State-of-the-Art Review

Assessment Methods of Network Resilience for Cyber-Human-Physical Systems

Sisi Duan, Ph.D.[1]; and Bilal M. Ayyub, Ph.D., P.E., Dist.M.ASCE[2]

Abstract: Cyber-human-physical systems are deeply intertwined systems of physical components, cyber components, and human activities. Cyber components provide communication and control to the physical systems. In addition, human activities can affect or be affected by the behaviors of cyber and physical components. Modern critical infrastructures are a perfect example of such systems. Specifically, physical infrastructures (e.g., power grid, transportation) rely heavily on cyber infrastructures [e.g., supervisory control and data acquisition (SCADA) system] for control and monitoring. Also, humans interact with critical infrastructures in a complex way such that the resilience of critical infrastructures can be heavily affected by human activities. Indeed, critical infrastructures can suffer as a result of both large-scale events such as natural disasters and all kinds of other types of events such as cyber attacks and human operational errors. Therefore, the modeling and analysis of such complex systems are desirable. Such complex systems and their behavior can be modeled appropriately by networks for the purpose of assessing their key attributes, such as resilience. This paper provides an in-depth review of the network modeling and analysis approaches for cyber-human-physical systems. The focus of this paper is critical infrastructures, while the reviewed approaches can also be applied in other application domains. **DOI: 10.1061/AJRUA6.0001021.**

Introduction

Modern cyber-physical systems, such as critical infrastructures (CIs), are vital to a country's national security, economy, and public safety and wellbeing. The resilience, continuous operation, protection, maintenance, and safety of CIs are national priorities. Indeed, the disruption of any system can trigger widespread failures in other infrastructures. The 2003 Italian blackout (Johnson 2007), 2003 Northeast US power outage (US–Canada Power System Outage Task Force 2004; Cowie et al. 2003), 2011 Southwest blackout (FERC/NERC 2012), and 2002 Hurricane Sandy (Kwasinski 2012; Agency 2013; FEMA 2013) are all examples of such interdependency. For instance, the 2003 massive Northeast US blackout was triggered by the failures of 3 transmission lines, which spread across several US states and affected nearly 50 million people. It cascaded to drinking and wastewater treatment systems, transportation, and communication systems.

Large-scale natural disasters such as hurricanes and earthquakes can cause considerable damage to physical infrastructures. Their vulnerabilities, however, can also be triggered or amplified by other scales and types of events, such as cyber attacks and human activities. Indeed, modern infrastructure systems rely heavily on cyber systems such as supervisory control and data acquisition (SCADA) systems (Boyer 2009) to monitor and control physical systems, e.g., power grids. Therefore, the resilience of the physical systems can be improved. Cyber attacks, however, can cause a severe impact on infrastructures. For instance, the Stuxnet worm (Falliere et al. 2011; Karnouskos 2011) against Iranian nuclear uranium enrichment facilities caused substantial damage to Iran's nuclear program and ruined almost one-fifth of Iran's nuclear centrifuges. Similarly, malware, such as BlackEnergy crimeware (F-Secure Labs 2016) against the Ukranian railway and electric power industries, Duqu (Chien et al. 2011), Havex (Rrushi et al. 2015), and Harvey (Garcia et al. 2017), shows that targeted attacks on critical infrastructures can evade traditional cybersecurity detection and cause catastrophic failure across countries. On the other hand, human activities, such as movement during evacuation (Barrett et al. 2010), maintenance of infrastructures, and social interaction, can cause significant impacts on critical infrastructures. To this end, the term *cyber-human-physical system* (CHPS) better captures all the nonphysical factors in today's interconnected cyber-physical systems.

As pointed out by *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21)*, published in 2015, dependencies and interdependencies and their integration into risk management and business continuity processes are important issues. A significant concern is the cybersecurity threat to industrial control systems (ICSs), as well as the interdependencies and cascading effects on physical security in federal facilities. Furthermore, as noted in the 2014 Department of Homeland Security Quadrennial Review (QHSR), the interconnected cyber-physical infrastructure consists of multiple systems that rely on one another to greater degrees for their operations and, at times, operate independently of human direction.

The term *resilience* has been used and studied in various domains such as ecology, psychology, computer systems, and critical infrastructure systems. It has been defined in different ways depending on the application scenarios. In a network, resilience refers to the capability of a network to defend against and maintain an acceptable level of service in the presence of uncertainties and potential failures and disruptions. Network resilience has been variously defined (Bruneau et al. 2003; Ayyub 2015; Gilbert and Ayyub 2016; Gao et al. 2016) and studied in different CHPSs (Johansen and Tien 2018; Ibáñez et al. 2016; Dwiartama and Rosin 2014; Masys 2016), which represents the capability of a system to recover from disruptions.

This article provides a comprehensive review of network resilience approaches in CHPSs. Specifically, the focus of the paper is

[1]Assistant Professor, Dept. of Information Systems, Univ. of Maryland, Baltimore County, MD 21250 (corresponding author). Email: sduan@umbc.edu

[2]Professor, Dept. of Civil and Environmental Engineering, Univ. of Maryland, College Park, MD 20742. Email: ba@umd.edu

Note. This manuscript was published online on October 22, 2019. Discussion period open until March 22, 2020; separate discussions must be submitted for individual papers. This paper is part of the ***ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering***, © ASCE, ISSN 2376-7642.

the modeling and analysis of critical infrastructures. However, the approaches, especially the analysis approaches reviewed here, can be applied in broader application domains such as supply chain resilience, business continuity, and others. Compared to previous efforts in summarizing the studies of CIs, this paper makes the following contributions. First, it provides an in-depth review of network-based modeling and analysis, which is one of the most efficient and effective methods in analyzing CIs. This attribute is a characteristic of network-based approaches that can support various tasks such as disaster management and risk analysis. Second, during the review, the modeling of CIs in networks and analytic approaches are intentionally separated. Such an organization contributes to enhancing the understanding and challenges, including the trade-offs of different approaches. Furthermore, different sections of the paper might be appealing to different groups of readers. Finally, this paper also provides a literature review of modeling nonphysical factors, i.e., cyber interdependency of the infrastructures and human factors.

This paper is organized as follows. A review is first provided on the definitions of resilience, network, and cyber-human-physical systems, followed by an overview of application domains of network resilience. Since this paper focuses on critical infrastructures as one application domain, the definitions and categories of ICIs are also provided. Then the network modeling and analysis approaches are categorized and described in detail. Finally, the approaches are compared, followed by a brief review of network resilience in other application domains and a summary of future research directions.

Network Resilience: Terms and Definitions

This section provides an overview of the definitions of network and resilience and the models to quantify resilience for a system.

Definitions of Resilience

The concept of resilience appears in different domains such as ecology, psychology, and infrastructure systems, as summarized in what follows (Ayyub 2014b, 2015; Henry and Ramirez-Marquez 2012; Hosseini et al. 2016):

- In ecology, resilience is defined as the persistence of relationships within a system and measured by the system's ability to absorb change-state variables, driving variables, and parameters and still persist (Holling 1973).
- In psychology, resilience is an individual's tendency to cope with stress and adversity.
- In the Presidential Policy Directive (PPD-21) (PPD 2013) on Critical Infrastructure Security and Resilience, the term resilience means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
- The National Research Council (Cutter et al. 2013) defines resilience as the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events as a consistent definition with US governmental agency definitions, i.e., Subcommittee on Disaster Reduction (SDR) (Bruneau et al. 2006), Department of Homeland Security (DHS) (DHS Risk Steering Committee 2008), PPD-8 (PPD 2011), and NRC (2011).
- The ASCE Committee on Critical Infrastructure (ASCE 2006) states that resilience refers to the capability to mitigate against significant all-hazards risks and incidents and to expeditiously recover and reconstitute critical services with minimum damage to public safety and health, the economy, and national security.
- The National Infrastructure Advisory Council defines infrastructure resilience as the ability to reduce the magnitude or duration of disruptive events. The effectiveness of a resilient system depends upon its ability to anticipate, absorb, adapt to, or rapidly recover from a potentially disruptive event.

