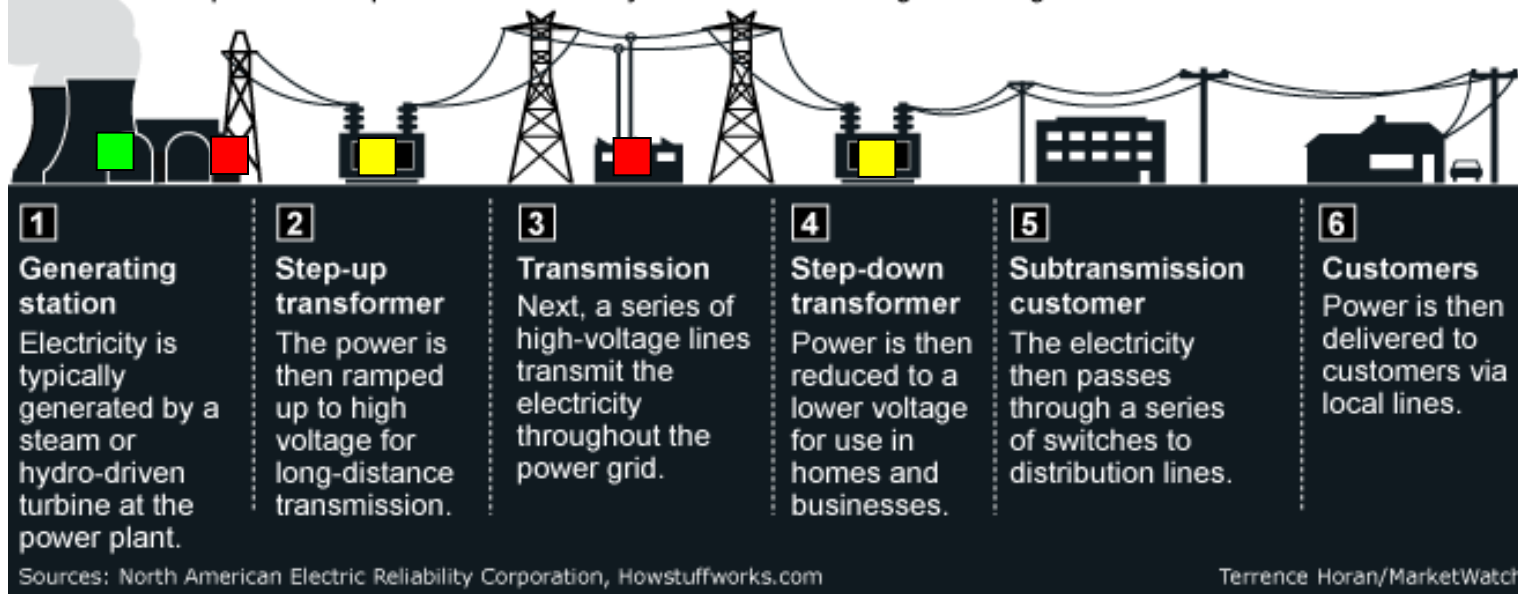
Transmission owned by over 500 independent companies.
Generation supplied by over 3000 utilities.



Grid Infrastructure

The power grid

Below is a simplified example of how electricity is distributed throughout the grid.



