



**CREDC**

CYBER RESILIENT ENERGY  
DELIVERY CONSORTIUM

**Seminar Series**



**E-ISAC**  
ELECTRICITY  
INFORMATION SHARING AND ANALYSIS CENTER

# Resiliency in the Electricity Subsector

Information Sharing and Exercises against Black Sky Events

Bill Lawrence, Director of Programs and Engagement  
Cyber Resilient Energy Delivery Consortium  
February 3, 2017

RESILIENCY | RELIABILITY | SECURITY



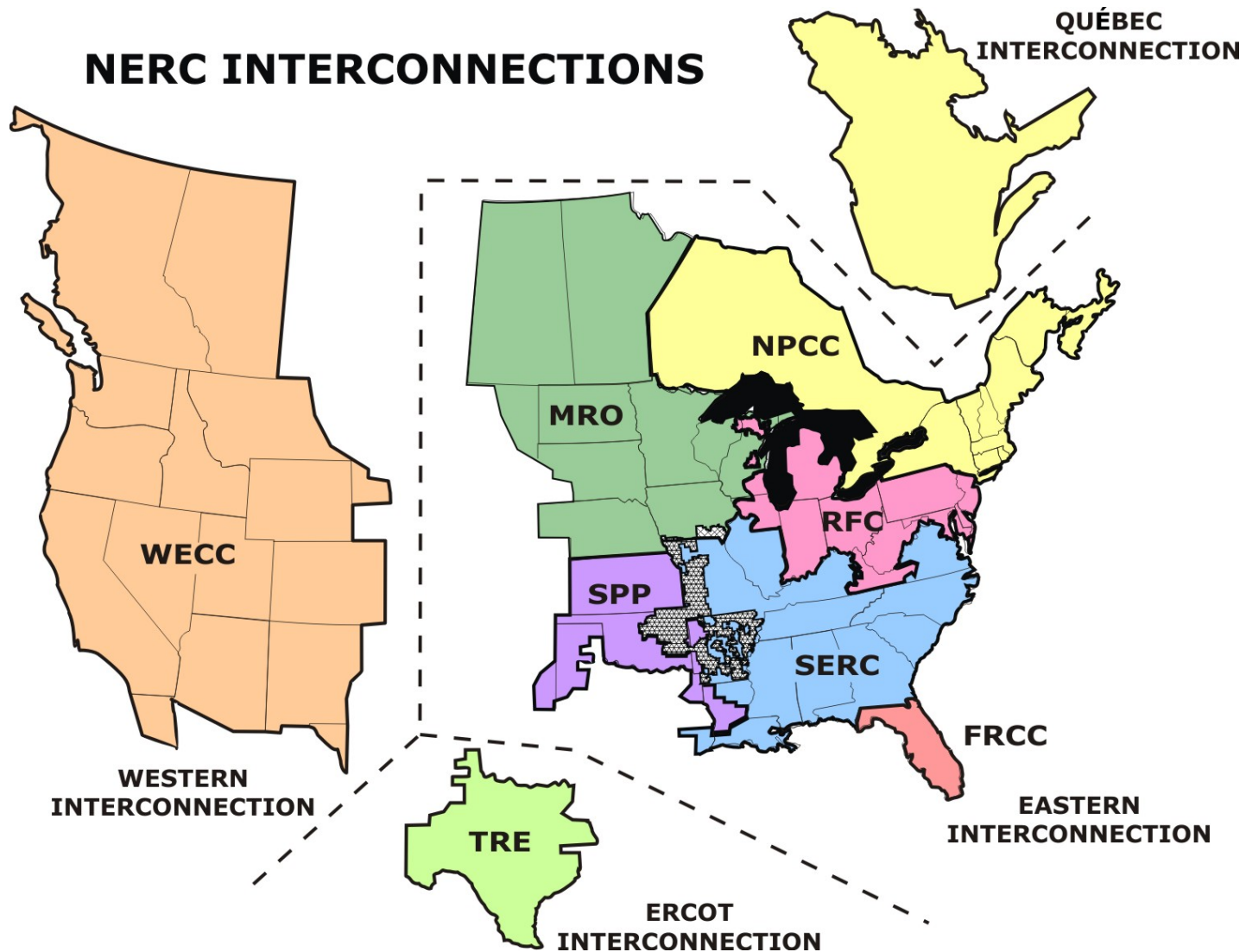
- Historical outages and NERC
- High Impact, Low Frequency (HILF) aka “Black Sky” events
- The Electricity Information Sharing and Analysis Center
- Recent threats and impacts
- GridEx