Ayyub (2014b) further defined resilience according to the PPD-21 (PPD 2013) as follows:

- Resilience notionally means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from disturbances of the deliberate attack types, accidents, or naturally occurring threats or incidents. The resilience of a system's function can be measured based on the persistence of a corresponding functional performance under uncertainty in the face of disturbances.

Resilience Models

Resilience can be quantified. For instance, Bruneau et al. (2003) proposed the concept of *resilience triangle*, which is widely used in the study of infrastructure networks (Zhang et al. 2018a). Specifically, the resilience triangle quantifies the loss of resilience after performance disruption. Assume that the performance index is $Q(t)$. When disruption takes place at time t_0 and the network recovers to the original level Q_0 using t_h time, a generic framework (Bocchini and Frangopol 2012) of resilience index R_{e1} can be defined as follows:

$$R_{e1} = \frac{\int_{t_0}^{t_0+t_h} Q(t)dt}{t_h Q_0} \tag{1}$$

Ayyub (2014b) provided a schematic representation of a system performance $Q(t)$ with aging effects and an incident occurrence with a rate (λ) according to a Poisson process. Such a resilience index takes a few simple inputs such as the probability of failure p and system capacity Q_0, and it offers the simplicity and practicality desired for systems with time-invariant performance.

Network

A network can be represented as a graph, which consists of nodes/vertices and links/edges. The graph can be an undirected graph, where all the edges are bidirectional, or a directed graph, where the edges have a direction associated with them. A weighted graph (in contrast to an unweighted graph) is a graph in which each edge is given a numerical value called a weight. A simple graph (also called a strict graph) is an undirected and unweighted graph without any graph loops or multiple edges (Gibbons 1985; West 2001). A bipartite graph (also called a bigraph) is a set of graph nodes decomposed into two disjoint sets such that no two graph nodes within the same set are adjacent. A bipartite graph is a special case of a k-partite graph, which can be directed or undirected, weighted or unweighted. Network topology refers to the physical or logical layout of the network. In the rest of the text, *network* and *graph* are used interchangeably.

A single-layer graph consists of one graph, as shown in Fig. 1(a). In contrast, as illustrated in Fig. 1(b), a multilayer graph consists of multiple layers of single-layer networks (Boccaletti et al. 2014; Kivelä et al. 2014; Danziger et al. 2014). The different layers of a network can be heterogeneous. In addition to the edges in each layer, nodes in the different layers may be connected by edges that represent certain relationships that are different from those in single-layer

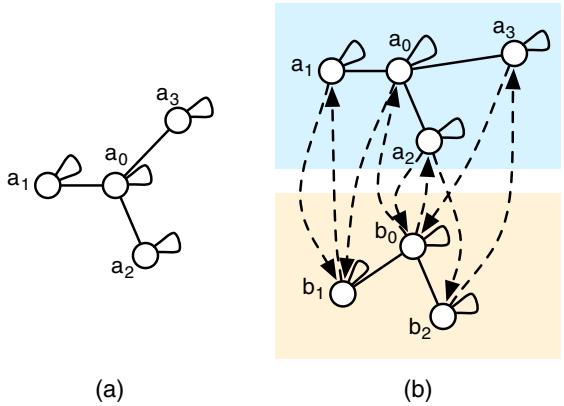

Fig. 1. Examples of graphs.

networks. Therefore, a multilayer network is also called a network of networks.

In network science or computer science, network theory is part of graph theory. The graphs can be represented as mathematical structures to model pairwise relations between objects/nodes. A flow network is a directed graph where each edge has a capacity, i.e., each edge receives a flow. In other words, the graph is weighted where the capacity of the edges are represented as weights.

Network Resilience in Cyber-Human-Physical Systems

This section defines CHPSs and reviews the need to study CHPSs, followed by an overview of application domains of network resilience, including critical infrastructures and supply chains. Furthermore, an overview of the categories of interdependent critical infrastructures is presented at the end of the section.

Cyber-Human-Physical Systems

Analyzing cyber-physical systems (CPSs) entails the integrations of relevant computations, network attributes, and physical processes. CPS naturally involves humans in the loop. Therefore, the term *cyber-human-physical systems* better captures all the factors in a CPS. The components in CHPSs are summarized in Fig. 2. The physical systems include applications such as military services and critical infrastructures. The cyber element of CHPS refers to the components that provide control, communication, and monitoring to the physical systems. On the other hand, the human element considers human activities that can affect or be affected by the other two elements, such as the economy, decision-making, and normal operations. In addition to the physical failures of traditional physical systems, cyber infrastructures may suffer from cyber failures caused by various factors, for example, adversary attacks or software bugs. Furthermore, human activities can cause both physical failures and cyber failures.

With the development of modern cyber technologies, communication systems have come to play an increasingly important role in today's infrastructure networks. Although cyber technologies have been shown to greatly increase the resilience of existing infrastructures, failures or cyber attacks can have a severe impact on many interdependent infrastructures (Zhu et al. 2011; Menashri and Baram 2015; Ebrahimy 2014). Waterfall Security Solutions (2017) published 20 cyber attacks against industrial control systems (ICSs). The attacks can have severe nationwide impacts on different sectors such as energy (Liu et al. 2011; Taft and Becker-Dippmann 2015), water (Amin et al. 2013), and transportation systems, ranging from extensive physical system downtime to false safety alarms and physical destruction. Because the number of Internet-accessible ICSs is increasing every year and smart technologies evolve (Siemens 2012; GL Communications 2008), the cyber threat is increasing in terms of the management of critical infrastructures. For instance, a cyber attack on the Washington, DC metro system in 2017 caused a disconnection between the control center and the tracks, which lasted for approximately 10 min. The small disruption, however, added as much as 90 min to some riders' commutes. Similar attacks on different sectors have been shown to have different types of losses, such as financial or physical damage (Duggan 2014).

Human activities, such as decision-making processes, movement (Cresswell 2010), and maintenance (Graham and Thrift 2007), can have a significant impact on the efficiency of critical infrastructures (Petit and Lewis 2017). For instance, evacuation due to events such as a subway fire could lead to changes in people's activity patterns (Chen et al. 2015, 2017b). Human behavior such as mobile phone usage can lead to the overloading of cellular towers and loss of cellular signals. In other words, human activities cause the interactions of communication systems and transportation systems. Such relationships, however, are difficult to capture. Furthermore, there is a balance between decreasing the impact of human-related social and economic activities and cyber events. For example, automatic systems such as automatic train (Siemens 2012) and SCADA systems (GL Communications 2008; Sivanandam 2016) aim at mitigating potential human errors. However, these could pose new safety, security, and resilience challenges (Petit and Lewis 2017).

Application Domain Overview

Network analysis can be used in a broad range of applications, for example, computer science, social science, and ecology. In this paper, network resilience in two major application domains in CHPSs are considered: critical infrastructures and supply chains. The paper presents an in-depth review of modeling and analysis in critical infrastructures and an overview of applying the approaches to supply chains.

The DHS identifies 16 critical infrastructure sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors/materials/waste, transportation systems, and water and wastewater systems (Department of Homeland Security 2018).