Generators



Circuit Breakers

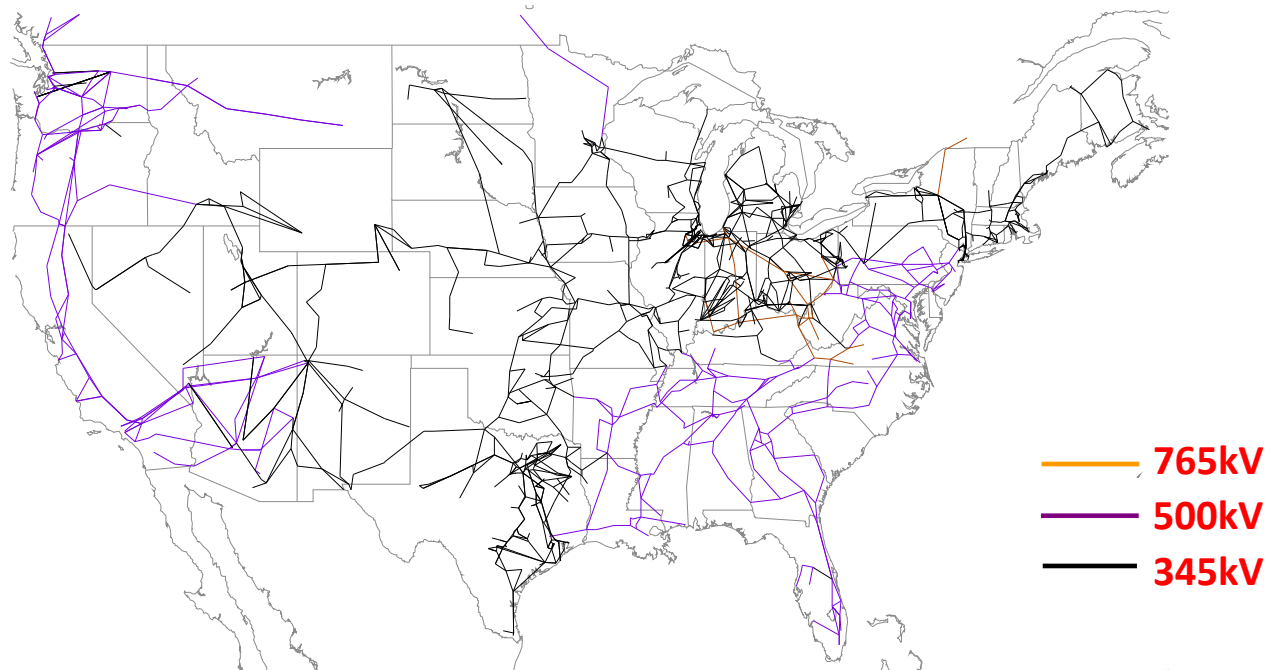


High Voltage Transformers



**Homeland
Security**

EHV Transformers



- US spares.
- *500KV and 765KV manufacturing capability.*
- 100+ tons.
- Lead time 6 to 18 months.



**Homeland
Security**

EHV Transformer



**Homeland
Security**

Moving EHV Transformers



**Homeland
Security**

Emergency Transformers



230 KV Mobile Transformer (Made in US)



**Homeland
Security**

Major US Grid Substations

There are more than 25,000 power substations in the United States with a voltage rating of 34 kV (kilovolts) and above. Figure 4 shows the location of relevant (i.e., high-side voltage rating equal to or greater than 34 kV) substations in the United States and in portions of Canada and Mexico (Platts PowerMap 2004)

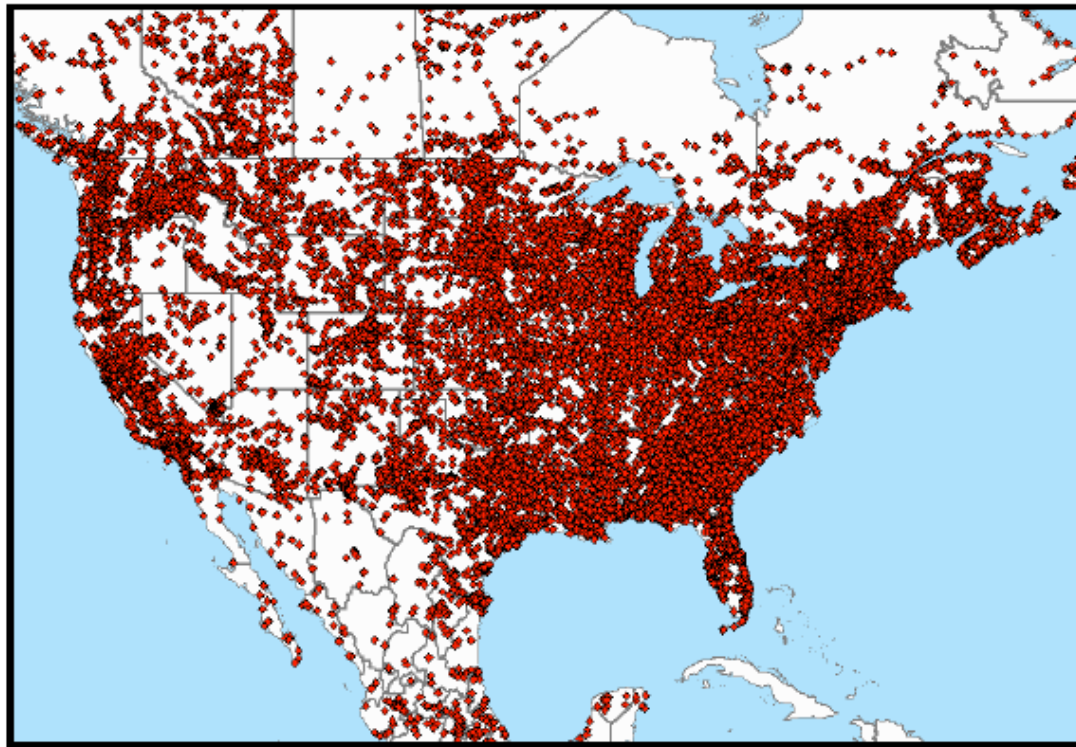


Figure 4 Locations and Density of “Major” Electric Substations in the United States (Source: Platts PowerMap 2004)



