

## Research Article

# Sociotechnical Network Analysis for Power Grid Resilience in South Korea

Daniel A. Eisenberg,<sup>1</sup> Jeryang Park,<sup>2</sup> and Thomas P. Seager<sup>1</sup>

<sup>1</sup>School of Sustainable Engineering and the Built Environment, Arizona State University, Tempe, AZ, USA

<sup>2</sup>School of Urban and Civil Engineering, Hongik University, Seoul, Republic of Korea

Correspondence should be addressed to Daniel A. Eisenberg; [daeisenb@asu.edu](mailto:daeisenb@asu.edu)

Received 31 May 2017; Accepted 5 September 2017; Published 23 October 2017

Academic Editor: Paul Hines

Copyright © 2017 Daniel A. Eisenberg et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

International efforts to improve power grid resilience mostly focus on technological solutions to reduce the probability of losses by designing hardened, automated, redundant, and smart systems. However, how well a system recovers from failures depends on policies and protocols for human and organizational coordination that must be considered alongside technological analyses. In this work, we develop a sociotechnical network analysis that considers technological and human systems together to support improved blackout response. We construct corresponding infrastructure and social network models for the Korean power grid and analyze them with betweenness to identify critical infrastructures and emergency management organizations. Power grid network analysis reveals important power companies and emergency management headquarters for responding to infrastructure losses, where social network analysis reveals how information-sharing and decision-making authority shifts among these organizations. We find that separate analyses provide relevant yet incomplete recommendations for improving blackout management protocols. In contrast, combined results recommend explicit ways to improve response by connecting key owner, operator, and emergency management organizations with the Ministry of Trade, Industry, and Energy. Findings demonstrate that both technological and social analyses provide important information for power grid resilience, and their combination is necessary to avoid unintended consequences for future blackout events.

## 1. Introduction

The increasing frequency and costs of catastrophic events have prompted concerted international efforts to study and design more resilient power systems. In the United States, national policy is encouraging technical efforts to improve the resilience of infrastructure systems, including energy, water, cyber security, communications, transportation, emergency management, healthcare, financial, and government systems [1, 2]. Global organizations like the United Nations [3] and Rockefeller Foundation [4] promote similar goals across partner nations to establish resilient cities to future catastrophes. In all cases, the resilience of electric power systems receives particular interest, as electricity is essential to the provision of nearly all other infrastructure services. Power grid resilience research now produces a constant stream of novel analytical techniques to predict and reduce

systemic losses associated with infrastructure failures, natural disasters, and terrorist attacks [5–7]. Despite these efforts, even the most modern power grids continue to experience large-scale blackouts. Countries like the US [8], India [9], Ukraine [10], and Australia [11] suffered major brownouts and blackouts between 2011 and 2016 from a broad range of events from extreme weather to cyberattack.

We argue that the lack of resilience in critical infrastructure is, in part, due to overemphasizing technological solutions that underestimate crisis decision-making and social context [12–15]. Currently, power system protection focuses on hardening existing system components and designing automated, redundant, smart, or otherwise technological solutions to reduce the probability of losses [13, 14]. However, reducing the *probability* of losses via technological solutions alone does not reduce their *consequences* (i.e., outcome of emergencies), which is dictated by human actions. For

example, the 2003 US Northeast blackout included a combination of infrastructure, control system, and decision-making failures that exacerbated unstable conditions and led to cascading damages [16]. Since 2003, postmortem analysis of several major blackout events continue to recommend improved communication within and across organizations to enhance crisis response [12, 17, 18]. Thus, research should expand awareness beyond technological limitations to include the diverse institutions that influence human decision-making and failure consequences, such as operations and management practices, economic constraints, organizational and industry cultures, and affected parties. We refer to the joint consideration of technological systems with these and other social institutions hereafter as “sociotechnical” analysis [19].

Network science enables one to model the components and interactions of human and infrastructure systems [21], suggesting the potential to develop a sociotechnical network analysis (STNA) for infrastructure resilience. Both electric power grids and human interactions are now studied as networks, yet isolated research does not treat engineering and social science perspectives as equals for sociotechnical guidance. The term “sociotechnical” is primarily used in network science to describe the study of human processes organized or mediated by technology, such as the formation of online social networks like Facebook and Twitter [22], traffic flows on transportation systems [23], or human interactions on communication networks [24–26]. Instead, we use the term STNA to describe the application of sociotechnical systems theory [19] to technological and human networks coupled by a single context. The tenets of sociotechnical systems theory can be translated into infrastructure network models by analyzing both social and technological networks together to avoid unpredictable and harmful recommendations from narrow perspectives on a single system [27] and by considering the tasks taken by social units and the expected function of technological systems alongside network structure [28]. A STNA of blackout management, thus, requires both infrastructure networks of substations, generators, transmission lines, and transformers as nodes and links [29] alongside social networks of human constructs like actors and their relational ties (e.g., who knows whom) [30], not one or the other. A STNA also requires knowledge of how power systems provide electric power services and the tasks people and organizations take to ensure services remain available. We argue that this form of STNA better supports the design of resilient power grids than those extant in the literature by integrating knowledge from engineering and social science without marginalizing either. To the best of the authors’ knowledge, this form of STNA is also novel as no network studies in the literature give built and human systems equal consideration.

In this work, we develop the first STNA of a power grid to improve blackout response. We construct corresponding infrastructure and social networks and study them to identify critical components. We use results from power grid analysis in a new way by converting knowledge of critical infrastructure into demographic data of the organizations that manage their failures when lost. We further combine

these results with a social network analysis of the formal institutions that dictate crisis coordination during large-scale blackouts [31–33]. The social network analysis reveals important organizations that fulfill coordination roles among them. Together, these analyses uncover which organizations are critical to power system protection from both engineering and administrative perspectives and can offer ways to improve blackout management policies that either analysis is incapable of offering its own.

Due to the significant amount of context-specific data required for STNA, this work centers on a single case study location: the South Korean power grid (KPG). In 2011, the worst brownout experienced in Korea caused roughly half of Seoul to lose power and was exacerbated by slowed decision-making processes across operator and regulatory agencies [34]. In 2013, corruption among regulatory officials led to nationwide power shortages after components in Korean nuclear power plants were found to have forged reliability documentation [35]. In 2014, the national tragedy of a ferry capsizing and killing 295 people (mostly children) [36] triggered the reorganization of the entire Korean emergency management industry to centralize crisis coordination efforts into a single agency [37]. In 2016, a city-wide blackout in Jeonggwan New City was exacerbated by a failure to deploy backup infrastructure stored on the other side of the country. Taken together, a case study of the KPG will have broad impacts on Korean society as the South Korean grid in need of social and technological guidance for blackout response.

## 2. Background on Korean Electric Power and Emergency Management Industries

The KPG is an islanded power system which has two primary parts, a large mainland grid serving the majority of Korea and a smaller, self-contained grid on the island state of Jeju-Do. In this work, we focus on the mainland KPG. The mainland grid has voltage classes from 765 kV to as low as 3.3 kV, yet ~55.1% of substation and 96% of power line infrastructure are 345 and 154 kV (Figure 1) [38]. The 345 and 154 kV transmission infrastructures are geographically clustered in population-dense regions such as the Seoul Metropolitan Area in the northwest. Korean power generation is dominated by coal, natural gas, and nuclear power technologies, and this power production is geographically centralized, where roughly 95% of installed capacity is located in 55 separate sites throughout the country [39].

