UNM National Security Studies Program

US Cyber Security Readiness

Key issues within Civilian Critical Power Generation Infrastructure

David Vazquez Cheatham, UNM National Security Studies Program

8-24-2017

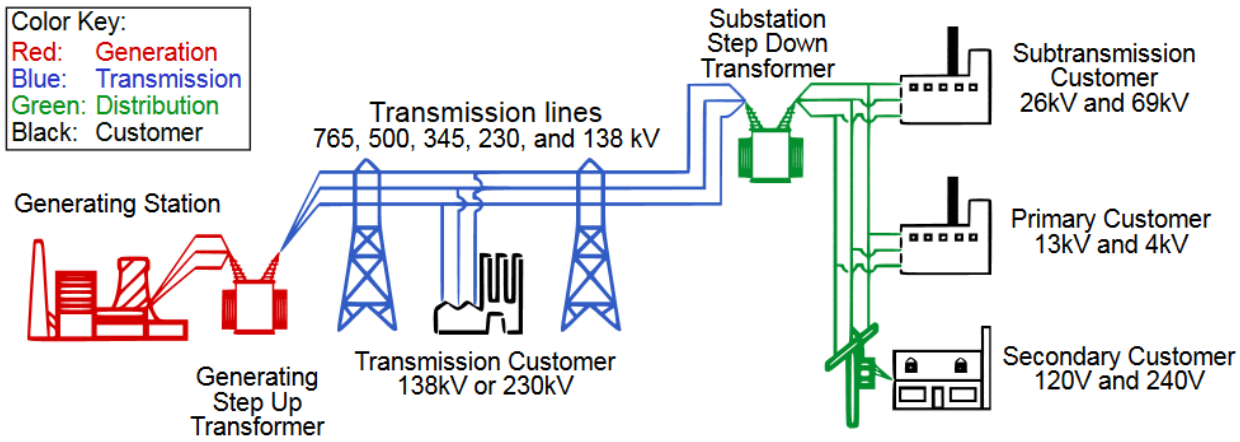
Findings & Recommendations:

It has been known for decades that the US Power infrastructure contains key weaknesses in both physical and cyber security countermeasures. In addition, hardware design of primary control centers and critical components are in need of a major overhaul by design engineers building in features that will address the known cyber security weaknesses. In order to address physical security weaknesses across the US, a standard must be set with a system to both guide and hold accountable energy providers physical security of critical infrastructure. Despite calls for action from the scientific community, analysts and even congressmen there has been little headway. The need for upgrades has become critical in nature for our national defense due to threats from a range of attacks: physical, cyber, electromagnetic pulse, directed energy weapons and certain severe weather conditions can all wreak havoc.

The range of threats comes from ever increasing sources to include nation states, terrorist groups, Individuals and organized crime groups here in the US and overseas. While there is a concerted effort to fix and upgrade the current grid system in progress the key issues of inherent weakness to cyber threats, attack or physical damage need to be addressed or the system will remain vulnerable. The economic effects of continued physical and cyber-attacks from threat actors on the grid will only increase as long as there is a dearth of political will, necessary to implement regulatory action.

Background: Power generation and distribution systems in the United States

Systems generating and delivering power are highly complicated and interconnected throughout the United States. They may be separated into major components as shown in the diagram below.



Power generation, transmission and distribution systems

The process begins with the generation of electricity using a multitude of currently available systems using fuel sources that include: coal, gas, nuclear, solar, wind, hydroelectric, and geothermal energy. Electricity in the United States grid is alternating current (AC).

Generation[1]

Generators convert kinetic (mechanical) energy into electrical energy to produce electricity for consumers to use. Power plants mostly use a turbine to drive the generators, although there are multiple other methods used to produce electricity.

1. Turbine generators: A moving fluid pushes a series of blades mounted on a shaft, which rotates the shaft connected to a generator. This, in turn, converts the

[1] Source: US Energy Information Administration (EIA) https://www.eia.gov/energyexplained/index.cfm?page=solar_photovoltaics

mechanical energy to electrical energy. Types of turbines include steam turbines, gas combustion turbines, water turbines, and wind turbines. Electricity may be produced by nuclear fission, coal, natural gas, geothermal, hydroelectric dams, thermoelectric generators, solar thermal and electric processes.

Transmission[2]

Transmission infrastructure refers to the transmission lines, transformers, circuit breakers, capacitor banks, and other equipment that make up the transmission system. The transmission system is generally defined as equipment used to transmit electricity from generators to distribution networks operated at 100 Kilo Volts (kV) or above. It does not include the local distribution network supplying consumers. [3,4]

At the generating station, bulk electrical power is generated and manipulated by operators to reduce line losses. The transmission system can be divided into two sub systems.

