Cyber and Physical Threats to the Grid

How extensive are they?
What can utilities do to minimize risk?

Presented by
Cecilia Klauber, Lawrence Livermore National Laboratory

Resilience Training for the Southeast
Public Service Commission of South Carolina

May 9, 2023

What threats and hazards keep you up at night?

Cyber

Physical/Kinetic

Physical/Natural

GDO
GRID DEPLOYMENT OFFICE

Cyber Threats

CYBERSECURITY ADVISORY

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

Last Revised: March 01, 2022

CYBERSECURITY ADVISORY

Chinese State-Sponsored Cyber Operations: Observed TTPs

Last Revised: August 20, 2021 **Alert Code:** AA21-200B

Who

- Russia
- China
- Iran/North Korea
- Cyber Criminals
- Hacktivists

- "**Russia** is particularly focused on improving its ability to target critical infrastructure, including…industrial control systems, in the United States…because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis"
- "**China** almost certainly is capable of launching cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines…"
- **North Korea** "probably possess the expertise to cause temporary, limited disruptions of some critical infrastructure networks…"
- "**Iran's** growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S….networks and data."

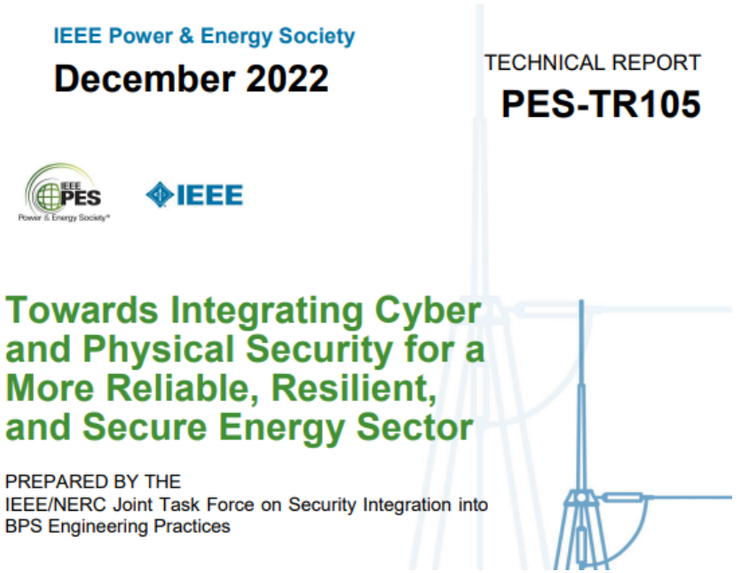
Critical infrastructure is "a lucrative target for **cybercriminals** who see owners as being more likely to pay ransom to avoid disruption." - Deloitte

"**Not all cybersecurity threats are equal**; threat groups have varied funding and levels of technical sophistication. While some operate at very high levels of competence and targeting, others conduct their operations quickly and cheaply by leveraging the exploits, tactics, and control mechanisms used (and often discarded) by higher caliber attackers."
– DOE, Cybersecurity Considerations for DERs on the U.S. Electric Grid

Cyber Threats

What

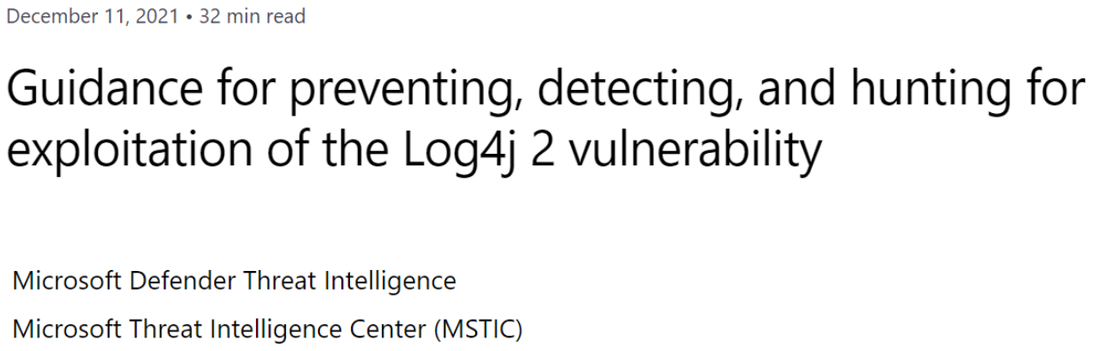
- Substations
- Generation/Natural Gas
- Control Centers (SCADA)
- DERs, IoT, GPS, etc.