KPG infrastructure is owned and operated by a few, key organizations (Table 1). Korean power transmission and distribution are managed by a single company, the Korea Power Exchange (KPX), and infrastructure ownership and maintenance are dominated by a separate company, the Korean Electric Power Corporation (KEPCO). During crises, KPX and KEPCO act as focal points for grid status, health, and management across the nation: KPX managing power flow and operations decisions and KEPCO managing power line and infrastructure recovery. KEPCO has 6 generation subsidiaries that independently operate and manage ~97% of Korean grid [40]. Liquid fuel, natural gas, and coal-fired power plants are owned and operated by 5 of the 6

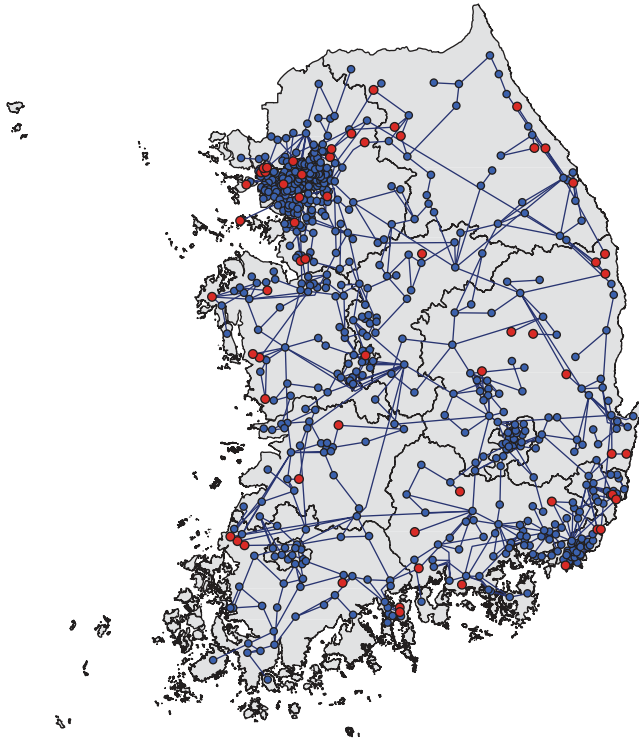


FIGURE 1: Map of the 2013 South Korean power grid. This map shows the connectivity of major power grid infrastructure in mainland Korea, that is, power plants (red circles), high-voltage transmission substations (dark blue circles), and power lines (dark blue lines). Transformers connect buses that are too close together to be shown in this image. For security purposes, data is simplified to only publicly available data from the Korean Power Exchange [20]. Jeju Island off the southern coast of Korea is also excluded from the image because it is not considered in the current analysis.

generation subsidiaries, each with roughly the same total generation capacity, 10–15 GW. The single largest generation subsidiary (~20 GW) is Korea's sole owner and operator of all nuclear power plants, Korea Hydro Nuclear Power (KHNP). Besides nuclear and fossil fuel generation, ~7% of electricity is generated from hydroelectric and renewable sources. KHNP and other KEPCO subsidiaries operate single purpose dams (power generation), whereas the Korean Water Administration (Kwater) manages all Korean multipurpose dams (power, water supply, and flood control).

Korean blackout response requires the coordination of electric power regulators (Table 1) and emergency managers for decision-making and crisis support (Table 2). KPX is the established hub for minor blackout incidents. Ministries and support organizations provide additional oversight in larger events depending upon the type of generation technologies involved (Table 1). For major fires, typhoons, earthquakes, and terrorist attacks, the power industry coordinates with first-responder and emergency management organizations (fire fighters, police, and crisis managers) to mitigate and recover failed infrastructure. Federal regulatory and crisis coordination agencies also become involved in decision-making in worst case scenarios where national power

availability is deemed vulnerable. The Ministry of Trade, Industry, and Energy (MOTIE) is the acting headquarters for man-made disasters including infrastructure failure due to human error or intentional attack and works with KPX and KEPCO to respond to national blackouts. MOTIE's disaster management division works with the National Emergency Management Agency (NEMA) and the Ministry of Security and Public Administration (MOSPA) to monitor and manage natural disasters. When MOTIE, NEMA, or MOSPA are involved in disaster management, MOTIE is the final decision-maker for built infrastructure and NEMA coordinates crisis support across a hierarchy of state and special city crisis headquarters to city, county, and district fire, police, and emergency management agencies.

Our description of the KPG and related crisis management organizations is based on 2013–2014 data collected from and verified by experts in formal interviews. We focus on this timeframe to ensure that power system analyses match with blackout management analyses. Since then, MOSPA and NEMA have become part of the same organization, the Ministry of Public Security and Safety (MPSS). Nonetheless, analysis of this blackout management system is a critical case relevant for many current policies and practices that remain intact, and all conclusions made in this work are applicable to the most recent organizational relationships.

### 3. Materials and Methods

#### 3.1. Data for Network Analysis

**3.1.1. Power Grid Networks.** The KPG data was directly provided as a PSS/E (power system simulation for engineering) printout by KEPCO and was converted into a complex network using methods similar to those described in Kim et al. [38]. We assessed the extracted KPG model with MATLAB packages for optimal power flow [41] and complex network analysis [42, 43]. We use the Direct Current (DC) power flow approximation for all analyses [41]. Power flow analysis was calculated with the summer-time generation and demand dispatch for peak system load used by KEPCO for power system planning.

**3.1.2. Korean Power Grid Emergency Response Networks.** Primary data for the interorganizational blackout management social network was collected through semistructured interviews with Korean electric power industry experts. 14 expert interviews ranging from 30 minutes to 2 hours in length were held in South Korea over two 3-month periods in 2014 and 2015. A total of 12.7 hours of interviews were held. Experts interviewed include industry and academic experts from the following organizations: KEPCO, KPX, KHNP, NEMA, KMA, Kwater, Seoul National University, and Ulsan National Institute of Science and Technology. In these interviews, experts provided researchers with 208 pages of primary documents outlining various power system emergency protocols that were verified among interviewees. These primary documents were coded to determine the specific roles of different power system organizations identified in Tables 1 and 2. Additional interviews were then held to clarify

TABLE 1: Electric power industry organizations.

Operation & management		Regulation & decision-making
<i>Power transmission:</i>		<i>Industry-wide:</i>
Korea Electric Power Corp		Ministry of Trade, Industry, and Energy
Korean Power Exchange		Korea Electricity Commission
<i>Thermoelectric power:</i>		<i>Sector specific, nuclear:</i>
	<i>% Gen capacity</i>	Nuclear Safety and Security Commission
Korea Midland Power*	12.0%	Korea Institute of Nuclear Safety
Korea Western Power*	10.6%	<i>Sector specific, hydroelectric:</i>
Korea East-West Power*	10.6%	Ministry of Land, Infrastructure, and Transport
Korea Southern Power*	9.6%	Kum River Flood Control Office
Korea Southeast Power*	9.6%	Youngsan River Flood Control Office
POSCO Power	3.1%	Nakdong River Flood Control Office
SK Energy	2.1%	Han River Flood Control Office
K-Power Ltd.	1.2%	
Korea District Heating Corp	1.2%	
Meiya Power Company	1.2%	
GS EPS	1.1%	
Hyundai Corporation	1.1%	
<i>Nuclear power:</i>		
Korea Hydro Nuclear Power*	29.0%	
<i>Hydroelectric power:</i>		
Korea Water Administration	2.9%	
Korea Hydro Nuclear Power*	—	

\*Subsidiary of Korean Electric Power Corporation. *Note.* Only companies with >1% of total generation capacity for Korea are listed.

TABLE 2: Disaster management industry organizations.

Local operations & management	Federal operations & management
<i>Crisis operations, state:</i>	
Gyeonggi Firefighting & Disaster HQ	<i>Crisis coordination:</i>
Gangwon Fire HQ	Ministry of Trade, Industry, and Energy
Chungcheongbuk HQ of Fire Mgmt.	Ministry of Security and Public Administration
Chungcheongnam Fire Safety Office	National Emergency Management Agency
Jeollabuk Fire Dept. HQ	<i>Oversight:</i>
Jeollanam Fire Safety HQ	Prime Minister's Office
Gyeongsangbuk Fire Protection HQ	National Security Office
Gyeongsangnam Fire Service HQ	<i>Additional federal support:</i>
Jeju Fire & Disaster Mgmt. HQ*	Ministry of Land, Infrastructure, and Transport
<i>Crisis operations, city:</i>	
Seoul Fire & Disaster HQ	Ministry of Strategy and Finance
Busan Fire Department	Ministry of Employment and Labor
Incheon Fire & Safety Mgmt. Dept.	Ministry of Health and Wellness
Daejeon Fire Fighting Head Office	Ministry of Defense
Gwangju Fire Safety HQ	National Police Agency
Daegu Fire Fighting HQ	Ministry of Culture, Sports, and Tourism
Ulsan Fire & Disaster HQ	Korean Communications Commission
	Korean Meteorological Agency

\*Jeju Island is not included in the current analysis. *Note.* Table based on 2013 data.

roles and explicit information sharing and decision-making relationships among power grid and emergency management organizations.