Most critical infrastructures can be represented naturally as networks. As illustrated in Fig. 3, this paper summarizes six key components in networks: *topologies, flows, components, functions, performance*, and *attributes*. Topologies, flows, and components together define the model of a network. For instance, a transportation system can be represented as a single-layer graph. Components such as stations and intersections are nodes, while others, such as roads and railroads, are edges. The flows are people or vehicles. Specifically, the weights of the network can be used to represent the capacity of the edges, and the real flow can be used to represent the actual traffic. The topologies of such a network can be either dynamic or static depending on the models. The size of the topology can be represented as different scales or types of networks, e.g., a small world network (Watts and Strogatz 1998; Latora and Marchiori 2002; Sen et al. 2003). The *functions* of networks can be used to describe actual CHPSs, e.g., transportation systems. Furthermore, *network performance* represents the functionalities or efficiency of real CI systems, e.g., the maximum number of vehicles

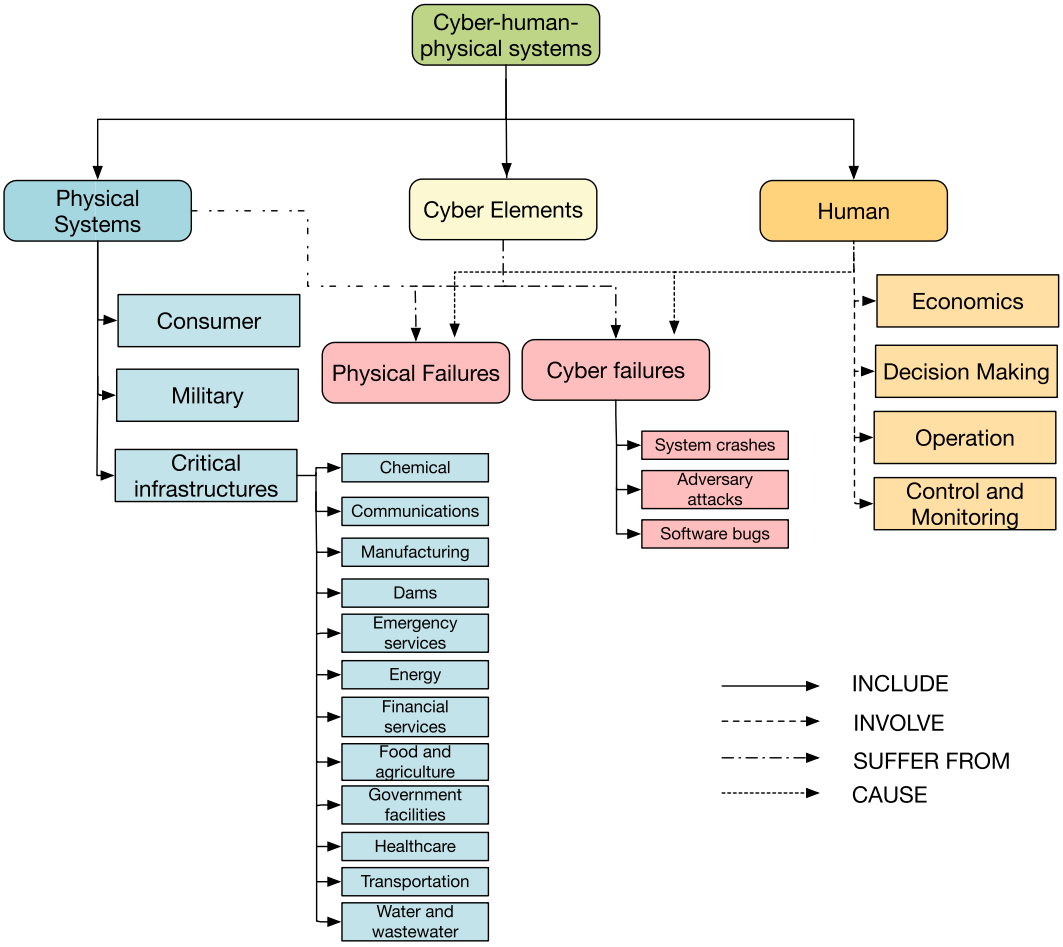

Fig. 2. Concept map of cyber-human-physical systems.

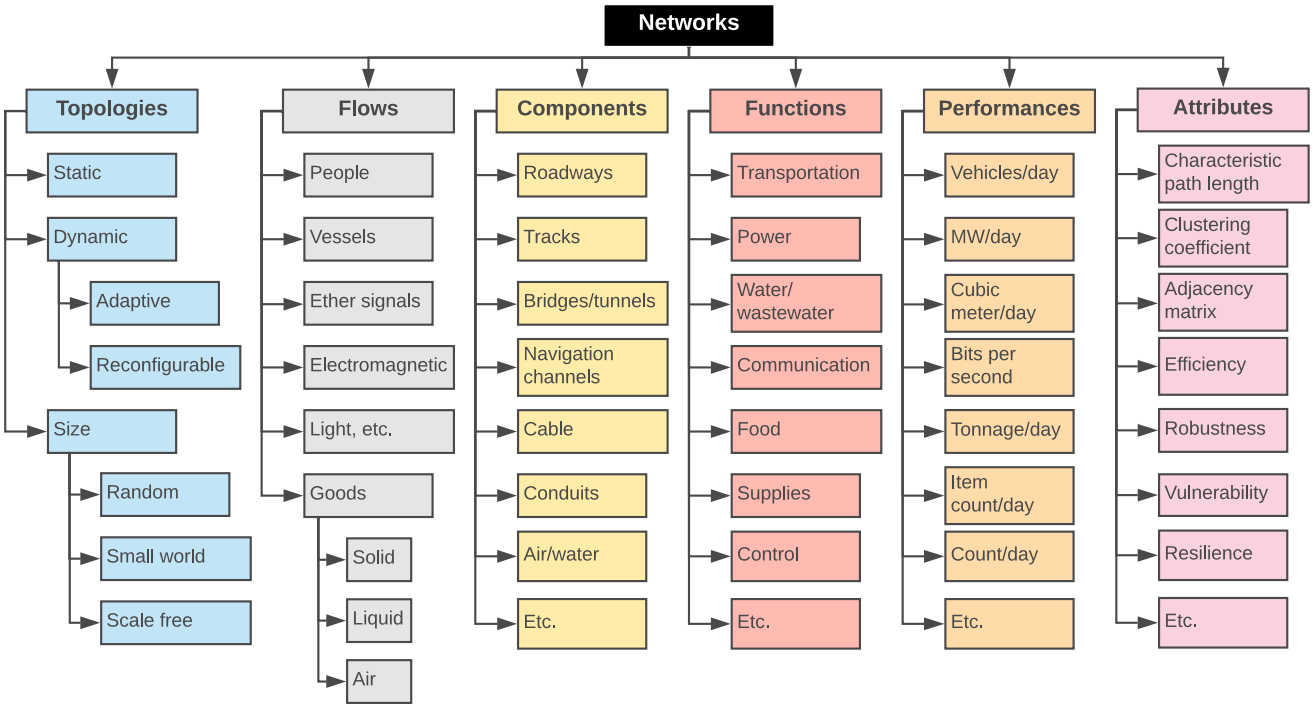

Fig. 3. Network classifications.

that passes through a particular road every hour. Because Cis are modeled CIs as networks, network attributes from network theory can be used to analyze the behavior of CHPSs. For instance, node degrees or clustering coefficients can be used to measure how networks are connected.

Surana et al. (2005) defined the function of a supply chain as transfering information, products, and money among suppliers and raw materials, manufacturers, distributors, retailers, and consumers. Like critical infrastructures, disruptions in the supply chain can have severe impacts. A supply chain can also be naturally modeled as a network (Perera et al. 2015). Specifically, the nodes represent spatially stable entities (e.g., manufacturers, distributors, warehouses, and retailers). Also, the edges represent the interactions between nodes through transportation, communication, and logistic routes between nodes, for example. Network flow or weights can be used to describe the information flow or the flows of goods among nodes.

Interdependent Critical Infrastructures

Critical infrastructures are naturally dependent on each other, so that the failure of one CI component can cause other components to fail (Vespignani 2010). *Dependency* refers to the unidirectional relationship, whereas *interdependency* connotes bidirectional interactions (Rinaldi et al. 2001). The interactions between a critical infrastructure and its environment can be categorized as *inner-infrastructure interdependency* and *inter-infrastructure interdependency*, defined in what follows:

- Inner-infrastructure interdependency [also called internal interdependencies (Rinaldi et al. 2001; Petit et al. 2015)]: As stated by Rinaldi et al. (2001), this refers to the interactions among internal operations, functions, and missions of the infrastructure. Internal dependencies are the internal links among the assets constituting a critical infrastructure (e.g., an electric generating plant that depends on cooling water from its own onsite water well).
- Inter-infrastructure interdependency: This refers to the interactions of different infrastructures.

In terms of types of failure, there are two types: *cascading* and *escalating failures*.

