Electric Power Grid Disruptions: A Time Series Examination

Brian K. Harte[1,2] and Umesh Kumar[3]

[1] Professor, St. John's University, [2] Corresponding Author, harteb@stjohns.edu

[2] Associate Professor, State University of New York, Canton

Abstract

It is important to empirically assess both the viability and defensibility of the national electric grid, which is becoming more complex with increasingly interdependent components. Moreover, the nation's critical infrastructure would quickly become degraded with prolonged grid outages that impact electrical power production and distribution.

This study examines time series data for 2,825 cases involving power outages in the U.S. over a 20-year (246-month) period, from January 2000 through June 2020. Data was acquired from the U.S. Department of Energy. Severe weather caused the majority of power outages recorded, but human factors accounted for a significant number of incidents. We found that 46% of electrical power outage causes relate to natural or weather-related events, 28% to grid system operations or failures, and 25% to human interactions. Further, we found that cyber-attack data was less forthcoming than other types of grid outage reporting. Based on these data, the number of power outages and energy loss attributable to outages continues to rise, while the duration of electric outages and the number of customers affected are declining.

Keywords: Critical Infrastructure, Electric Power Outages, DOE Data Form OE-417

Introduction

One cannot overstate the importance of maintaining reliable functioning of the Nation's electric power systems. Among the sixteen critical infrastructure sectors, energy is considered one of four life-line sectors during a disaster (water, communication, and transportation complete the list). Minor and small area electric

 doi: 10.18278/jcip.1.2.11

power outages occur on a daily basis across the country, but unless these events cascade further, it is the larger scale electric outages that have significant impact.

Power failures can have both financial and economic impacts on electricity providers, government, organizations, businesses, and community operations. The ability to maintain an efficient and protected electrical power grid is essential to support critical infrastructure and key resources. A national electric grid with many aging, legacy components has raised questions regarding whether or not substantial improvement investments are necessary and, if so, what the priorities should be. Unless properly configured, growing demand on electricity supplies from renewable, intermittent energy sources like wind and solar power can increase grid instability. It is widely anticipated that extreme weather events driven by climate change will heighten the risk of future grid impairment.

Significant electrical power outages, both long- and short-term, are an area of concern for not only energy producers and operators, but also consumers, other critical infrastructure systems, legislators, policy analysts, and researchers. Overall, the U.S. grid has been stable, and Americans are used to the provision of electricity without extended blackouts. The World Bank has reported that the U.S. has ranked well in electric system quality compared to other countries (World Bank 2019).

In the aftermath of the widespread 2003 electricity blackout that cascaded across the northeast and Midwest U.S. and parts of Canada, market forces and government entities increased the impetus for electric power reform. This included calls for enhanced, mandatory electricity reliability standards. In an attempt to reduce the likelihood of future large-scale disruptions, U.S. and Canadian government energy authorities issued recommendations to help prevent further incidents of this type.

The geographic scale of large-scale power outages can transcend county, city, region, state, and/or national boundaries (U.S. Department of Homeland Security 2017). Based on the interdependence of critical infrastructure sectors and their need for electricity, a sustained grid failure would significantly weaken the nation's homeland security posture. When they do occur, power outages can have considerable economic impact. Costs attributable to outages fluctuate significantly, but are highest when major storms hit.

Our paper makes two significant contributions. First, we use a publicly available U.S. Department of Energy (DOE) dataset to present a 20-year time series of reported power outages (January 2000 through June 2020). These data are collected and organized by the DOE Office of Electricity (OE) using its "Electric Emergency Incident and Disturbance Report." The data include the type of event, geographical location, average annual and monthly frequency of events, characteristics of power loss, average number of customers affected, and duration of outages.

Second, we hope to expand awareness of these data for various types of analyses and use by others concerned about electric power reliability. In particular, there is a need for multi-disciplinary study of the electric grid, including risk analyses, potential financing options for grid improvement, and the evaluation of alternative policy options. These data have limitations which are important to consider in time series analyses. We describe several of the limitations, expecting that others in the field can advocate for improved data quality and utility over time. The ability to conduct meaningful policy analysis in this arena requires reliable baseline data.

Background

Research to quantify and describe electric power system outages covers a wide range of issues and uses a variety of data sources and analytic methods. In a brief report, Wirks-Brock used the DOE dataset (Form OE-417) and described compiling the information through yearly summaries of major power outage reports (Wirfs-Brock 2014). Limited information was included such as outage causes, findings by day, time, and region for each reported case.

A data report by Mukherjee and colleagues described their use of publicly available data sources from several federal agencies such as the Department of Energy (DOE), National Oceanic and Atmospheric Administration (NOAA), and the National Climate Data Center (NCDC), among other sources (Mukherjee, Nateghi, & Hastak 2018a). In a recent study, Mukherjee et al. analyzed electrical outage failures for the period 2000 to 2016 and found that severe weather events accounted for 53% of outages (Mukherjee, Nateghi, & Hastak 2018b). An earlier study proposed a model for risk-based decision-making to assess the impacts of weather induced power outages (Mukeherjee 2017).

