Grid Vulnerability Assessment

Steve Chill and Mike Swearingen

"Vulnerability Assessment — A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. Also called VA. (JP 3-07.2)"[1]

The electric grid is the most critical infrastructure for the survival of the United States. This paper assesses vulnerabilities of the grid in order to identify areas for improvement to withstand, mitigate, or deter terrorism or any other violence/attack against the grid. This effort was undertaken after a review of open-source data revealed a critical lack of understanding of a wide variety of grid vulnerabilities. This lack of understanding is reflected in grid security policy, doctrine, and procurement which has resulted in (and continues to result in) an insecure grid.

This paper covers sections of the grid (e.g., distribution or the Eastern Interconnect) as well as elements of the grid (e.g., power lines, substations). If enough elements of the grid are destroyed, then sections of the grid will be inoperable. If enough sections of the grid become inoperable, then a Black Sky Event will result. For this paper a Black Sky Event is defined as a nationwide or near-nationwide power outage lasting 30 days (or longer) without the critical infrastructures that rely on electricity. While a thirty-day Black Sky Event is sufficient to destroy U.S. critical infrastructure and kill vast swaths of the population, a lesser amount of destruction can shut down the grid for fewer days (still causing death and societal upheaval).

The vulnerabilities in this paper are described individually, however, multiple events occurring in sequence or simultaneously are possible. For example, a physical attack against transformers and high-power transmission lines can be conducted repeatedly with reasonable chances of success. If repaired, they can be attacked again. Vulnerabilities are assessed against the below threats (these threats occur in a sufficient amount to cause a Black Sky Event):

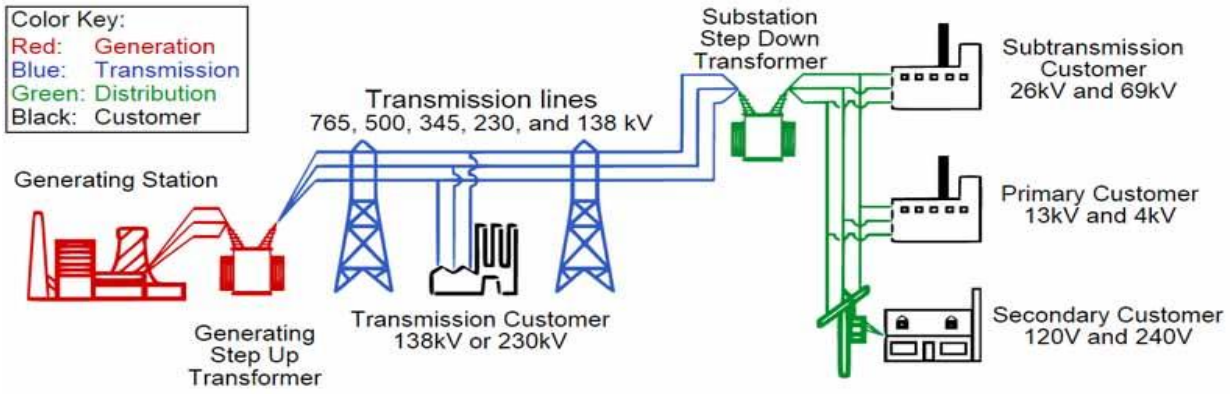
[1] JP 1-02, DOD Dictionary of Military and Associated Terms, p 577, https://dcsg9.army.mil/assets/docs/dod-terms.pdf

- Physical Attack: multiple teams using small arms, explosives, and commercial tools (physical attack may incorporate directed energy weapons/Unmanned Aerial Vehicles (UAV) and may continue for weeks)
- Cyber Attack: shut down sufficient grid-supporting Information Technology (IT) through destruction, denial, degradation, or disruption
- High-Altitude Electromagnetic Pulse (HEMP): sufficient E1 strength to damage grid electronics and sufficient E3 to couple with long line conductors to damage transformers. E1 will also remove the critical loads needed for electricity generation to operate.
- GMD: Carrington level event

It is important to remember that the grid (for the most part) is set up where generation from one station does not feed just one user (microgrids have this type of relationship but they are a small percent of the electric system). The Bulk Power System (BPS) comprises generation/transmission facilities that are interconnected to feed the entire grid, distribution facilities, and balancing areas. Distribution feeds electricity to the users. The diagram below shows the elements of the grid, but the linear nature of the diagram is slightly misleading. For example, one might think that cutting a transmission line would separate the generation from the user, but transmission would simply flow through another transmission path. Some use the analogy of getting from point A to point B on a spider web; there are many paths. Effective Black Sky attack planning (and defense) must take this into account.

The following diagram (Diagram 1) shows a typical layout of an electrical power grid with generation, transmission, and distribution.[2]

Diagram 1- The Electric Grid



[2] Daware, K., Electricaleasy.com, Electrical Power Grid- Structure and Working, https://www.electricaleasy.com/2016/01/electrical-power-grid-structure-working.html

An area of the grid may be attacked by determining the feeder systems for that particular area and destroying them. A more complex attack can create an imbalance that can start a cascade of power outages due to frequency imbalance that knocks out balancing authorities or even the interconnects.

Currently, the security of the BPS (mostly transmission) is focused on key elements (e.g., "major" substations) while ignoring other vulnerabilities that could cause a Black Sky Event (e.g., the loss of combinations of "minor" substations). Very little attention is focused on attacking multiple sections/elements simultaneously or over time.

The North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC)) regulate the security of the majority of the grid. They focus on the most critical facilities while ignoring most of the vulnerabilities addressed in this paper. [3] [4] [5]

A further weakness is that security is very subjective. For example, transmission owners are tasked to perform risk, vulnerability, and threat assessments on their own[6], then come up with mitigation strategies. This "self-evaluation" technique causes varying results depending on the evaluators and their company and often leaves transmission substations with chain link fences as the only security measure. Many of these self-designed security plans will fail against even an amateur physical attack.

It is important to consider that the electric grid does not operate independently of other critical infrastructures (e.g., communications or IT). The simultaneous loss of other critical infrastructures will only increase the severity of a Black Sky Event. Joint Base San Antionio created a matrix (based on DHS analysis) showing the interdependencies of critical infrastructures. The table (below) shows the interdependencies that can cause or contribute to a Black Sky Event. The blue boxes show critical dependencies that, if unavailable, will cause the supported infrastructure to fail (note that the top categories (supported) require the categories on the left of the table (supporting) in order to function).

---

[3] NERC, Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk-Power System , p 4, 14 Apr 2023, https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/NERC%20Report%20on%20CIP-014-3.pdf

[4] NERC, CIP-014-3, Physical Security, p 1, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf

[5] NERC, CIP-002, BES Cyber System Categorization, p1, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

[6] NERC, CIP-014-3, Physical Security, p 5, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf

SUPPORTING CRITICAL INFRASTRUCTURE SECTORS \ SUPPORTED CRITICAL INFRASTRUCTURE SECTORS	Chemical	Commercial Facilities	Comms	Critical Manufacturing	Dams	Defense Industrial Base	Emergency Services	Energy	Financial Services	Food and Agriculture	Govt Facilities	Healthcare	Information Technology	Nuclear	Transportation	Water and Wastewater
Chemical	■			■		■		■		■		■		■	■	■
Commercial Facilities									■	■	■	■			■	
Comms	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Critical Manufacturing				■		■										
Dams								■		■					■	■
Defense Industrial Base			■			■										
Emergency Services												■				
Energy	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Financial Services	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■
Food and Agriculture										■						
Govt Facilities							■		■							
Healthcare							■									
Information Technology	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Nuclear								■				■				
Transportation	■	■		■		■	■	■		■	■	■		■	■	■
Water and Wastewater	■	■		■		■	■	■		■	■	■		■	■	■

Analysis of Sector Interdependencies[7]

All elements of the grid are vulnerable to supply chain disruptions. These disruptions may be caused by deliberate attack, high demand causing time delays, implanted malware on cyber purchases, predatory market practices and other types of damage. Many elements of the supply chain are overseas raising the potential for disruption. The most critical supply chain is for transformers (both transmission and distribution). While supply chain attack will not cause a BSE, it has the potential to enhance the effect of all forms of attack.