- Cascading failures: Failures in one infrastructure component subsequently cause failures in other components.
- Escalating failures: The disruption of one component can cause the independent disruption of another component.

Different papers categorize interdependencies into different types (Rinaldi et al. 2001; Zimmerman 2001; Dudenhoeffer et al. 2006; Zhang and Peeta 2011; Petit et al. 2015). This paper summarizes and groups them into three major categories: *physical*, *cyber*, and *social and economic interdependencies*. The types of interdependencies can be briefly defined as follows:

- Physical interdependencies: The relationships among physical infrastructure systems, such as functional dependencies and geospatial relationships;
- Cyber interdependencies: The relationships between infrastructures that are caused by telecommunication systems and cyber systems;
- Social and economic interdependencies (also called *human-related interdependencies*): The relationships of infrastructures arising from human activities.

As shown in Table 1, this paper summarizes the definitions provided in previous studies and groups the definitions under each category. The names and the syntax of the interdependency types are defined slightly differently in different papers.

Extensive efforts have been made to model ICIs using different approaches. Several survey papers have attempted to compare the studies according to different criteria (Min 2014; Satumtira and Dueñas-Osorio 2010; Pederson et al. 2006). Pederson et al. (2006) presented a vertical overview of the approaches according to several metrics, including a simulation technique, hardware/software requirements, intended users, and maturity level, for example. The review focuses on the simulation scenarios and techniques, so it is generic in terms of understanding the approach instead of the modeling of ICIs. Satumtira and Dueñas-Osorio (2010) reviewed the modeling approaches of stochastic interdependence, cascading failures, and the establishment of risk mitigation principles. The survey focuses on criteria such as the mathematical methods, quality and quantity of data, and scale of analysis. Min (2014) categorized the ICI studies into empirical approaches, agent-based approaches,

Table 1. Summary of interdependency categories (names and syntax of interdependency types might be defined slightly differently in different papers)

Interdependency categories	Interdependency types	Definitions
Physical	Physical (Rinaldi et al. 2001; Dudenhoeffer et al. 2006; Wallace et al. 2001; Petit et al. 2015)	State of one infrastructure system is dependent on output of another infrastructure
	Geospatial (Rinaldi et al. 2001; Dudenhoeffer et al. 2006; Zimmerman 2001; Petit et al. 2015)	A local environmental event can create state changes in two or more infrastructure systems
Cyber	Cyber (Rinaldi et al. 2001; Petit et al. 2015)	State of one infrastructure system depends on information transmitted through information infrastructure
	Informational (Dudenhoeffer et al. 2006)	There is a binding or reliance on information flow between infrastructure systems
Social and economic/human-related	Policy (Dudenhoeffer et al. 2006)	There is a binding of infrastructure components due to policy or high-level decisions
	Budgetary (Zhang and Peeta 2011)	Infrastructure systems involve some level of public financing, especially under a centrally controlled economies or during disaster recovery
	Market and economic (Zhang and Peeta 2011)	Infrastructure systems interact with each other in the same economic system or serve the same end users who determine the final demand for each commodity/service subject to budget constraints or are in the shared regulatory environment where the government agencies may control and impact the individual systems through policy, legislation, or financial means such as taxation or investment

system dynamics–based approaches, economic theory–based approaches, and network-based approaches. Salehi et al. (2015) reviewed the models and analysis methods for multilayer networks. Banerjee et al. (2017) reviewed and compared a few network-based models of ICIs.

Models

This section presents a review of the network modeling of critical infrastructures. The models are categorized in this paper into the following types: *single-layer network, network flow, Bayesian network, multilayer network, cyber interdependency, human activities*, and *data-driven modeling*. There are overlaps between the models, and some models may fall into more than one category. If one approach can be described by more than one category, it is placed under one category that can better represent the work. In each of the categories in this section, the type of modeling is first introduced, followed by the description of the existing models. Finally, the benefits, drawbacks, and challenges of the approaches are discussed.

Single-Layer Network

Single-layer network modeling refers to the representation of CIs as a single-layer graph. It can be used to model one or a few CIs. The graph can be directed or undirected, dynamic or static, unweighted or weighted. To model CIs as a single-layer network, it is necessary to define the nodes and edges and how the network dynamics or weights are constructed.

Many infrastructures can be modeled as a single-layer graph. For instance, transportation systems can be modeled naturally as a network, as described in the previous section. A straightforward approach is to model transportation systems as an *unweighted or weighted network*, where the intersections of roads are the nodes and the roads are the edges (Taylor 2017; Zhang et al. 2018a, b). Such a model usually assumes all the nodes are homogeneous. However, there are many nuances in modeling transportation systems as networks (Derrible and Kennedy 2010, 2009). Derrible and Kennedy (2010) also used an *undirected network* to model a metro system where stations are nodes and rail tracks are edges. Unlike other researchers, Derrible and Kennedy distinguished between monotonic stations and diatonic stations and gave mathematical representations of them. Thus, the model can be more practical. Similarly, Pagani and Aiello (2013) modeled a power grid (or energy system in general) as a network. For instance, electric power delivery networks can be modeled as *undirected graphs*, where the power stations are the nodes and the power lines are the links (Holmgren 2006).

Transportation system traffic, when modeled as network flows, is always found to match the traffic in telecommunication system. A few works (Choo and Mokhtarian 2007; Lindsey 2007) modeled transportation systems as networks and mapped cell phone usage data to the transportation network. Travel demand is found to match the demand for telecommunication. Interdependency can, therefore, be modeled accordingly. Lee et al. (2004) used a *single-layer simple graph* model for the interdependency of telecommunication systems and power grid systems. The study focuses on the reliability of power grid systems and models the systems according to geographical information. Such information is then converted into a network that can be analyzed. The interdependencies between the two systems are represented as logical edges in addition to the actual physical links.

Wang et al. (2012) modeled power and water systems as a *simple weighted graph*. The interdependencies of nodes in the two systems are defined as edges according to case studies of real events. Furthermore, the weights of the edges represent the interdependency level/load of the components. Korkali et al. (2017) modeled power and communication systems as a *weighted undirected graph*. The approach provides a few variants on how one failure will cause changes to connections in the graph. Winkler et al. (2011) utilized an *undirected and unweighted bipartite graph* to represent the interdependency between energy and water systems. The components in different systems are modeled as different types of nodes. Interdependencies are defined as edges according to the geographical distances of the nodes.

Single-layer network modeling provides a simple and intuitive representation of CHPSs. If an undirected graph is used, the model can be extremely useful to analyze topological properties. Furthermore, if the geographical information of the components in a CHPS can be obtained, the network modeling of a single-layer network can be easily visualized, which can be useful for decision-making.

The major challenge or drawback of the single-layer graph is that it cannot capture well the heterogeneity of different components. To differentiate heterogeneous components, additional attributes must be included in the graph, which makes it more difficult for analysis.

Network Flow

In network flow modeling, the CHPS is also modeled as a single-layer network with a number of nodes and edges. The focus of such a model, however, is the flow of the network, e.g., the number of unit flows from one node to the other and the corresponding cost. Such an assumption enables the modeling of the CHPS through mathematical methods according to network theories. Therefore, the network flow model can be extremely useful in applications such as transportation systems and energy systems.

Quelhas et al. (2007) developed a multiperiod generalized network flow model for energy systems. Specifically, gas and electricity can flow between transmission lines. In addition, fuel supply and electricity demand can flow via a transportation network. Based on such a model, the goal is to find the most efficient allocation of quantities and corresponding prices. Gil and McCalley (2011) used a similar model in the energy system for evaluating large-scale disasters such as hurricanes.

Ibáñez and McCalley (2011) proposed a tool, NETPLAN, for modeling energy and transportation systems. As with models in energy systems, gas and electricity can flow between transmission lines. Traffic can flow on roads and railroads. The model contains two levels: an operational level and a planning level. The operational level requires that each system satisfy demand with its capacity. The planning level enables analysis for optimal planning of CIs. Krishnan et al. (2015) further enhanced NETPLAN and integrated a multimodal passenger transportation model. Based on NETPLAN, a few subsequent works also expanded the model to focus on the interdependency of the two systems (Ibáñez et al. 2010, 2016).