NationalJournal.com

nationaljournal.com > Insider Interviews

HOME THE MAGAZINE THE HOTLINE CONGRESSDAILY

About Us
NEWS
Earlybird
Insider Interviews
Poll Track
Markup Reports
The Promise Audit
BLOGS
Hotline On Call
Expert Blogs
Transition Blog
Lobbying Blog
Blogometer
Tech Daily Dose
MULTIMEDIA
Play of the Day
Sunday Snapshot
Hotline TV
National Journal On Air
Audio & Video
COLUMNS
Mark Blumenthal
Ronald Brownstein
Eliza Newlin Carey
Charlie Cook (Tues.)
Charlie Cook (Fri.)
Oliver Crook
John Mercurio
Jonathan Rauch
Bruce Stokes
William Schneider
Stuart Taylor
Amy Walter
SUBSCRIBER

Insider Interviews

Q&A: JIM LANGEVIN

Langevin Determined To Prevent A 'Cyber 9/11'

Rhode Island Democrat Supports White House Oversight Of Cybersecurity But Opposes Giving It To Any One Agency

Saturday, April 25, 2009

It's been a bleak April for the nation's cybersecurity. With hacks reported in the U.S. electrical grid and the Pentagon's Joint Strike Fighter program — not to mention the continuing specter of debilitating worms and viruses — officials are facing a battery of new questions about a persistent problem.

Rep. Jim Langevin, D-R.I., co-founded and co-chairs the House Cybersecurity Caucus, and he recently co-chaired a cybersecurity report from the Center for Strategic and International Studies for the 44th presidency. In a recent interview with *National Journal's* Winter Casey, Langevin discussed the importance of a national cyberspace office in the White House and a comprehensive security effort throughout not just the government, but the private sector as well.

Edited excerpts follow. Read the [Insider Interviews](#) archives for more discussions in the series.

NJ: What do you know about spies from Russia and China penetrating the U.S. electrical grid?

Langevin: I would rather not get into any classified intelligence information. But I will say that the threats to our electric grid and our vulnerabilities to potential cyber attack in general are very real, and they continue to grow, and they do concern me. I spent a great deal of time in the last year on this issue and will continue to pay a lot of attention to it.

NJ: Have spies penetrated other U.S. infrastructure?

Print
Email
Reprints
TOOLS SPONSOR:



"The threats to our electric grid and our vulnerabilities to potential cyber attack in general are very real."
-- Jim Langevin



Homeland Security

THE WALL STREET JOURNAL Digital Network WSJ.com MarketWatch BARRONS All Things Digital SmartMoney

Wednesday, April 8, 2009

THE WALL STREET JOURNAL. TECH

U.S. Edition Today's Paper Video Columns Blogs Graphics Journal Community

Home World U.S. Business Markets Tech Personal Finance Life & Style

Digits Personal Technology

TOP STORIES IN Technology 1 of 10 2 of 10

Founders Step Aside at MySpace
iPhone Sales Boost Apple Pro

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

Article Video Comments (146)