Another study examined major electrical distribution disturbances and unusual occurrences for the period 2002 through 2013 (Nateghi, Guikema, Wu, & Bruss 2016). The authors concluded that extreme event repercussions are important, and that the risks associated with high impact low-frequency events may not be fully acknowledged and understood.

Adderly et al. (2019) used the DOE database to project the potential impacts of smart grid financing to reduce the economic impacts of U.S. large outage events. Applying residential and small, medium, and large business customer data as well as outage duration, a metric was developed to gauge the economic impact of outages on electricity customers. They found that the infusion of $4.5 billion by the Department of Energy in smart grid technologies in 2010 led to billions of dollars of financial benefits between 2011-2016 compared to 2003-2010 (Adderly et al. 2019).

Three studies noted the importance and challenges of consequential low frequency power failures. One study examined the repercussions of high impact, low probability (HILP) power failure inducing events, known as "black swans," and the

complexities they present for power grid and infrastructure resiliency (Mukhopadhyay & Hastak 2016). They postulated that the following energy sector factors hindered adequate infrastructure investments: 1) a lack of knowledge regarding HILP events and their impact on power system infrastructure; 2) strict regulatory requirements; 3) a lack of a strong value proposition for business resilience cases; and 4) a lack of strong incentives for infrastructure investment (Mukhopadhyay & Hastak 2016).

Other research has examined major electrical distribution disturbances and unusual occurrences for the periods 2002 through 2013 (Nateghi, Guikema, Wu, & Bruss 2016). The authors concluded that extreme event repercussions are most important, and, consistent with other research, that risks associated with high impact low-frequency events do not appear to be fully acknowledged or understood.

A study by the RAND Corporation used a combination of new and existing data to examine the risk assessment process that could be employed to prepare for high impact-high probability as well as high impact-low probability events (Willis, Tighe, Lauland, et al. 2018).

The relationship between severe weather events and power outages has been well documented. During and in the aftermath of natural disaster incidents, including, but not limited to, severe weather producing storms, high winds, flooding, and winter weather conditions, power grid failures are not only probable, but should be expected. Probabilistic models can assist in preparing for the most likely threats, based on historical analysis of past conditions contributing to grid failure. The objective is to reduce economic impacts and loss of life.

Since a variety of events can lead to large scale outages, this paper explores both weather and non-weather-related causes of known power failures. A variety of human threats, including system and operational issues are reported. Human causes may be the result of miscalculations, poor judgement, or failure(s) to act. They may also be categorized as intentional actions to harm, impede, disrupt, dismantle or destroy components of the power grid itself. Component and/or equipment failures refer to parts, or components of parts, with material defects, or damaged or unserviceable parts that cause component and/or equipment failure. These defects or damages result in the inability of the component(s) to operate properly or at all. Systems must have the capability to flexibly respond to critical requests from other systems. For example, electric utilities frequently import electricity from surrounding states while experiencing peak load conditions.

Methods

Department of Energy Form OE-417 Reporting Requirements

This study uses a DOE dataset reported through Form OE-417, the *Electric Emergency Incident and Disturbance Report,* that has been in place across the U.S. since

2000. Since Form OE-417 is our principle source of data, we describe relevant reporting requirements (DOE 2020). A sample page of OE-417 reporting in January 2020 is shown in Table 1.

Table 1. OE-417 Electric Emergency and Disturbance Report Format

OE-417 Electric Emergency and Disturbance Report - Calendar Year 2020										
Month	Date Event Began	Time Event Began	Date of Restoration	Time of Restoration	Area Affected	NERC Region	Alert Criteria	Event Type	Demand Loss (MW)	Number of Customers Affected
January	01/09/2020	11:07 PM	01/09/2020	11:19 PM	Arkansas: Yell County;	SPP RE	Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing).	Severe Weather/Transmission Interruption	0	0
January	01/09/2020	8:45 PM	01/10/2020	9:23 PM	Washington: King County;	WECC	Cyber event that could potentially impact electric power system adequacy or reliability.	Suspicious Activity	0	0
January	01/09/2020	7:40 AM	01/09/2020	8:48 AM	Minnesota: North Dakota: Wisconsin:	MRO	Complete loss of monitoring or control capability at its staffed Bulk Electric System control center for 30 continuous minutes or more.	System Operations	0	0
January	01/09/2020	11:07 PM	01/09/2020	11:18 PM	Arkansas:	SPP RE	Electrical System Separation (Islanding) where part or parts of power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system.	System Operations	Unknown	Unknown
January	01/10/2020	2:53 PM	Unknown	Unknown	Tennessee: Hamilton County;	SERC	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Or suspicious device or activity at its Facility.	Suspicious Activity	Unknown	Unknown
January	01/11/2020	2:25 AM	01/11/2020	7:56 AM	Arkansas: Cross County;	SPP RE	Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing).	Severe Weather/Transmission Interruption	22	7541
January	01/11/2020	11:02 PM	01/12/2020	2:01 AM	North Carolina: South Carolina:	SERC	Loss of electric service to more than 50,000 customers for 1 hour or more.	Severe Weather	Unknown	66475
January	01/11/2020	3:30 AM	01/11/2020	5:30 PM	Arkansas: Texas:	SPP RE	Loss of electric service to more than 50,000 customers for 1 hour or more.	Severe Weather	Unknown	68138