Cyber Threats

How

- Ransomware
- Network Intrusion: IT to OT
- Supply Chain
- Advanced Technologies



Advanced Technologies
Artificial Intelligence/Machine Learning
Cloud infrastructure
Edge Devices and Computing

Cyber Threats

Who

- Russia
- China
- Iran/North Korea
- Cyber Criminals

What

- Substations
- Generation/Natural Gas
- Control Centers
- DERs, IoT, GPS, etc.

How

- Ransomware
- Network Intrusion: IT to OT
- Supply Chain
- Advanced Technologies

With many actors, targets, and vectors – how do we assess the risk and determine an actionable response?

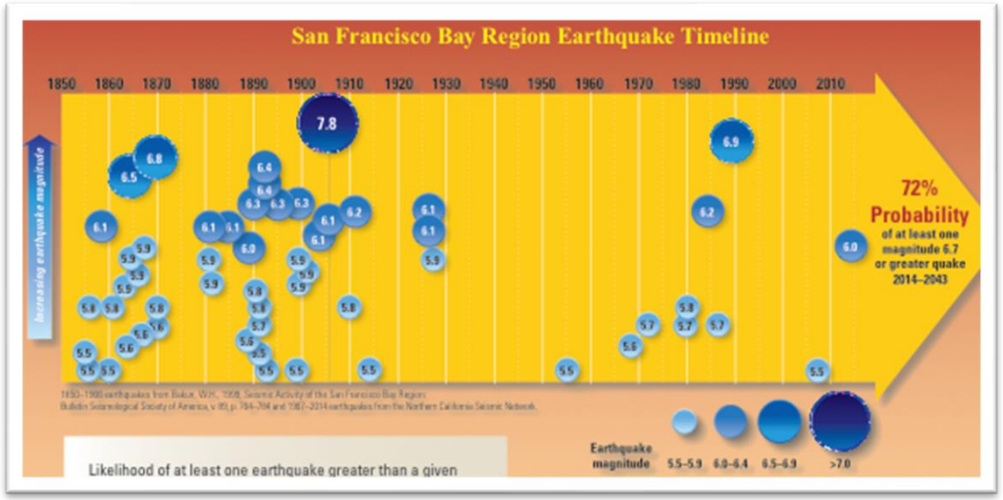
GRID DEPLOYMENT OFFICE

How do we assess the risk?

Probability-Based Approaches are Suitable for Assessing *Natural Hazard* Risk

- Have many historical examples (including frequency and associated impacts)
- Can derive reasonable probabilities
- Events are random in nature
- Events are not optimized to maximize damage

Intelligent adversary attacks require a different approach



GDO
GRID DEPLOYMENT OFFICE

Example Scenario

- What **action** would you take if I told you **the probability** of this attack?
- What **action** would you take if I told you the attack would be 3 orders of magnitude **more difficult** if you applied a specific mitigation?

Effective risk methodology must provide specific, actionable recommendations and the ability to quantify risk reduction when mitigation measures are deployed

GRID DEPLOYMENT OFFICE

Start with Consequences and Quantify Difficulty

Quantitative Intelligent Adversary Risk Analysis (QIARA) starts with the consequence, not the threat actor

- We know what we want to protect

Quantify *difficulty* of each path, not probability

- We know what it would take to overcome our protections

Map the risk landscape

- Relative risk information enables prioritization of investments across **hazards and sectors**
- Does **not** provide information about absolute risk