[7] Domestic Electromagnetic Spectrum Operations (DEMSO), Joint Base San Antonio, p 19, https://www.jbsa.mil/Portals/102/Documents/DEMSO%20Resiliency%20Guide%20(CAO%208%20June%202022).pdf?ver=XFSaIcKg27Y8nJkm8-iFtQ%3D%3D

The following sections/elements of the grid are assessed against the threats of physical attack (adequate numbers of attackers, minimal competence), cyber-attack, HEMP (sufficient strength which may require multiple warheads), and GMD (sufficient strength):

Sections

- Grid Balance
- Interconnects
- Microgrids
- Economics/markets
- Generation
- Transmission
- Distribution

Elements

- Control Centers/Balancing Authorities
- Power lines (conductors)
- Towers
- SCADA/Control Systems
- Transformers
- Transmission Breaker Stations
- Grid Workers
- Electricity Customers

(Note: The term “substation” is used to denote a location with transformers, breakers or both transformers and breakers. The above sections include substations. Substations will also contain some of the above elements.)

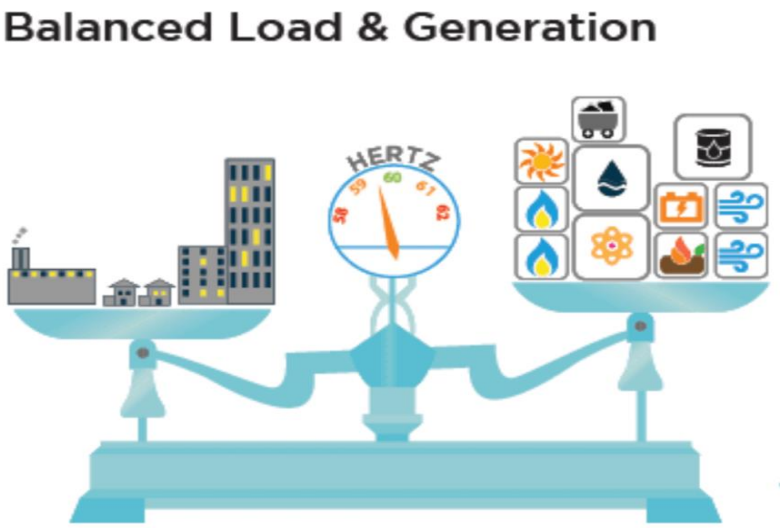
The following table summarizes vulnerabilities of different entities of the grid. Red means high chance of creating a BSE, yellow means a potential chance of creating a BSE, green means little chance of creating a BSE.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Balance				
Threat ability to create a Black Sky Event by attacking Interconnects				
Threat ability to create a Black Sky Event by attacking Microgrids				
Threat ability to create a Black Sky Event by attacking Energy Economics/Markets				
Threat ability to create a Black Sky Event by attacking Generation				
Threat ability to create a Black Sky Event by attacking Transmission				
Threat ability to create a Black Sky Event by attacking Distribution				
Threat ability to create a Black Sky Event by attacking Control Centers/Balancing Authorities				
Threat ability to create a Black Sky Event by attacking Power Lines (conductors)				
Threat ability to create a Black Sky Event by attacking Towers				
Threat ability to create a Black Sky Event by attacking SCADA				
Threat ability to create a Black Sky Event by attacking Transformers				
Threat ability to create a Black Sky Event by attacking Transmission Breaker Stations				
Threat ability to create a Black Sky Event by attacking Grid Workers				
Threat ability to create a Black Sky Event by attacking Electricity Customers				

Grid Balance

"The grid, and everything connected to it – power plants, power lines, even your home appliances – are designed to work at a specific frequency: 60 Hz. As the electric grid constantly adapts to changes in how much energy consumers are using and how much energy is being generated, frequency fluctuates."[8] If there is an uncorrected mismatch between the amount of electricity being generated and the amount being used (balance), then system frequency is disrupted. The U.S. grid runs at 60hz and can generally tolerate a plus or minus one hertz deviation. Once the deviance exceeds plus or minus one, blackouts (load shed) occur, or generation is shut down. Diagram 2 (below) represents balancing load and generation with the impact on frequency.[9]

Diagram 2



Attacking Grid Balance

Attacking the balance of the grid creates blackouts beyond the physical location of an attack (cascade). Almost any form of grid attack will impact grid balance. The ability of balancing authorities to continue to respond to imbalances is what prevents cascades.

Cyber and physical attacks can create imbalance, but they must be orchestrated in time and space. Cyber and physical attacks can be more effective if there is an understanding of key nodes and where/when to strike for maximum effect on the balance. Insider threat (e.g., at a

[8] Wirfs-Brock, J. and Paterson, L. IE Questions: What Keeps Our Electric Grid Humming?, https://insideenergy.org/2015/07/10/ie-questions-what-keeps-our-electric-grid-humming/#:~:text=The%20grid%2C%20and%20everything%20connected,is%20being%20generated%2C%20frequency%20fluctuates.

[9] Multin, M., What Are Vehicle-to-Grid Services?, https://www.switch-ev.com/blog/vehicle-to-grid#brwhat-are-ancillary-servicesbr

balancing authority (BA)) can also impact balance. Once a cascade is started, selective targeting can increase cascade scope.

HEMP will impact large areas causing direct damage, but HEMP also causes imbalance. HEMP (in addition to its direct effect) can, in of itself, cause enough imbalance to start a cascade. HEMP attacks many sections/elements of the grid so there are many types of HEMP-caused failures that can impact balance.

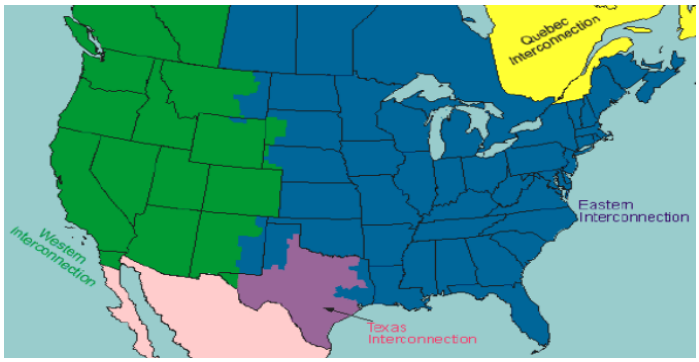
GMD is like HEMP E3 and can attack balance through long-line conductors.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Balance				

Interconnects

The U.S. grid is made up of interconnects (Eastern Interconnect, Western Interconnect, Texas Interconnect). Interconnects provide a means to group geographical elements of the grid. The interconnects have a limited number of unsynchronized "links" using High Voltage DC Back-to-Back Ties (HVDC B2B) that connect interconnects having different frequencies and phases. Within the Interconnects are balancing authorities that monitor/control the grid. A generation/use mismatch causing a blackout will have a cascading effect on other portions of an interconnect. Simultaneous attacks on many sections of an interconnect optimize the chances for interconnect destruction. Repeated attacks amplify the potential for mass blackouts. Once an interconnect is down, attacks may continue to inhibit restart (called black start…a difficult evolution in of itself). The diagram below shows the three U.S. Interconnections (with Quebec added)[10].

Diagram 3- North American Interconnections



[10] NERC, Balancing and Frequency Control, p 5, https://www.nerc.com/comm/OC/BAL0031_Supporting_Documents_2017_DL/NERC%20Balancing%20and%20Frequency%20Control%20040520111.pdf

Attacking the Interconnects

While Interconnects have some exchange (which can be exploited by attacks on three or more of the tie stations causing disruption of interstate transmission of power), they are largely independent of each other. If the goal of an attack is a country-wide blackout, then all three interconnects must be attacked separately, or at one-time using well-positioned HEMP.

Interconnects have large footprints and are unable to be secured physically. This lack of security makes physical attack easy. Physical attack therefore does not require high-end forces. It requires a very simple level of competence. While elements of the interconnects are easy to attack, the "easy to attack" targets are numerous, and many will need to be attacked to create a Black Sky Event. This will require a larger number of attackers.