Together, the interviews and coded documents resulted in social network models of the formal institutions for

blackout management in South Korea, where nodes represent organizations in Tables 1 and 2 and links represent bidirectional information sharing and decision-making relationships. These networks are detailed representations of real policies and protocols to the best of the authors' knowledge

and incorporate additional expert input for their accuracy of relationships.

The shifting context of power grid operations and decision-making changes with power system health, defined by system reserve margin, and requires the creation and analysis of six blackout management social networks. Six reserve margin thresholds are defined in Korean policies, one for Normal Operations, one for minor events that do not reduce reserve margin past set thresholds, and four for increasing blackout risks as backup power becomes less available and the system becomes more unstable. We label these thresholds by associated titles denoted within the protocols themselves, with increasing risk of blackout from Prevention activities to Alarm Red.

(i) *Normal Operations*. State/city emergency management agencies coordinate infrastructure failure response directly with power infrastructure owners and operators. This network applies when infrastructure losses do not affect power grid reserve margin.

(ii) *No Alarm: Prevention*. KPX provides blackout coordination to protect the power grid and some coordination still exists between state/city emergency managers and infrastructure owner/operators.

(iii) *Alarm Blue: Concern*. KPX serves primary blackout coordination role between electric power and emergency management industries. Industry-specific regulators like the MOTIE provide industry oversight.

(iv) *Alarm Yellow: Caution*. Additional oversight ministries were involved in coordination efforts and first responder decision-making shifts from emergency management agencies to city/state governor offices.

(v) *Alarm Orange: Alert*. Crisis coordination and decision-making switch from electric power industry organizations to the MOSPA and the NEMA.

(vi) *Alarm Red: Serious*. All communication and decision-making between industries are mediated by Korean Federal Ministries with increasing ministerial participation (e.g., inclusion of military support).

### 3.2. Network Analysis Methods

3.2.1. *Betweenness of Infrastructure and Social Networks*. The resilience of a power grid must be understood with respect to the service it provides [27], the delivery of electricity from generation to distribution substations that then serve point of use. This generation-demand relationship corresponds to social network theory via “package” based flow processes [44]. Unlike other social processes such as gossip that transfers information among actors in an unregulated, probabilistic way, packages are assumed to have explicit destinations. Information sharing and decision-making among blackout crisis managers follow a similar package delivery relationship due to the regulated nature of the industry.

The “package delivery” structure and function of the KPG indicate that *betweenness*, which measures the flow contribution of network elements, can be used to identify critical components in both infrastructure and social networks. Betweenness in abstract graphs is based on the “geodesic path (or shortest path)” from nodes  $i$  to  $j$ . The set of all geodesic paths between any two nodes  $i$  and  $j$  is referred to as the “minimum cut set” of  $i$  and  $j$ . Following this definition, the “betweenness” of a node or link ( $B_v$ ) is the total number of geodesic paths the network element  $v$  resides on ( $\sigma_{ij}^v$ ) normalized by the total number of geodesic paths ( $\sigma_{ij}$ ) in a network [21], following

$$B_v = \sum_{i \neq v \neq j \in N} \frac{\sigma_{ij}^v}{\sigma_{ij}}. \quad (1)$$

When used in power grid networks, betweenness identifies critical infrastructure whose loss may initiate cascading failures [45]. The same measure in crisis management networks identifies authoritative actors that broker emergency information and decision-making rights among disconnected groups [31, 33, 46]. Thus, betweenness analysis should identify infrastructures that have the greatest influence on power delivery and partnerships that dictate crisis coordination activities.

3.2.2. *Additional Power Grid Betweenness Measures*.  $B_v$  in (1) assumes that all links and nodes are equivalent (unweighted and homogeneous), which is not true for real power grids. Within the KPG, different characteristic infrastructures extract electricity from the network, constraining the total number of origin-destination flow paths within the resulting graph. Moreover, power system infrastructure (e.g., power lines) has electrical properties that impede and limit electricity from travelling along paths, further constraining potential flow. Thus, (1) may produce an unrealistic ranking of critical network elements by ignoring relevant power system characteristics.

In response to the perceived impracticality of (1) for power grids, researchers have developed betweenness measures that include relevant power system data for assessing flow contribution. At least two novel electrical betweenness metrics ( $EB_v^1$  and  $EB_v^2$ ) are proposed in the literature to build upon the formation and purpose of (1). The method developed by Nasiruzzaman et al. [47] combines network science and power system engineering by using geodesic paths weighted based on the amount of power flowing through them

$$EB_v^1 = \sum_{i \neq v \neq j \in N} \frac{P_{ij}^v}{P_{ij}}, \quad (2)$$

where  $P_{ij}$  is the maximum power flowing in the shortest path between nodes  $i$  and  $j$  and  $P_{ij}^v$  is the maximum of inflow and outflow of power at bus  $v$  on this shortest path. The feasibility of (2) for ranking nodes has been studied on numerous IEEE test power systems using both AC [48, 49] and DC [47, 50, 51] power flow models.

Another method developed by Arianos et al. [52–54] does not calculate shortest paths and instead uses simplified power grid vulnerability methods [55] and combines their output to recreate a measure comparable to betweenness. This method measures the sensitivity of nodes and links to the changes in generation and load throughout the system to assess their potential contribution to power flow. First, links are considered to be power lines and transformers ( $|\mathbf{L}| = M_{\text{lines}}$ ) and nodes are power system buses organized into three sets: generation ( $|\mathbf{G}| = N_{\text{Gen}}$ ), transmission ( $|\mathbf{T}| = N_{\text{Trans}}$ ), and distribution ( $|\mathbf{D}| = N_{\text{Dist}}$ ). Then, power transfer distribution factors [56],  $f_i^{gd}$ , are calculated for each power line,  $l \in \mathbf{L}$ , for a unit injection of electricity at a given generation bus,  $g \in \mathbf{G}$ , and a comparable increase in load at distribution bus,  $d \in \mathbf{D}$ . This value is used to determine how the structure of the KPG influences power transmission capacity across all  $g$  to  $d$  relationships. In addition, it is used to calculate a total transfer capability factor,  $C_g^d$ , to ensure all power lines remain within maximum power flow limits for each generation-demand relationship:

$$C_g^d = \min_{l \in \mathbf{L}} \left( \frac{P_l^{\max}}{f_l^{gd}} \cdots \frac{P_l^{\max}}{f_l^{gd}} \cdots \frac{P_M^{\max}}{f_M^{gd}} \right). \quad (3)$$

The bus betweenness of bus  $v$  combines these two elements, the sensitivity of power lines connected to it and total transfer capability of the grid, and is defined as

$$\text{EB}_v^2 = \frac{1}{2} \sum_{g \in \mathbf{G}} \sum_{d \in \mathbf{D}} C_g^d \sum_{l \in \mathbf{L}^v} |f_l^{gd}|, \quad g \neq v \neq d, \quad (4)$$

where  $\mathbf{L}^v$  is the set of power lines connected to bus  $v$  and the factor of  $1/2$  deals with double counting flow into and out of nodes. As  $(1/2)C_g^d \sum_{l \in \mathbf{L}^v} |f_l^{gd}|$  can be interpreted as the security constrained contribution to power flow of node  $v$  for a single generation-load pair, (4) calculates the total power flowing through  $v$  relative to all generation, distribution pairs within the system. Thus, (4) directly measures the contribution of node  $v$  to flow without determining geodesic paths or minimum cut sets, which is computationally difficult for large networks. The feasibility of (4) for ranking nodes has been studied on numerous IEEE test power systems and the Italian high voltage transmission grid [52–54, 57, 58].

**3.2.3. Converting Infrastructure Network Results into Demographic Results.** We use all three betweenness measures to find critical power grid infrastructure in the KPG because there is no established “best” option among power grid betweenness measures. Then we aggregate results into demographic data useful to blackout management organizations. We treat each betweenness score as the relative importance of each power grid bus within the KPG characterizing its criticality. Then, we sum normalized scores based on demographic information of where each node is located in South Korea (longitude/latitude location) and ownership information. These two pieces of information aggregate individual node betweenness values into the infrastructure companies that own and operate them (Table 1) and the state or special city emergency management agency (Table 2).

**3.2.4. Additional Social Network Measures.** We use general social network analysis measures outlined below to characterize the six blackout management networks and (1) to identify the critical organizations that broker information for blackout coordination. Social network visualization and analysis were completed using ORA-LITE social network analysis software [59] developed by the Carnegie Mellon Center for Computational Analysis of Social and Organizational Systems.