Image: Wikipedia



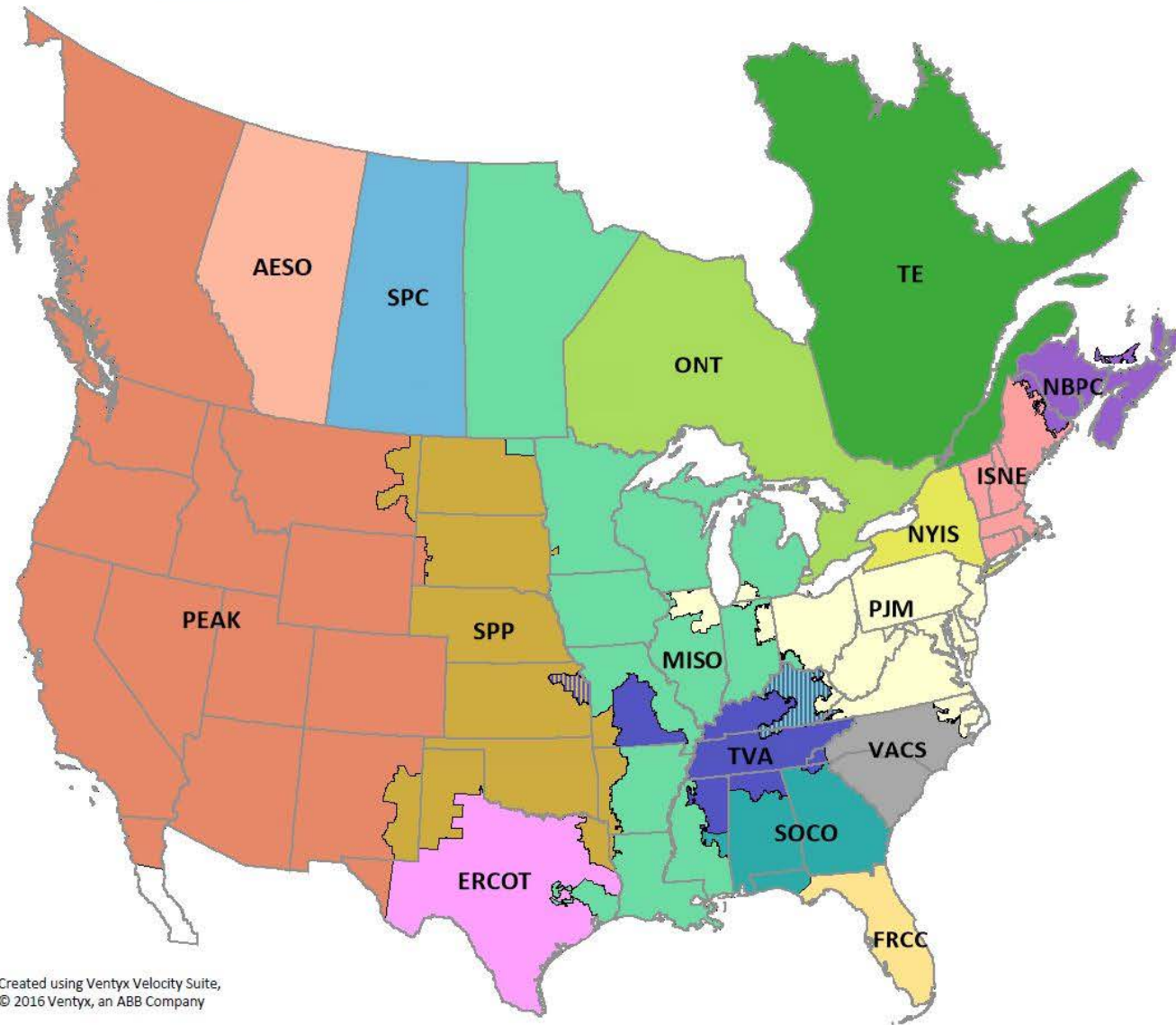
Image: Wikipedia







### NERC Reliability Coordinators As of June 1, 2015



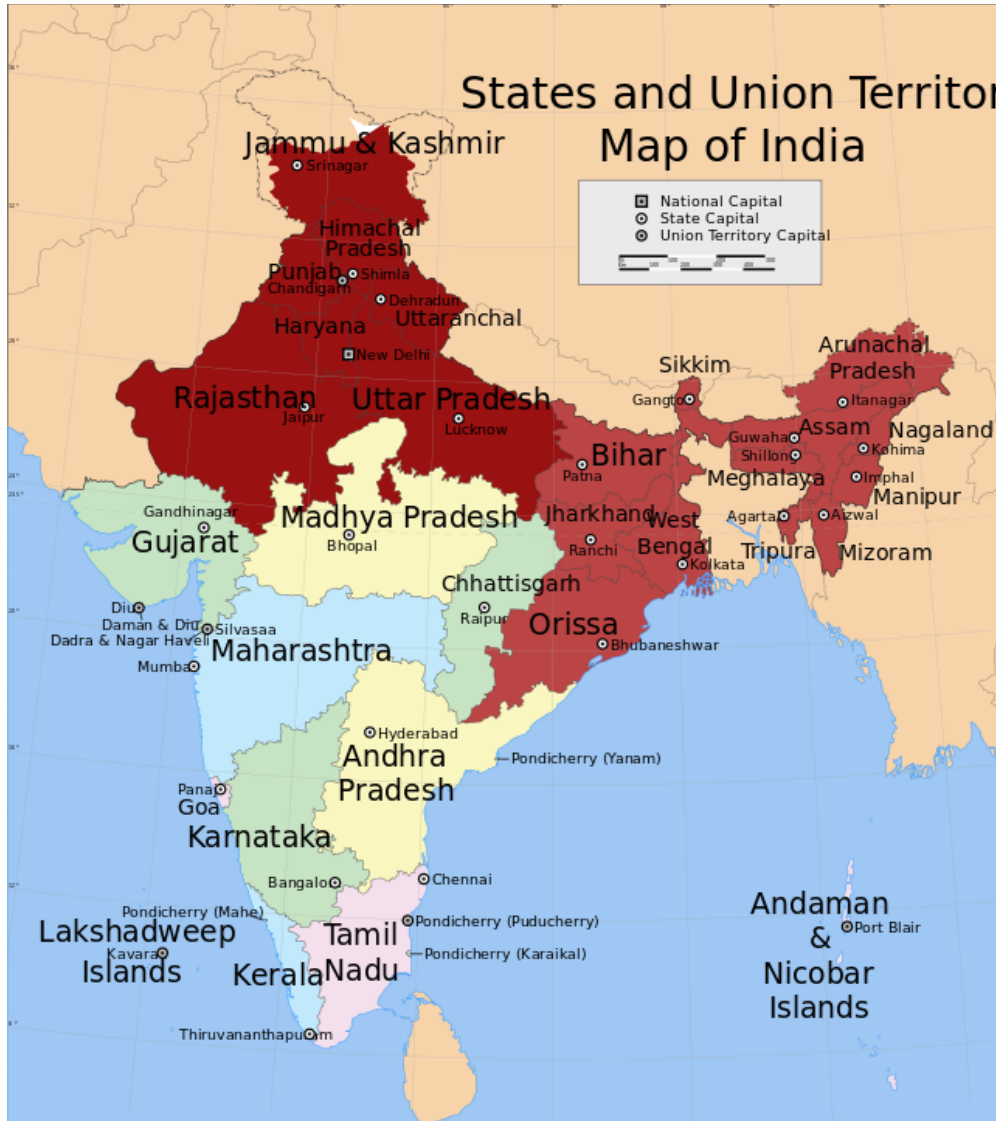
- Alberta Electric System Operator
- Electric Reliability Council of Texas
- Florida Reliability Coordinating Council
- Hydro Quebec TransEnergie
- ISO New England, Inc.
- Midcontinent ISO
- New Brunswick Power Corporation
- New York Independent System Operator
- Ontario Independent Electricity System Operator
- Peak Reliability
- PJM Interconnection
- Saskatchewan Power Corporation
- Southern Company Services, Inc.
- Southwest Power Pool
- BAs receive RC services from SPP or TVA
- Tennessee Valley Authority
- BAs receive RC services from TVA or MISO
- VACAR South

Created using Ventyx Velocity Suite,  
© 2016 Ventyx, an ABB Company



Image: Wikipedia





Indian states

- affected 2 days by the power outages (on 30 and 31 July)
- affected 1 day by the power outages (on 31 July)

Image: Wikipedia

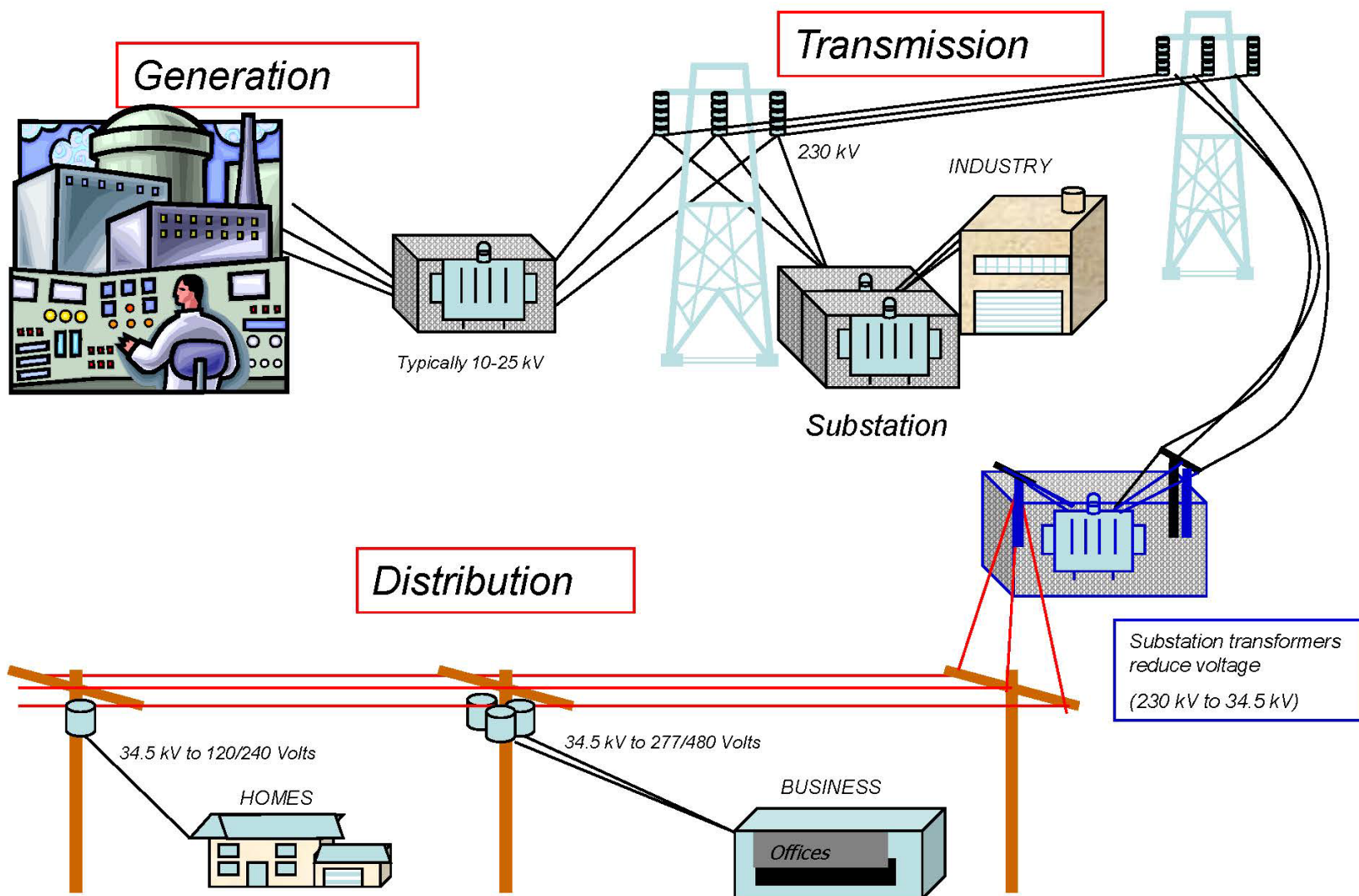
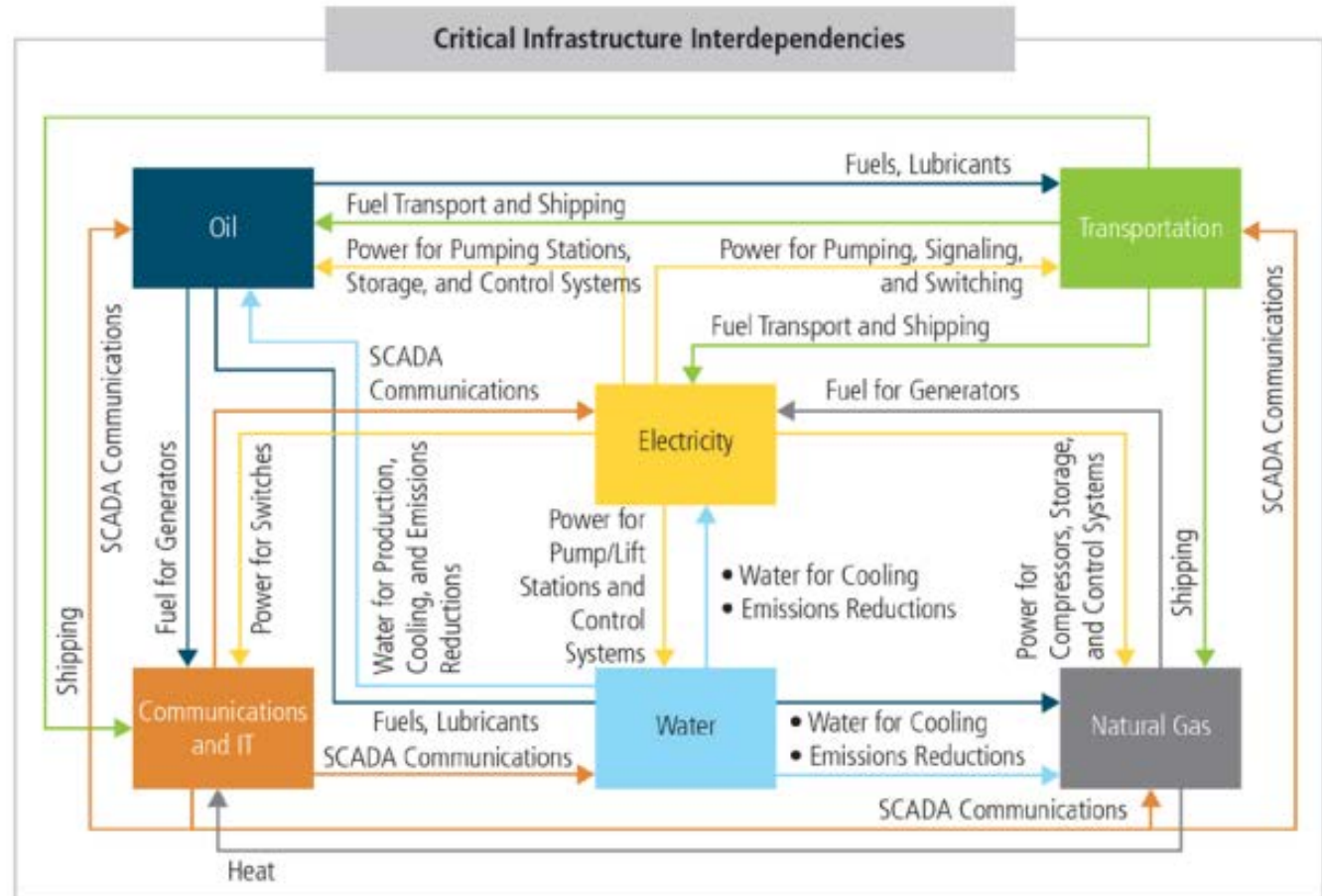


Figure S-2. Critical Infrastructure Interdependencies

- [Quadrennial Energy Review \(QER 1.2\)](#)



Key critical infrastructure interdependencies represent the core underlying framework that supports the American economy and society. The financial services sector (not pictured) is also a critical infrastructure with interdependencies across other major sectors supporting the U.S. economy.