Cyber-attack can also be tailored to many targets in an interconnect (starting a cascade). Cyber-attacks can also be engineered to persist and to create and spread outages.

HEMP and GMD can impact all the geography of an interconnect simultaneously. Damage will be sufficient to destroy/disable an interconnect.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Interconnects				

Microgrids

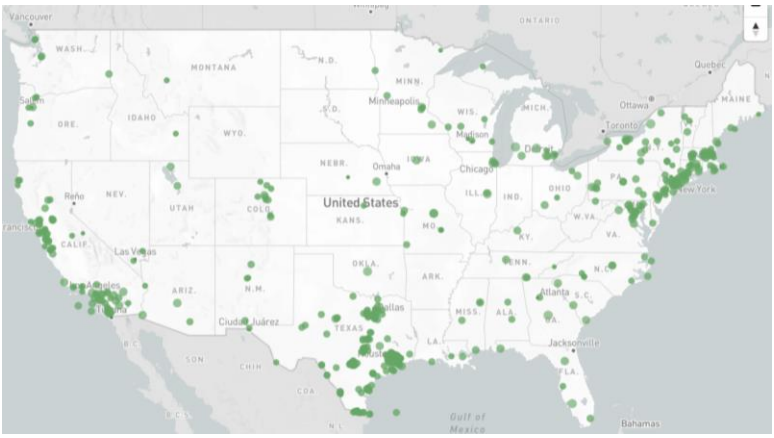
Microgrids are separate from the Interconnects. "A microgrid is a local grid with an independent source of energy capable of disconnecting or "islanding" from the utility grid. Microgrids improve resilience by allowing critical facilities to continue operating in the event of a utility-grid outage."[11] Microgrids have their own power source. There are approximately 461 independent microgrids[12] of varying sizes identified by the U.S. Department of Energy. However, many other uncounted microgrids are emerging as alternative power generation occurs "behind the meter", mitigating electricity price spikes for more and more residential and non-residential power consumers. The separation of microgrids from the rest of the grid allows for a degree of resilience (albeit microgrids currently make up a very small fraction of power usage in the US). However, as microgrids become more prevalent certain microgrids in cities and industrial areas can present convenient localized targets whose loss may not affect large areas of the grid but

[11] US Dept of Energy, U.S. Department of Energy Combined Heat and Power and Microgrid Installation Databases, https://doe.icfwebservices.com/microgrid

[12] Dept of Energy, Office of Energy Efficiency and Renewable Energy, Department of Energy Releases New Tool Tracking Microgrid Installations in the United States, 26 May 2021, https://www.energy.gov/eere/amo/articles/department-energy-releases-new-tool-tracking-microgrid-installations-united

can cripple vital infrastructure. Major microgrids in Continental U.S. are depicted in Diagram 4 (below).[13]

Diagram 4- Major US Microgrids



While microgrids may be self-sufficient, they are rarely considered in concert with other microgrids in an area or region, whether as elements of a grid or as separate, interconnected groups (a potential way to increase resilience).

Attacking Microgrids

Microgrids use a generation, transmission, distribution construct but the transmission requirements are often lessened due to the proximity of distribution. They may be similarly attacked directly, but as microgrids they do not have the same threat of a cascade causing a Black Sky Event.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Microgrids				

Energy Economics/Markets

Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) are the main functionaries in the U.S. energy market. "RTOs [and ISOs] typically run two energy markets: the day-ahead and real-time markets. The day-ahead market, which represents about 95 percent of energy transactions, is based on forecasted load for the next day and typically occurs the prior morning to allow generators time to prepare for operation. The remaining energy market transactions take place in the real-time market, which typically run once every

[13] US Dept of Energy, U.S. Department of Energy Combined Heat and Power and Microgrid Installation Databases, https://doe.icfwebservices.com/microgrid

hour and once every five minutes to account for real-time load changes that must be always balanced with supply.

RTOs use energy markets to decide which units to dispatch, or run, and in what order. In the day-ahead market, RTOs compile the list of generators available for next-day dispatch and order them from least expensive to most expensive to operate."[14] (known as Reliability Unit Commitments (RUC)).

Generation depends on the market for their guidance on when to function. Not only does the market determine when generation functions, but it also determines if generation functions. Balancing Authorities, RTOs, and Companies are designed to fix problems even if the markets are temporarily shut down, but the incentive for generation to function is financial. Absent compensation, generation plants will function for a period of time without coordination, then will eventually shut down. It is unclear how long this charitable generation capability will last.

Attacking the Energy Economics/Market

Electricity markets will not function in a Black Sky scenario. Physical attack may take out some of the market nodes but physically creating a Black Sky Event would require large, professional, and dispersed forces. A more realistic attack would be a cyber-attack causing havoc in the market, crippling its function, distorting information, or shutting it down. A HEMP would also be able to shut down the market as all aspects of the market require IT, communications, and electricity. The grid will continue to function for a period as grid workers and generation may continue to work without finance (therefore yellow for first order cyber and HEMP impact). The grid will eventually shut down without a functioning market.

GMD can disrupt the power supply to markets (causing market shutdown) but will not have a sizable impact directly on market equipment (allowing for quick recovery).

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Energy Economics/Markets				

Generation

"As of December 31, 2021, there were 24,645 electric generators at about 11,925 utility-scale electric power plants in the United States. Utility-scale power plants have a total nameplate electricity generation capacity of at least 1 megawatt (MW). A power plant may have one or

[14] Cleary, K. and Palmer, K., US Electricity Markets101, https://www.rff.org/publications/explainers/us-electricity-markets-101/#:~:text=In%20an%20energy%20market%2C%20electric,ascending%20order%20of%20offer%20price.

more generators, and some generators may use more than one type of fuel."[15] They feed the transmission system (except for microgrid generators which generally feed the distribution system or behind-the-meter operations).

> One megawatt equals one million watts or 1,000 kilowatts, roughly enough electricity for the instantaneous demand of 750 homes at once.- California ISO

Generation (the amount of electric power created) requirements start by using historic analysis and seasonal norms. The base load (minimum amount of electric power delivered or required over a given period of time at a steady rate[16]) is determined. A number of generators are identified to provide base load. Peak load (maximum load during a specified period of time[17]) is estimated, and those generators are identified. For example, early morning hours (sleeping hours) use less electric power (base load) while later afternoon hours (daytime when people return home) often use the most electric power (peak load). The load between base load and peak load is referred to as intermediate load.

Start-up time for generation plants to come online varies from minutes to days. The spinning reserve (That reserve generating capacity running at a zero load and synchronized to the electric system.[18]) provides flexibility to generation capability. Spinning reserve therefore cuts down on start-up time delays.

Generation normally is flexible (can source many plants) and has a reserve (plants that are standing by in some state of readiness), so attacking during hours where there is little/no reserve (peak hours) may cause the largest grid problems.

Coal and nuclear generation take longer to spin up while natural gas and hydroelectric generation spin up more rapidly. A coordinated attack will require analysis on a plant-by-plant basis (increased difficulty for the attacker).

Nuclear generation plants pose their own type of risk. Attacking nuclear generation can have the further effect of creating meltdowns and scattering radioactive material. Most generation, to include nuclear generation, uses external power from the grid. A Black Sky event, therefore, can cause nuclear generation to become a problem in of itself. Nuclear plants are required to have backup fuel on site, but when the onsite backup fuel is depleted, there is no guarantee that more fuel will be available. Not only will nuclear plants cease functioning, but they will present a significant hazard.

---

[15] U.S. Energy Information Association, How many power plants are there in the U.S.?, https://www.eia.gov/tools/faqs/faq.php?id=65&t=2

[16] U.S. Energy Information Association, Base Load definition, https://www.eia.gov/tools/glossary/?id=B#:~:text=Base%20load%3A%20The%20minimum%20amount,around%2Dthe%2Dclock%20basis.