When more than one or two infrastructures are modeled, the network flow model can be used to model network interdependencies (Lee et al. 2007). In other words, the disruption of one may lead to disruption in all other dependent systems due to the supply and demand differences.

A network flow model is useful in modeling the supply and demand relationships of a network. Therefore, it can be used for most critical infrastructures to study the dynamics of the network. Furthermore, it can be integrated with the economic model to study impacts of items such as electricity prices. The limitation of the network flow model is that it cannot easily model multiple critical infrastructures. Specifically, the interdependency of different infrastructures cannot be easily included in a single-layer network and integrated into the network flow model.

Bayesian Network

A Bayesian network is a probabilistic graph model that represents conditional dependencies via a directed acyclic graph. It is a useful framework to assess the reliability of infrastructures. Johansen and Tien (2018) modeled water, gas, and power systems as a Bayesian network. They modeled three types of interdependencies: service provision, geographic, and access to repairs. The service provision interdependency is similar to the physical interdependency introduced in the section "Interdependent Critical Infrastructures." The access-to-repair interdependency combines physical interdependency, cyber interdependency, and human-related interdependency. The model specifies that both physical and cyber access must be available to report the failures of CI components. CI components such as power substations are modeled as nodes, and the interdependencies are modeled as edges.

A Bayesian network takes into account complex interdependencies and enables assessments to be performed probabilistically. Therefore, it can be used to capture unknown or probabilistic factors for risk and network resilience assessment.

Multilayer Network

A multilayer network models multiple objects according to their functionalities. A straightforward method is to model each CI as a layer of a multilayer graph. The interdependencies are modeled as edges between different layers. This model can also be used to capture the heterogeneity of different networks and analyze them in an efficient way.

Several studies used a two-layer graph to model the interdependencies between communication and energy systems. A few works used a model where the communication system and the energy system are each modeled as an *undirected graph* (Buldyrev et al. 2010, 2011b). The interdependencies between the two systems are modeled as undirected edges between nodes in different systems. The model considers the clustering problem, where only the largest cluster with the largest number of connections are operational. Huang et al. (2015, 2013b) built a similar model. The difference is that Huang et al.'s model differentiates the roles of control nodes (e.g., SCADA control center) and relay nodes (e.g., routers) in the communication system. Therefore, the model captures features of the CIs beyond topology. Gao et al. (2012) used another similar multilayer model to model two networks. The difference is that the framework by Gao et al. utilized a different cluster-based model to represent the interdependencies.

Sturaro et al. (2016) named the model in Buldyrev et al. (2010) a *uniform model*, where all the nodes are considered homogeneous, and called the model in Huang et al. (2015) a *small clusters model*, which differentiates particular roles in a communication system. A more practical model, called Heterogeneous Interdependent NeTworks (HINT), was then proposed; it differentiates between logical and physical interdependencies. Wang et al. (2013) modeled two interdependent networks also as a two-layer graph. The approach assumed that the interdependency links were predefined. The failure of one node has a set probability of causing failures of neighbors. This is a similar model with network epidemics (Moreno et al. 2002; Newman 2002b). Such a model has been applied to the spreading of disease, viruses in communication networks (Kleinberg 2007; Wang et al. 2009), and information in social networks (Guille et al. 2013; Borge-Holthoefer et al. 2013).

A two-layer graph model of a communication system and an energy system was used in several works (Parandehgheibi and Modiano 2013; Parandehgheibi et al. 2014; Habib et al. 2015; Duan et al. 2017a, 2018). It is different from the models described earlier in this section since interdependency edges can be *directed or undirected*. In this setting, if a node loses all the incoming interdependency edges, it fails and cannot provide any outgoing interdependency edges. Later, Duan et al. (2016) generalized the model and proposed several variants to model cyber interdependencies. Specifically, different types of graphs, such as weighted graphs and a combination of directed and undirected graphs, can be used to capture different properties.

Nan and Sansavini (2017) proposed a hybrid multilayer model, where each layer can be independently modeled. The interaction between different layers can also been modeled. Zhu and Milanović (2017) used a weighted multilayer graph to model the interdependency between the power system and communication system. Specifically, in the power system, the power bus can be naturally modeled as a network where the weights of the power buses represent the electrical distances, e.g., power flow. Similarly, in the communication system, routers are the nodes and communication links are the edges, where the gross bitrates are the weights. An interdependency edge is built if one communication node sends data to a power node.

A multilayer network provides the flexibility of capturing the heterogeneity of CHPS components. It also differentiates the edges in every single layer and the interdependencies between different layers. Therefore, it is a nice framework for modeling multiple CIs or similar CHPSs.

Cyber Interdependency

Cyber and communication events include phone calls, Internet access, and so forth. Unlike traditional infrastructures that suffer most from physical failures, cyber infrastructures can cause severe impacts due to events such as cyber attacks. Such an impact, however, is very difficult to capture, especially in an interdependency model (Menashri and Baram 2015; Hadjsaid et al. 2010; Kim et al. 2005).

Indeed, there are too many cyber components whose failures can spread to other components of physical CIs (Sun and Song 2017). For instance, in a SCADA system (Sivanandam 2016), there are, for example, routers, sensors, and programmable logic controllers (PLCs). The failure of each component can cause the failures of other components. However, they are all heterogeneous and the types of failures can vary. Therefore, the cyber system cannot be easily modeled as a network. Indeed, cyber infrastructures such as cellular towers can be directly modeled as a CI. However, cyber events that may have a severe impact on ICIs cannot be easily captured. Ebrahimy (2014) investigated cyber attacks that can cause SCADA failures. A model was proposed where all the Internet and Communication Technology (ICT) components (e.g., sensors, routers) are modeled as infrastructures and the behaviors of the CIs are simulated under cyber events.

Technically, cyber interdependency is not a specific model. Most existing works simply treat a cyber infrastructures as they do other infrastructures, e.g., using single-layer or multilayer graphs. However, the spread of failures should not be modeled in the same way. Therefore, there is still a gap between a mature model and the existing state of the art.

Human Activities

Human activities interact with critical infrastructures in a complex and dynamic manner. Barnes and Newbold (2005) and Howe et al. (2016) modeled human activities as an infrastructure. Specifically, humans receive services from other infrastructures and provide operations to other infrastructures. Clark and Seager (2017) prioritized the supporting human infrastructures according to Maslow's hierarchy of human needs. Like cyber interdependency, human activities are very difficult to capture in network resilience models.

Santos-Reyes et al. (2015) studied the interdependency of the Mexico City Metro transit system. The ideas of *horizontal interdependency* and *vertical interdependency* were highlighted. Horizontal interdependency includes facts such as operational, managerial, and environmental factors. Vertical interdependency refers to the interactions of different levels. The model separates the roles of humans, human-physical operations, and the physical systems that consider different aspects of the CHPS.

Barrett et al. (2010) modeled human movements in the interdependency of a wireless cellular network and a transportation network. Specifically, the approach builds a multilayer network that consists of both transportation traffic and wireless cellular network traffic. By analyzing the traffic during an evacuation, the interdependencies between the two networks can be identified. In other words, the interdependencies between networks are not predefined but instead are analyzed based on real events.

Ernstson and colleagues conducted a survey of qualitative data of a social network and used the data to study the resilience of an urban green area (Ernstson et al. 2008; Ernstson 2008a). The survey focused on the collaborative interaction of different organizations in the area, which is converted to a network that can be quantified. The studies were also generalized later into a framework where human and physical systems can be modeled and analyzed through the biophysical processes of an urban environment (Ernstson 2013). The framework consists of two levels. At the city-wide level, a network is constructed for the physical system. At the local level, the urban struggle over land use is studied to track how humans utilize social arenas to study the impact of biophysical processes. Although these series of studies do not directly target the relationships of CIs, they especially focus on human interactions and their impact on the resilience of infrastructure systems.