- High Impact, Low Frequency
  - 1987 – NERC committee formed to address terrorism and sabotage
  - 1999 – Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
  - 2004 – Critical Infrastructure Protection Committee (permanent)
  - 2009/10 – [HILF Report](#) (joint DOE and NERC)
    - Pandemic Illness
    - Geomagnetic and Electromagnetic Events
    - Coordinated Cyber/Physical Attack
  - 2011 – [GridEx 2011](#)
  - 2012 – [Severe Impact Resilience](#) report
  - 2012 – [Cyber Attack](#) report
  - 2013 – [GridEx II](#)
  - 2015 – [GridEx III](#)



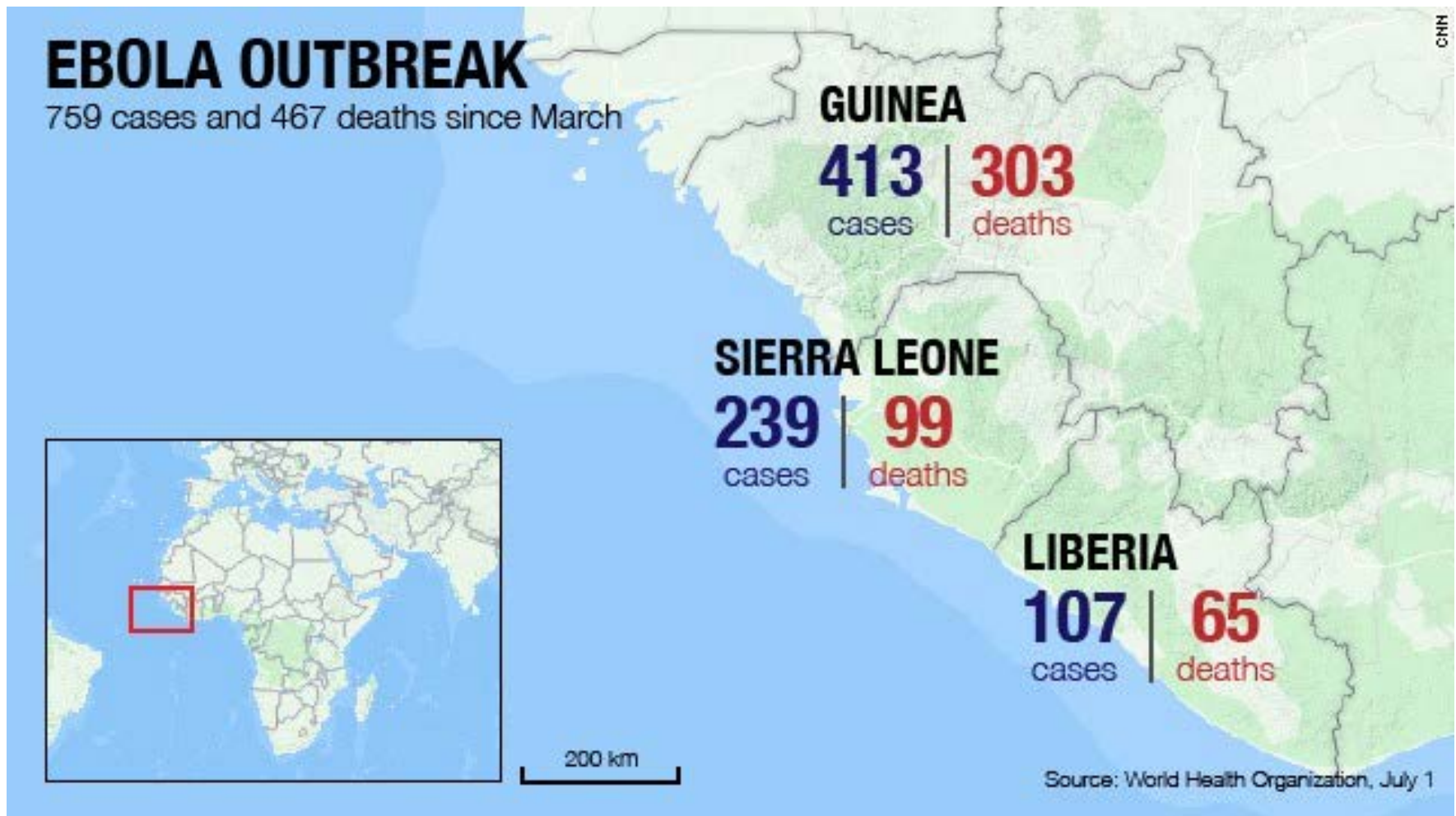
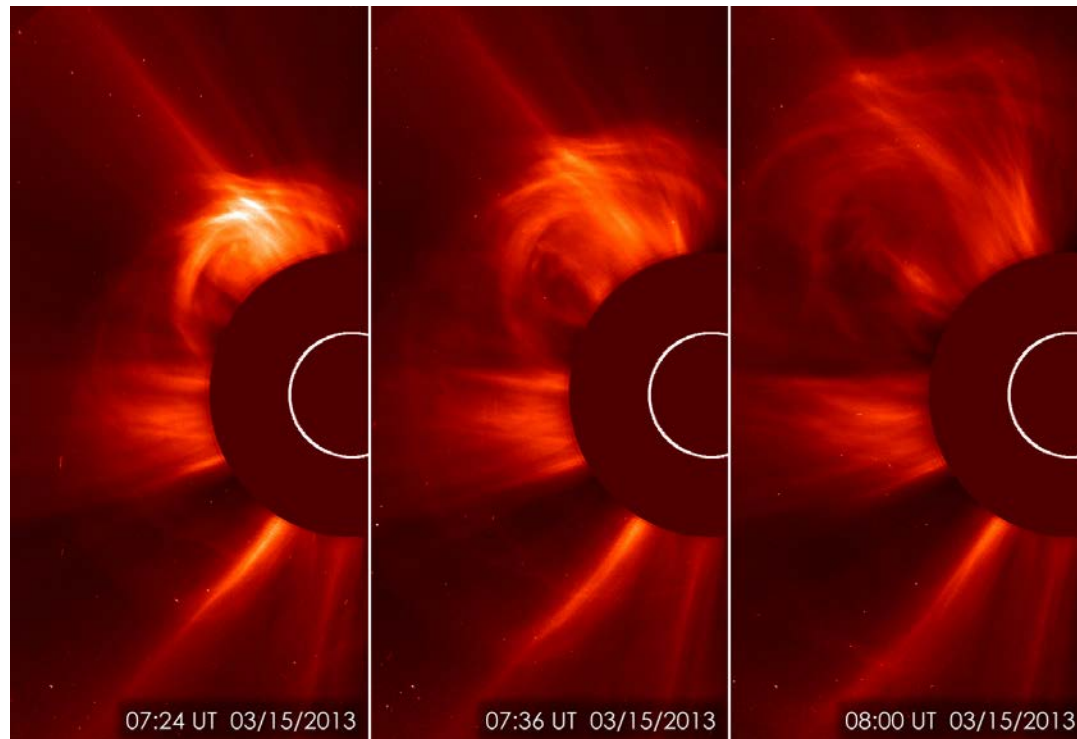


Image: CNN (4 July 2014)



*Image: NASA*



*Image: Scientific American*



- Stuxnet, Shamoon, Dragonfly/Energetic Bear, Havex/Black Energy
- Metcalf in California