[17] Ibid, Peak Load

[18] Ibid, Spinning reserve

"Without a steady coolant supply, a hot reactor core will continuously boil off the water surrounding it until the fuel is no longer immersed. If fuel rods remain uncovered, they may begin to melt, and hot, radioactive fuel can pool at the bottom of the vessel containing the reactor. In a worst-case meltdown scenario, the puddle of hot fuel could melt through the steel containment vessel and through subsequent barriers meant to contain the nuclear material, exposing massive quantities of radioactivity to the outside world."[19]

Generation plants include SCADA, transformers, power lines, protection equipment, engineers, workers, and other IT (addressed in subsequent sections).

Attacking Generation

Physically attacking generation offers little probability of creating a Black Sky Event. There are too many generation plants, and grid localities normally have spinning reserves. In addition, generation plants have security. Physical attack against generation, however, can assist in destabilizing grid balance. The northeastern power plant below has manned towers with firing ports, sensors, and concertina/concrete obstacles.[20] Of note, this kind of robust security occurs infrequently in the transmission portion of the grid.

Diagram 5- Generation Plant Security

[19] Matson, J. Scientific American. https://www.scientificamerican.com/article/nuclear-energy-primer/
[20] Funk, J. Cleveland.com, Federal security concerns since 9/11 have turned U.S. nuclear power plants into armed fortresses, https://www.cleveland.com/business/2011/08/nuclear_security_911_firstener.html

There is a phenomenon known as AURORA which affects equipment by “closing in” (electrifying) grid equipment out of phase with the electric grid causing heat which would impact the life of equipment in various ways. The equipment that AURORA has the greatest effect on is rotating equipment (generators and motors). The heat and torque impacting the rotating equipment will damage the equipment quickly resulting in the loss of generators or motors used by large industrial facilities and server farms (chilling equipment). Other equipment that can be affected by AURORA is large power transformers in electric stations. The heat of the out of phase close will cause damage to the transformer core and its insulation (reducing the operating life of the power transformer).

Generation plants are often “air gapped” for cyber so cyber-attack will be more difficult (hence yellow). As renewable energy is becoming more prevalent their interconnection to the grid poses a problem to the grid due to these facilities having limited to no cyber security (Cyber security is supervised by NERC. Many renewable assets are independent and not subject to NERC CIP.).

HEMP attack on generation will be effective because plants are mostly unhardened. Both HEMP and GMD can attack and destroy step up transformers (an element of generation) causing a Black Sky Event.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Generation				

Transmission

The transmission grid provides bulk electric power from generation to the distribution grid and large-scale manufacturing and industrial facilities.

Attacking Transmission

Physically attacking transmission is likely the most straightforward means for creating a Black Sky Event.

A physical attack would benefit from open information on location and exterior layout of major transformers and transmission lines. A combination of Google Earth, Google Street View, DOE information (i.e., OE-417), NERC (NERC SOR Report), EIA information, RTO and ISO reports and publicly available utility data would provide this information. Many transmission facilities reside in rural areas making access and reconnaissance easier. Ground reconnaissance would be simple and draw little suspicion. Weapons do not have to include explosives as grounding, rifle fire and the use of brute force (e.g., pulley system used on a transmission line) allows almost anyone to destroy transmission elements.

An understanding of load patterns would allow an attacker to better use his attack options. Select nodes can be attacked by attacking their transmission lines, others can be attacked directly (direct physical attack at remote sites can be repeated over and over again). Multiple attacks simultaneously can be employed. Attackers can bounce back and forth against lines and transformers.

Even if the load pattern is not understood, a mediocre team with mediocre equipment has the capability to keep bringing down lines and transformers. For example, if a team brings down one line or transformer per hour, they could bring down eight during the hours of darkness in one night. Multiply by the number of teams available and the numbers can add up quickly. It is not a stretch to think that a hundred teams could take down one thousand transmission targets in one day…just with physical attack and sabotage.

Cyber or an insider threat could increase loads making transmission nodes more vulnerable. Cyber-attack can target individual transformers or many transformers at once. Transformer SCADA systems are often air-gapped potentially limiting the cyber threat.

HEMP can attack the entire transmission system simultaneously causing direct effects and imbalance. GMD can also attack the transmission system as long power lines would overload transmission transformers.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Transmission				

Distribution

The distribution portion of the grid, which makes up 89.5% of the national electric grid, provides electric power from transmission to the end users.[21] The ubiquity of distribution makes it an easy target while also making it a less attractive target for a Black Sky Event (too big for several types of attack). Distribution assets are widespread. Power lines, transformers, and SCADA are similar to the transmission portion of the grid, except smaller and more widespread.

Power line protection devices exist throughout the distribution grid. These devices exist to both protect and control distribution. Currently the majority of control systems are digital devices but there remains a significant amount that are electromechanical devices.

Attacking Distribution

Physical attack on distribution elements is almost unstoppable. Local blackouts can easily be created, but a full Black Sky Event would require too much effort if only attacking distribution.

[21] American Public Power Association (APPA), 2024 Supplemental Report *Number of Providers by Utility Type EIA 861 EIA 861s, 2022* Page 17, https://www.eia.gov/electricity/data/eia861/

However, there are some distribution substations that are electrically interconnected that could cause large scale outages. A selective distribution attack could be orchestrated to help attack grid balance.

Cyber-attack is also possible, but it would have to be widespread to create a Black Sky Event.

HEMP can attack a large portion of the distribution grid simultaneously. The impact of a massive HEMP attack against distribution has been largely ignored. The ability of the grid to maintain balance in this scenario is doubtful. GMD can use long line distribution conductors (e.g., power lines) to overload distribution transformers.

HEMP/GMD attack against protection devices will vary in effectiveness. In cases where control system devices are digital, impact will be immediate. In the case of electromechanical control system devices, the impact may not be as immediate or as vast.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Distribution				

Control Centers/Balancing Authorities (CC/BA)

A Balancing Authority (BA) is "The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time."[22] Each BA is responsible for a Balancing Authority Area: "The collection of generation, transmission, and loads within the metered boundaries of the Balancing Authority. The Balancing Authority maintains load resource balance within this area."[23] The lack of balance causes shutdowns or blackouts.

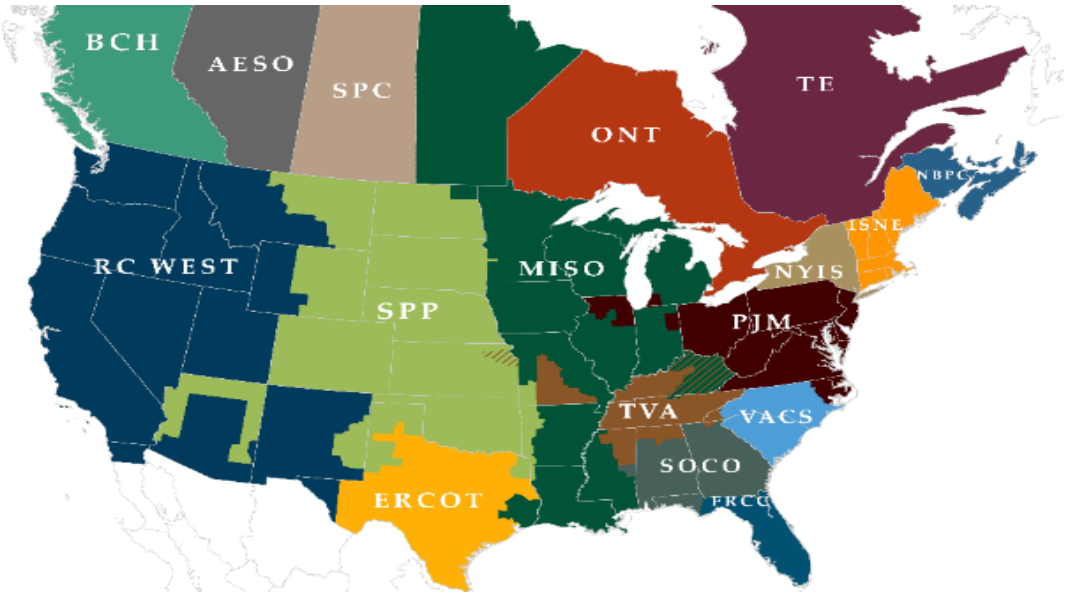
A balancing authority is responsible for a geographic area in which electric power balance must be maintained (supply vs demand for a particular area)(areas may overlap). This balance involves management of the internal supply/demand as well as the BA interaction with external supply/demand. The BAs act as "brains" of the grid.