GRID DEPLOYMENT OFFICE

Assessment of Attack Difficulty Rather than Likelihood

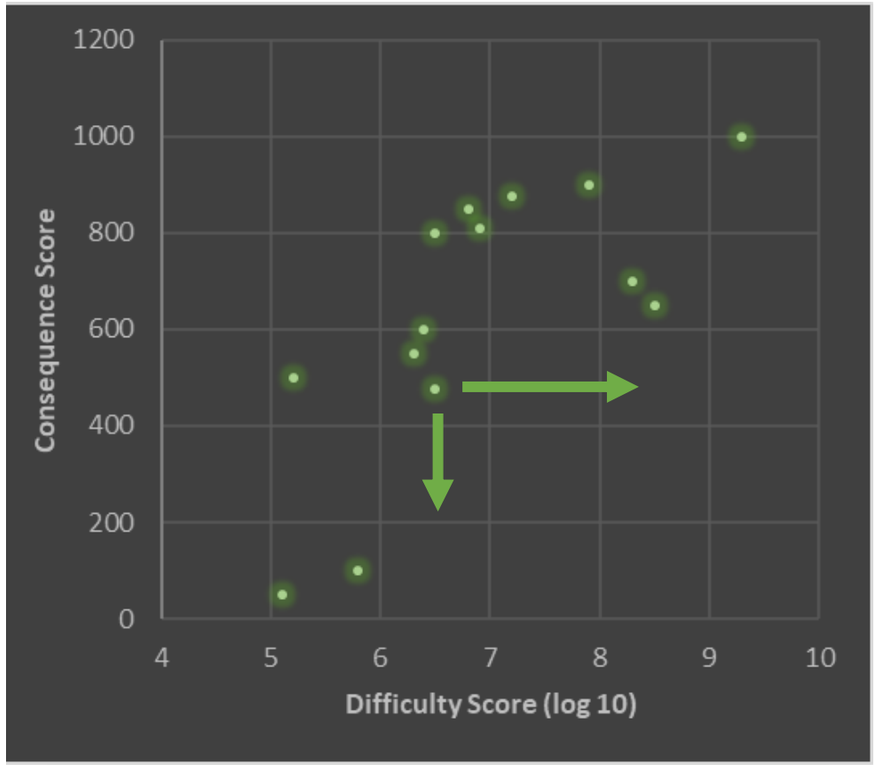
What steps are taken?

- MITRE ATT&CK techniques, SANS ICS Cyber Kill Chain
- Techniques require resources – how difficult are they to acquire?

System Vulnerability – How vulnerable is the target/system to being exploited?

Network Segmentation – How difficult is it to navigate network segmentation to gain access to the ultimate or intermediate target?

Risk is a function of **difficulty** and **consequence**
Risk landscape also informs **mitigation effectiveness**



Mitigations should increase difficulty and/or decrease consequences

GRID DEPLOYMENT OFFICE

Mitigations and Best Practices

- **Good cyber hygiene**
  - strong passwords, patched software, phishing awareness
- **Network Segmentation**
  - Firewalls, DMZs
  - Put hurdles between IT and OT
- **Encryption**
- **Least Privilege**
- **Multifactor Authentication**
- **Supply Chain Policies**
- **NIST Cybersecurity Framework, NERC CIP standards**

GDO
GRID DEPLOYMENT OFFICE

Physical Threats

Who

- Disgruntled insiders
- Domestic terrorists
- Nation states

What

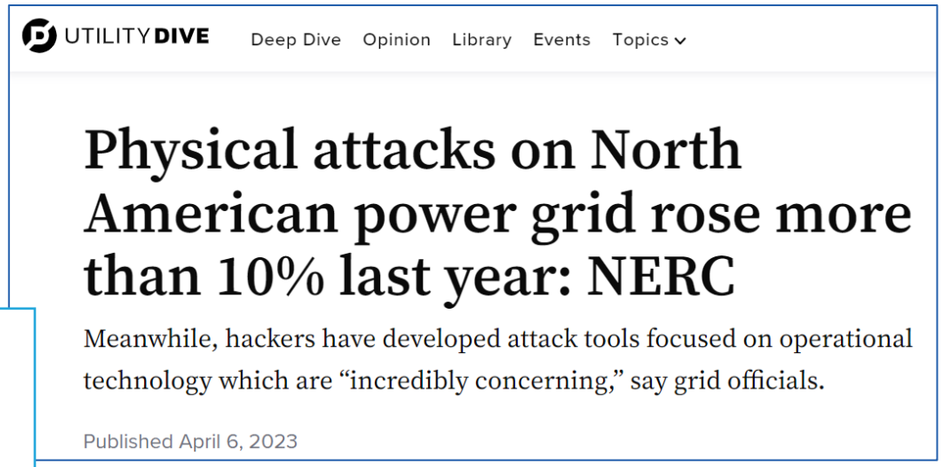
- Transformers/Substations

How

- Gunfire
- Electromagnetic pulses (EMPs)
- Intrusion/Tampering
- Vandalism

1,700 physical security incidents reported to E-ISAC in 2022
Only 3% resulted in outage/operating impacts

Washington – 15,000 outages
North Carolina – 45,000 customers


UTILITY DIVE Deep Dive Opinion Library Events Topics

Physical attacks on North American power grid rose more than 10% last year: NERC

Meanwhile, hackers have developed attack tools focused on operational technology which are "incredibly concerning," say grid officials.