There are three main reporting criteria for electrical outages and incidents for Form OE-417: 1) reporting under normal circumstances; 2) reporting emergency incidents; and 3) system operations. In normal reporting, all routine incidents must be submitted within six hours of the incident's occurrence (DOE 2020). In emergency situations, electrical incidents, or those incidents with the potential of causing major electrical disruptions or damage, incidents must be reported within one hour of the occurrence. System operation incidents resulting in damage or failure, not categorized as emergency situations, are required to be reported within 24 hours of the event, but no later than the next business day.

The following occurrences constitute an emergency as defined by DOE:

- Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations
- Cyber event that causes interruptions of electrical system operations
- Complete operational failure or shut down of the transmission and/or distribution electrical system
- Electrical System Separation (Islanding) where part or parts of a power grid

remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system

- Uncontrolled loss of 300 Megawatts or more of firm system loads for more than 15 minutes or more from a single incident
- Firm load shedding of 100 Megawatts or more implemented under emergency operational policy
- System-wide voltage reductions of 3 percent or more
- Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System

OE-417 instructions describe the voluntary and mandatory requirements for incident reporting, including identifying the entities that must submit information.

- The Balancing Authorities (BA), Reliability Coordinators (RC), some Generating Entities, and Electric Utilities, including those located in Puerto Rico, the Virgin Islands, Guam, and other U.S. possessions are responsible for completing all relevant portions of the form when any of the criteria are met requiring the filing of Form OE-417
- All electric utilities must provide information to a Balancing Authority (BA) when necessary for their reporting obligations, and file Form OE-417 in cases where a BA will not be involved
- Foreign utilities handling U.S. balancing authority responsibilities may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation must inform DOE that these filings will come from a foreign-based electric system (DOE 2020, 1).

Data Analysis

Our research presents data for 2,825 reported power outage cases over a 246-month period from January 2000 through June 2020. We used a consistent methodology to both standardize and normalize common terms reported, and the types of outages by classification: year, month, date, geographic region, outage duration, customers affected, and electricity demand loss.

Geographic electric council regions are categorized by the North American Electric Reliability Corporation (NERC) and its divisions as recorded by the U.S. Census Bureau. The territorial oversight of NERC regions and councils were adjusted in 2000 and 2005. The new NERC reliability assessment areas are a mixture of NERC reliability entities, entity sub-regions, regional transmission organizations and system operators. Figure 1 shows regions for NERC long-term reliability assessment areas since 2010. Figure 2 illustrates the NERC regions from 2005-2010 (Map 2).

Figure 1. Regional Entities and Regional Councils since 2010
Source: North American Reliability Corporation
https://www.eia.gov/electricity/data/eia411/#tabs_NERC-1

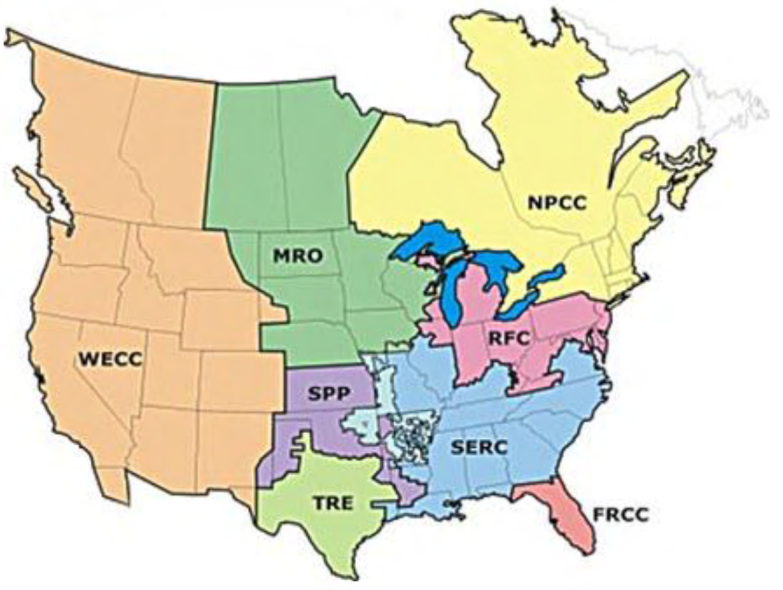

Figure 2. NERC Regions 2005–2010
Source: North American Reliability Corporation
https://www.eia.gov/electricity/data/eia411/#tabs_NERC-2