1. Primary transmission - The electrical power is transmitted by 3-phase 3-wire over-head line system to the area to be serviced (typically a metropolitan area).
2. Secondary transmission – Occurs after the primary transmission line terminates at a substation and the voltage is reduced using a step-down transformer for use by customers.

[2] *Transmission and distribution system, Kumar Venkat, July 4 2014, kumar, v. (2014, July 4). Transmission and distribution system . Retrieved from All About Electrical World: http://allaboutelectricalworld.blogspot.com/2014/07/transmission-and-distribution-system.html*

[3] NERC (2014a): http://www.nerc.com/pa/RAPA/BES%20DL/bes_phase2_reference_document_20140325_ final_clean.pdf

[4] On March 20, 2014, FERC approved the NERC definition of Bulk Electric System (BES), which includes system elements down to 100 kV, with provisions for including lower voltage equipment if operated as a transmission facility, or excluding higher voltage equipment if not operated as a transmission facility. This definition became effective July 1, 2014.

Distribution[5]

The distribution system carries electricity at lower voltages over short distances locally and is divided into two sub systems:

1. Primary distribution – After the secondary transmission line ends at the substation the lower voltage is transmitted from substation to the home over low voltage distribution lines.
2. Secondary distribution - The electrical power from the primary distribution lines are delivered to the consumer after passing through a secondary transformer on the distribution pole and stepped down to 120v or 240v for customer use.

Interconnections[6]

There are four major electric system networks in North America, serving a population of over 80 million. The Federal Energy Regulatory Commission (FERC) is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil.[7] The North American Electric Reliability Corporation (NERC), subject to oversight by FERC, is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system in North America. NERC develops and enforces Reliability Standards; monitors the Bulk Electric Systems (BES) through system awareness; and educates, trains, and certifies industry personnel.[8]

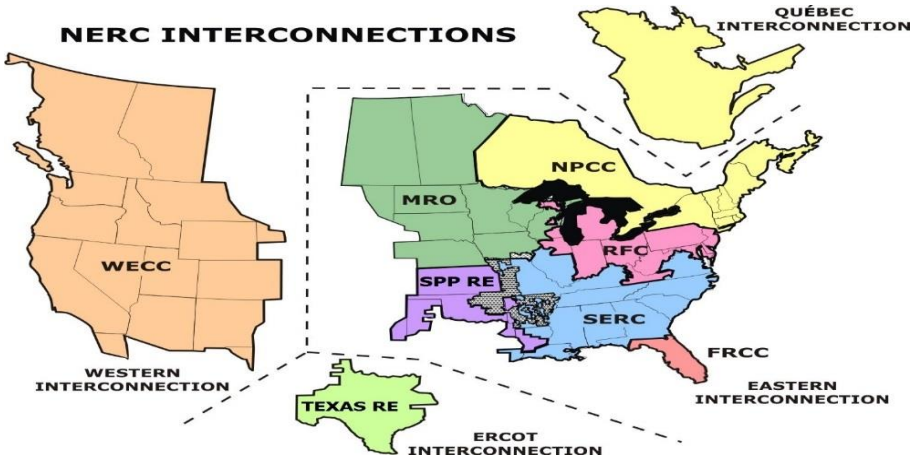
[5] *Transmission and distribution system, Kumar Venkat, July 4 2014, kumar, v. (2014, July 4). Transmission and distribution system . Retrieved from All about electrical world: http://allaboutelectricalworld.blogspot.com/2014/07/transmission-and-distribution-system.html*

[6] https://www.eia.gov/todayinenergy/detail.php?id=27152

[7] https://www.ferc.gov/about/ferc-does.asp

[8] http://www.nerc.com/AboutNERC/Pages/default.aspx

The Bulk Electric Systems (BES) covers all transmission elements operated at 100 kV or higher composing the interconnections and spans more than 1.8 million square miles in all or part of 14 states, and links all the minor local grids across the United States.[9]



Source: Western Electricity Coordinating Council

NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people. North America is divided by NERC into the following assessment areas for monitoring reliability in different areas.

NERC Assessment areas

[9] National Electric Transmission Congestion Study (2015), Page v

Reliability Functions

NERC registers entities according to Reliability Functions. The Nuclear Regulatory Commission (NRC) has additional authorities over nuclear power plants, though not related to interconnectivity.[10] Authorities with NERC certification are as follows:

1. Reliability Coordinators (RC) have the authority to prevent or mitigate operational emergencies in both next-day analysis and real-time operations.
2. Balancing Authorities (BA) balance load and generation within their footprint and maintain interconnection frequency.
3. Transmission Operators (TOP) direct the operations of their local transmission system.

The balancing authorities within the United States and Canada interconnect and coordinate through a series of transmission lines and authority regions. These are shown in attachment 1 to this report.