Email Printer Friendly Share: Yahoo Buzz Text Size

By SIOBHAN GORMAN



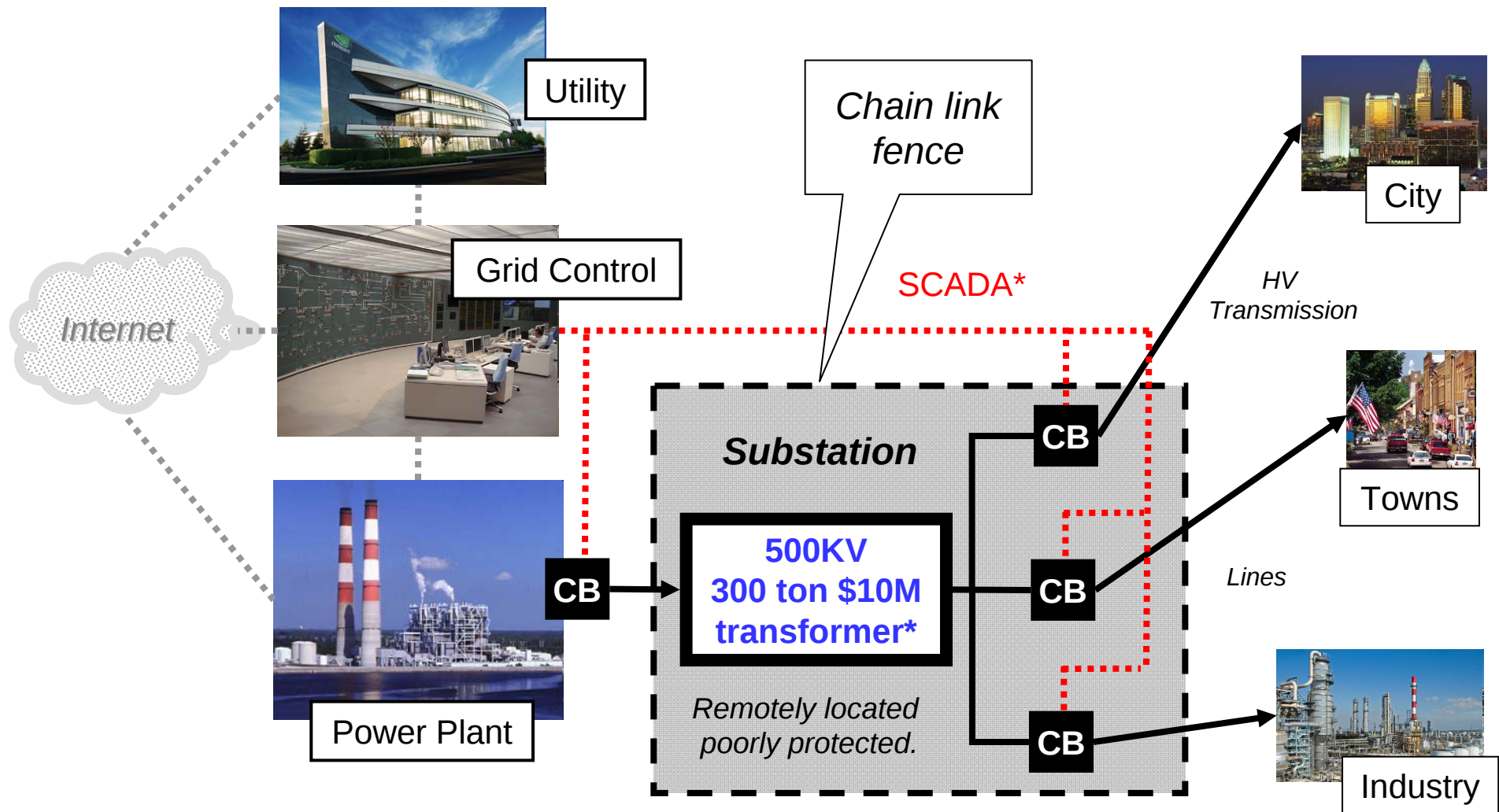
Associated Press

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.

System Control And Data Acquisition (SCADA) System



**Homeland
Security**

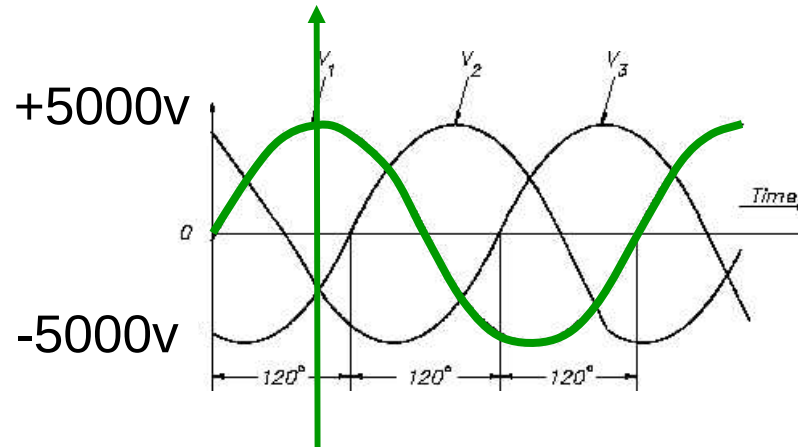
CB = Circuit Breaker (remotely operable)