To compare and contrast blackout management contexts, additional measures are used to characterize network-level properties of all six social networks, including the following [60]:

(i) *Network Size.* It is the number of organizations (nodes) in each network and the number of interactions (links) among organizations.

(ii) *Network Density.* Density is calculated as ratio of network interactions to the total number of possible interactions. Density is a normalized measure ranging from 0 to 1, where 0 indicates an unconnected network and 1 indicates a completely connected network.

(iii) *Network Centralization (Degree and Betweenness).* Network centralization measures the relative importance of highest ranking node for a single network measure to rest of the network. This is expressed as a ratio of the sum of the differences between the highest ranking node and the rest of the nodes in the network to the maximum possible sum of the differences. Freeman [61] defines standard ways to calculate degree and betweenness centralization with the following equations:

$$\begin{aligned} &\text{Network Centralization, Degree} \\ &= \frac{\sum_{i=1}^n \text{Deg}_{\max} - \text{Deg}_i}{(n-1)(n-2)}, \end{aligned} \quad (5)$$

Network Centralization, Betweenness

$$= \frac{\sum_{i=1}^n \text{Bet}_{\max} - \text{Bet}_i}{(n-1)(n-2)(n-3)},$$

where  $\text{Deg}_i$  is the number of links connected to node  $i$  (referred to as the degree of  $i$ ) and  $\text{Deg}_{\max}$  is the degree of the node with the most links. Likewise,  $\text{Bet}_i$  is the betweenness of node  $i$ , and  $\text{Bet}_{\max}$  is the highest betweenness in the network. All centralization values are between 0 and 1, where 0 indicates no centralization (all nodes equal) and 1 indicates complete centralization (one node dominates the measure).

## 4. Results

**4.1. Aggregated Power Grid Criticality Results.** Linking the Korean blackout management industry organizations and infrastructure criticality analysis results implicates the involvement of different power system and emergency management organizations in protecting infrastructure for future blackout events. Figure 2 presents the aggregated and

Power industry organizations	Generation and transmission			% of installed gen capacity	Generation only		
	$B_v$	$EB_v^1$	$EB_v^2$		$B_v$	$EB_v^1$	$EB_v^2$
KEPCO	100.0%	99.9%	49.9%	—	—	—	—
KHNP	0.0%	0.0%	12.7%	29.0%	0.0%	5.6%	25.3%
KOSEPO	0.0%	0.0%	5.4%	9.6%	0.0%	0.0%	10.8%
KOSPO	0.0%	0.0%	5.1%	9.6%	0.0%	16.9%	10.1%
EWP	0.0%	0.0%	7.0%	10.7%	0.0%	8.5%	13.9%
KOWEPO	0.0%	0.0%	4.5%	10.3%	0.0%	22.6%	8.9%
KOMIPO	0.0%	0.1%	6.3%	12.0%	100.0%	46.4%	12.5%
Kwater	0.0%	0.0%	0.4%	2.9%	0.0%	0.0%	0.7%
Posco Power	0.0%	0.0%	1.7%	3.1%	0.0%	0.0%	3.3%
GS Power Co	0.0%	0.0%	0.3%	0.9%	0.0%	0.0%	0.7%
K-Power Ltd.	0.0%	0.0%	0.5%	1.2%	0.0%	0.0%	0.9%
Korea District Heating	0.0%	0.0%	0.2%	1.2%	0.0%	0.0%	0.5%
Posco E&C LTD	0.0%	0.0%	1.0%	0.8%	0.0%	0.0%	2.0%
GS EPS	0.0%	0.0%	0.6%	1.1%	0.0%	0.0%	1.2%
Meiya Power Co	0.0%	0.0%	0.5%	1.2%	0.0%	0.0%	1.0%
STX Energy	0.0%	0.0%	0.0%	0.1%	0.0%	0.0%	0.0%
Korea Energy Mgmt. Corp	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Daelim Mitsubishi	0.0%	0.0%	1.5%	1.2%	0.0%	0.0%	3.0%
S-Power	0.0%	0.0%	0.1%	0.7%	0.0%	0.0%	0.2%
SK Energy	0.0%	0.0%	2.4%	2.2%	0.0%	0.0%	4.7%
Hyundai Corp	0.0%	0.0%	0.0%	1.1%	0.0%	0.0%	0.0%

FIGURE 2: Criticality of KPG buses aggregated by power industry organizations.

normalized criticality scores for the infrastructures owned by power system organizations. All measures implicate KEPCO as owning and operating the majority of critical KPG infrastructure. In particular,  $B_v$  and  $EB_v^1$  only identify power generation companies owning and operating fractions of a percent of the critical infrastructure. In contrast,  $EB_v^2$  identifies a much larger participation of power companies in owning and operating critical infrastructure, suggesting that KEPCO and KPX only operate ~50% of the critical infrastructure within the KPG.

The differences between power organizations become more apparent when excluding transmission infrastructure and only comparing the critical generation buses. Even though few power plants are identified as critical, it is important to pinpoint these infrastructures to identify the importance of generation assets to the KPG. We present the relative importance of just these infrastructures to determine which organizations may operate these few central plants. Here,  $B_v$  identifies only a single generation company, Korea Midland Power, as owning and operating critical infrastructure.  $EB_v^1$  and  $EB_v^2$  each identify multiple generation companies, but with varying importance of generation technologies.  $EB_v^1$  implicates thermoelectric power companies as more important than nuclear, and, in contrast,  $EB_v^2$  implicates the

exact opposite. Moreover,  $EB_v^2$  produces results quantitatively similar to the percent total installed generation capacity and is the only measure to suggest power producers not affiliated with KEPCO to own and operate critical buses.

We combine infrastructure scores for geographic regions to predict which emergency management headquarters may be involved in crisis response. Figure 3 presents the aggregated infrastructure results including a frequency plot of power generation and transmission infrastructure in South Korea compared and normalized criticality scores for infrastructure in each state and city region. Although more power system infrastructure is located in the northwest region surrounding the Seoul Metropolitan Area and the Southern coast (Figure 3(a)), the measures indicate that critical infrastructure may be located elsewhere. Method  $B_v$  suggests that the vast majority of critical infrastructure is located in the state Gyeonggi-do (GGD) surrounding Seoul and to a lesser extent the three states making up the center of the country: Chungcheongnam-do (CCND), Chungcheongbuk-do (CCBD), and Gyeongsangbuk-do (GSBD), from east to west, respectively (Figure 3(b)). Method  $EB_v^1$  produces results similar to the physical location of infrastructure with greater emphasis on the central and northwest regions of the country instead of Seoul and Incheon cities (Figure 3(c)). Method  $EB_v^2$