Cascading

One important factor in assessing reliability and threats lies in the physical makeup of the grid network and interconnection that can have a cascading effect. Cascading is the result of a fault or damage somewhere in the grid, which may create a sustained and growing effect that ultimately forces a generator to shut down. The load placed on other generators puts further stress on the grid, which may lead to more generator failures, causing large geographical power outages. Isolated and independent grids, would be spared from the cascading effect. Generator failures and a major cascading event can result in a societal collapse due to the following conditions: failure of critical

[10] National Electric Transmission Congestion Study (2015), Page 35

communications networks, lighting and heating, loss of refrigeration and perishable food stuffs, disruption of emergency and medical services, banking services disappear and access to currency scarce, lack of proper sewage treatment and water purification.

Assessment: Grid Controllers and Structural Weaknesses

This section examines the type of threats and threat actors that could induce a cascading incident and identifies structural weaknesses in system infrastructure.

Threats

Attacks to the power grid may come in a variety of methods, including through natural occurrences. The Center for the study of the Presidency and Congress has categorized them as follows.

1. Cyberattack – A Cyber-attack can result in either an incident or a breach, "an incident is a security event that compromises the integrity, confidentiality or availability of an information asset while a breach is an incident that results in the confirmed disclosure, not just potential exposure, of data to an unauthorized party."[11] During the cyber-attack threat actors attempt to breach the grid primary control systems or supervisory control and data acquisition system (SCADA) through different attack vectors like weak security protocols, or Smart technologies directly linked to the internet allowing direct access to grid control. While older systems had "air gaps" between the public Internet and SCADA and primary control systems as a security feature. However, as Smart Grid

[11] Source: 2017 Verizon Data Breach Investigations Report (10th Edition)

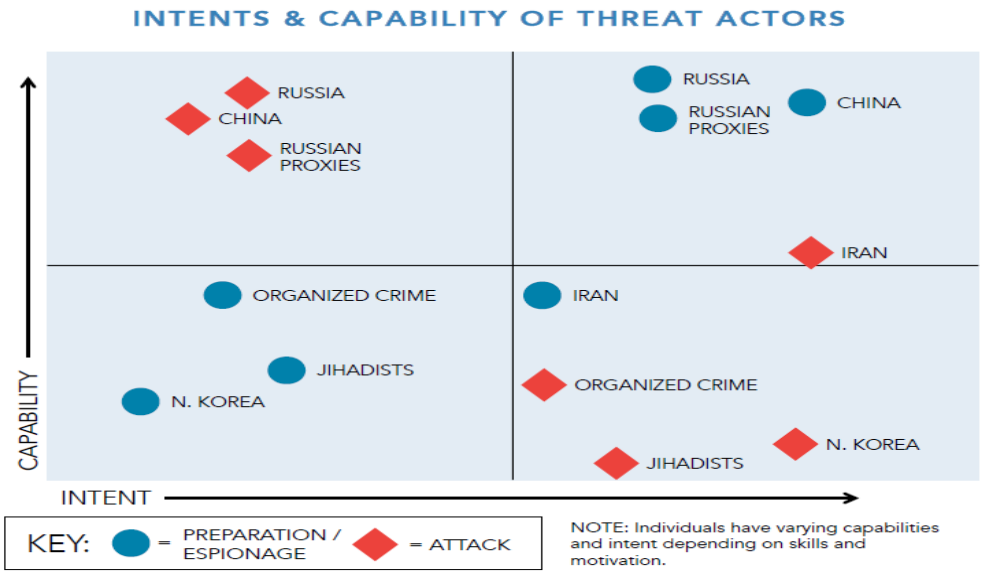
technologies are installed, there will be a greater number of access points to the critical networks.

2. Physical Attack – This includes threat actors using small arms fire, homemade improvised explosive devices, Molotov cocktail style explosives, vehicular destruction or blunt force.
3. Electromagnetic Pulse (EMP) – EMP refers to a very intense, short duration pulse of electromagnetic energy, deliberately caused by the detonation of a nuclear or other high-energy explosive device, that will cause extensive outages in the nation's electrical grids, and creates the potential for a cascading effect.
4. Directed Energy Weapons (DEWS) –DEWs may use highly focused energy to create destructive effects across the electromagnetic spectrum—radio waves, visible light, or infrared heat. DEWs that may produce effects similar to an EMP are of particular concern for electrical grid security.
5. Geomagnetically-Induced Currents (GIC) – A GIC is caused by variations in the Earth's magnetic field, producing currents in transmission lines that can damage transformers and other electrical equipment. A massive GIC emitted in a solar storm may have a severe impact on both grid security and society as a whole.
6. Severe Weather – Severe weather is one of the most common causes of damage to the electrical grid. A combination of aging infrastructure, increased population in vulnerable areas, and climate change has increased the likelihood of damaging weather events. However, the utility industry has significant experience in both preparation for, and response to, severe weather.[12]