Published April 6, 2023

Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

June 17, 2014


WORLD & NATION Los Angeles Times

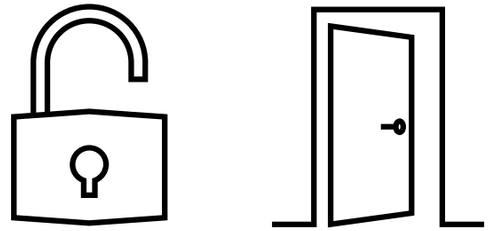
Sophisticated but low-tech power grid attack baffles authorities


FORBES > BUSINESS > ENERGY

Protecting America's Power Grids From EMP Attacks

GRID DEPLOYMENT OFFICE

Risks and Mitigations



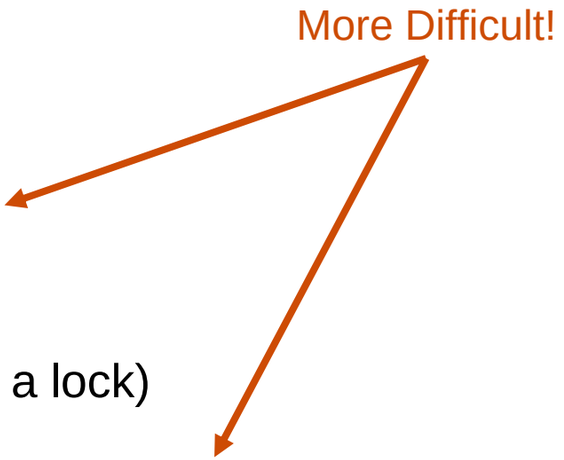
These are also intelligent adversaries – and risk should be assessed accordingly

Adversaries must still progress through the kill chain, and require resources along the way

Example: Target Protection | Intrusion/Initial Access

- Cyber
  - Single-factor protection can be overcome by simple means (brute force)
  - If you implement multi-factor authentication,
    - Adversary requires theft, duplication, or spoofing to access target

- Physical
  - Simple protection can be overcome by simple means (ex. cutting through a lock)
  - If you implement strong protection,
    - Adversary must overcome biometric or security (two-person integrity) methods



GRID DEPLOYMENT OFFICE

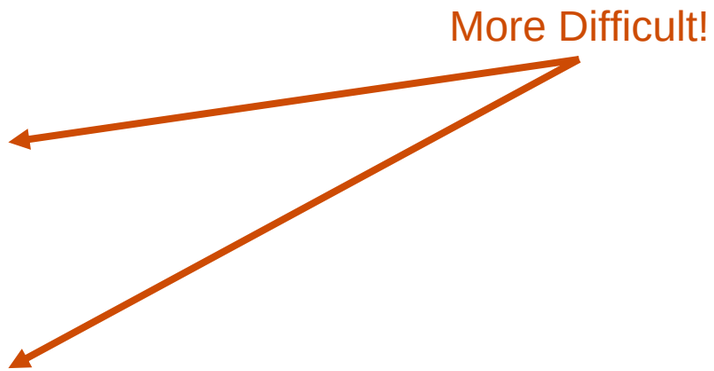
Risks and Mitigations

These are also intelligent adversaries – and risk should be assessed accordingly
Adversaries must still progress through the kill chain, and require resources along the way

Example: Detection Avoidance | Attack Planning and Development

- Cyber
  - If you monitor network traffic,
    - Adversary must deceive/circumvent monitoring systems

- Physical
  - If you install video cameras/motion detectors,
    - Adversary must avoid/circumvent monitoring systems



GRID DEPLOYMENT OFFICE

Risks and Mitigations

Remember: in addition to *increasing* the difficulty of a particular attack, *decreasing* the consequences also *lowers the risk*
Other resilience investments are also steps in the right direction

- Microgrids
- Interconnections
- Energy Storage
- Redundancy
- Advanced Metering

GRID DEPLOYMENT OFFICE

Physical/Natural Threats

What

- Loss of distribution/transmission
- Loss of generation
- Increased load

How

- Hurricanes
- Floods
- Wildfire
- Drought

ENVIRONMENT

PG&E Will Bury 10,000 Miles of Power Lines So They Don't Spark Wildfires

July 21, 2021 · 10:46 PM ET

By The Associated Press

Pacific Gas & Electric plans to bury 10,000 miles of its power lines in an effort to prevent sparks that can start wildfires.