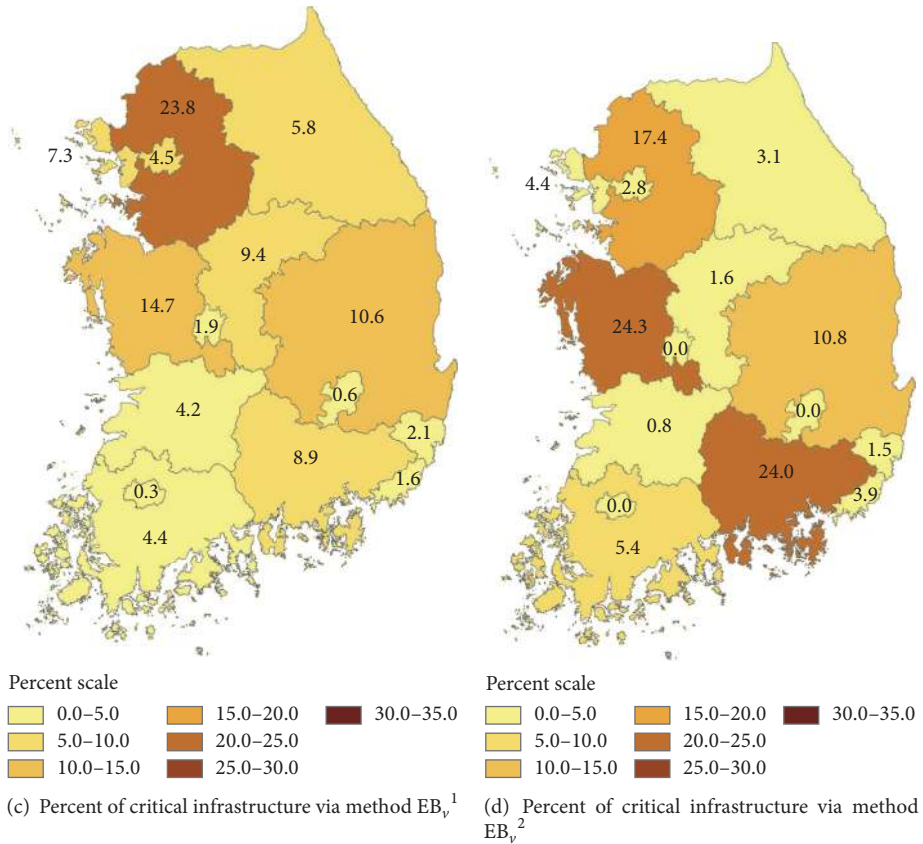
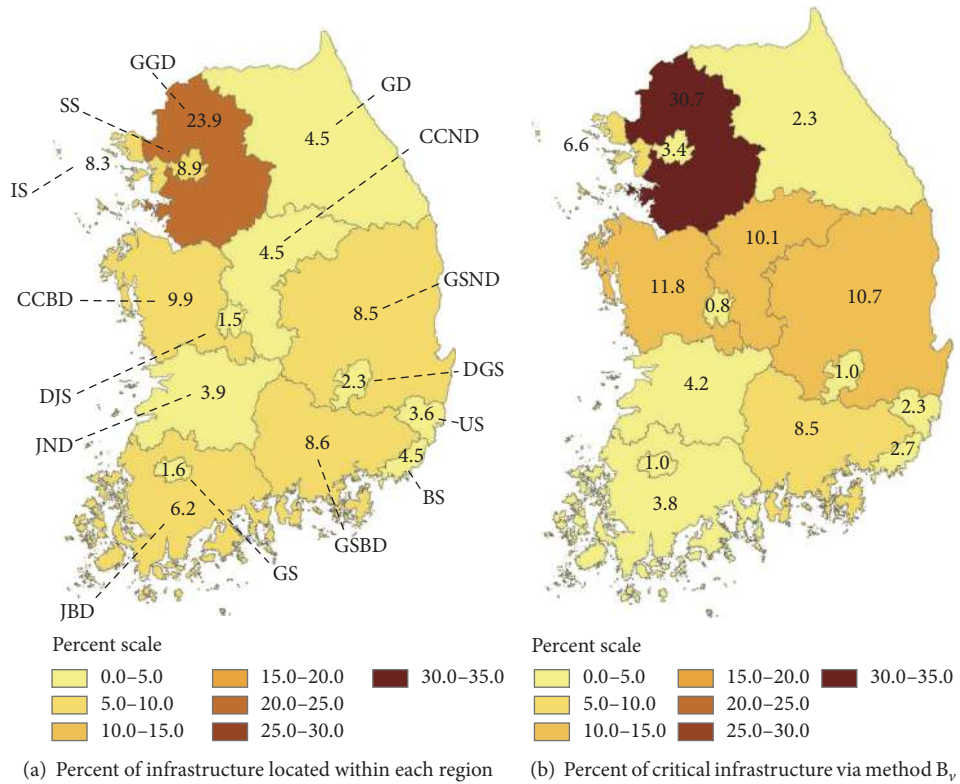


FIGURE 3: Aggregate criticality scores for Korean power grid infrastructure by emergency management region. The top left image of Korea presents the amount of generation and substation buses located in each region (a), where all other images show the normalized total criticality score for each region (b, c, and d). Thus, percent scale refers to quantity of infrastructure (a) and aggregated criticality score (b, c, and d). Regions are labelled in (a) with abbreviations: Gyeonggi-do (GGD), Gangwon-do (GD), Chungcheongnam-do (CCND), Chungcheongbuk-do (CCBD), Gyeongsangnam-do (GSND), Gyeongsangbuk-do (GSBD), Jeollanam-do (JND), Jeollabuk-do (JBD), Seoul-si (SS), Incheon-si (IS), Daejeon-si (DJS), Gwangju-si (GS), Daegu-si (DGS), Ulsan-si (US), and Busan-si (BS).



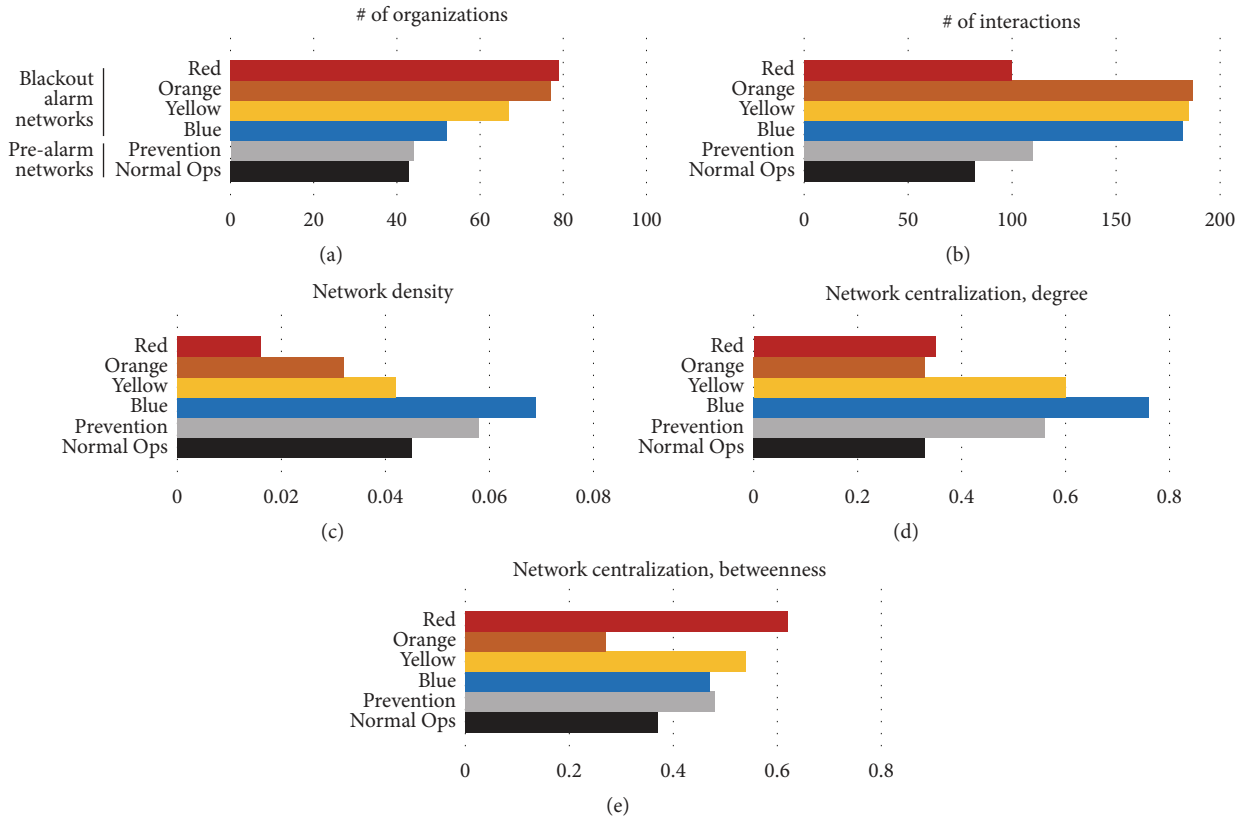


FIGURE 4: Network-level results for Korean blackout management social networks. We characterize the 6 blackout management social networks ( $y$ -axes) with five characteristic network-level measures ( $x$ -axes). (a-b) Social network size is measured by the total number of organizations and interactions (i.e., links). (c) Network density, (d) centralization of degree, and (e) centralization of betweenness are normalized values ranging from 0 to 1 (see Methods).

suggests that Gyeonggi-do (GGD) is not the most important region, but rather Chungcheongnam-do (CCND) and Gyeongsangnam-do (GSND), together, contain nearly 50% of all critical infrastructure (Figure 3(d)). Across all methods, the top ranked infrastructures are more often located in three states of Chungcheongnam-do (CCND), Gyeongsangnam-do (GSND), and Jeollabuk-do (JBD).