[12] Source: The Center for the Study of the Presidency and Congress; Securing the U.S. Electrical Grid, Pg. 11

Threat Actors

Threat actors can be categorized in four major subsets, displaying varying degrees of capabilities and motivations: State Actors (Russia, North Korea, China); Non-State Actors (terrorist organizations; drug cartels and organized crime); and hacktivists, eco-terrorists, and insider threats. The intent and capabilities are shown below.[13]



Source: Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Labs Pg.21

Primary Control Centers and Industrial Control Systems

"The primary control center that operationally controls each transmission station or transmission substation, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or cascading within an Interconnection."[14] Industrial Automation Control Systems (IACSs) are a collection of personnel, hardware, and software that ensures the safe, secure, and reliable operation of an industrial process.

[13] Source: Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, Idaho National Labs, Pg. 21; https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

[14] Source: CIP-014-1 - Physical Security, Guidelines and Technical Basis, Identification of Primary Control Centers, Pg. 26

These systems include but are not limited to industrial control systems (ICSs), distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), Intelligent Electronic Device (IEDs), and supervisory control and data acquisition systems (SCADA). IACS controls the manufacturing process within a defined set of operational limits. The mission of the system that encompasses the IACS is to maintain integrity and availability of the overall IACS system. This includes security." (Weiss, 2010)

Physical Security Components

Enhanced physical security features are used to protect nuclear power plants. The physical security of the nuclear sector is held to higher standards than other generation sources. In most cases one or more of the following security measures are part of the nuclear facility security protocol:[15]

1. Physical barriers and electronic detection and assessment systems.
2. Electronic surveillance and physical patrols.
3. Bullet-resisting protected positions with robust barriers to critical areas.
4. Employee background checks, access control, trained security personnel.

With the advent of commercial drones, the risk for remote reconnaissance and attacks can be undertaken without fear of capture or early notice by local law enforcement officials or security managers.[16]

[15] Source: https://www.nei.org/Master-Document-Folder/Backgrounders/Fact-Sheets/Nuclear-Power-Plant-Security-and-Access-Control
[16] Source: YouTube: https://youtu.be/pL9q2lOZ1Fw / Watch hackers break into the US power grid

Grid Structure Components Most at Risk

These components are generally at a higher risk because of ease of access. This includes transformers, distribution lines, power generators, primary control centers and networks. Currently, within the United States, the majority of the physical attacks are perpetrated by individuals and other groups. By contrast, nation state and non-state terrorist threats largely use cyberattacks for reconnaissance and intelligence gathering efforts.

Recommendations:

EMP and Natural Disaster Type Threats

The primary threat of an EMP is damage to unshielded digital equipment, including Supervisory Control and Data Acquisition (SCADA) systems, control systems, protection relays and systems, communication systems, smart meters, and intelligent switches. An EMP can induce damaging voltages on electronics that create rapid and total failure. A solution developed by engineers at the University of Nebraska is Electromagnetic Shielding Shotcrete (EMSS), which works by both absorbing and reflecting electromagnetic waves. This material has the capability to cost-effectively protect buildings from High Altitude Electromagnetic Pulse (HEMP), Intentional Electromagnetic Interference (IEMI), Emanations Eavesdropping (TEMPEST), terrorist ballistic / blast attacks and natural disasters.[17] A possible weaknesses to this solution is the cost to retrofit all the critical structures in the US may be too high for representatives

[17] Source: Press release from American Business Continuity (ABC) group for building the first international Building Code (IBC) compliant EMP shielded Shotcrete/concrete building. http://www.omnithreatstructures.com/downloads/files/2_american-business-continuity-group-llc-successfully-completes-the-first-int_507076.pdf

to agree to pay with taxpayer dollars while leaving the vulnerabilities open for exploitation.

Cyberattacks

According to the Center for Study of the Presidency and Congress there is an opportunity to build security in to software and hardware systems currently under development.[18] The next generation of ICSs and electronics that will control the Smart Grid are still being designed and deployed, allowing for implementation of modifications to correct known deficiencies.

Physical Security

Physical Security standards set forth by the nuclear regulatory agency can be used as a starting point to establish a uniform set of criteria for maintaining secure critical infrastructure. In addition to creating a standard, delegating authority to a regulatory agency to enforce the standard and hold industries accountable of maintaining physical and cyber security compliance.

Structural Grid Components

There needs to be legislative action supporting the improvement of critical US infrastructure and the power grid through injection of capital. While the cost to secure all the critical segments of the grid would cost billions of dollars in most estimates, a failure to act by Congress and our country's leadership will cost in the hundreds of billions in the event of a major attack collapsing the grid.

END OF REPORT

[18] Source: The Center for the Study of the Presidency and Congress; Securing the U.S. Electrical Grid, Pg. 8