Results

Reported Events

Twenty categories of outage-related events are reported in Table 2. When organized by three broad topics, the counts include: nature/weather events (1,311 events, 46%), human events (714, 25%), and system operations or failure events (800, 28%). The most prevalent nature/weather events were severe weather and various types of storms (winter, wind, and thunderstorm). Few events were reported for wildfires and lightening during the study period. Among human events, vandalism represented the most common type of occurrence, and suspected cyberattack was the least reported event. This paper treats cyber event as a suspected cyberattack.

Table 2. Reported Events Connected to Power Outages

Reason	Outages	Percentage
Severe Weather	581	20.6
Vandalism	573	20.3
Wind Storm	297	10.5
Thunderstorms	226	8.0
System Operations	180	6.4
Winter Storm	171	6.1
Transmission Interruption	145	5.1
Public Appeal	99	3.5
Generation Inadequacy	92	3.3
Shed Firm Load	90	3.2
Units Tripped	59	2.1
Physical Attack	58	2.1
Suspicious Activity	50	1.8
Islanding	49	1.7
Voltage Reduction	45	1.6
Others	41	1.5
Suspected Cyber Attack	33	1.2
Natural Disaster	15	0.5
Lightening	13	0.5
Wildfire	8	0.3
Total	2,825	

Sabotage events or deliberate harm to the electrical grid are rarely reported as such. The data suggests that most of these events are reported as vandalism (20.3%) instead of physical attack (2.1%). An event is treated as vandalism when it does not constitute a physical attack or theft.

Outages due to cyberattack on critical infrastructure is an area of concern. As seen in Table 3, only 33 suspected cyberattacks were reported from 2003 through 2019, and these were distributed across several years. No clear time trend across years was apparent. Thus far, respondents from no region have reported demand loss or the number of customers affected by such outages. Outages exceeding a day were reported in 21 of 33 suspected attacks. The NERC data indicated that eight regions had between one and five suspected cyberattacks. The ninth region, Western Electricity Coordinating Council (WECC) was an outlier with 11 events. A possible explanation is that WECC oversees the largest and most geographically diverse region, known as the Western Interconnection. Its footprint includes all or portions of the 14 Western states between. This large concentration of connected grids could be targeted for cyberattack.

Arguably, the most well-known successful grid cyberattack occurred in 2015 in the Ukraine. It is believed that hackers, allegedly linked to the Russian government, targeted portions of Ukraine's energy grid with a denial of service attack and cut off electricity for several hours to tens of thousands of people (University of Washington 2017). Were this type of outage to occur in the U.S., it could potentially cause hundreds of millions of dollars in damage and could result in loss of life.

Table 3. Power Outages—Suspected Cyber Attack

Year	Number of Events	NERC Region	Number of Events
2003	1	ECAR	1
2011	6	FRCC	2
2012	4	MRO	3
2013	2	NPCC	4
2014	3	RFC	5
2016	5	SERC	3
2017	3	SPP	1
2018	4	TRE	3
2019	2	WECC	11
2020 (June)	3		
	N = 33		

Outages and Consequences Across Years, Months, and Geographic/FERC Regions

Over the study's 20-year period, a notable increase in outage events occurred during 2011, and this upturn has continued into mid-2020 (Table 4). Between 2000 and 2010, there were 845 events, with an average of 77 per year; between 2011 and mid-2020 there were 1,980 events with an average of 208 per year. This shift has been noted by others, but not fully explained.

A different timespan pattern emerged for energy demand loss, which had an average of 908 MW per year (Table 4). Individual years (2003, 2018, 2019) experienced high average demand losses. This may be due to one or more high impact events during these years. For example, the massive 2003 power outage and blackout was triggered locally and rapidly cascaded across a large swath of the Northeast and Midwest regions. Similarly, severe weather resulting in high demand loss occurred in 2018 and 2019. There was an increase in annual energy demand loss from an average of 612 MW losses (2000-2010) to an average of 1,248 MW losses (2011- mid-2020). These findings likely reflect the increase in the number of outage events in these years.