- SQUIRRELS 

---

- NATURAL DISASTERS 

---

- PHYSICAL ATTACK/THEFT 

---

- CYBER ATTACK 

---

- INSIDER THREAT/  
CATASTROPHIC HUMAN ERROR 

---

- COORDINATED  
PHYSICAL & CYBER ATTACK 

---

- SUPPLY CHAIN  
DISRUPTION OR COMPROMISE 

---

- PANDEMICS 

---

- GEOMAGNETIC DISTURBANCE 

---

- DIRECT ENERGY WEAPON 

---

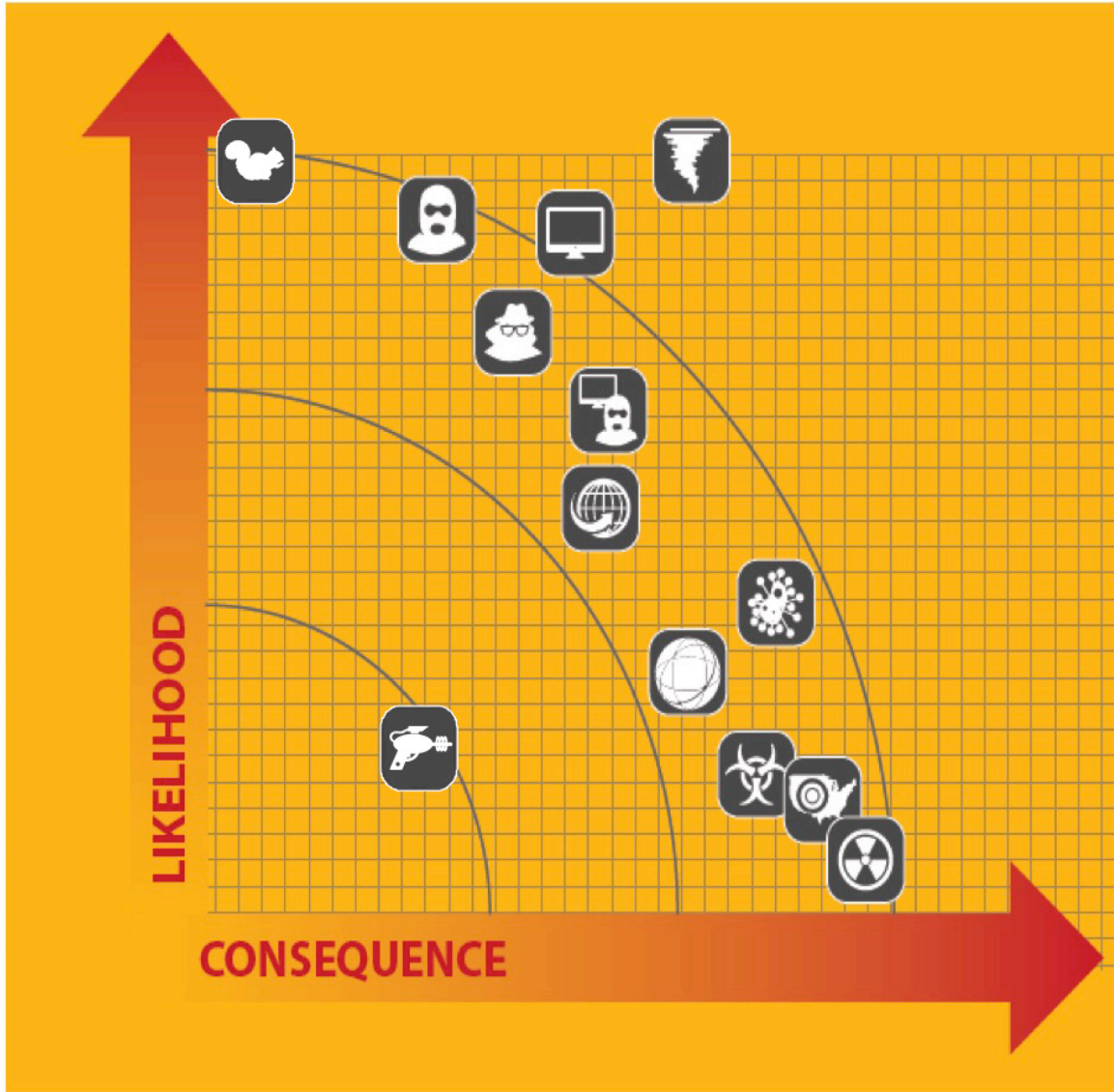
- CBR ATTACK 

---

- HIGH-ALTITUDE EMP 

---

- NUCLEAR 

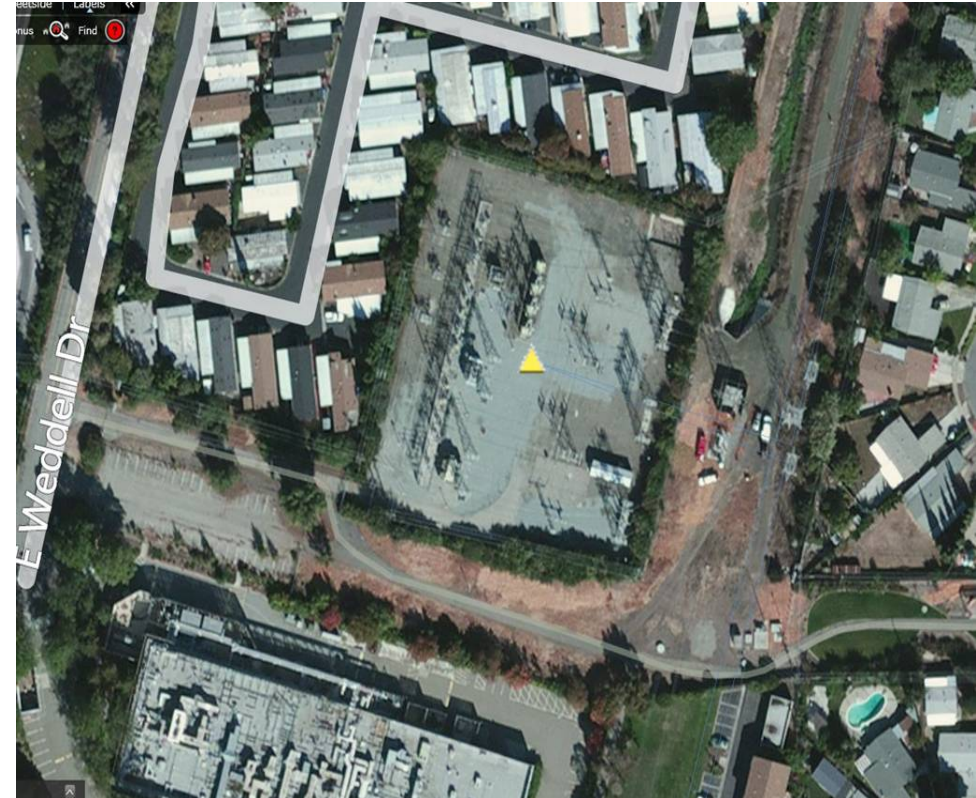




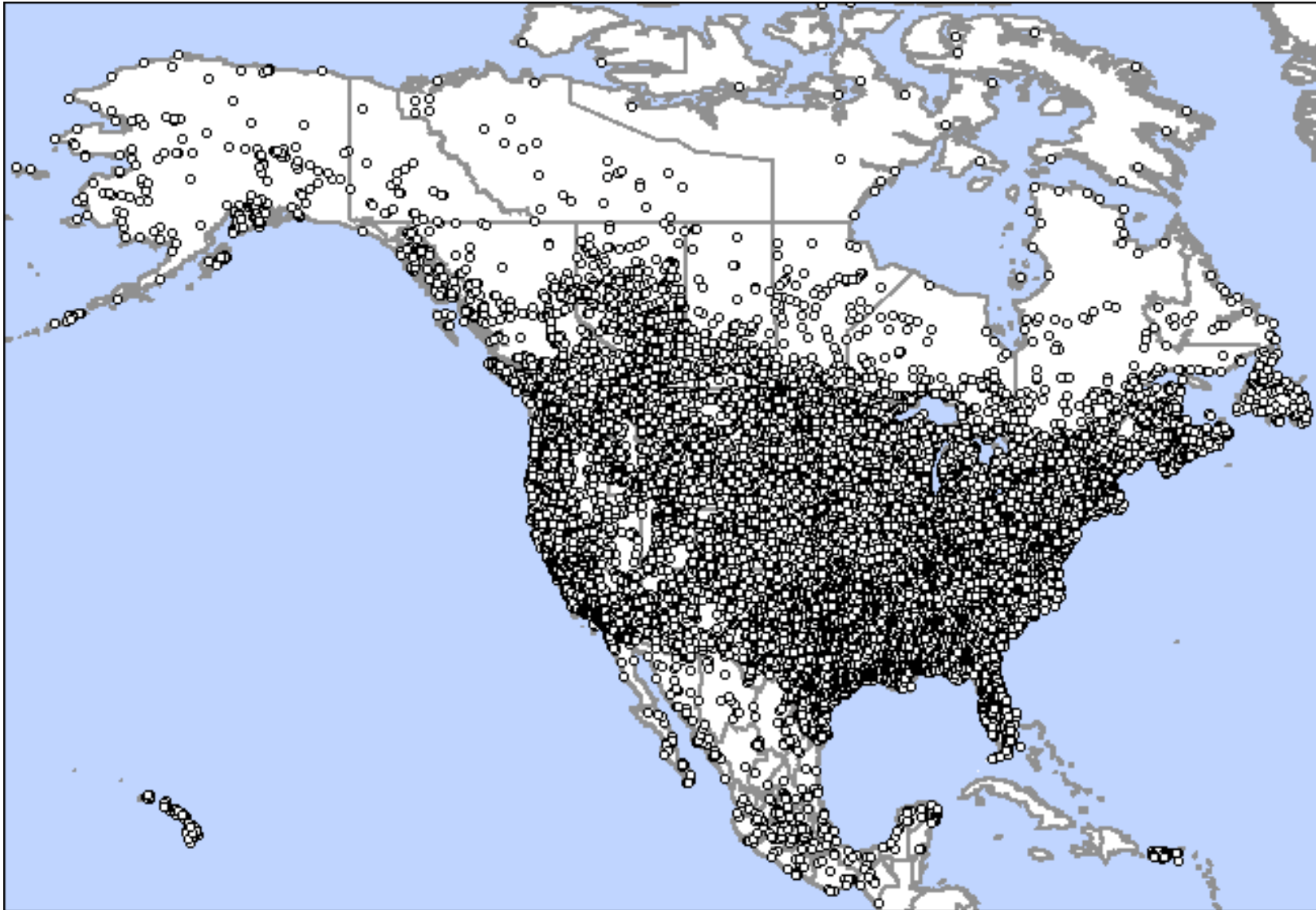
Agent	Success
Squirrel	879
Bird	434
Snake	83
Raccoon	72
Rat	36
Marten	22
Beaver	15
Jellyfish	13
Human	3*