EHV Circuit Breakers



3 Phase Circuit Breaker Operation

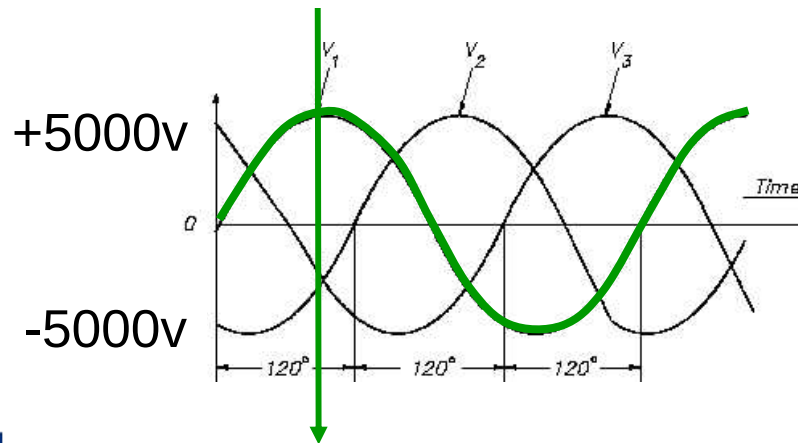
Power Plant



$$V_1 = +5000 \text{ vac}$$

In Phase

Grid



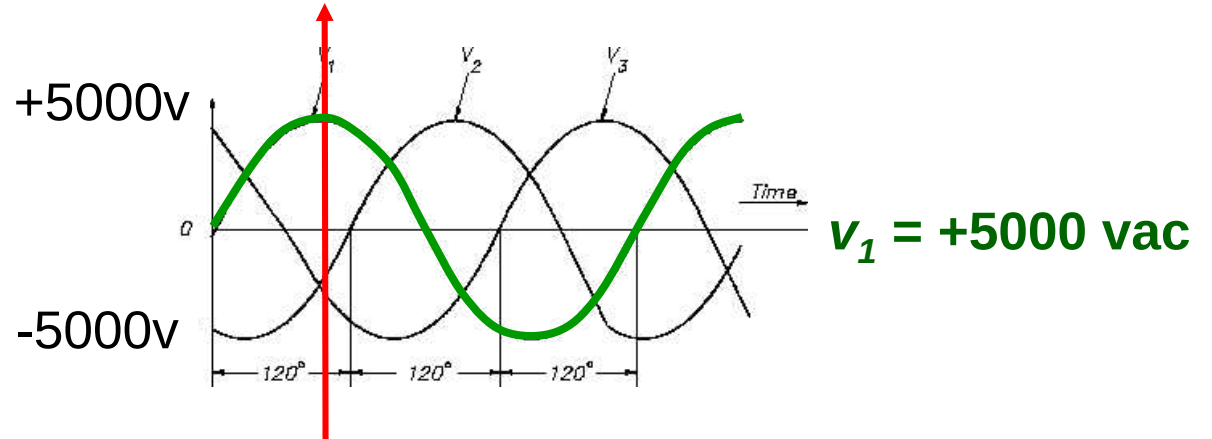
$$V_1 = +5000 \text{ vac}$$



**Homeland
Security**

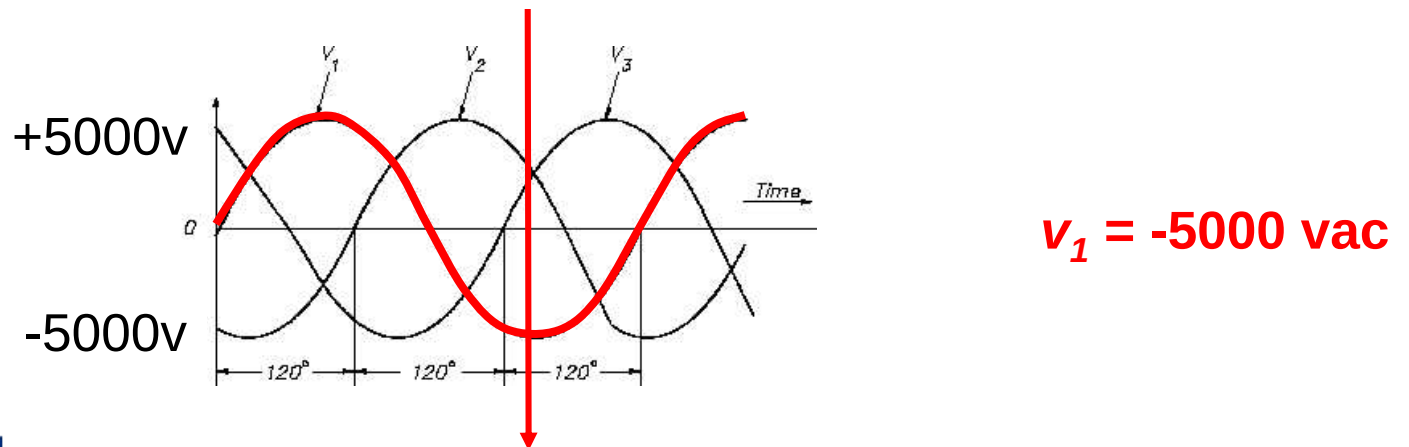
3 Phase Circuit Breaker Operation

Power Plant



Out of Phase

Grid



Homeland
Security

2007 Grid Cyber Test at INL

CNN.com / US

HOME WORLD **U.S.** POLITICS CRIME ENTERTAINMENT HEALTH TECH TRAVEL LIVING BUSINESS SPORTS TIME.COM

Hot Topics » First 100 Days » Gas Prices » Focus On Giving » The Economy » more topics »

Weather Forecast International Edition

updated 11:06 p.m. EDT, Wed September 26, 2007

Sources: Staged cyber attack reveals vulnerability in power grid

STORY HIGHLIGHTS

- Sources: Similar attack could hurt generators that produce nation's electricity
- Experts fear attacks could cause damage that would take months to fix
- Department of Homeland Security said staged attack took place in March
- DHS official: A lot of risk has been "taken off the table" since experiment

Next Article in U.S. »

READ VIDEO

From CNN's Jeanne Meserve

WASHINGTON (CNN) — Researchers who launched an experimental cyber attack caused a generator to self-destruct, alarming the federal government and electrical industry about what might happen if such an attack were carried out on a larger scale, CNN has learned.