It is not straightforward to integrate human activities into network models for several reasons. First, human activities are unpredictable. They cannot be easily converted to certain components in the network. Second, human activities cannot be easily quantified to be considered in network models. Therefore, modeling of human activities in a CHPS remains a challenging task.

Data-Driven

Data-driven approaches usually involve three steps: data collection, data simulation/analysis, and vulnerability/resilience assessment. First, ground truth data, such as data from past events or current events, are collected. The relationships of different CI components are then analyzed based on the data. Finally, a vulnerability or resilience assessment is obtained. This approach yields a prediction of future events or real-time analysis of an ongoing event for disaster management.

Alger et al. (2004) collected mobile phone signaling data and mapped the data to the real-time traffic in a transportation system. Subsequently, Singha and Kalita (2013) proposed a more generic model. Based on a similar idea, Duan et al. (2017b) studied the impact of a metro collision using mobile phone data. Through the analysis of mobile phone usage data, the approach can be used to understand evacuation behavior during metro station failures. Such a study can be useful in emergency management. Although this type of study does not aim at the interdependency of two networks, the approaches define the impact of human activities on different physical infrastructures. Based on such a study, the traffic in a transportation system can be predicted.

Oak Ridge developed a tool that can be used to visualize the impact of hurricanes on the electric grid (Barker et al. 2013). The hurricane tracks are downloaded and processed, analyzed, and visualized. The resilience of the system can then be assessed. Hawelka et al. (2014) collected geo-located Twitter feeds to study human mobility in the world. Wang and Taylor (2015) conducted a similar study for a typhoon. The spatiotemporal graphs of human movements can be constructed and analyzed. The purpose herein is to analyze the resilience of human mobility.

Hasnat et al. (2018) sampled the data of 350 buildings in Dhaka, Bangladesh, and conducted an earthquake vulnerability assessment of the buildings based on a rapid visual screening (RVS) method developed by FEMA. The vulnerability scores are then assigned based on the earthquake and fire hazard, as well as the social vulnerability conditions of the study area.

Abdalla et al. (2007) utilized an event-triggered data model for interdependent networks. Specifically, event data are first collected according to a survey of water systems after flooding. The data are converted to GIS format so as to visualize the event. Finally, the data are analyzed according to the spatial modeling to identify the interdependency.

Lee et al. (2016a, b) modeled multiple infrastructures as a multilayer graph including the transportation, the water, and the energy systems. The nodes include roles such as road intersections, rail stations, water reservoirs, substations, and others. The links include, for example, roads, water streams, and transmission links. The interdependencies of the nodes are determined based on their geographical distances. Real data of infrastructures are utilized to construct the networks for analysis. Chen et al. (2017a) built the interdependencies between different components in the power system such as substations, power plants, and natural gas stations. A single graph is constructed based on the real data of the infrastructures, where interdependencies are captured according to their geographic relationships.

The benefits of such approaches are twofold. First, since the analysis and modeling are based on data from real events, the analysis results will be more convincing. Second, such an approach makes it easier to visualize the results for decision-making. The challenges here lie in the conversion of data into a model. Also, it is not straightforward to collect data that can be directly used in the study of ICIs.

Analysis Approaches

Network analysis has been widely studied in multiple application domains. It is useful for multiple purposes, e.g., resilience or vulnerability analysis (Ayyub 2015), disaster management (Masys 2016), and infrastructure protection (Auerswald et al. 2005). This section reviews network analysis approaches, some of which rely on the model described in the previous section. The models and the analytical approaches are summarized in Tables 2 and 3.

Network Theory

When a CI or several CIs are modeled as a single-layer or multilayer network, network characteristics from mathematical models (Newman 2008; Watts and Strogatz 1998; Albert et al. 2000) can be analyzed to assess the resilience and robustness of the CIs (Holmgren 2006; Pagani and Aiello 2013).

The metric *global efficiency* is used in several works for assessing network vulnerability in transportation systems (Latora and Marchiori 2002; Zhang et al. 2018b; Taylor 2017). Network efficiency is calculated based on the number of nodes in the network and the distances between any pair of nodes. The distances between nodes can either be the physical distance between two stations or the distance given other factors such as water level rise (Zhang et al. 2018a, b).

Table 2. (Part 1) Summary of models and approaches

Model	None	Single-layer network	Bayesian network	Multilayer network	Cyber interdependency	Data-driven	Human activities
None	—	Lee et al. (2007) and Lindsey (2007)	—	Moreno et al. (2002), Newman (2002b), Kleinberg (2007), Wang et al. (2009), Guille et al. (2013), Borge-Holthoefer et al. (2013), and Duan et al. (2016)	Menashri and Baram (2015), Ebrahimy (2014), Kim et al. (2005), Hadjsaid et al. (2010), Sun and Song (2017), and Ebrahimy (2014)	Alger et al. (2004), Duan et al. (2017b), Singha and Kalita (2013), Barnes and Newbold (2005), Howe et al. (2016), Wang and Taylor (2015), Hawelka et al. (2014), Barker et al. (2013), and Santos-Reyes et al. (2015)	—
Network theory	Newman (2002a, 2003), Choo and Mokhtarian (2007), Leskovec et al. (2010), Boccaletti et al. (2014), Kivelä et al. (2014), Gao et al. (2016), Newman (2008), Watts and Strogatz (1998), and Albert et al. (2000)	Taylor (2017), Derrible and Kennedy (2010), Derrible and Kennedy (2009), Zhang et al. (2018a), Latora and Marchiori (2002), Zhang et al. (2018b), Pagani and Aiello (2013), Holmgren (2006), Wang et al. (2012), and Nan and Sansavini (2017)	—	Zhu and Milanović (2017)	—	—	—
Network flow	—	Ibáñez et al. (2010), Ibáñez and McCalley (2011), Ibáñez et al. (2016), Krishnan et al. (2015), Quelhas et al. (2007), and Gil and McCalley (2011)	—	—	—	—	—
Probabilistic	Tien and Der Kiureghian (2016, 2017), Tong and Tien (2017), Eldosouky et al. (2017), Ayyub (2014a), Ayyub et al. (2009a), Henley and Kumamoto (1996), Modarres et al. (2016), and Ayyub et al. (2009b)	—	Johansen and Tien (2018)	—	—	—	—

Note: The models that correspond to the "None" analysis method are approaches that do not include analysis. Similarly, the analysis approaches with a "None" model are generic analysis approaches.

Table 3. (Part 2) Summary of models and approaches

Model	None	Single-layer network	Bayesian network	Multilayer network	Cyber interdependency	Data-driven	Human activities
Topological-based	Huang et al. (2013a), Buldyrev et al. (2011a), Li et al. (2011), Dickison et al. (2012), Funk et al. (2009, 2010), and Jo et al. (2006)	Korkali et al. (2017), Lee et al. (2004), and Koc et al. (2014)	Wang et al. (2013)	Parandehgheibi and Modiano (2013), Duan et al. (2017a, 2018), Habib et al. (2015), Buldyrev et al. (2010, 2011b), Huang et al. (2013b), Gao et al. (2012), Huang et al. (2015), and Sturaro et al. (2016)	—	Lee et al. (2016a, b)	—
Simulation-based	Chen et al. (2015, 2017b) and Wang and Taylor (2013)	—	—	Huang et al. (2015) and Parandehgheibi et al. (2014)	—	Abdalla et al. (2007)	Barrett et al. (2010)
Social network, Economic, and psychology theory	Chen et al. (2009a), Gilbert and Ayyub (2016), Schlake et al. (2011), Masys (2014), Farías and Bender (2012), Chen et al. (2010, 2009b), Medd and Marvin (2005), Clark and Seager (2017), Wasserman and Faust (1994), Simone (2014), Dwiartama and Rosin (2014), and Vertesi (2014)	—	—	—	—	Chen et al. (2017a)	Ernstson et al. (2008), Ernstson (2008a, 2013, 2008b)
Expert opinion	Chang et al. (2014), McDaniels et al. (2015), Adey et al. (2015), Amoore (2013), Harvey and Knox (2015), and Grove (2013)	—	—	—	—	Hasnat et al. (2018)	—
Other	Vale (2014), Short (2016), Yates et al. (2012), Luque-Ayala and Marvin (2016), and Denis and Pontille (2014)	Winkler et al. (2011)	—	—	—	—	—

Note: The models that correspond to the "None" analysis method are approaches that do not include analysis. Similarly, the analysis approaches with a "None" model are generic analysis approaches.