*<http://cybersquirrel1.com/>*





*CIP 014, Design Basis Threat document*





- ISAC concept introduced in Presidential Decision Document 63, published in 1998
  - Electric power was identified as a critical sector along with 14 others
  - Homeland Security Presidential Directive 7 (2003)
  - Presidential Policy Directive 21 (2013)
- Electricity sector's ISAC has been hosted by NERC since 1999
  - Recent concerns about sensitive information shared with the ISAC
  - Could “leak” to NERC compliance and enforcement groups
  - Caused a rethinking about the proper relationship
- ESCC identified strategic review of the ES-ISAC as a priority national security issue for 2015
  - Strategic review initiated in January 2015, completed in June 2015
- ES-ISAC renamed to E-ISAC in September 2015



## **Mission**

*The E-ISAC reduces cyber and physical security risk to the electricity sector across North America by providing unique insights, leadership, and coordination*

## **Vision**

*To be a leading, trusted source for the analysis and sharing of Electricity Subsector security information*







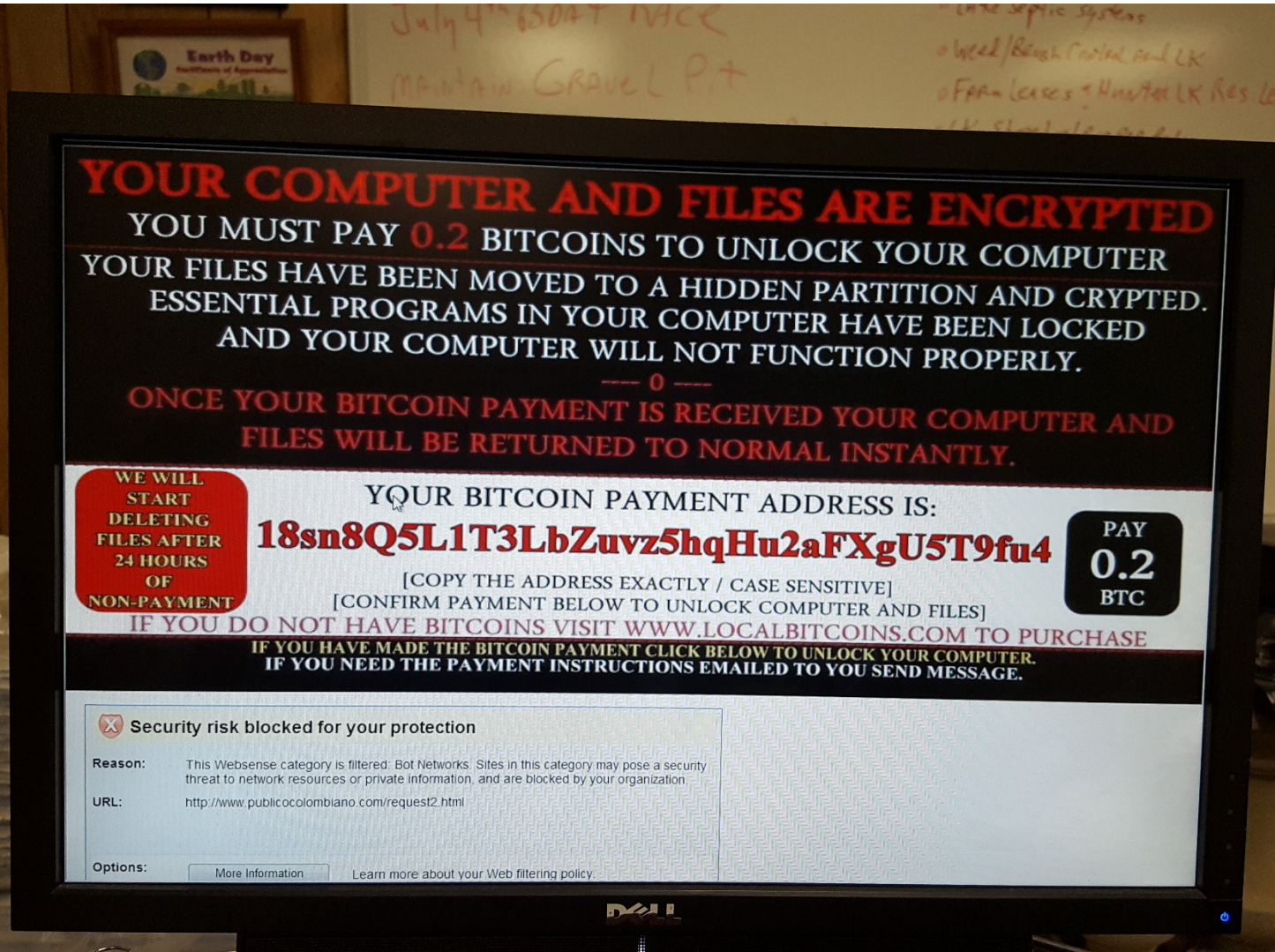












***We encourage voluntary information sharing!***

- **Cyber Security-related information sharing**
  - Indicators of compromise (such as IP addresses, domains, URLs, MD5s, etc.)
  - Forensics artifacts or samples (malicious email, malware, malicious binaries, logs or packet captures)
  - Reports (forensics, after action reports, or analysis)
  
- **Potential Operational Technology (OT) vulnerability issue sharing**
  - Unknown or unexplained PLC or RTU freezes, reboots, or failures
  - Discovered zero day vulnerabilities

***We encourage voluntary information sharing!***

- **Physical Security-related Information Sharing**
  - Breach/attempted intrusion of electricity facilities
  - Misrepresentation – presenting false information or misusing insignia, documents, and/or identification to misrepresent one’s affiliation as a means of concealing possible illegal activity
  - Theft/loss/diversion of key safety or security system, item, or technology
  - Sabotage/tampering/vandalism of facilities
  - Expressed or implied threats
  - Unusual observation or surveillance of facilities



- Products

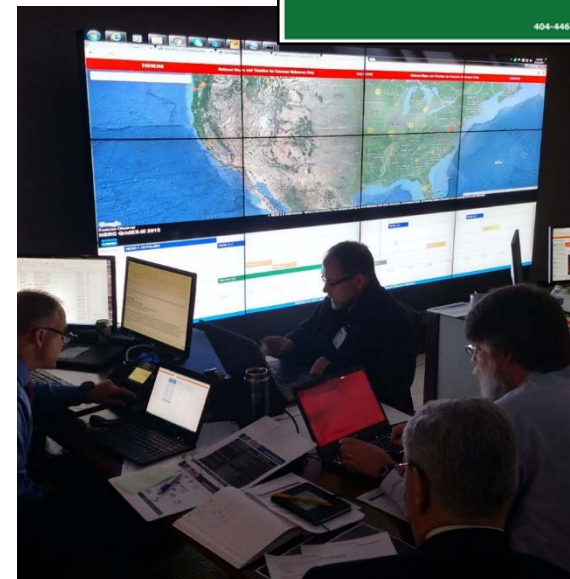
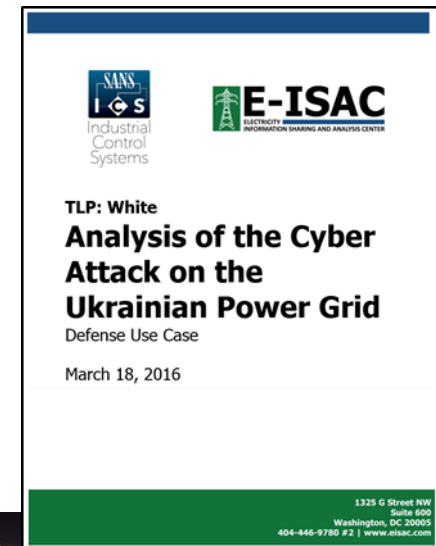
- NERC Alerts
- Incident (cyber and physical) bulletins
- Daily, weekly, and monthly summary reports
- Issue-specific reports

- Programs and Services

- Monthly briefing series, first Tuesday of the month
- Training at quarterly CIPC meetings
- Grid Security Conference (GridSecCon)
- Grid Exercise (GridEx)
- Cyber Risk Information Sharing Program (CRISP)
- Physical security outreach visits

- Tools

- E-ISAC portal ([www.eisac.com](http://www.eisac.com))
- Emergency notifications
- STIX/TAXII automated information sharing