**4.2. Blackout Management Social Network Results.** Figure 4 presents general results of network analysis for the six blackout management social networks. Results show that formal policies produce social networks that have increasing organizational inclusion with blackout risk. Formal institutions assume that less risky scenarios require less regulated interactions among electric power and emergency management sectors, and vulnerable situations with lower reserve margins and greater grid instability require more oversight and federal involvement. This is represented in the network size (Figure 4(a)) as the number of organizations connected to the network almost doubles from 43 organizations in Normal Operations to 79 in Alarm Red. The majority of these new nodes represent either emergency managers or federal ministries not involved in minor blackouts, such as governor-level crisis management HQs and the Ministry of Defense.

The decision-making authority of the electric power industry peaks when the first blackout alarm is activated (Alarm Blue) and then shifts to the emergency management industry, as represented by the number of links (Figure 4(b)), network density (Figure 4(c)), and centralization of node degree (Figure 4(d)). All three measures show peaking trends as blackout alarms increase in severity. Even though the number of nodes among networks steadily increase with crisis risk level, the number of links peaks around ~180 links and then decreases to 100 at Alarm Red. This sudden drop in links corresponds with the transition of decision-making and information-sharing authority from the electric power to the emergency management industry. Moreover, the network density and centralization of degree peak at Alarm Blue and decrease across all four alarms, corresponding with the initial centralization of authority among the electric power industry and its diffusion into emergency management organizations as they join to the network.

Figure 4(e) also demonstrates variability in the centralization of blackout coordination activities among sectors with the centralization of betweenness. The centralization of betweenness increases across the first four networks, drops to its minimum at Alarm Orange, and is at its maximum in Alarm Red. The low centralization of betweenness of Alarm

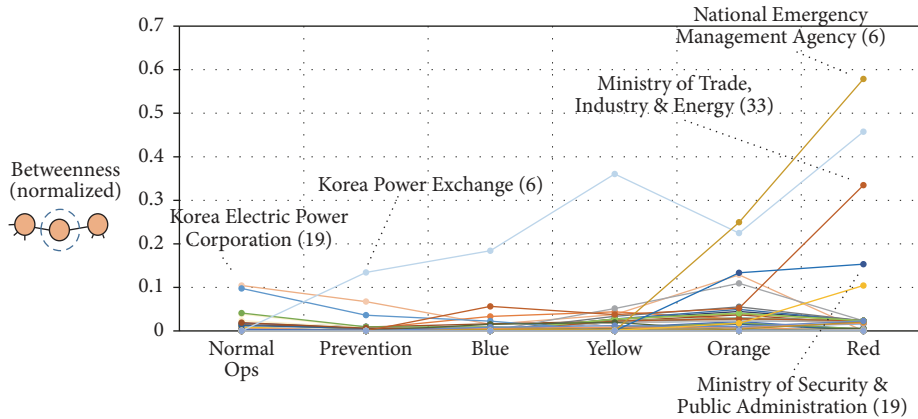


FIGURE 5: Betweenness and number of roles for Korean blackout management organizations. Each line represents a different organization. As the majority of organizations are periphery actors, they have low betweenness compared to few central, coordinating organizations. These central and important organizations are labelled: name (number of crisis management roles). Results demonstrate that few organizations from both electric power and emergency management sectors are the key crisis coordinator for different blackout risks, specifically KEPCO, KPX, and NEMA. In contrast, MOTIE and MOSPA are key decision-making organizations, yet they remain periphery to information brokerage.

Orange when compared to Alarm Yellow or Red corresponds to the electric power and emergency management industries sharing information brokerage activities almost equally for that interorganizational configuration. All other instances with high centralization of betweenness will have a single organization as the most central crisis coordinator.

Nodal betweenness identifies that organizations with fewer decision-making roles than others tend to broker information during blackouts. Betweenness results presented in Figure 5 identify the specific organizations that act as information hubs for blackout response. KEPCO and Gyeonggi-do Fire Mgmt. HQ share central crisis coordination roles for Normal Operations, KPX is the most central organization for Prevention, Alarm Blue, and Alarm Yellow, NEMA and KPX share coordination for Alarm Orange, and NEMA is the central coordinator for Alarm Red. These results correspond to general perspectives held by blackout management experts that either KPX or NEMA is the crisis management HQ for blackouts. Still, KPX and NEMA have fewer decision-making roles as outlined in formal protocols and may not be best suited for being the central information broker. The number of roles assigned to each organization (labelled next to its name) reveals that MOTIE (33), KEPCO (19), and MOSPA (19) have far more blackout management roles to fulfil than KPX (6) and NEMA (6). This result indicates that decisions made by authoritative organizations must travel through intermediary organizations before reaching their final destination.

## 5. Discussion

*5.1. Implications for Blackout Management Protocols from the Infrastructure Perspective.* Results suggest that certain generation companies may be more involved in future blackout scenarios. Current blackout management policies make limited differentiation between organizational roles between generation companies, which may be inappropriate when each company owns and operates different amounts of

critical infrastructure. For example, both  $B_v$  and  $EB_v^1$  would recommend that increased protection and recovery capacity be located at generation facilities owned and operated by Korea Midland Power, where  $EB_v^2$  results emphasize nuclear power plants managed by KHNP and relatively equivalent treatment of other KEPCO subsidiaries. Moreover,  $EB_v^2$  highlights differences among private power producers that manage an appreciable amount of critical infrastructure like SK Energy, Posco Power, and Daelim Mitsubishi that are not reflected in crisis management protocols. Based on these results, we recommend that crisis management policies make more explicit roles for the KEPCO subsidiaries and private power companies that operate these critical infrastructures to emphasize their potential involvement in blackout response.

Specific state and city headquarters have a greater chance of being the crisis management authority in large-scale blackout support activities than others. Combining results across measures, Chungcheongnam-do (CCND), Gyeongsangnam-do (GSND), and Jeollabuk-do (JBD) house more critical power grid infrastructure than other regions. Moreover, aggregate scores for regions consistently score states higher than cities, with Gyeonggi-do (GGD), Chungcheongnam-do (CCND), Gyeongsangbuk-do (GSBD), and Gyeongsangnam-do (GSND) receiving top ranks across multiple methods. Whereas existing national blackout management policies treat emergency management HQs equivalently, more focused policies may highlight power system protection and response in these regions. For example, the most recent blackout in Korea which occurred in the South-eastern region of Gyeongsangnam-do (GSND) was exacerbated as backup infrastructure was only housed in Seoul. Reorienting crisis response resources to match these results would have led to a shorter blackout duration by maintaining backup transformers near more critical substations.

*5.2. Implications of Blackout Management Protocols from the Social Network Perspective.* This analysis is the first to

take a system-wide perspective on blackout management and identify when decision-making and information-sharing authority shifts between industries. Policies and protocols outline explicit decision-making and information-sharing roles, and experts are aware of the interactions among multiple sectors. However, explicit transitions in authority are not outlined in formal institutions making it difficult for actors to predict which electric power or emergency management organization will be the central coordinating body when alarms are activated. Network-level analysis demonstrates a transition in authority between the electric power and emergency management industries associated with a drop in number of links, network density, average degree, and centralization of degree and an increase in centralization of betweenness. Decision-making is most centralized in the power industry for Alarm Blue and makes a transition to the emergency management industry between Alarms Orange and Red. Experts can use this information to determine if current reserve margin and power system stability measures are effective for creating the wanted decision-making context to handle blackout risk.

Betweenness results indicate that there may be a mismatch between blackout decision-making authority and information brokerage in South Korea, suggesting a need to restructure current policies. Although KPX and NEMA are identified as central hubs for power grid and emergency management information, they are not the central decision-makers. Having central actors involved in information-sharing is vital for successful blackout response, as effective coordination avoids the duplication of work, hindrance of first responders, delays due to misunderstanding, and inappropriate allocation of resources [62]. Crises including the 2011 Seoul Brownout, 2013 Corruption Scandal, 2014 Ferry Tragedy, and 2016 Blackout were exacerbated by hindrances like the infeasibility to centrally manage, role ambiguity, and unbalanced workload distribution. Restructuring blackout response policies to centralize actors with greater decision-making authority may alleviate this issue. MOTIE, in particular, is identified through interviews as an important organization for decision-making and oversight, yet a periphery node remains within all networks for information brokerage. Making MOTIE a central node is a possible way to improve coordination activities. We recommend doing this for intermediary networks that transition authority between sectors like Alarm Yellow and Orange as MOTIE has equal authority to other federal organizations where KPX does not. Thus, we recommend restructuring future policies to centralize MOTIE for Alarms Yellow and Orange to support decision-making and shifting authority among industries.