"Customer demand and generation are constantly changing within all Balancing Authorities."[24] This constant change, if exacerbated, presents a vulnerability.

[22] NERC, Glossary of Terms Used in Reliability Standards, p 2, https://www.nerc.com/pa/Stand/MOD%20V0%20Revision%20RF%20DL/Glossary.pdf
[23] IBID, p 2
[24] NERC, Balancing and Frequency Control, p 10, https://www.nerc.com/comm/OC/BAL0031_Supporting_Documents_2017_DL/NERC%20Balancing%20and%20Frequency%20Control%20040520111.pdf

"There are over 100 Balancing Authorities of varying size in North America. Each Balancing Authority in an Interconnection is connected via high voltage transmission lines (called tie-lines and flow gates) to neighboring Balancing Authorities. Overseeing the Balancing Authorities are wide-area operators called Reliability Coordinators. The relationship between Reliability Coordinators and Balancing Authorities is similar to that between air traffic controllers and pilots."[25] "Reliability Coordinators (RC) monitor the grid in real-time and interact with individual operators and other RCs to maintain reliable operations."[26] Diagram 6 (below) depicts the US/Canada Reliability Coordinators[27]

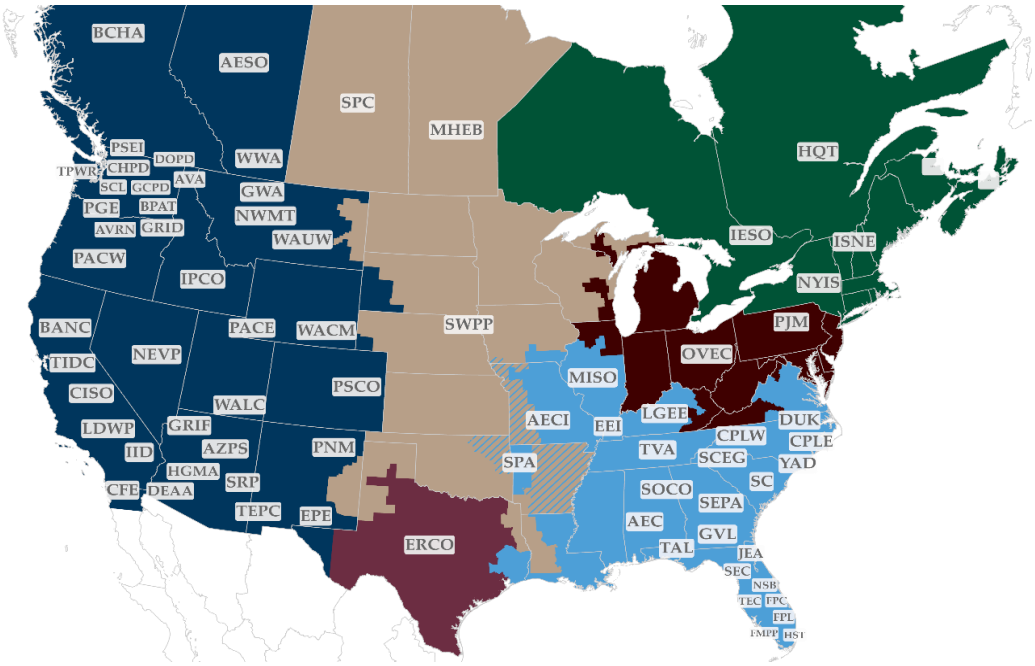
Diagram 6- US/Canada Reliability Coordinators



The Eastern and Western Interconnects have many balancing authorities (The Texas Interconnect has one). Diagram 7(below) shows regions and balancing authorities.[28]

[25] NERC, Balancing and Frequency Control, p 6, https://www.nerc.com/comm/OC/BAL0031_Supporting_Documents_2017_DL/NERC%20Balancing%20and%20Frequency%20Control%20040520111.pdf
[26] WECC, The Bulk Power System, https://www.wecc.org/epubs/StateOfTheInterconnection/Pages/The-Bulk-Power-System.aspx
[27] WECC, The Bulk Power System, https://www.wecc.org/epubs/StateOfTheInterconnection/Pages/The-Bulk-Power-System.aspx
[28] WECC, The Bulk Power System, https://www.wecc.org/epubs/StateOfTheInterconnection/Pages/The-Bulk-Power-System.aspx

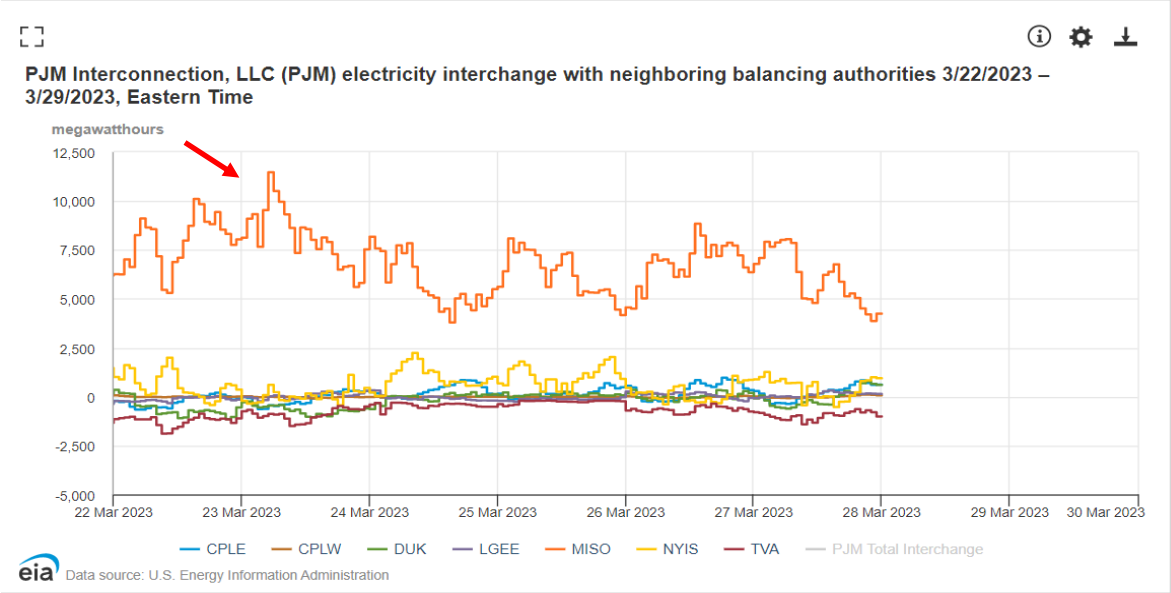
Diagram 7- Regions and Balancing Authorities



Not only must balancing authorities maintain balance on their portion of the grid, but they must maintain their balance with other balancing authorities in the interconnect. Diagram 8 (below) is an electricity interchange graph depicting PJM's (North Carolina through Pennsylvania and west through Ohio) electricity exchange with its neighboring balancing authorities. If the neighboring MISO (located in the Midwest) went offline when the exchange was over 10,000 megawatt hours[29] (see red arrow on diagram) then PJM would be challenged to maintain their own grid balance. If PJM then failed, the other balancing authorities connected to PJM would be challenged (the other lines on the graph). This is the type of problem that causes a "cascade". A cascade occurs because the balance is sufficiently upset to mandate blackout, which causes a neighbor to blackout and so on. A cascade can be "helped along" by simultaneously damaging neighboring BAs.