***Kyivoblenergo (KOE)***



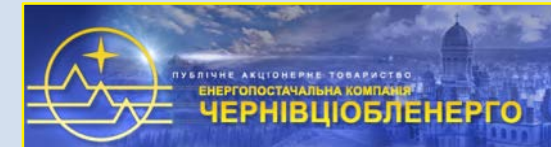
Київобленерго



***Prykarpattiaoblenergo (PKO)***



***Chernivtsioblenergo (CHE)***

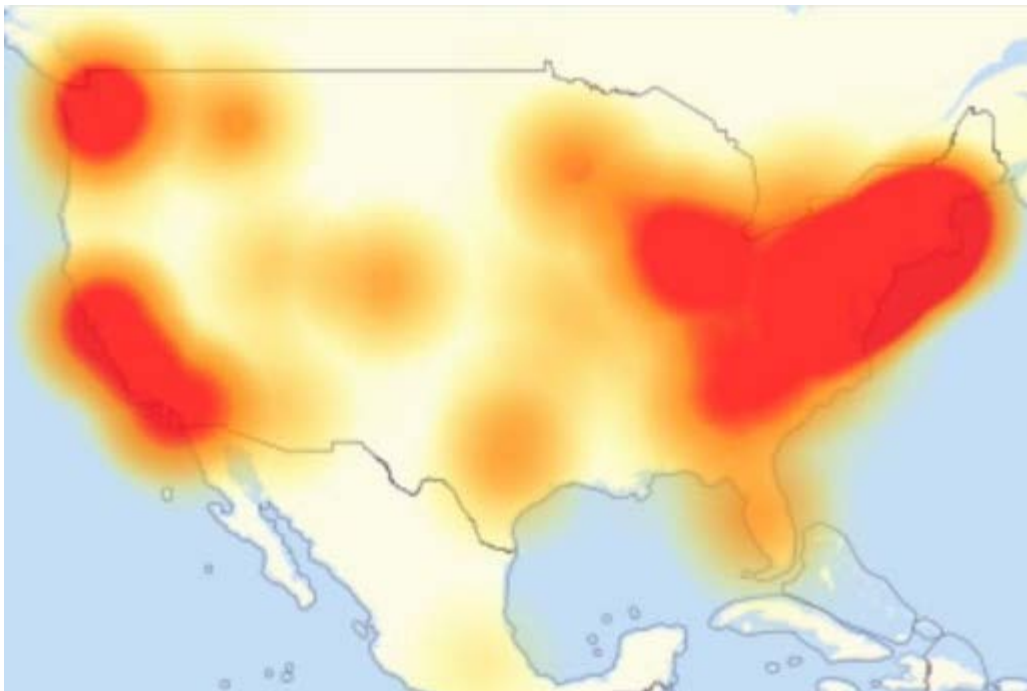


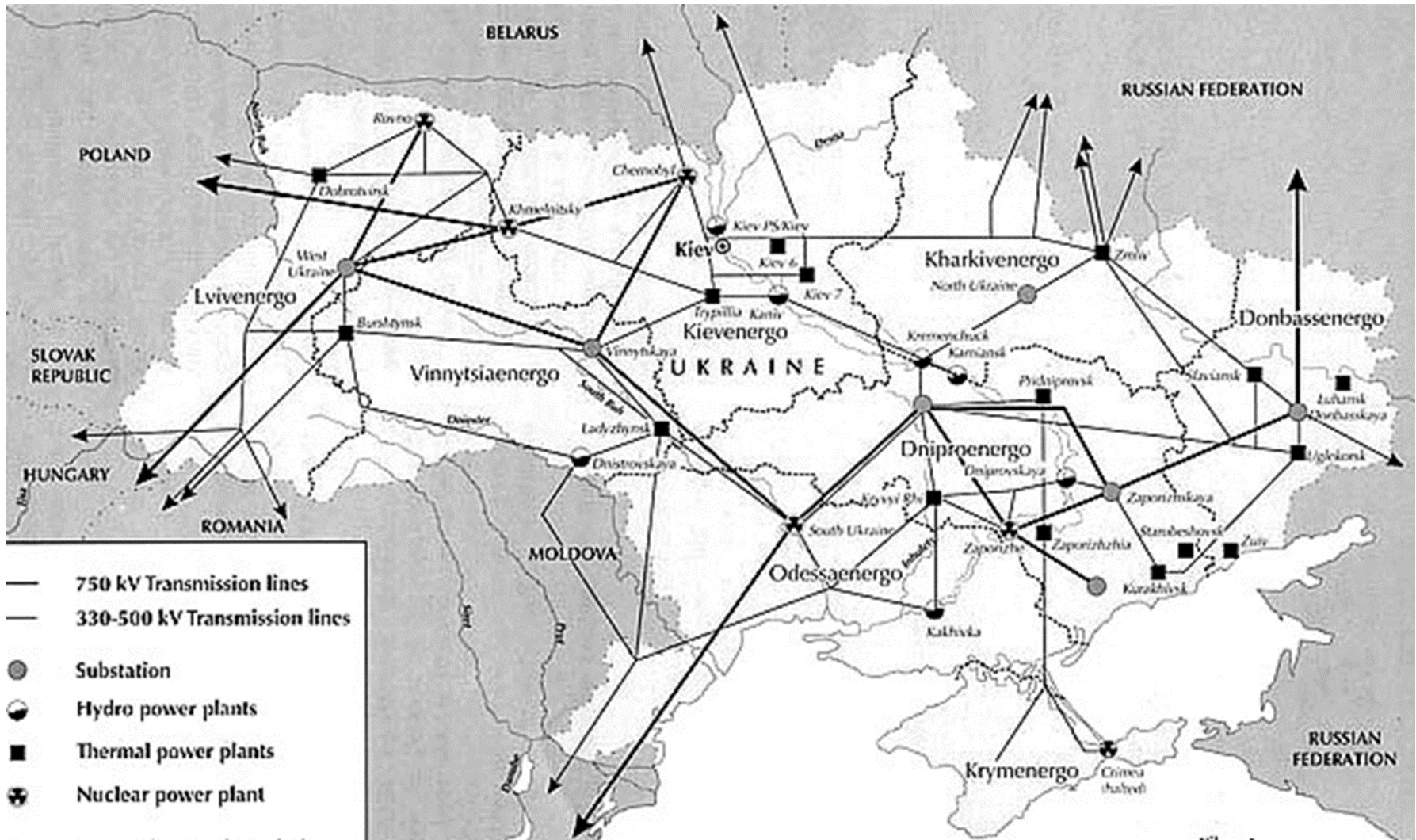
- Lately, we have seen opportunities to educate through events like E-ISAC/SANS Ukraine [DUC – Defense Use Case](#)
  - Common threat and vulnerabilities and top twenty type controls
  - Substantial opportunities in improved ways to view and manage OT environments
- Lessons learned from red team penetration tests



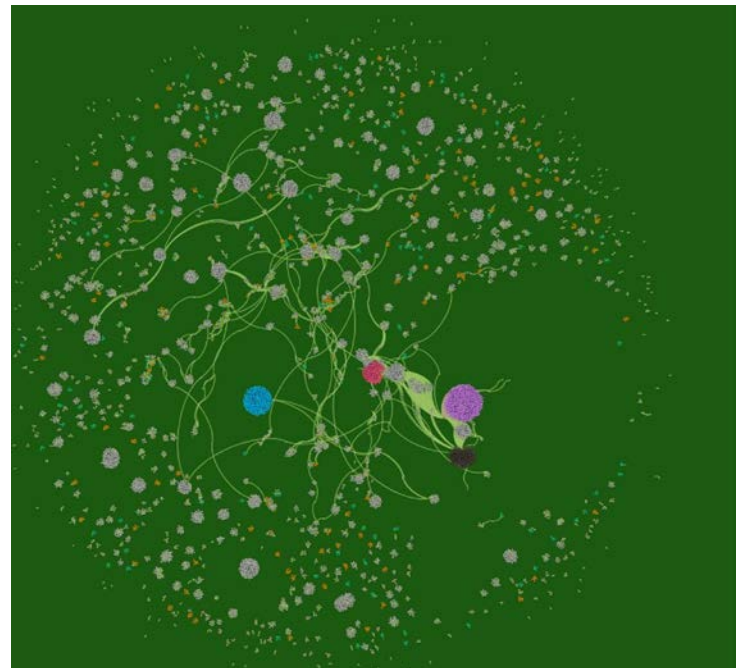


- NERC Level 2 Alert (two weeks prior)
- [Internet of Things / DDoS White Paper](#)

