Cyber-Security Vs. Physical Security
High Voltage vs. Low Voltage: Which Should Be A Priority?
Harvard Electricity Policy Group
June 13, 2014
Threats

Lions and Tigers and Bears, Oh My!

Source: The Wizard of Oz, Metro-Goldwyn-Mayer (1939)
Threats

➢ Natural Events
   ➢ Weather
      ➢ Wind Storm
      ➢ Snow/Ice Storm
      ➢ Hurricane
      ➢ Space Weather

➢ Human Intervention
   ➢ Cyber Attack
   ➢ Physical Attack
      ➢ Kinetic Attack
      ➢ Electromagnetic Interference Attack (EMI)
      ➢ High Altitude Electromagnetic Pulse Attack (HEMP)
Threats

Threat Landscape: ELECTRIC POWER SECTOR

Source: EEI Perspectives, May/June 2014 page 32
Space Weather

Coronal Mass Ejection/Aurora Two Days Later

Source: ESA and NASA Solar Heliospheric Observatory (SOHO); Aurora over Prudhoe Bay, Alaska. 3/17/2013 Image Courtesy of Greg Syverson
**Space Weather**

**Impact on Power System**

![Diagram showing the impact of space weather on power systems](image)

- **Geomagnetically-induced currents (GIC)** can cause:
  - Increased reactive power consumption
  - Transformer heating
  - P&C misoperation

Source: Draft TPL-007-1 Standards Drafting Team Industry Webinar, page 6 (Apr. 24, 2014)
Physical Security

Kinetic Attack

Shots in the Dark
A look at the April 16 attack on PG&E’s Metcalf Transmission Substation

1. 12:58 a.m., 1:07 a.m. Attackers cut telephone cables
2. 1:31 a.m. Attackers open fire on substation
3. 1:41 a.m. First 911 call from power plant operator
4. 1:45 a.m. Transformers all over the substation start crashing
5. 1:50 a.m. Attack ends and gunmen leave
6. 1:51 a.m. Police arrive but can’t enter the locked substation
7. 3:15 a.m. Utility technician arrives

Sources: PG&E; Santa Clara County Sheriff’s Dept.; California Independent System Operator; California Public Utilities Commission; Google (image)
The Wall Street Journal

Electromagnetic Interference Attack

Fictional Truck Device

Source: Ocean’s 11
Electromagnetic Interference Attack

Compact Device?

Source: Photograph Courtesy of Steven T. Naumann
HEMP Attack

- Detonation of a nuclear device at altitude
- Starfish Detonation 1962 as seen in Hawaii

HEMP Attack

- Detonation of a nuclear device at altitude
  - Gamma-yield enhanced weapons
  - Line of Sight Effect
- E1 Impact
  - Line of sight effect
  - Substation and Generation Controls and Communications
  - Control Centers and SCADA
  - Possible Insulator Flashover on Distribution Lines
  - Smart Grid Semiconductor Devices
- E3 Impact
  - Similar to impact of space weather
Impacts

- Natural Events
  - Weather
    - Wind Storm - Distribution
    - Snow/Ice Storm – Distribution/Some Transmission
    - Hurricane – Distribution/Some Transmission
    - Space Weather – High Voltage Transmission
  - Human Intervention
    - Cyber Attack – Transmission/Distribution/Generation
    - Physical Attack
      - Kinetic Attack – Transmission/Distribution/Generation
      - EMI Attack – Transmission/Control Centers/Generation (not widespread)
      - HEMP Attack – Entire System
Prevention - Mandatory Reliability Standards

- Natural Events
  - Weather
    - Space Weather
      - Reliability Standards for Geomagnetic Disturbances, Order No. 779, 143 FERC ¶ 61,147 (2013)
      - EOP-010 filed Nov. 13, 2013; RM14-1 (awaiting FERC action)
      - TPL-007 (under development)
  - Human Intervention
    - Cyber Attack
      - CIP-002 through CIP-011 (CIP V5)
    - Physical Attack
      - Kinetic Attack
        - FERC Order in Docket No. RD14-6, 146 FERC ¶ 61,166 (March 7, 2014)
        - CIP-014: Docket No. RM14-15 (filed May 23, 2014)
Prevention – Other Processes

- Response to Threats
- Information Sharing – Electric Sector – Information Sharing and Analysis Center (ES-ISAC)
- DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Transfer of tools and technologies from the government
- Physical Security at stations not required by CIP-014
Resiliency and Restoration

- Spare Transformer Equipment Program (STEP)
  - Sharing assets following an event – a terrorist attack resulting in the destruction or long-term disabling of transmission transformers
  - Transmission-to-Transmission Transformers
  - 50 Utilities participating
  - Binding contractual arrangement
- Spare Connect
  - Voluntary programs – open to all utilities
  - Transmission-to-Transmission Transformers, Generator Step-Up Transformers, Auxiliary Substation Components (bushings, fans, radiators)
- Transformer Transportation
- Recovery Transformer (RecX)
  - EPRI/DHS
  - Modular, small and lighter allowing for easier transportation and more rapid installation
  - 20 hours St. Louis – Houston/Energized in Five Days
- Incident Response – Planning and exercising coordination
Resiliency and Restoration

200 MVA 345/138kV Single Phase Recovery Transformer

Source: Photo Courtesy of DHS S&T
Priorities

- Distribution Level Outages More Frequent and Cause Outages
- Transmission Level Outages Less Frequent and Rarely Cause Customer Outage
- But:
  - Some Transmission Events (Coordinated Physical Attacks, Coordinated Cyber Attacks, Severe GMD Storm, HEMP Attack) are **High Impact, Low Frequency (HILF)** Events – these affect everyone
- Cannot Prevent Everything
- Three-Legged Policy
  - Prevention
  - Resiliency
  - Restoration
What Should Be Done?

- Electricity is Critical to Modern Society
- New Threats to Continuity of Service/Time for Restoration
- Intersection Between Utility Operations and National Security
- Public-Private Partnership
- Electric Sub-Sector Coordinating Council (ESCC)
  - Serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure
  - Includes utility CEOs and trade association leaders representing all segments of the industry
  - Government counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations
- Need a balance – everything cannot be a priority
- Role for the government also
Cost Recovery

- This all costs money
- Distribution risks
  - More frequent, directly affect customers
  - Physical attacks
    - Cannot protect each distribution station and limited scope of damage to system as a whole
  - Are there specific very critical distribution substations to national and economic security?
- Transmission risks
  - New risks – high impact, low frequency
  - What threat to plan for?
- Balance between prevention, resiliency and restoration
- For high-impact, low frequency events, need policy developed by industry and government