Leskovec et al. (2010) proposed the concept of Kronecker graphs and an algorithm, KRONFIT. KRONFIT can be used to generate large synthetic networks that share similar properties of real networks. Several metrics are used to evaluate the networks, including *degree distribution* and *eigenvalue distribution*, for example. Gao et al. (2016) built an analytical framework to evaluate the resilience of complex networks. Kivelä et al. (2014) and Boccaletti et al. (2014) presented a number of characteristics that can be used to evaluate multilayer networks. The characteristics can be useful in evaluating the resilience of CIs that are represented as multilayer graphs.

Choo and Mokhtarian (2007) utilized *structural equation modeling* (SEM) to analyze the causal relationships of the nodes in a telecommunication network and a transportation network. The study focuses on travel delay in the transportation network. Therefore, the approach focuses on the case where the transportation system depends on the telecommunication system but not vice versa.

Derrible and Kennedy (2009) assessed the resilience of transportation systems using several measurements in graph theory, including *transit coverage*, *maximum number of transfers*, and *transfer possibilities*, to assess the design efficiency of world subway systems. Derrible and Kennedy (2010) subsequently extended the work by considering several other indicators such as *average connections* under a setting of scale-free networks and small-world networks. They also used the concept of *assortativity*, first introduced by Newman for analyzing robustness (Newman 2002a, 2003). Assortativity measures the extent to which nodes with connection indices b are linked to other nodes with similar connection indices b.

Wang et al. (2012) used three properties to analyze the interdependency of water and power systems: *betweenness*, *clustering coefficient*, and *degree*. The approach can serve as a methodological framework to analyze the resilience of CIs as well as to identify the key components in networks. Based on a *weighted multilayer graph* model, Zhu and Milanović (2017) proposed a characteristic called the *vulnerability-weighted node degree* (VMND). Specifically, instead of using the degree of nodes in single-layer simple graphs, the VMND value distinguishes between incoming edges and outgoing edges. The in-degree and out-degree of edges are calculated correspondingly. In association with the weights of edges, the index can be used to represent the vulnerability of two systems by considering their interdependency.

The benefits of network theory approaches are twofold. First, since most CIs can be naturally modeled as networks, various network characteristics in network theory can be utilized to assess the vulnerability and resilience of CIs. Second, network characteristics are usually quantifiable values, which makes it easy to compare different network topologies and structures.

Network theory approaches have their drawbacks and challenges. Specifically, network characteristics treat nodes and edges equally so as to convert them into quantifiable indicators. However, the network components in CHPSs are heterogeneous. Indeed, different components in the network may have different properties. These factors cannot be easily considered using one uniform set of quantifiable network characteristics. Furthermore, some properties of CIs cannot be easily quantified and integrated into models.

Network Flow

Network flow algorithms naturally model the flows between nodes (Ahuja 2017). Therefore, network flow can be used to study the supply and demand needs for optimal planning of critical infrastructures (Quelhas et al. 2007; Gil and McCalley 2011).

The NETPLAN tool (Ibáñez and McCalley 2011) uses a multiobjective evolutionary algorithm for energy and transportation systems. The evolutionary algorithm can be used to achieve optimal planning of CIs at minimum cost. Later on, Ibáñez et al. (2010) generalized NETPLAN into a framework to simulate events in CIs. An event can be chosen to analyze the impact, and the results can be visualized in the end.

Since network flow algorithms naturally capture the supply and demand relationships between nodes, such approaches can easily integrate nonphysical factors such as economic factors. Furthermore, the result can be easily visualized since such approaches usually employ network models that can be directly mapped to physical systems. The major challenge of network flow–based analysis is the high computational cost, especially when detailed operations of different network components are specified. As a result, heuristic algorithms are usually proposed for analysis.

Probabilistic Analysis

A probabilistic graphical approach, such as a Bayesian network, captures the property of conditional dependencies. Therefore, it enables numerous analysis methods that are natural to CIs. A number of algorithms have been proposed to analyze system reliability in a Bayesian network model (Tien and Der Kiureghian 2017, 2016; Tong and Tien 2017). Johansen and Tien (2018) combined the analysis of a Bayesian network and minimum link set (MLS) to analyze the fragility of systems considering the effect of interdependencies. Eldosouky et al. (2017) combined a Bayesian network with a Markov chain. A *resilience index* was proposed under the probabilistic model, which considers both individual CIs and their collective contribution to an entire system of multiple CIs.

Probabilistic risk analysis in critical infrastructures has been widely studied in hurricane protection systems (Ayyub 2014a; Ayyub et al. 2009a; Henley and Kumamoto 1996; Modarres et al. 2016; Ayyub et al. 2009b). For instance, Ayyub et al. (2009a) presented a framework with three components (steps): *influence diagram* representing the dependability of different procedures in a hurricane protection system, a *probability tree* that converts the influence diagram into a probabilistic and quantitative model, and *risk quantification and analysis* to quantify the factors in the probability tree and assess the risk. Such a framework provides the flexibility of capturing the heterogeneity of CI components and assessing different factors in a complex system.

Probabilistic analysis approaches take into account the complex interdependencies of CIs and enable assessments to be performed probabilistically. Therefore, they can be used to capture unknown and probabilistic factors for risk and network resilience assessment.

One major limitation of such probabilistic approaches lies in the actual probabilities of the relationships between different network components. Indeed, the relationships are meaningful only if the probabilities are obtained through other approaches such as expert opinions. Furthermore, they also share the same challenge with network theory approaches, where it is difficult to capture heterogeneous relationships between network components.

Topology-Based Approaches

Topology is an important factor in the resilience of a network. Topology-based analysis approaches usually analyze the cascading failures according to network connections.

In a multilayer graph model, *the minimum number of nodes to take down the whole network* is one problem addressed by a number of studies. Multiple solutions have been proposed, including heuristic algorithms (Parandehgheibi and Modiano 2013), an analytical solution based on percolation theory (Buldyrev et al. 2010; Gao et al. 2012), and an analytical method based on recursion

(Buldyrev et al. 2011b). Huang et al. (2013b) studied the failure propagation problem using methods that rely on generating functions and percolation theory.

Another research topic in multilayer graphs is *the resilience and robustness of particular topologies*. In such approaches, the interdependency of nodes is pre-specified based on criteria such as the geographical distances of the nodes. Random failures are injected to evaluate the failure propagation according to both mathematical methods of percolation theory and simulation. The topologies previous studies focus on include lattice interdependent multilayer networks (Li et al. 2011), networks where nodes from different layers are mutually dependent and have the same degree (Buldyrev et al. 2011a), and clustered networks (Huang et al. 2013a). Lee et al. (2004) proposed a search algorithm based on the single-layer network modeling of a telecommunication system and power grid system. A search algorithm is used to find all the nodes that are reachable by one node. The vulnerable points can then be assessed.

Failure propagation is also a research topic for topology-based approaches. Specifically, failures can be injected by removing nodes from networks. Then the number of remaining operational nodes after cascading failures can be analyzed (Huang et al. 2015; Sturaro et al. 2016). Wang et al. (2013) analyzed a probabilistic failure propagation problem in multilayer networks. Dickison et al. (2012) utilized the susceptible-infected-recovered (SIR) process of interdependency networks, which is often used for studying the characteristics of disease (Funk et al. 2010, 2009; Jo et al. 2006). Such an approach analyzes both failure propagation and failure recovery of multilayer networks. Korkali et al. (2017) injected random node failures based on a model of a power grid and a communication network. Failure propagation is simulated, and the network can be assessed after all the cascading failures. Different topologies of the initial networks are used to assess resilience.