[29] US EIA, Hourly Electric Grid Monitor, PJM Interconnect, https://www.eia.gov/electricity/gridmonitor/dashboard/electric_overview/balancing_authority/PJM

Diagram 8- Example of BA Electricity Exchange



All balancing authorities are control centers; however, all control centers are not balancing authorities. Control centers are used by multiple entities and "control" many aspects of the electric grid that are not specifically focused on maintaining balance.

Attacking Control Centers/Balancing Authorities (CC/BA)

CC/BAs may be attacked physically as they are housed in buildings. CC/BAs have some degree of security. Orchestrating physical attack on occupied buildings would certainly draw a quick response (unlike remote powerlines or transformers) so physically attacking CC/BAs requires more finesse/expertise. An insider threat can target a control center/balancing authority from the inside. Attacking sister control centers is also an option for an insider threat as they are mutually supporting.

Communications are essential to the functioning of a CC/BA so communications for the site may also be physically attacked. NERC addresses the compromise of communications (CIP-012 Communications) between Control Centers which addresses Control Centers having mitigation plans on hand. It is unclear if all control centers review and modify these plans on an established recurring time frame or if the alternate communication plan is unaffected by HEMP/GMD/cyber-attack.

CC/BAs are also vulnerable to cyber-attack through their SCADA systems or through other transmission/distribution control/monitoring systems. BA coordination with generation and the financial system is also required and cyber vulnerable. Given enough engineers, balance may be restored and maintained without BAs (making the threat red with the potential for yellow).

HEMP presents a direct threat to unhardened BA facilities, but also to the information that BAs require to maintain the grid. A massive loss of SCADA/control systems or market information could make BAs inoperable even if the facility was EMP hardened.

GMD will have minimal direct impact on control centers/balancing authorities. NERC established a GMD reporting requirement and the procedure to submit reports for CC/BA.[30] This reporting requirement does not define a standard for recovery of equipment or communication. The reporting of GMD is based on a NERC Taskforce for GMD.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Control Centers/Balancing Authorities				

Power Lines (Conductors)

Transmission and most distribution lines are made of exposed uninsulated metal. They extend through varying geographies, such as cities, suburbs, farmland, woodland, wetlands, and deserts. They extend across rivers, roads, mountains, and other terrain features. There are approximately 160,000 miles of high-powered transmission lines in the United States.[31] Millions of miles of distribution lines are also not insulated by coating. The exposed lines are "insulated" by the air that is surrounding them. This "air insulation" obviously fails if something that causes grounding comes into contact with the line (e.g., trees) causing the protection systems (breakers, reclosers, and fuses) on the line to operate.

Power lines that are in use have some degree of designed sag to limit contact between phases due to weather and aeolian vibration (vibration caused by wind effects on lines). Large line transmission can cause sag in excess of 10 feet. As lines sag, they become more vulnerable to contact or grounding.

Attacking Conductors/Power Lines

Physical attack cutting through thick metal distribution/transmission lines is difficult, but they may be grounded with relative ease. A physical attack on the line could cause grounding by shooting (e.g., crossbow with grounding line), drone (e.g., dropping grounding line) or throwing a conductor creating a ground. Another alternative is dropping trees onto the lines. Regulations (such as NERC FAC-003 Transmission Vegetation Management) cause transmission lines to be well apart from potential treefall so grounding using trees is not a good attack method against most transmission. Some utilities have vegetation management for their distribution lines, but

[30] NERC, Geomagnetic Disturbance Data, https://www.nerc.com/pa/RAPA/GMD/Pages/GMDHome.aspx
[31] US Environmental Protection Agency, U.S. Electricity Grid & Markets ,https://www.epa.gov/green-power-markets/us-electricity-grid-markets

such measures are often not required. Many distribution lines are not protected from treefall, and in times of drought, have been the cause of wildfires.

Conductive wire can also be used to link the transmission lines. Linking transmission lines with different voltages causes voltage differences leading to the flow of current. If there is enough difference in the magnitude of the voltage and resulting current, then the fault current will cause the protection devices on the lines to trip open (shutting down the line) due to phase imbalance.

There are too many lines to physically protect from this type of attack. While this type of attack will not physically damage power lines, it will ground them disrupting electric flow and balance for any given line. It is also very simple and may be repeated with relative impunity for both transmission and distribution lines. Larger numbers of power lines must be destroyed/grounded to create a Black Sky Event. Power line attacks will yield more disruption if done repeatedly and coordinated with other types of attack.

Cyber will not impact power lines. HEMP/GMD will use power lines to impact other elements of the grid, but HEMP/GMD will not destroy power lines.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Power Lines (conductors)				

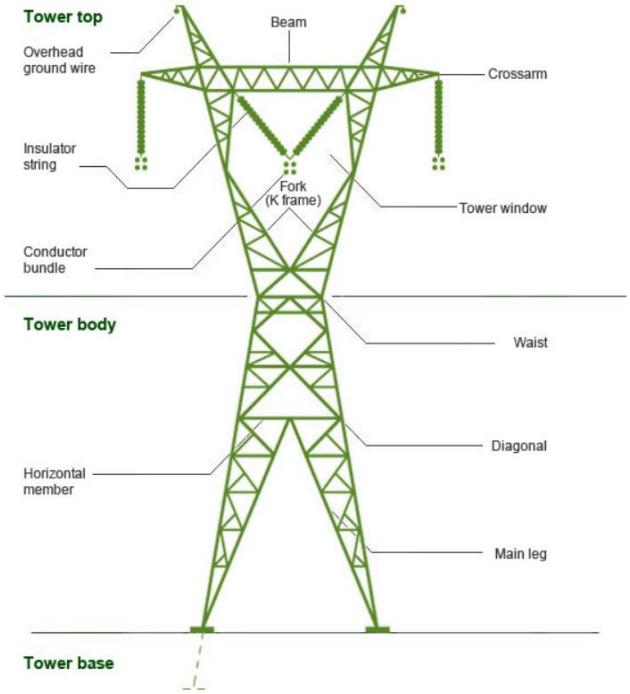
Towers

Electric towers are used to raise power lines off the ground (preventing grounding and allowing for “air insulation”). Towers also provide a path for grounding lightning strikes. Towers are placed where they can best support the weight of powerlines based on the terrain. Towers come in many configurations, but they have similarities. The transmission tower body (and some larger distribution towers) is most often a lattice construction although tubular construction is becoming more popular. Many other transmission lines use wood poles in a H structure or tall (often 65 feet or taller) single pole structures. Additionally, single pole and H structures of steel and concrete are used in transmission lines.

Towers have grounding paths and an overhead ground wire for lightning. Insulators are designed to separate powerlines from the tower, so powerline grounding does not occur. Insulators are primarily made of porcelain, glass, or some other nonconductive composite. Towers usually have three lines or three sets of lines that are easily distinguished as the three phases of electric power. Towers also have static wires at the top of the structures that function

as lightning protection and may contain fiber optics within the static wire for communications. Diagram 9 (below) depicts a waist-type tower[32].

Diagram 9- Waist Type Tower



Attacking Towers

Towers are required for holding up power lines (approximately 160,000 miles of transmission line and millions of miles of distribution line) and exist almost everywhere, therefore physically attacking towers offers many options. Towers are not secured so attackers can take more time. Towers that support powerlines across water, over steep terrain or other physical obstacles are the most difficult to repair or replace. An attack on the static wires would influence the communication of control centers' SCADA systems as many transmission line static wires contain fiber optics.

The structure of the tower may be attacked several ways. For example, the above tower may be crippled at the crossarm or the waist causing powerline grounding through the tower. The legs of the tower offer the easiest access for felling a tower. Explosives, welding tools and brute force (dependent on tower size) are all options to fell a tower. An easier attack venue is to shoot/destroy fragile insulators that are made of porcelain, glass, or composites. Insulators,

[32] Hydro Quebec, Power Transmission Towers, http://www.hydroquebec.com/learning/transport/types-pylones.html

however, are easier to replace than towers. A downed tower requires a major effort to replace. Detailed descriptions on how to take down a tower are available online.

Larger numbers of towers must be destroyed to create a Black Sky Event. Tower attacks will yield more disruption if done repeatedly and coordinated with other types of attack.