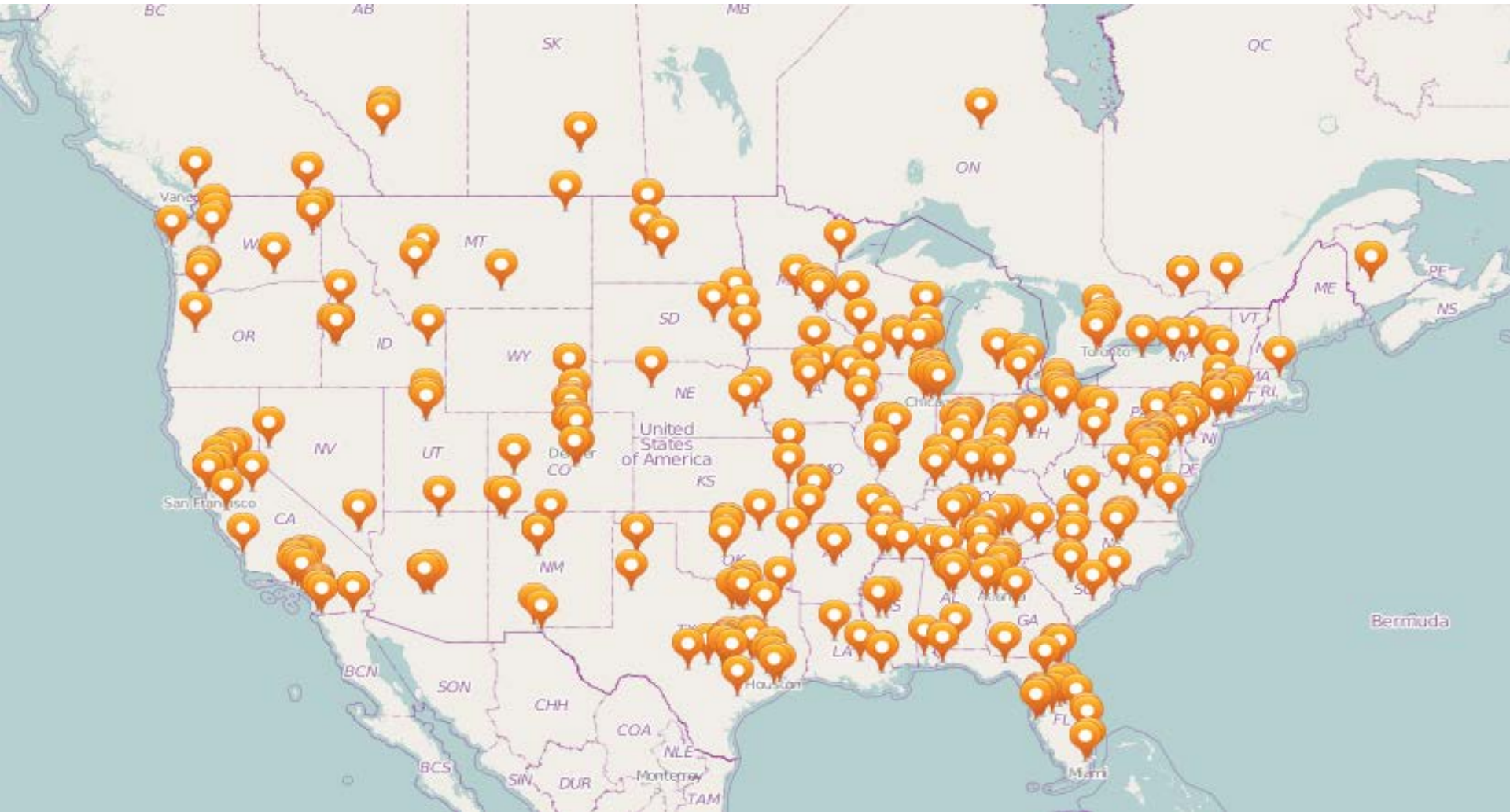




- CRISP and Data Repository, OT Pilot
- Cyber Automated Information Sharing System (CAISS) Pilot
- Portal Improvements / Platform Initiative
- Virtual Forensics (Malware Analysis Dropbox)
- DOE National Laboratory system
- DARPA RADICS