Jeff Chiu/AP

Why Hurricane Ida crippled the New Orleans power grid

By Tim Mclaughlin and Stephanie Kelly

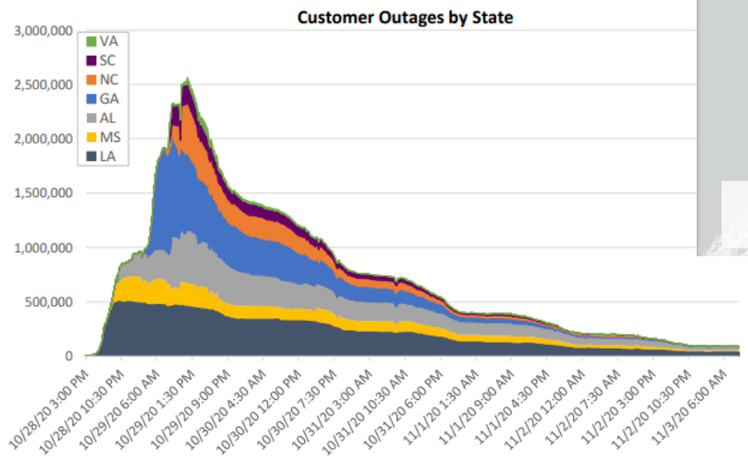
[1/3] Damaged power lines and homes can be seen days after hurricane Ida ripped through Grand Isle, Louisiana, U.S., September 2, 2021. REUTERS/Leah Millis

GRID DEPLOYMENT OFFICE

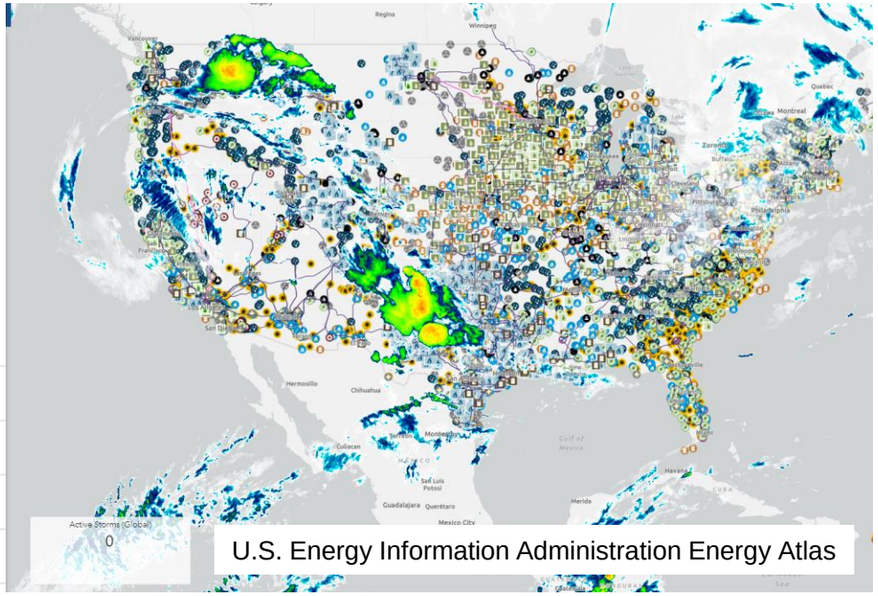
Hurricane Risks and Mitigations

There are many historical examples to learn from

- DOE CESER Situation Reports
- EIA Energy Atlas



Hurricane Zeta | Update #6



U.S. Energy Information Administration Energy Atlas

What utilities are doing to improve resilience to hurricanes (GAO)

- Implementing storm hardening measures
- Adopting operational capacity enhancing technologies
- Participating in mutual aid programs, training exercises

GRID DEPLOYMENT OFFICE

Summary

Cyber, Physical, Natural Threats/Hazards

- Who, What, How

Assessing Intelligent Adversary Risk

- Difficulty x Consequence

What can we do?

- Adopt basic security protections, regardless of utility size
- Assess and address difficulty/likelihood of priority threats
- Emerging technologies can introduce additional threat vectors, but can also play a role in reducing risk

GRID DEPLOYMENT OFFICE

GRID DEPLOYMENT OFFICE

Contact

https://www.energy.gov/gdo/grid-deployment-office

Cecilia Klauber, klauber1@llnl.gov

Lawrence Livermore National Laboratory

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

LLNL-PRES-848876