Table 4. Power Outages by Year

Year	Electric Outages	Average Demand Loss in MW	Average No. Customers Affected	Duration > One Day
2000	30	330	190,233	47%
2001	15	391	178,926	27%
2002	23	223	295,568	62%
2003	61	2,243	312,116	67%
2004	93	820	227,823	68%
2005	85	662	278,938	59%
2006	91	340	195,900	56%
2007	78	648	137,281	43%
2008	149	431	212,049	55%
2009	97	287	127,648	63%
2010	123	363	129,901	63%
2011	307	688	168,986	51%
2012	196	872	252,005	47%
2013	174	575	113,184	39%
2014	214	1,215	210,637	41%
2015	143	1,362	97,012	38%
2016	141	688	143,362	45%
2017	150	402	195,329	40%
2018	220	1,903	168,105	41%
2019	278	2,745	101,978	31%
2020 (June)	157	1,403	96,619	29%
Average		908	176,342	46%

Among the average number of customers affected per year (176,342), there were no clear patterns, with the exception that the 2003 blackout had the largest number of affected customers (312,116). The length of time needed to restore electrical power supply is an important indicator of both the reliability and dependability of the electrical power grid. Electric disruption for more than one day also showed a reduction beginning in 2011.

Reporting events and consequences by month may shed light on seasonal climate impacts. The highest number of electric outages were reported in the summer months of June, July and August at about 300 per month. The remaining months averaged about 215 events per month. It is possible that seasonal outages, floods, and other natural events may explain the uptic in power outages during the aforementioned months.

Table 5. Power Outages by Month

Month	Number of Electric Outages	Average Demand Loss in MW	Average No. of Customers Affected	Duration > One Day
January	239	2,726	187,971	50%
February	242	780	140,163	47%
March	195	391	130,236	43%
April	238	507	145,991	38%
May	218	385	139,022	45%
June	312	874	180,608	46%
July	300	550	125,555	48%
August	289	1,386	230,329	44%
September	202	1,130	340,574	49%
October	240	1,234	209,521	48%
November	145	255	122,502	46%
December	205	274	149,571	51%
Average		874.2	175,170	46%

Average demand loss was highest in January (2,726 MW loss), with a cluster of high months in August, September and October (average of 1,250 MW loss). The average across other months was 502 MW loss. These data suggest that severe weather and voltage reduction caused above average demand loss in megawatts. The highest number of customers affected were reported in August, September, and October. There was no observable pattern or outliers for interruptions lasting more than a day across the months covered.

Information reported across the 13 NERC regions is the most varied among Tables. (Table 6). In part, this reflects the changing alignment of NERC organizations over time. For example, three reliability organizations (ECAR, MAAC, and MAIN) became part of RFC after January 2006. These organizations would no longer carry out independent reporting and shifted to RFC reporting. A similar situation occurred with ERCOT joining TRE in 2010.

Among the nine Regions that did not experience re-designation, the largest number of outages were reported by the Western Electricity Coordinating Council (WECC) 782 outages, Reliability First Corporation (RFC) 598 outages, and

Southeastern Reliability Council (SERC) 479 outages. Only one of these regions was among the three highest reporting demand loss in MW: with East Central Area Reliability Coordination (ECAR) 1,873 MW, SERC 1,543 MW, and Northeast Power Coordinating Council (NPCC) 1,308 MW. Among those regions with the highest number of customers affected were the Florida Reliability Coordinating Council (FRCC) 403,302, ECAR 257,383, and Texas Regional Entity TRE with 248,877.

Table 6. Power Outages by NERC Region

NERC Region	Number of Electric Outages	Average Demand Loss in MW	Customers Affected	Duration > One Day	Suspected Cyber Attack
ECAR	35	1,873	257,383	97%	1
ERCOT	27	479	182,329	36%	
FRCC	73	1,045	403,302	57%	2
MACC	24	995	175,982	96%	
MAIN	15	294	73,589	47%	
MRO	111	598	165,459	42%	3
NPPC	273	1,308	149,837	50%	4
Other	118	397	222,607	27%	
RFC	598	495	167,189	63%	5
SERC	479	1,543	132,539	50%	3
SPP	123	186	139,227	47%	1
TRE	167	719	248,877	53%	3
WECC	782	771	183,637	26%	11
Average		823	192,458	53%	

Discussion

A goal of this study was to answer the questions, "What are common threats and events associated with large-scale power outages? How has time changed the outage threats and the effects on communities (duration of outage, consumers without electricity, and demand electricity loss in MW)?" This study offers preliminary answers to these questions, with recommendations provided for future research.

We report on 2,825 large electric grid outages or threats that have been identified across 20 categories of events or threats. In broad terms, we found that 46 % relate to natural or weather-related events, 28% to grid system operations or failures, and 25% to human interactions.

Over the 2011 through mid-2020 timeframe, the number of power outages increased compared to earlier years, and this trajectory could continue. Energy demand loss follows a generally similar trajectory of increasing losses in recent years. The number of customers affected varied but evidenced no clear trend, nor

connection to changes in demand loss by year. Notably, the number of outages lasting more than one day has decreased.