Towers are immune to cyber or HEMP/GMD attack.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Towers				

Supervisory Control and Data Acquisition (SCADA) and Control Systems

Many of the functions of the grid are automated. That automation requires data. That data is often provided automatically through SCADA systems. SCADA also controls physical system functions. For example, if a situation arises where a generator is required to provide unplanned power (reactive power) due to an unforeseen event, the situational awareness is often beyond the capability of generator operators. As a result, reactive power is often provided automatically using SCADA systems. SCADA systems interact with the rest of the grid's control systems. "A control system is a set of mechanical or electronic devices that regulates other devices or systems by way of control loops. Typically, control systems are computerized."[33] SCADA/Control systems are required for generation, transmission, and distribution elements of the grid. SCADA/Control systems are also used for other critical infrastructure. Sensors and their proper functioning are vital to all SCADA systems; however, they are generally not considered when conducting vulnerability and risk assessments.

Attacking SCADA/Control Systems

SCADA/Control systems, like power lines, towers and transformers are located throughout the electric system. SCADA equipment may be attacked physically as there are often SCADA equipment sheds and control houses at substations and on select equipment. Physically destroying SCADA equipment, or SCADA systems will not create a Black Sky Event. Most utilities are capable of operating without SCADA. As long as the control systems still work, then they (control systems) will continue to coordinate with each other.

SCADA/Control systems can be attacked through cyber-attack although many SCADA/Control systems are air-gapped (not touching outside networks). SCADA/Control system communications present vulnerabilities whether or not they are air gapped. Mass

[33] Kirvan, P. Definition Control System. TechTarget. https://www.techtarget.com/whatis/definition/control-system

SCADA/Control system attack will directly affect systems, but it will also impact grid balance resulting in a potential cascade of blackouts.

Without SCADA the grid does have some resilience. Engineers coordinate control systems and facilities amongst each other without any SCADA. The electric grid worked before SCADA and the practice of control system coordination will allow the grid to continue to operate in the absence of SCADA. A danger lies in seizing effective control of the control systems through malware that allows the threat to use SCADA as a conduit to the relays. For example, the threat could reset the relay logic settings thus changing the coordination of relays and devices and lock out the system operators from SCADA (allowing the attackers to have effective control over the system).

Other Critical Infrastructures use SCADA/Control systems and are also vulnerable. A large disruption in Critical Infrastructure SCADA/Control Systems will adversely affect grid balance.

Unless hardened, SCADA/Control Systems can be disrupted/destroyed by HEMP on a broad scale. GMD may be effective against SCADA equipment and control systems if they are attached to long line conductors.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking SCADA/Control Systems				

Transformers/Transformer Substations

The grid relies on transformers. "A transformer is a static device which transfers electrical energy from one circuit to another through the process of electromagnetic induction. It is most used to increase ('step up') or decrease ("step down') voltage levels between circuits."[34] This allows the power from, say a nuclear reactor, to be distributed to thousands of households. When a transformer is disabled, power is provided through alternate routes. If the alternate routes are not functioning, there is a power outage. Transformers are ubiquitous throughout the electric system. One can see them on power poles or at major substations, albeit much larger. The larger transformers, or High Voltage (HV) transformers take over three years[35] for delivery and often come from foreign countries. They are not easy to replace.

Distribution substations are substations that step down the voltage of the transmission system to a lower voltage to deliver to residential consumers, businesses, and other loads. The location

[34] Electrical4U, What is a Transformer?, https://www.electrical4u.com/what-is-transformer-definition-working-principle-of-transformer/

[35] Jao, N, U.S. Renewable, Grid Battery Projects Battle Transformer Shortage, https://www.reuters.com/business/energy/us-renewable-grid-battery-projects-battle-transformer-shortage-2023-11-15/

of distribution substations is determined by engineering analysis of loads to be served and other factors such as maintaining voltage levels and distribution system capacities.

The Congressional Research Service has stated, "According to power industry experts, certain parts of the U.S. transmission network are particularly vulnerable to HV (High Voltage) substation disruption. These areas may have severely constrained transmission paths relying on a small number of HV transformers in extremely critical network locations. According to press accounts, a FERC power flow analysis in 2013 identified 30 such critical HV transformer substations across the continental United States; disabling as few as nine of these substations during a time of peak electricity demand reportedly could cause a "coast-to-coast blackout." Not all industry experts agree on the potential severity and duration of a blackout from a multi-transformer attack, though it is generally accepted that severe outages may be technically possible."[36] While the number may be debatable, a finite number of transformers destroyed will cause a Black Sky Event.

Substation transformers are harder to replace because they are engineered to specific requirements due to available fault currents, capacity based on current load to be served, and space requirements for future load as well as other factors engineering may require. Because of global concentration of production, many are produced in non-friendly countries and lead times for the larger units extend into years. This factor, coupled with the cost of high voltage power transformers and the number of substations, limits investment in back up transformers for substations.

As a result, utilities evaluate and prioritize the purchase of back up transformers. A limited number of 5 MVA to 100 MVA transformers are often available through power transformer brokers. These transformer brokers purchase old, retired transformers or transformers in need of repair and will remanufacture them to the specification of utility engineers. The purchasing of these power transformers helps reduce the time in receiving a transformer when the lead time of a new transformer is too long. In some cases, utilities will purchase a power transformer and store it as an emergency backup. Some utilities develop specifications for multiple voltage portable transformers on trailers that can be used at multiple substations as a backup. Engineers may also develop complete mobile substations with a multiple voltage transformer that can be used at substations or interconnected to transmission lines for temporary operation until the system is restored.

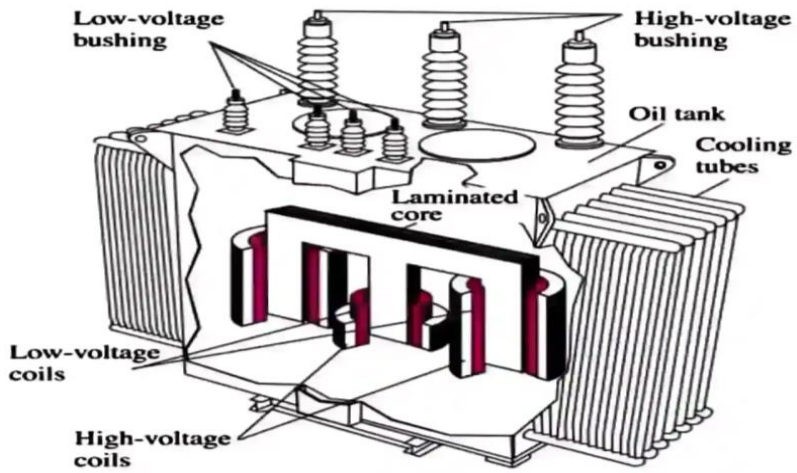
Diagram 10 (below) shows the major parts of a transformer.[37]

---

[36] Congressional Research Service, Physical Security of the US Power Grid: High-Voltage Transformer Substations, 2014, p6, https://fas.org/sgp/crs/homesec/R43604.pdf

[37] Electrical Technology, 12 Different Parts of a Transformer, https://www.electrical-technology.com/2021/09/parts-of-transformer.html

Diagram 10- Major Parts of a Transformer



Attacking Transformers/Transformer Substations

Transformers may be attacked in several ways. Transformers have many physical attack vulnerabilities. Good marksmanship is not required to attack a transformer as they are on the ground and easily approached. Different transformers have different tank thickness with higher capacity transformers having thicker tanks. Some companies place fencing around transformers but without prompt reaction forces, fencing is merely a delay/nuisance obstacle. Rifles/shotguns can destroy bushings/insulators as they are made of fragile materials. Penetrating oil tanks and cooling tubes will require weapons with additional power (commercial small arms have proven effective in penetrating transformer oil tanks). The coils and core are the parts of the transformer that, if physically damaged, will often require a full transformer replacement. The core/coils housing is usually better protected and may require higher capability rifles/shotguns for penetration. These weapons are available for commercial purchase. In sum, physical attack/destruction of transformers can easily be accomplished using commercial rifles/shotguns. Explosives are equally as effective.