Department of Homeland Security video shows a generator sparking smoke after a staged experiment.

Sources familiar with the experiment said the same attack scenario could be used against huge generators that produce the country's electric power.

Some experts fear bigger, coordinated attacks could cause widespread damage to electric infrastructure that could take months to fix.

CNN has honored a request from the [Department of Homeland Security](#) not to divulge certain details about the experiment, dubbed "Aurora," and conducted in March at the Department of Energy's Idaho lab.

In a previously classified video of the test CNN obtained, the generator shakes and smokes, and then stops.

DHS acknowledged the experiment involved controlled hacking into a replica of a power plant's control system. Sources familiar with the test said researchers changed the operating cycle of the generator, sending it out of control.

"Aurora"

Most Popular on CNN

▼ STORIES

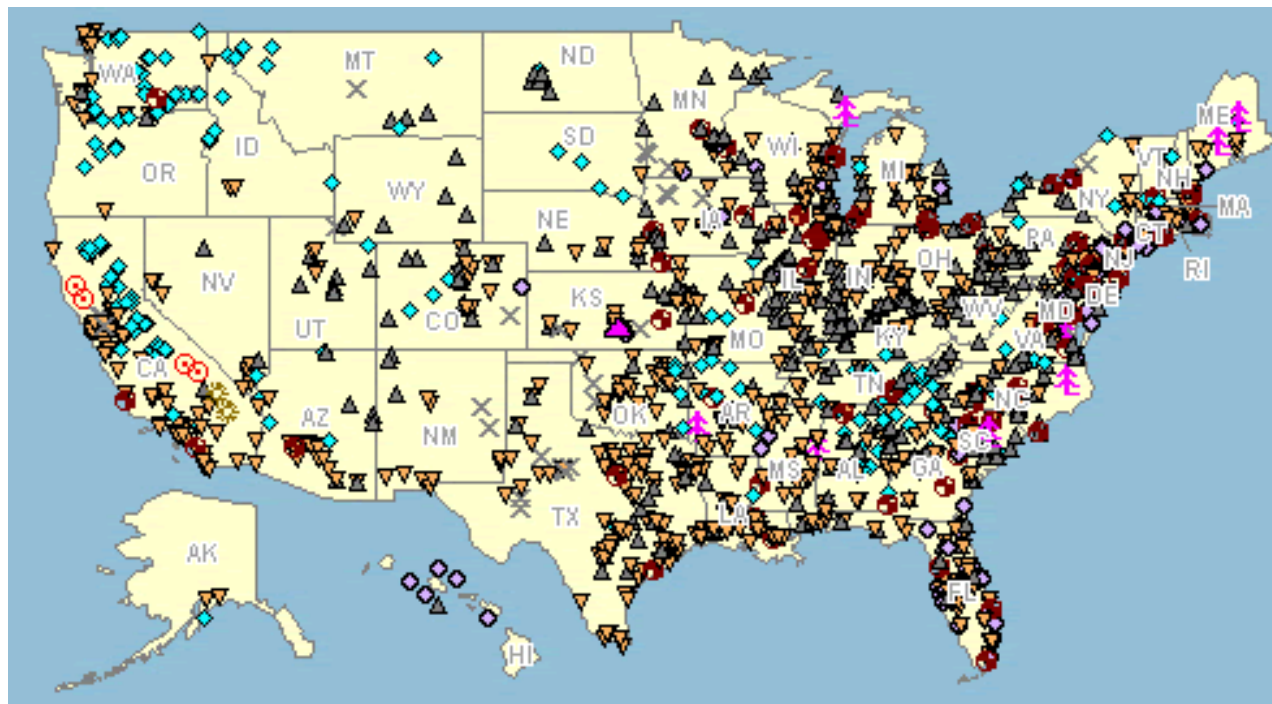
Most Viewed	Most Emailed	Top Searches
1	Drinking's toll leads to crackdown	
2	Search for Florida girl continues	