Physical threats to the power grid are a concern. While reports of vandalism against the power grid are high, reported suspected cyber-attack activity was relatively low, as compared with other causes of power outages. Cyber-attacks could result in widespread loss of electrical services including long-duration, and large-scale blackouts. It is important to note that the relatively small numbers of reported cyberattacks do not necessarily correlate with the overall level of cyber-attacks upon systems; rather, they represent those cyber-attacks resulting in significant threat or power outage.

A greater reliance on digital computing and connectivity increases the visibility of today's electric grid system (National Conference on State Legislatures 2020). This new visibility increases the prospect of targeting from malign actors both inside and outside the country. Overall system reliability can be impaired by cyber-attacks on both the information and operational technology components supporting grid operations.

Utilities are routinely faced with new cyber-attack challenges and consequently maintain a set of best practices to keep systems secure and up to date. The increasing risk of cyber-attacks to the grid is related to several factors. Increasingly, systems may be controlled from remote locations and existing control systems may contain internet vulnerabilities. Potential risk also exists in the form of compromised supply chains. In June 2018, the North American Transmission Forum (NATF) issued guidelines for member entities when contracting for vendor equipment and services. Selecting vendors and equipment that meets industry best practices can reduce vulnerabilities to cyberattack. However, due to interconnections among adjacent utilities and dependencies on vendor services, prudent procurement is beneficial but not a guarantor of adequate cyber protection.

Concern about electric utility underreporting of cyber incidents may have prompted FERC to issue an order in mid-year 2018 to strengthen the reporting of such incidents under the Critical Infrastructure Protection Act (CIP) reliability standards (Cyber Security Incident Reporting Standards, July 19, 2018). New standards requiring minimum information standards, deadlines and a requirement that reports be sent to the Department of Homeland Security will become effective on January 1, 2121 (Eke 2019).

Other information sources suggest that cyber-attack data is less forthcoming than one would expect. S & P Global (2020) in its report dated September 25, 2020, suggests that due to security risks, the FERC and NERC may prefer to keep cyber violation details concealed from a security risk perspective. Obviously, without adequate transparency in reporting cyber-related incidents, it will not be possible to ascertain the full scope of cyber-attack activity. This would compromise the safety and security of the grid, and would continue to impact grid safety metrics.

Apart from cyber-attack, the U.S. Department of Homeland Security considers space weather and power grid failure as "significant risk events." Today's complex, integrated, and inter-connected power grid system can be severely affected and damaged from severe solar storms (NASA 2020) or human-related EMP events. It is incumbent on electricity providers and others to assess the benefits and costs to mitigate these types of low probability-high impact contingencies. Policies should enable and require the grid to devote sufficient resources to mitigate such eventualities.

Limitations

One noteworthy limitation of this research is that from 2000-2014, OE-417 reported power outage causes in abbreviated terminology or labels rather than through descriptive narrative. That is, standard terms are provided, e.g., vandalism, cyber-attack, and suspicious activity. But no qualifying narratives, further direction, or clear explanations of events are provided.

In 2018, modifications to OE-417 added definitions for causes of outages, which improved the accuracy of reported information. However, the reported causes of outages would significantly benefit from additional information to assist both power suppliers and researchers in understanding the full scope of the cause of the power outages.

Another notable limitation is that this database is compiled from public reports of power outages from jurisdictions with mandatory reporting requirements. Thus, these reports do not capture unreported power outage data not required for submission by policy, statute or law (Wirfs-Brock 2014). Additionally, reporting outage information using OE-417 provides incomplete data regarding the range of variables that may be implicated in a single or multiple outage events. Additional supportive information as obtained through Energy Information Administration surveys and other sources could assist in triangulating the causation and characteristics of power outages. This could assist more comprehensive and accurate disclosure of power grid disruptions and outages.

Conclusions

This study suggests future research to expand and improve the understanding of large power outages, their consequences for multiple stakeholders, and strategies to reduce their occurrence and impacts. The first approach, described above, would involve DOE collecting and curating additional information using Form OE-417. Linking additional DOE with other information sources, such as data sharing by NERC members, could enable important researchable topics. Ideally, this would be augmented by a forensic capacity to validate key occurrences and to upgrade information post event deemed important for database integrity.

Additional power outage narratives could allow triangulating both the underlying causation and sources of reported outages. This additional information could prove valuable in driving policy development decisions to address outage vulnerabilities. More detail on the types of customers affected in both the commercial and residential domains would be welcome. Similarly, demand loss in megawatts could be reported for commercial or residential customers. The incorporation of these features in the core data set would assist researchers and policy makers to better assess economic impact due to power outages.

Researchers can combine other sourced external data to these data to answer a much broader group of questions. For example, systematically compiling additional data from NERC reliability councils would expand the topics that could be considered.

The utilization of these types of aggregate data to estimate likely causes of outages and preferred responses should be useful for energy providers. Technological advances and use of various smart technologies and SCADA (Supervisory Controlled and Data Acquisition) systems have improved incident response time and situational awareness among energy providers. While the number of outages has been increasing, the outage durations are shorter.