Orchestrating cyber-attacks through their SCADA/control systems can be effective but these types of attacks would have to be done on many transformers to achieve a Black Sky Event.

Transformers are vulnerable to both the E1 and E3 portions of HEMP. Both could cause transformer destruction/failure.[38] HEMP occurs over a wide area so many transformers could be attacked simultaneously. The strength of the E1 and E3 induced current will vary at each transformer. Field strength and other field factors (e.g. under load or not under load) will

[38] Sandia National Laboratories, Modeling Failure of Electrical Transformers due to Effects of a HEMP Event, P 8, https://www.osti.gov/servlets/purl/1644736

determine whether a transformer survives any given HEMP attack. It is safe to assume that many will be affected during a HEMP attack causing both direct grid damage and widespread balance issues.

The most vulnerable target to GMD is transformers by way of power lines.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Transformers				

Transmission Breaker Stations

A transmission breaker station is a station within the transmission grid that isolates sections of transmission lines that branch off the main transmission line. Their purpose is to reduce the overall impact of a fault on the transmission grid.

Diagram 11-Transmission Breaker[39]

Transmission Breaker Stations consist of breakers and the relays to control them. Planning engineers determine the location of the transmission breaker stations and the equipment to be used based on engineering analysis of the transmission grid. They are usually placed where the transmission lines tap off in several directions from the mainline. They are also placed to sectionalize a mainline.

A transmission line may be thought of as a leaf in the sense that a leaf has a main spine and several veins that branch off from the leaf's spine. The main transmission line originating in the transmission substation is the spine and transmission lines that branch off from the main

[39] Csanyi, E., Six System Requirements of HV and EHV Circuit Breakers, https://electrical-engineering-portal.com/hv-ehv-circuit-breakers

transmission line are like leaf veins. Breakers stationed along the transmission mainline (spine) are placed to reduce the effect of downline (vein) transmission breakers failing and taking out large areas of the main transmission line by isolating segments of the main transmission line.

To ensure that any faults that originate on a transmission branch do not affect the main transmission line (in effect isolating the transmission branch) a breaker is installed on the transmission line branch where it connects to the main transmission line.

If the main transmission line is a long line, then engineers may place breakers further down the main transmission line in order to isolate parts of the main transmission line from the rest of the upline main transmission line (should a fault occur further down the main transmission line). These breakers are large enough, due to the high voltages involved in the transmission system, that they are set on foundations in a transmission breaker station.

If line/branch breakers are physically destroyed, then the "downstream lines/branches" will be de-energized. Should the relay systems be compromised, the operation of the transmission line branch would depend on how the relay systems are compromised. There are several scenarios where compromise of the relay systems would de-energize the transmission line branch.

Attacking Transmission Breaker Stations

Transmission Breaker Stations are vulnerable to physical attack as they are unprotected or lightly protected and unmanned. Direct fire can disable most components located within these stations. Explosives would be easy to emplace.

Cyber-attacks on the relay systems of the breakers on the transmission line could cause outages to the transmission lines controlled by the relay systems. Another scenario would be that an attack on the relay systems of a transmission line breaker would allow the attackers to seize control of the relay systems further allowing the attackers to have effective control of the breaker and the transmission line it protects. In the case of electro-mechanical relay systems, a physical attack would be necessary to cause compromise of the breaker they control. Electro-mechanical relays are not vulnerable to cyber-attack (digital relays are vulnerable causing a partial vulnerability to cyber-attack (yellow)).

HEMP could cause the disabling of the relay systems and de-energize the breakers they control if the relay systems are digital relays. If the relay systems controlling the breaker are electro-mechanical relays, then the breaker and the line it protects may be unaffected. If the relay systems upline of the breakers with the electro-mechanical relays are digital, then all systems downline of the digital relay systems will be affected and de-energized. In the case of GMD, the scenario would be similar.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Transmission Breaker Stations				

Grid Workers

The grid relies on qualified and experienced workers in control centers (which includes balancing authority nodes). The grid also relies on workers for repair of generation, transmission, and distribution.

Attacking Grid Workers

Grid workers are not combatants or warriors. Physical attack on control center personnel may be used to sow fear into other control centers. Insider threats can cause significant damage. Given the finite number of control centers, physical attack against the personnel of several will have outsized impact to balancing efforts. Building security efforts are effective enough to mandate that attackers will require some professional skills (explosive demolition, marksmanship, etc.) to impact control personnel. Control personnel may also be turned or intimidated into providing attack information (insider threat).

Linesmen and other repair personnel are especially vulnerable to physical attack. The linesman working in an elevated bucket truck in a remote area is an easy target. Securing a perimeter that allows for repair is almost impossible in this scenario. Snipers in this situation will have little fear of discovery while creating fear amongst civilian repairmen. Ground targets are only slightly less vulnerable.

Cyber and HEMP will not directly affect workers, but the systems that workers use can be degraded by both.

Historically, blackouts have prompted riots and disorder. Personnel from the electric industry will have family/home concerns that will impact their ability to repair the grid. If the grid workers are not available, the grid will neither function for long nor be repaired. Some companies have contingency plans to address this issue.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Grid Workers				

Electricity Customers

Electricity Customers and electronic equipment are generally not hardened. This presents several major problems for the grid.

As with grid workers, the grid's supporting infrastructures require electricity to function (e.g., grid workers require communications personnel to go to work). If these infrastructures aren't prepared for a Black Sky Event, then grid functionality degrades, and repair will not happen.

Customers also make up the load. “Residential, commercial, and industrial customers each account for roughly one-third of the nation’s electricity use.”[40] The loss of this load ends grid balance.

Attacking Electricity Customers

Physical attack on customers is not a viable course of action to create a Black Sky Event. Cyber may contribute to load loss at the customer level, however, this level of cyber-attack would be extremely difficult as it would have to be widespread. The most viable attack against the customers is via HEMP. Widescale and permanent loss of household, commercial and industrial electric computers/appliances/machines (to include the Internet of Things (IOT)) will create an imbalance even if the rest of the grid is completely hardened. This imbalance will create a Black Sky Event.

GMD will have a much smaller impact on customer load.

Threat type	Physical	Cyber	HEMP	GMD
Threat ability to create a Black Sky Event by attacking Electricity Customers				

Conclusions

This paper summarizes grid vulnerabilities. Grid vulnerability assessments not only point out the grid areas in need of improved security, but they also are used to evaluate the thoroughness of grid security solutions. For example, security measures that focus only on transformer substations do not secure the grid as other elements of the grid (e.g., towers) remain vulnerable. This vulnerability assessment may be used to understand, shape, and evaluate grid security solutions.

[40] EPA, Electricity Customers, https://www.epa.gov/energy/electricity-customers

Authors

Steve Chill is a retired Marine with decades of security experience in domestic and overseas environments. He has executed or created DOD/Service policy for the security of special weapons, ships and bases of all types and units ranging in size from Combatant Commands down to the individual Marine. He was recently an author/editor of both Joint Base San Antonio's guide titled "Domestic Electromagnetic Spectrum Operations" and Infragard's "Powering Through; Building Critical Infrastructure Resilience".

Mike Swearingen is a retired electric cooperative power systems engineer with 20+ years of experience. He has worked in every aspect of power systems operation including control systems, protection systems, transmission design, substation design, distribution design and NERC compliance as well as regulatory matters. He represented his cooperative as member of the Transmission Working Group (TWG), Market Operations and Policy Committee (MOPC) and Market Working Group (MWG) at the Southwest Power Pool (SPP). He served as an analyst and independent merit reviewer on several projects at the Department of Energy (DOE), was a technical advisor for the National Electric Energy Testing Research and Applications Center (NEETRAC), is an IEEE Senior Member and was named Smart Grid Pioneer by Smart Grid Today.

The Secure the Grid Coalition is a group of policy, energy, and national security experts, legislators, and industry insiders who are dedicated to strengthening the resilience of America's electrical grid. Learn more at: www.SecureTheGrid.com