<http://www.cnn.com/2007/US/09/26/power.at.risk/index.html>



Homeland Security

Large US Power Plants



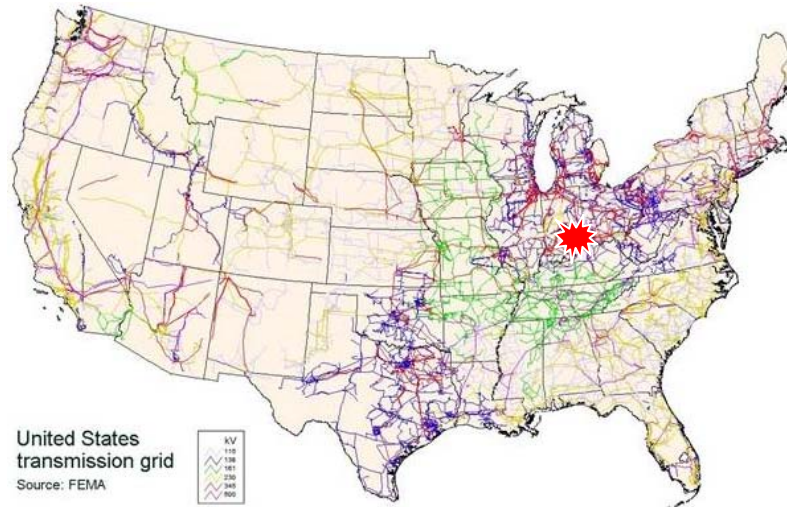
Electric Power Plants

Min. net summer capacity of
100 megawatts
(Values below are U.S. totals)

- ▽ Natural Gas (731)
- ▲ Coal (401)
- ◆ Hydro (183)
- ◆ Petroleum (108)
- Nuclear (66)
- × Wind (31)
- ▲ Wood (8)
- ⊙ Geothermal (4)
- ▲ Biomass (2)
- ★ Solar (2)



Wargame Scenario



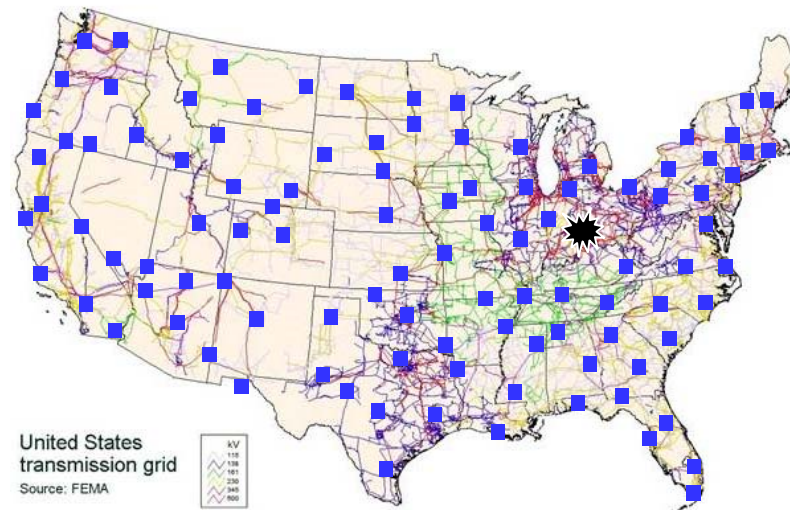
0500 – Columbus attacked.

0600 – Terrorist group claims responsibility and issues demands through media.



**Homeland
Security**

Wargame Scenario

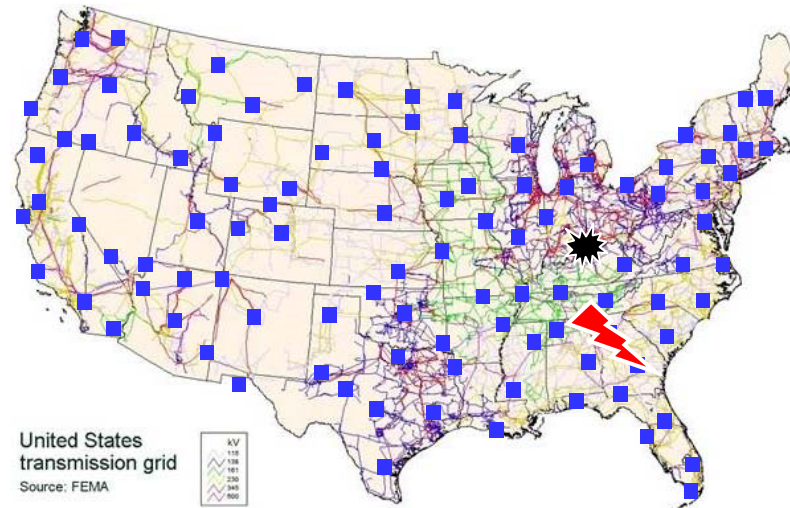


0900 – Government evaluates options for protecting EHV transformers.