Future exploratory studies should examine how organizations, both for profit and non-profit, are affected by power outages. A more accurate examination of the financial impacts of electrical failure could stimulate efforts to maintain a consistently reliable and dependable power grid to strengthen business continuity planning of potentially affected entities.

Acknowledgements

The primary dataset was obtained from the US Department of Energy Office of Cybersecurity, Energy Security & Emergency Response (CESER):
https://www.oe.netl.doe.gov/OE417_annual_summary.aspx.

Appendix

U.S. Department of Energy. OE-417 Electric Emergency Incident and Disturbance Report.

The North American Electric Reliability Corporation (NERC) currently delegates its compliance monitoring and enforcement authority across six regional council entities. These entities are designated as the Federal Reliability Coordinating Council (FRCC), Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), Reliability First (RF), SERC Reliability Corporation (SERC), Texas Reliability Entity (Texas RE), Western Electricity Coordinating Council (WECC), and formerly the East Central Area Reliability Coordination Agreement (ECAR) – pre-2004.

North American Reliability Corporation (NERC) Geographical Regions

ECAR = East Central Area Reliability Coordination Agreement

ERCOT = Electric Reliability Council of Texas

FRCC = Florida Reliability Coordinating Council

MAAC = Mid-Atlantic Area Council

MAIN = Mid-America Interconnected Network

MRO = Midwest Reliability Organization

NPCC = Northeast Power Coordinating Council

RFC = Reliability First Corporation

SERC = Southeastern Electric Reliability Council

SPP = Southwest Power Pool

TRE = Texas Regional Entity

WECC = Western Electricity Coordinating Council

Author Capsule Bios

Dr. Brian K. Harte is Professor of Homeland Security within the Division of Criminal Justice, Legal Studies and Homeland Security at St. John's University. Previously, Dr. Harte worked as a Professor of Criminal Justice within the State University of New York system, and as a probation administrator in the State of Texas. Collectively, Dr. Harte has over 17 years of experience teaching criminal justice and homeland security students at both the college and university levels. He currently serves as the Master of Professional Studies in Homeland Security and Criminal Justice Leadership Program Director, and as Interim Associate Dean of External Affairs and Graduate Studies within the Lesley H. and William L. Collins College of Professional Studies.

Umesh Kumar, PhD is Associate Professor of Finance at the State University of New York, Canton. He received his PhD in Finance from the University of Texas, San Antonio. He has had extensive teaching and research experience in the field of finance and economics. His broad teaching experience ranges from corporate and personal finance, investments, to risk management. Having industry background in a regulatory organization, he is skilled at explaining a variety of complex financial theories and practices clearly and accessibly to professional and non-professional audiences.

References

Adderly, Shawn, Peterson, Todd, Manukian, Daria, Sullivan, Timothy, Son, Mun, & Mickey, Ruth. 2019. "Evaluating the Potential Impact of Large Outage Events in the United States from 2003 to 2017." *Technology and Economics of Smart Grids and Sustainable Energy* 4, no. 6: 1-10.

American Society of Civil Engineers. 2017. "America's Infrastructure Grade." *American Society of Civil Engineers*. Retrieved from: https://www.infrastructurereportcard.org/americas-grades/

American Society of Civil Engineers. 2013. "Report Card for American Infrastructure." *American Society of Civil Engineers*. Retrieved from: https://ascelibrary.org/doi/ pdf/10.1061/9780784478837

Baker, George. Goldberg, Ed, Harris, William, & Winks, David. 2020. "*Powering Through: Building Critical Infrastructure Resilience.*" InfraGard National Disaster Resilience Council.

Committee on Energy and Commerce. 2003. "2003 Blackout: Why Did This Hap-

pen and How?" https://www.govifo.gov/content/pkg/CHRG-108hhrg89467/html/CHRG-108hhrg89467.htm

Cyber Security Incident Reporting Reliability Standards. 164 FERC, 18 CFR Part 40 [Docket No. RM18-2000; Order No 848], July 19, 2018.

Eke, Patricia. 2019. Cybersecurity Updates and Audits - Lessons Learned Report, Federal Energy Regulatory Commission. September 25, 2019.

Homeland Security News Wire. 2015. "2013 Attack on Metcalf, California Power Grid Substation Committed by an Insider: DHS." Retrieved from:

Melvin, Jasmin, & Jackson, Valerie. 2020. "Citing security risks, FERC, NERC to keep cyber violation details under wraps." Retrieved from: https://www.spglobal.com/platts/en/market-insights/latest-news/electric-power/092520-citing-security-risks-ferc-nerc-to-keep-cyber-violation-details-under-wraps

Mukherjee, Sayanti. 2017. "Towards A Resilient Grid: A Risk-based Decision Analysis Incorporating the Impacts of Severe Weather Induced Power Outages." PhD diss., Purdue University.