*5.3. Combined Guidance.* Completing infrastructure and interorganizational network analyses side-by-side offers combined recommendations to improve blackout management in South Korea. The results from both network analyses are complementary as infrastructure analysis identifies which periphery organizations own, operate, and respond to critical infrastructure failures and social network analysis identifies which organizations coordinate decision-making and information-sharing among them. Betweenness results for

the social network further indicate that there is a mismatch between organizational authority and information brokerage that may require updating protocols to restructure the network. While the above recommendations for improving formal policies may be helpful, they remain superficial by not specifying how improvements are to be made. For example, social network analysis can offer the recommendation to restructure the social network to centralize MOTIE for Alarms Yellow and Orange but cannot specify which paths or organizations should be involved in restructuring. Instead, the results from infrastructure network analysis identify critical organizations that should be involved in these heightened blackout risk scenarios. Our combined recommendation is then to restructure formal institutions to increase information flow among the power companies, Korea Midland Power, SK Energy, Posco Power, and Daelim Mitsubishi, the emergency management agencies in Chungcheongnam-do, Gyeongsangnam-do, and Jeollabuk-do, and MOTIE.

## 6. Conclusion

Blackouts continue to occur across the globe due to failed blackout coordination activities, and power grid resilience depends upon effective formal policies and protocols to handle emergency response. We identify critical cases in which blackout coordination does not match infrastructure failure needs in South Korea by conducting STNA with matching data from 2013 for KPG infrastructure and blackout management policies. In the KPG, separate analysis of infrastructure and interorganizational networks provides insight into the cause of recent, exacerbated events. Power grid criticality analysis shows that some infrastructures and organizations may be disproportionately involved in large-scale events, yet formal policies do not distinguish between them. Social network analysis characterizes the transition of authority among sectors and organizations to help guide more precise use of policies to manage future events. Still, each analysis on its own can only provide broad recommendations for improving institutions rather than specific changes to policy. Combined results instead pinpoint the specific social networks and organizations that needed to be changed when updating future policies.

This work demonstrates that the growing number of studies comparing criticality measures for other real-world power systems [57, 63–65] or developing social networks around infrastructure systems [23] would benefit from linking technological analyses to social context. Since the majority of academic literature does not bridge infrastructure and social contexts, power grid protection and resilience may be undermined by overlooking the social consequences of technical recommendations. The inclusion of ownership and jurisdictional boundaries in this work revealed Korean organizations whose actions may have greater influence on power grid protection than others. In interconnected grids, a similar analysis may highlight local decision-makers that have disproportionate authority over power system security that crosses utility, state, and country borders. The same is true for social network analysis of actors that manage infrastructure systems. Taking a public administration

perspective while ignoring the interconnected and complex infrastructure system it surrounds may overlook salient interactions that connect social entities but exist in the technology. Crisis management protocols made without reference to the physical limitations of existing infrastructure creates latent weaknesses embedded in policy which may exacerbate damages in future emergencies. The sociotechnical network analysis presented herein offers one way to overcome these issues.

## Disclosure

Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF or NRF.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

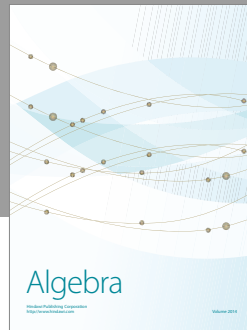
The authors would like to acknowledge Donghwan Kim for assistance with analysis, Younghun Chun for helping acquire South Korean power system data, and Taehun Lee for assisting with translation of technical documents. This material is based upon work supported by the National Science Foundation (NSF) (Grants nos. 1311230, 1441352, and 1415060). Jeryang Park was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2016RIC1B1011770).

## References

- [1] R. L. Wilby and R. Keenan, "Adapting to flood risk under climate change," *Progress in Physical Geography*, vol. 36, no. 3, pp. 348–378, 2012.
- [2] Department of Homeland Security (DHS), *National Infrastructure Protection Plan (NIPP): Partnering for critical infrastructure security and resilience*, 2013.
- [3] United Nations International Strategy for Disaster Reduction, *Hyogo Framework For Action 2005-2015: Building the resilience of nations and communities to disasters*, 2007.
- [4] The Rockefeller Foundation and ARUP, *City Resilience Index*, 2015, The Rockefeller Foundation and ARUP, "City Resilience Index," p. 16, 2015.
- [5] *Committee on Determinants of Market Adoption of Advanced Energy Efficiency and Clean Energy Technologies, The Power of Change: Innovation for Development and Deployment of Increasingly Clean Electric Power Technologies*, The National Academies Press, 2016.
- [6] *Committee on Analytical Research Foundations for the Next-Generation Electric Grid, Analytic Research Foundations for the Next-Generation Electric Grid*, The National Academies Press, 2016.
- [7] *Quadrennial Energy Review Task Force, The Department of Energy (DOE), Quadrennial Review: Transforming the Nation's Electricity System: The Second Installment of the Quadrennial Energy Review*, 2017.
- [8] North American Electric Reliability Corporation, *September 2011 Southwest Blackout Event*, 2011.
- [9] O. P. Veloza and F. Santamaria, "Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes," *The Electricity Journal*, vol. 29, no. 7, pp. 42–49, 2016.
- [10] C.-C. Sun, C.-C. Liu, and J. Xie, "Cyber-physical system security of a power grid: State-of-the-art," *Electronics (Switzerland)*, vol. 5, no. 3, article no. 40, 2016.
- [11] Australian Energy Market Operator (AEMO), *Preliminary Report 3rd Oct – Black System Event in South Australia on 28 September 2016*, Report no. September, 2016.
- [12] M. M. Adibi and L. H. Fink, "Restoration from cascading failures," *IEEE Power & Energy Magazine*, vol. 4, no. 5, pp. 68–77, 2006.
- [13] M. Panteli and P. Mancarella, "The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience," *IEEE Power & Energy Magazine*, vol. 13, no. 3, pp. 58–66, 2015.
- [14] M. Panteli and P. Mancarella, "Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies," *Electric Power Systems Research*, vol. 127, pp. 259–270, 2015.
- [15] M. Panteli and P. Mancarella, "Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events," *IEEE Systems Journal*, vol. PP, no. 99, 2015.
- [16] P. Pourbeik, P. S. Kundur, and C. W. Taylor, "The anatomy of a power grid blackout," *IEEE Power & Energy Magazine*, vol. 4, no. 5, pp. 22–29, 2006.
- [17] G. Andersson, P. Donalek, R. Farmer et al., "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1922–1928, 2005.
- [18] D. Kirschen and F. Bouffard, "Keep the Lights On and the Information Flowing," *IEEE Power & Energy Magazine*, vol. 7, no. 1, pp. 50–60, 2009.
- [19] G. Walker, "Come back sociotechnical systems theory, all is forgiven . . ." *Civil Engineering and Environmental Systems*, vol. 32, pp. 170–179, 2015.
- [20] Korea Power Exchange (KPX), *Korea Power Exchange Transmission Map*, 2016, <https://www.kpx.or.kr/eng/contents.do?key=333>.
- [21] M. E. J. Newman, *Networks: An Introduction*, Oxford University Press, Oxford, UK, 2010.
- [22] F. Hu, A. Mostashari, and J. Xie, Eds., *Socio-Technical Networks: Science and Engineering Design*, CRC Press, 2011.
- [23] A. Vespignani, "Modelling dynamical process in complex socio-technical systems," *Nature Physics*, vol. 8, no. 1, pp. 32–39, 2012.
- [24] P. M. Salmon, N. A. Stanton, G. H. Walker, D. Jenkins, C. Baber, and R. McMaster, "Representing situation awareness in collaborative systems: A case study in the energy distribution domain," *Ergonomics*, vol. 51, no. 3, pp. 367–384, 2008.
- [25] N. A. Stanton, "Representing distributed cognition in complex systems: How a submarine returns to periscope depth," *Ergonomics*, vol. 57, no. 3, pp. 403–418, 2014.
- [26] N. A. Stanton and C. Harvey, "Beyond human error taxonomies in assessment of risk in sociotechnical systems: a new paradigm with the EAST 'broken-links' approach," *Ergonomics*, vol. 60, no. 2, pp. 221–233, 2017.