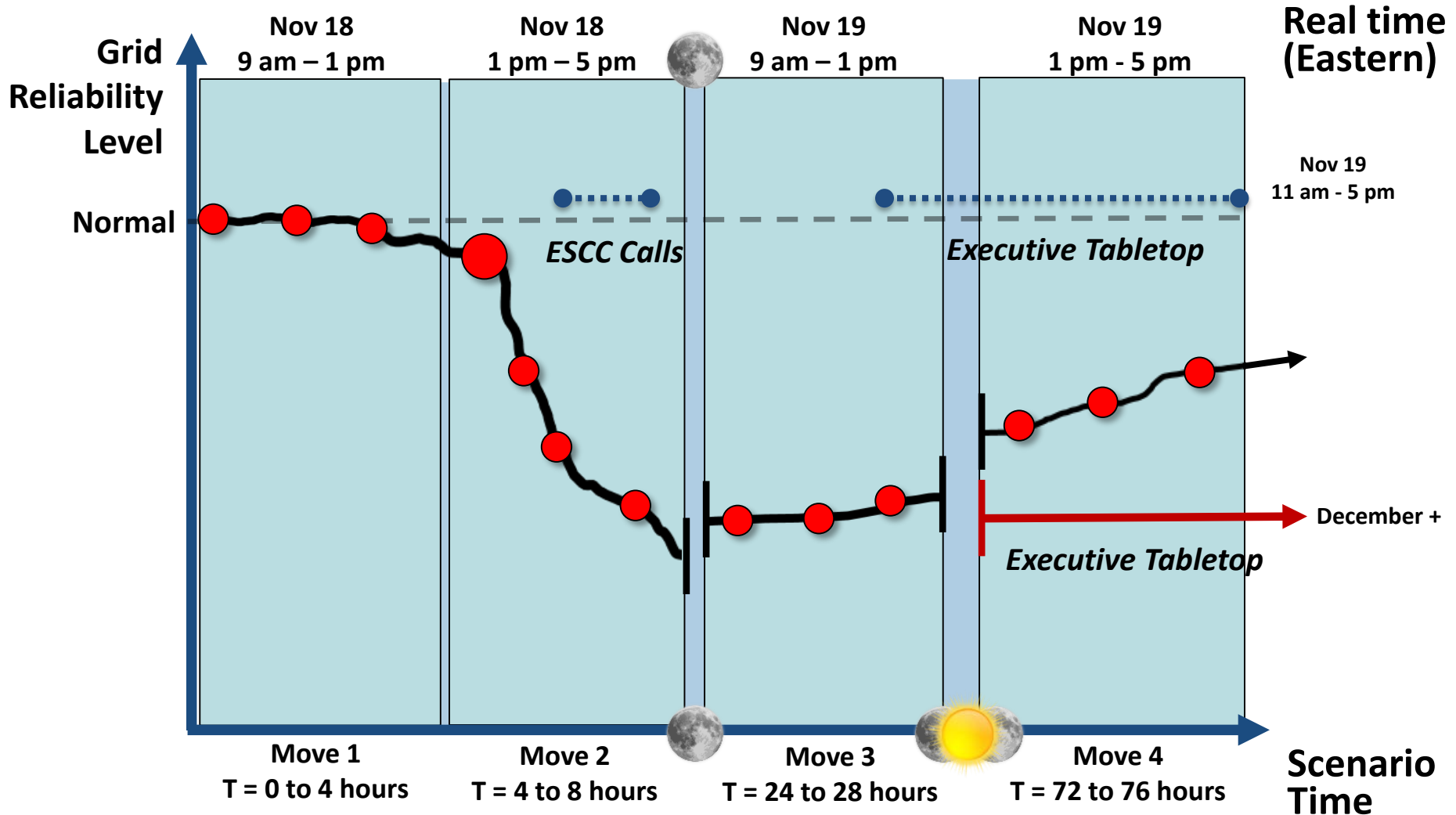






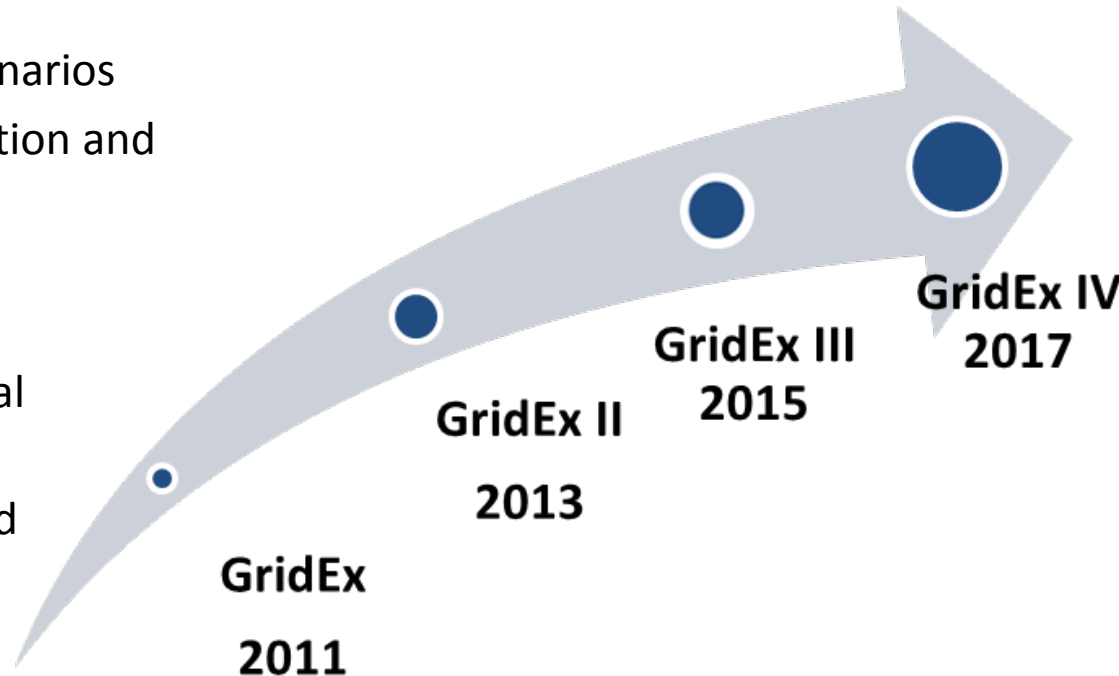


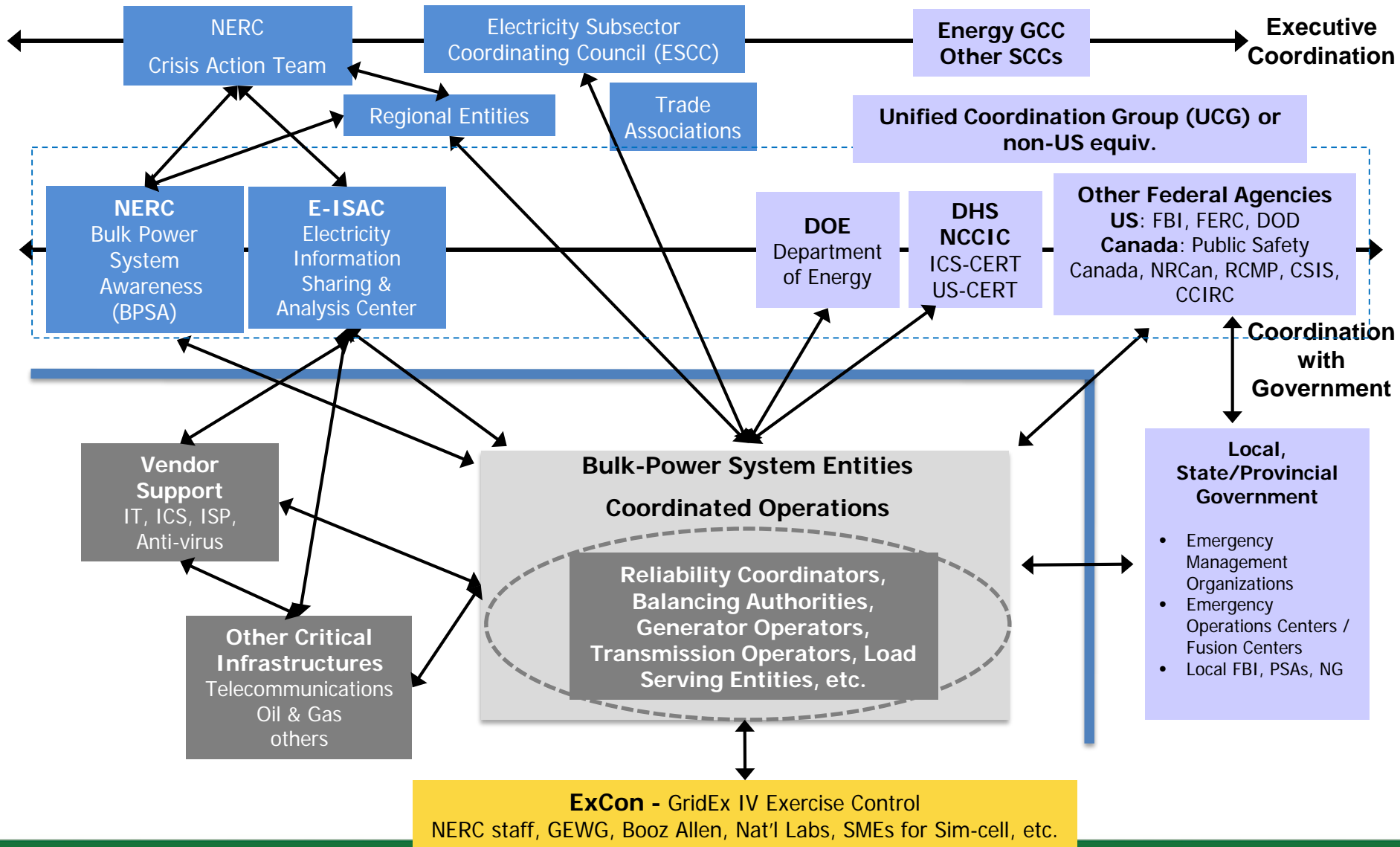
### Distributed Play

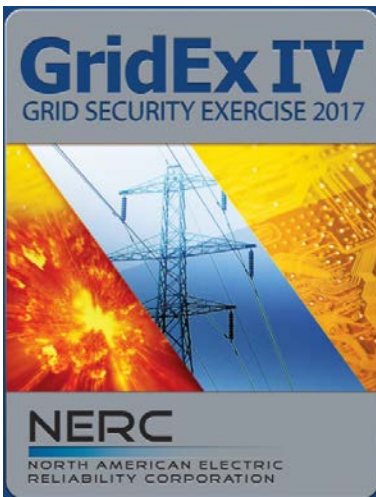


**The vision of the GridEx Program is to strengthen capability to respond to and recover from severe events**

- Exercising timely, real-world scenarios
- Increasing stakeholder participation and training value
- Increasing integration with BPS operations
- Greater state/provincial and local government participation
- Greater integration with U.S. and Canadian senior executives and government officials
- Including other most critically interdependent infrastructure sectors
- Increasing interactive simulation into joint simulation

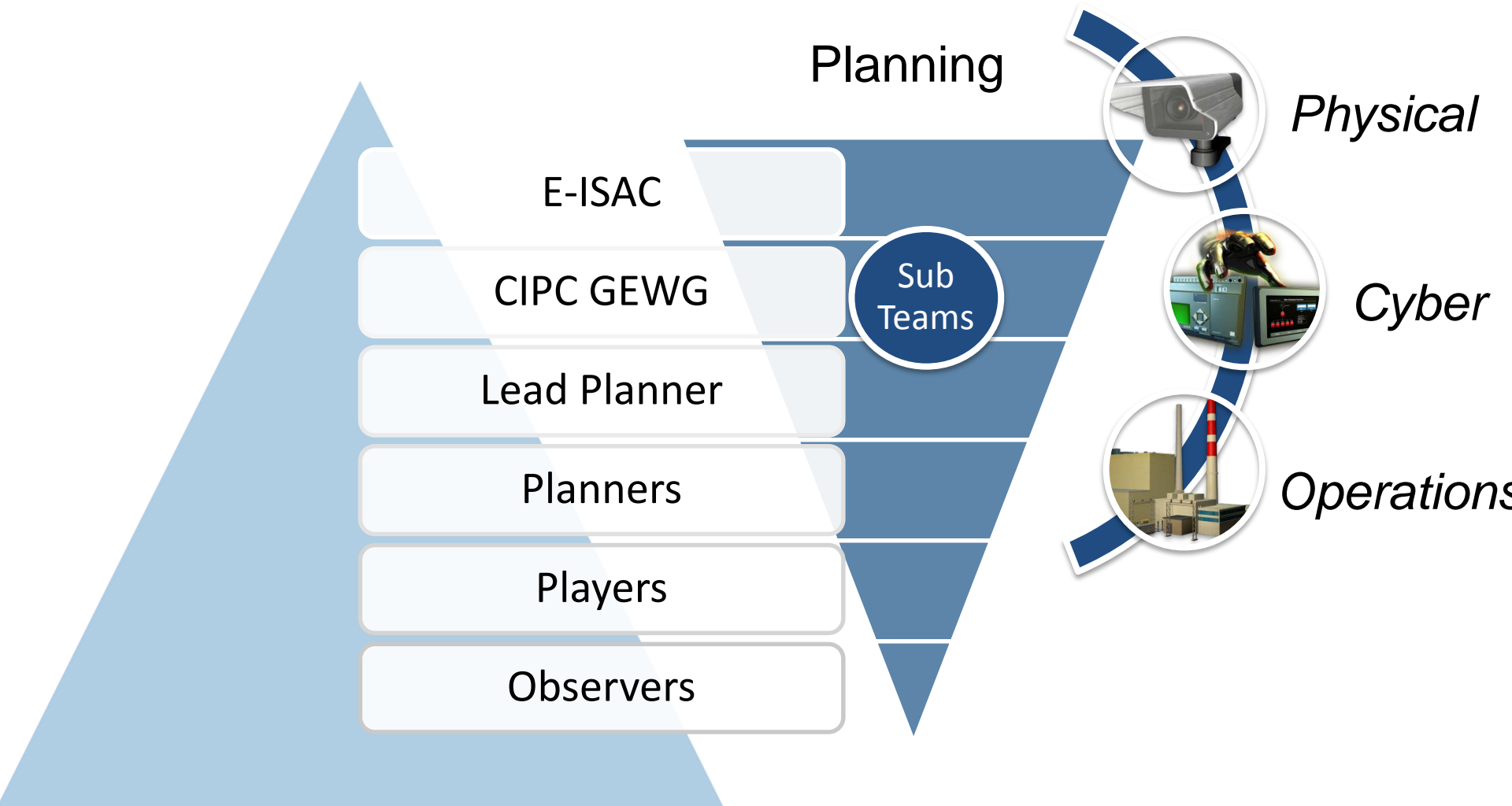






- Exercise incident response plans
- Expand local and regional response
- Engage critical interdependencies
- Improve communication
- Gather lessons learned
- Engage senior leadership





# 65+

*Members*



Physical



Cyber



Operations



RC-to-RC





Training Task Force


## GEWG scenario themes and potential attack vectors from GE3

### Open Issues/ Boundaries







#### 'Yes'

- Distribution 
- Simulated time of year
- Key personnel unavailability 

#### 'No'

- NERC/DOE as patient zero 
- PMU/PDC
- GPS, EMP, GMD

### Cyber Attacks

- Watering hole/HAVEX
- USB in substation
- Shared tools/applications 
- Comms links/MPLS 
- Supply chain corruption
- Remote access infiltration 
- Spearphishing 
- Degradation of monitoring tools 
- BCS issues 

### Physical Attacks

- UAV threats
- Transmission line attack 
- Leak of critical substations
- Scrubber damage
- Control center habitability 
- Water intake degradation
- Fuel supply
- Active Shooter / explosives
- Vendor access to multiple sites
- Exfiltration of security plans





⚠ Exercise Only: Confidential and Restricted to Registered Participants ⚠



Exercise Directory

🔍 search

📅 Exercise Times Daily

## SDN TV

📺 SimDeck TV News

📻 Online Radio

🌐 Agency News

💬 BleatDeck

😊 Frogger

📺 SimTube

## Continuing Coverage of the Power Grid Under Attack



SimDeckNewsSubmitted by on Thu, 11/19/2015 - 12:59

AN EXERCISE MESSAGE THIS IS AN EXERCISE MESSAGE T



**GRID UNDER ATTACK**

SDN Matt Lancaster  
POWER GRID UNDER ATTACK

- Organizations can voluntarily [participate](#) and set their [level of involvement](#) and internal level of effort
- Observing organization:
  - Access to all planning/training materials and meetings, as well as the simulated social media tools
- Active organizations:
  - Simplest
    - Partner with electric utilities (potentially with customers/providers) in local area and help with planning
    - Exercise how electricity outages would impact your organization
  - More involved
    - Use the cyber/physical attack scenario materials to plan own-organization impacts with corresponding impacts to partner electricity utilities

- Real world
- HILF – “what if?”
- Cyber / physical interdependencies
- Information sharing
- Exercising and customization
  
- Research leading to technologies and tools that improve the cyber-security of EDS OT

The background features a photograph of hands writing on a notepad, overlaid with a semi-transparent map of the United States. A horizontal blue bar is positioned across the middle of the page, behind the main title.

# Questions and Answers

*[eisacevents@eisac.com](mailto:eisacevents@eisac.com)*