Mukherjee, Sayanti, Nateghi, Roshanak, & Hastak, Makarand 2018a. "Data on Major Outage Events in the Continental U.S. Data in Brief."

Mukherjee, Sayanti. 2019. "A Data-Driven Approach to Assessing Supply Inadequacy Risks Due to Climate-induced Shifts in Electricity Demand." *Risk Analysis* 36, no. 1: 4–15.

Mukherjee, Sayanti, Nateghi, Roshanak, & Hastak, Makarand. 2018b. "A Multi-hazard Approach to Assess Severe Weather-induced Major Power Outage Risks in the U.S." *Reliability Engineering & System Safety* 175: 283–305.

Mukhopadhyay, Sayanti, & Hastak, Makarland. 2016. "Public Utility Commissions to Foster Utility Investment in Power Grid Infrastructure." Retrieved from:

National Academy of Sciences. 2020. "The Power Renewable: Opportunities and Challenges for China and the United States." Accessed March 6, 2020. https://www.nap.edu/read/ 12987/chapter/8#155

National Conference on State Legislatures. 2020. "Modernizing the Electric Grid: State Role and Policy Options. Accessed March 6, 2020. https://www.ncsl.org/research/energy/ modernizing-the-electric-grid-state-role-and-policy-options.aspx

Nateghi, Roshanak, Guikema, Seth D., Wu, Yue, & Bruss, C. B. 2016. "Critical Assessment of Power Transmission and Distribution Reliability Metrics and Standards." *Risks Analysis* 41, no. 1: 4–15. https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12401

North American Transmission Forum, Cyber Security Supply Chain Risk Management Guidance, Charlotte, NC. June 2018. http://www.natf.net/docs/natf/documents/resources/natf-cyber-security-supply-chain-risk-management-guidance.pdf

Executive Office of the President. The White House. 2013. "Economic Benefits of Increasing Electric Grid Resilience to Weather Outages."

Standard & Poor's. 2020. "Citing Security Risks, FERC, NERC to Keep Cyber Violation Details Under Wraps." Retrieved from: https://www.spglobal.com/platts/en/market-insights/latest-news/electric-power/092520-citing-security-risks-ferc-nerc-to-keep-cyber-violation-details-under-wraps.

TVA Nouvelles. 2019. "Le réseau d'Hydro-Québec constamment pris d'assaut par des cyberattaques." Retrieved from: https://www.tvanouvelles.ca/2019/08/05/le-reseau-dhydro-quebec-constamment-pris-dassaut-par-des-cyberattaques.

U.S.-Canadian Power Outage Task Force. 2006. "Final Report on the Implementation of The Task Force Recommendations. https://www.energy.gov/oe/downloads/us-canada-power-system-outage-task-force-final-report-implementation-task-force

U.S. Department of Homeland Security. 2017. "The Power Outage Incident Annex: Managing Impacts from a Long-term Power Outage." https://www.fema.gov/media-data/1512398599047756540643 8d0820111177a9a2d4ee3c6/POIA_Final_72017v2_(Compliant_pda) 508.pdf

U.S. Department of Homeland Security. 2008. "DHS Risk Lexicon."

U.S. Department of Energy. 2020. "OE-417." Retrieved from: https://www.energy.gov/ceser/activities/energy-security/monitoring-reporting-analysis/electric-disturbance-events-oe417#:~:text=The%20Electric%20Emergency%20Incident%20and,well%20as%20for%20analytical%20purposes.

University of Washington. 2017. "Cyberattack on Critical Infrastructure: Russia and the Ukraine Power Grid Attack." Retrieved from: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

U.S. Energy Information Administration. 2018. "Independent Statistics & Analysis." Retrieved from: https://www.eia.gov/electricity/data/eia411/#tabs_NERC-1

U.S. Energy Information Administration. 2018. "Independent Statistics & Analysis." Retrieved from: https://www.eia.gov/electricity/data/eia411/#tabs_NERC-2

Willis, Henry H., Tighe, Mary, Lauland, Andrew, Ecola, Lissa, Shelton, Shoshana R., Smith, Megan L., Rivers, John G., Leuschner, Kristin J., Marsh, Terry, & Gerstein, Daniel M. 2018."Homeland Security National Risk Characterization: Risk Assessment Methodology." Rand Corporation." Accessed March 6, 2020. https://www.rand.org/pubs/ research_reports/RR2140. html

Wirfs-Brock, Jordan. 2014. "Data: Explore 15 years of Power Outages." Inside Energy. Accessed February 21, 2020. http://insideenergy.org/2014/08/18/data-explore-15-years-of-power-outages/

World Bank. 2019. Doing Business 2020–Sustaining the pace of reforms. Accessed September 27, 2020. https://www.worldbank.org/en/news/feature/2019/10/24/doing-business-2020-sustaining-the-pace-of-reforms