**Homeland
Security**

Wargame Scenario

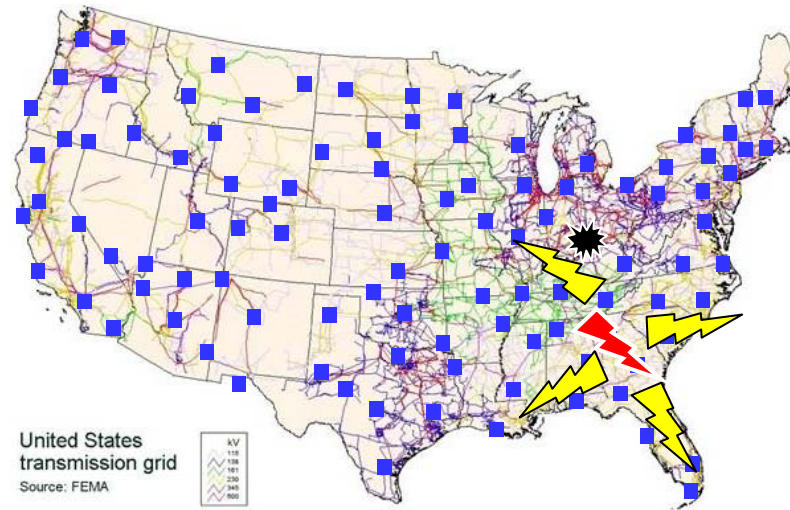


1215 – Cyber attack against a major utility SCADA system in US southeast.



**Homeland
Security**

Wargame Scenario

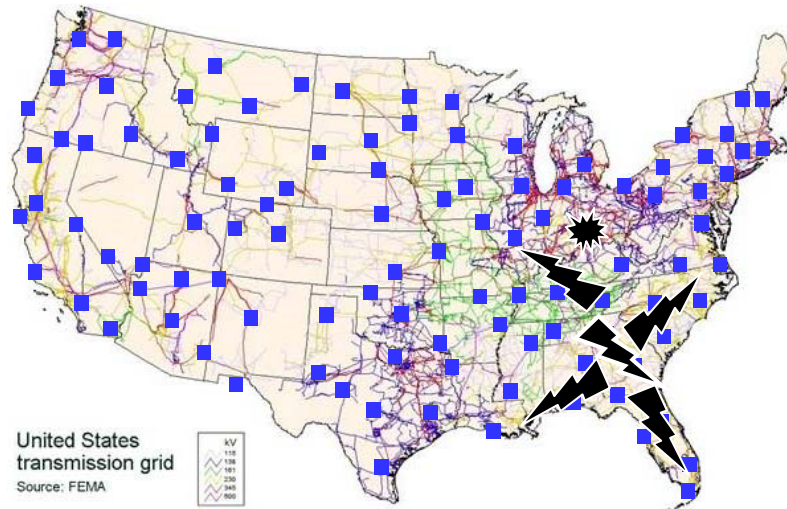


1220 – effects of major utility loss propagate through the US eastern interconnection.



**Homeland
Security**

Wargame Scenario



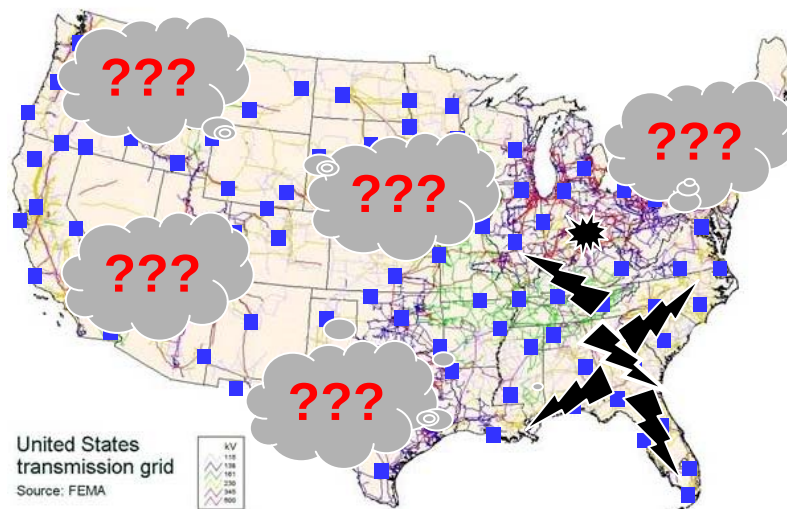
1230 – Columbus and most of Georgia, Florida, Alabama, South Carolina, North Carolina are blacked out.

1245 – terrorist group claims responsibility and issues new demands.



**Homeland
Security**

Wargame Scenario



1400 – Government considers options.
1500 – Intel intercepts provide new info.
1700 – Game over.



**Homeland
Security**

DHS Recovery Transformer Program

Single 3 phase



Large & Heavy

3 single phase



Smaller & Lighter



Movable



**Homeland
Security**

Smart Grid



Shift from coal to renewables is a big driver.



**Homeland
Security**



**Homeland
Security**

FROM SCIENCE...SECURITY

Explosives



Chemical/Biological



**Command, Control, &
Interoperability**



Borders/Maritime



Human Factors



Infrastructure/Geophysical



FROM TECHNOLOGY...TRUST