- [27] D. A. Eisenberg, J. Park, D. Kim, and T. P. Seager, "Resilience analysis of critical infrastructure systems requires integration of multiple analytical techniques," *Urban Sustainability and Resilience*, 2014.
- [28] S. Amir and V. Kant, "Sociotechnical Resilience: A Preliminary Concept," *Risk Analysis*, 2017.
- [29] P. H. J. Nardelli, N. Rubido, C. Wang et al., "Models for the modern power grid," *The European Physical Journal Special Topics*, vol. 223, no. 12, pp. 2423–2437, 2014.
- [30] K. M. Carley, "Computational organizational science and organizational engineering," *Simulation Modelling Practice and Theory*, vol. 10, no. 5-7, pp. 253–269, 2002.
- [31] K. Jung and M. Song, "Linking emergency management networks to disaster resilience: Bonding and bridging strategy in hierarchical or horizontal collaboration networks," *Quality & Quantity*, vol. 49, no. 4, pp. 1465–1483, 2015.
- [32] N. Kapucu and V. Garayev, "Designing, Managing, and Sustaining Functionally Collaborative Emergency Management Networks," *The American Review of Public Administration*, vol. 43, no. 3, pp. 312–330, 2013.
- [33] N. Kapucu and V. Garayev, "Structure and Network Performance: Horizontal and Vertical Networks in Emergency Management," *Administration and Society*, vol. 48, no. 8, pp. 931–961, 2016.
- [34] T. Kim, *Blackouts Hit Korea Nationwide*, The Korea Times, 2011.
- [35] C. Sang-Hu, *Scandal in South Korea over nuclear revelations*, New York Times, 2013.
- [36] T.-E. Kim, S. Nazir, and K. I. Øvergård, "A STAMP-based causal analysis of the Korean Sewol ferry accident," *Safety Science*, vol. 83, pp. 93–101, 2016.
- [37] Y. Kim and H. Kim, "Improving Korea's societal security by preparing for unforeseen disasters: Focused on the horizontal collaboration approach," *International Journal of Security and Its Applications*, vol. 10, no. 3, pp. 11–20, 2016.
- [38] D. H. Kim, D. A. Eisenberg, Y. H. Chun, and J. Park, "Network topology and resilience analysis of South Korean power grid," *Physica A: Statistical Mechanics and its Applications*, vol. 465, pp. 13–24, 2017.
- [39] Korea Power Exchange (KPX), *Electric Power Statistics Information System*, 2016, <http://epsis.kpx.or.kr/epsis/ekesStaticMain.do?sessionId=Y0JXXWdKvpwzLnLpXTn5fy0Z4sLvbZzlQytHgtwF2kN2phJJQsR1241999982?cmd=001001&flag=&locale=EN>.
- [40] D. Ngar-yin Mah, J. M. van der Vleuten, J. Chi-man Ip, and P. Ronald Hills, "Governing the transition of socio-technical systems: A case study of the development of smart grids in Korea," *Energy Policy*, vol. 45, pp. 133–141, 2012.
- [41] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.
- [42] *Matlab Tools for Network Analysis (2006-2011)*, 2011, [http://strategic.mit.edu/downloads.php?page=matlab\\_networks](http://strategic.mit.edu/downloads.php?page=matlab_networks).
- [43] D. Gleich, *MatlabBGL*, 2008, <https://www.mathworks.com/matlabcentral/fileexchange/10922-matlabagl?requestedDomain=www.mathworks.com>.
- [44] S. P. Borgatti, "Centrality and network flow," *Social Networks*, vol. 27, no. 1, pp. 55–71, 2005.
- [45] M. Rosas-Casals, S. Bologna, E. F. Bompard et al., "Knowing power grids and understanding complexity science," *International Journal of Critical Infrastructures*, vol. 11, no. 1, pp. 4–14, 2015.
- [46] N. Kapucu, "Interorganizational Coordination in Dynamic Context: Networks in Emergency Response Management," *Connections*, vol. 26, no. 2, pp. 33–48, 2005.
- [47] A. B. M. Nasiruzzaman, H. R. Pota, and M. A. Mahmud, "Application of centrality measures of complex network framework in power grid," in *Proceedings of the 37th Annual Conference of the IEEE Industrial Electronics Society, IECON 2011*, pp. 4660–4665, aus, November 2011.
- [48] A. B. M. Nasiruzzaman, H. R. Pota, and A. Anwar, "Comparative study of power grid centrality measures using complex network framework," in *Proceedings of the 2012 IEEE International Power Engineering and Optimization Conference, PEOCO 2012*, pp. 176–181, mys, June 2012.
- [49] A. B. M. Nasiruzzaman, H. R. Pota, A. Anwar, and F. R. Islam, "Modified centrality measure based on bidirectional power flow for smart and bulk power transmission grid," in *Proceedings of the 2012 IEEE International Power Engineering and Optimization Conference, PEOCO 2012*, pp. 159–164, mys, June 2012.
- [50] A. B. M. Nasiruzzaman and H. R. Pota, "Transient stability assessment of smart power system using complex networks framework," in *Proceedings of the 2011 IEEE PES General Meeting: The Electrification of Transportation and the Grid of the Future*, usa, July 2011.
- [51] A. B. Nasiruzzaman and H. R. Pota, "Complex network framework based comparative study of power grid centrality measures," *International Journal of Electrical and Computer Engineering*, vol. 3, no. 4, 2013.
- [52] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 19, no. 1, Article ID 013119, 2009.
- [53] E. Bompard, R. Napoli, and F. Xue, "Extended topological approach for the assessment of structural vulnerability in transmission networks," *IET Generation, Transmission & Distribution*, vol. 4, no. 6, pp. 716–724, 2010.
- [54] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, 2011.
- [55] G. C. Ejebe, J. Tong, J. G. Waight, J. G. Frame, X. Wang, and W. F. Tinney, "Available transfer capability calculations," *IEEE Transactions on Power Systems*, vol. 13, no. 4, pp. 1521–1527, 1998.
- [56] A. J. Wood, B. F. Wollenberg, and G. B. Sheble, *Power Generation, Operation, and Control*, John Wiley & Sons, 2014.
- [57] E. Bompard, L. Luo, and E. Pons, "A perspective overview of topological approaches for vulnerability analysis of power transmission grids," *International Journal of Critical Infrastructures*, vol. 11, no. 1, pp. 15–26, 2015.
- [58] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Systems Journal*, vol. 6, no. 3, pp. 481–487, 2012.
- [59] K. M. Carley, J. Pfeffer, J. Reminga, J. Storricks, and D. Columbus, "ORA User's Guide 2013," Defense Technical Information Center, 2013.
- [60] A. Abbasi and N. Kapucu, "A longitudinal study of evolving networks in response to natural disaster," *Computational and Mathematical Organization Theory*, vol. 22, no. 1, pp. 47–70, 2016.
- [61] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, vol. 1, no. 3, pp. 215–239, 1978-1979.
- [62] B. Petrenj, E. Lettieri, and P. Trucco, "Towards enhanced collaboration and information sharing for critical infrastructure

- resilience: Current barriers and emerging capabilities,” *International Journal of Critical Infrastructures*, vol. 8, no. 2-3, pp. 107–120, 2012.
- [63] E. P. R. Coelho, J. C. Thomazelli, M. H. M. Paiva, and M. E. V. Segatto, “A complex network analysis of the Brazilian Power Test System,” in *Proceedings of the IEEE PES Innovative Smart Grid Technologies Latin America, ISGT LATAM 2015*, pp. 113–118, ury, October 2015.
- [64] Z. Wang, A. Scaglione, and R. J. Thomas, “Electrical centrality measures for electric power grid vulnerability analysis,” in *Proceedings of the 2010 49th IEEE Conference on Decision and Control, CDC 2010*, pp. 5792–5797, usa, December 2010.
- [65] H. Bai and S. Miao, “Hybrid flow betweenness approach for identification of vulnerable line in power system,” *IET Generation, Transmission & Distribution*, vol. 9, no. 12, pp. 1324–1331, 2015.




**Hindawi**

Submit your manuscripts at  
<https://www.hindawi.com>