Duan et al. (2018, 2017a) utilized the idea of undirected graphs for analysis. Specifically, when a node loses all incoming interdependency edges, it is no longer operational. Based on this finding, the impact under any cyber events can be estimated. Habib et al. (2015) quantified resilience metrics as a constraint number, which is the number of cascading failures after a single-node failure. Based on this constraint, they developed an algorithm to design a resilient system given the constraint. Lee et al. (2016a) provided several topology-based analytic tools based on a multilayer network, such as the efficiency score of the network and vulnerable nodes.

Topology-based approaches are useful in tasks such as evaluating the resilience of a network and identifying the vulnerability of nodes. If real data are used to construct the network, the results and the network can be easily visualized for decision-making. Furthermore, topology-based approaches can be integrated with other models such as probabilistic models to capture the heterogeneity of network components. One challenge of topology-based approaches is the efficiency of analysis. Indeed, compared with other approaches such as network theory, topology-based analyses are more difficult to calculate and simulate. Therefore, most of these approaches propose efficient algorithms for analysis.

Simulation-Based Analysis

The simulation-based analysis category is a generic term. Indeed, simulations are used in other approaches as well, e.g., in topology-based approaches, random failures can be injected to simulate the cascading failures. Here, simulation-based approaches include other types of simulations, e.g., simulation software–based approaches, failure propagation simulations that combine multiple categories of approaches, and agent-based network simulations.

Wang and Taylor (2013) conducted an agent-based simulation of online social networks to understand how energy-saving information travels through an online social network. In addition to understanding the resilience of CIs, this study simulated the behavior of humans disseminating information, which may be useful in understanding human involvement and reactions after failures of CIs. Chen et al. (2017b) presented a generic model and analysis of emergency evacuation following metro station failures. The approach provided a very detailed multiagent-based simulation of several evacuation scenarios in metro systems.

Chen et al. (2015) used Legion and Fire Dynamics Simulation (FDS) software to simulate pedestrian behavior during evacuation in a subway fire. The study does not focus on multiple infrastructures. Instead, it specifically studies human mobility during the failure of physical infrastructures, which can help guide disaster management and policymaking.

Abdalla et al. (2007) collected data on a real flooding event, converted them into GIS format, and then simulated the behavior of the water system. Instead of using a given model to simulate the behavior of the infrastructure, the approach utilized the simulation to analyze the known information. Such an approach is useful for identifying the interdependencies between different network components.

Parandehgheibi et al. (2014) developed two algorithms to simulate the effect of control policies. Specifically, the approach studied the impact of a simple load shedding mechanism and a load control mitigation policy. Barrett et al. (2010) analyzed the interdependencies between a transportation network and a cellular network by considering human activities during an evacuation. The approach simulated the changes in human calling behavior to the resilience of the two networks. Based on an analysis of spatiotemporal graphs, the approach highlights the impact of human activities on physical infrastructures.

Simulation-based approaches can be used for tasks such as the prediction of failure propagation and the impact of failures on a CHPS, which is suitable for predisaster management. For example, simulation can be used to estimate the loss from an upcoming hurricane with a known path. In addition, if the model is carefully designed, the approaches can be used to predict the affected areas of upcoming events.

Simulation-based approaches, however, can be useful in predisaster management only if the network is constructed based on real data. In other words, both the network and estimated results need to be visualizable and accurate. Otherwise, the result would probably make less sense for informing decisions. However, for large-scale systems like today's infrastructures, a detailed presentation and modeling based on real data can be very challenging, and any analysis may incur a high computational cost, if it is not outright impossible.

Social Network, Economic, and Psychology Theory

Social network theories and psychology theories are useful in analyzing CHPSs since they naturally consider human factors in the physical world (Medd and Marvin 2005). Furthermore, social network theories such as influence maximization (Chen et al. 2017a) can be useful in analyzing the vulnerability and resilience of a system.

Chen et al. (2017a) modeled a multilayer graph as a dominator tree and studied the *influence maximization* problem, which is usually used to analyze social networks (Chen et al. 2009b, 2010). The results can be used to evaluate vulnerable nodes in a system that can cause the maximum damage. Through a case study of the 2003 US

blackout, the approach simulated the areas that are affected after the initial failures.

Actor network theory (ANT) is a methodological approach to social theory (Latour 2005; Callon and Blackwell 2007). It is a method that connects human and nonhuman entities where all the actors form a network. Specifically, human and nonhuman actors are treated equally, and their activities affect entire networks. As a social theory that traditionally explores the relationships between social and natural worlds, ANT has been applied to many different areas (Farías and Bender 2012). ANT can be used to evaluate the resilience of CHPSs (Dwiartama and Rosin 2014). Two case studies are conducted to evaluate the agricultural production systems. The paper concluded that ANT offers a different understanding of resilience by involving both human and nonhuman interactions. Ernstson et al. conducted a series of work on the resilience of urban landscapes and explained the urban resilience problem using actor network theory (Ernstson 2008a, 2013, 2008b). By translating the actors and their relationships into graphs, social network analysis could be applied to analyze the resilience of infrastructures. The analysis approaches include spatial social-ecological network analysis and ecological connectivity. For instance, Ernstson et al. (2008) studied the social network structure of human movement in the setting of urban green areas in Stockholm. The approach focused on the patterns of interaction between movement organizations and converted the social network data to a graph. Through a correlation analysis of a network based on social network theory (Wasserman and Faust 1994), the paper pointed out that social networks may facilitate some collective actions yet constrain others. A qualitative case study was conducted based on over 6 years of ethnographic fieldwork of two large-scale distributed planetary science team (Vertesi 2014). Since the team conducted their fieldwork on layers of infrastructures, the approach utilized ANT to analyze how humans and physical CIs interact with each other. Masys (2014) explored how key actors within a network can interact with other actors to create *unseen* vulnerabilities in critical infrastructures. A case study utilized ANT to explain the cascading failures of the 1998 ice storm in Ottawa (Simone 2014).

Schlake et al. (2011) simulated the train delay and estimated the economic delay cost for in-service failures. A microeconomic approach was proposed to balance the costs and benefits from the implementation of disaster mitigation measures (Gilbert and Ayyub 2016). Specifically, the recovery cost and the loss from a disaster are both considered. Based on the goal of maximizing the net benefit of a mitigation plan, the optimal plan can be determined. This is a similar consideration with an economic input-output model (Chen et al. 2009a), where the principle is used to trace resources and products by purchases. Included in the modeling of critical infrastructures, the approach can be used to analyze how CIs provide input to and use the output from other CIs. Similar to the network flow model, such a model can be used to specifically capture the supply and demand relationships between different CI components.

Clark and Seager (2017) used Maslow's theory of human motivation (Maslow 1943) to develop a human-centered approach to prioritize disaster management jobs across different CI sectors. According to the hierarchy of needs of the theory, the paper presented a list supporting infrastructures that should be prioritized during a crisis.

The social network, economic, and psychology theory approaches can be extremely useful in considering nonphysical factors in network resilience analysis. Also, these approaches can help identify unseen relationships among network components. However, the major challenge is that the nonphysical factors cannot be easily quantified and integrated with other models and analysis approaches.

Expert Opinions

Expert opinions are important in studying resilience in multiple disciplines. However, expert opinions can be difficult to integrate and quantify in one model. Chang et al. (2014) and McDaniels et al. (2015) employed a four-step approach:

1. structuring and conditioning that summarizes the experience from previous events;
2. expert interviews, which summarize cross-sector opinions and expectations;
3. data synthesis, which integrates interview results and merges data into one diagram/model; and
4. information sharing, feedback, and revision, which lead to a single report for further analysis and decision-making.

Ayyub (2001) proposed a process for expert opinion elicitation that was followed in several studies for private- and public-related issues.

Adey et al. (2015) reviewed the policies and procedures related to emergency management and summarized them as preemption (Amoore 2013), anticipatory surveillance and premeditation, logic to prepare for emergency management, and resilience (Grove 2013). Harvey and Knox (2015) studied transportation systems and their stabilization regarding both physical infrastructures and social environments. These studies reveal the inherent challenges in modeling resilience: many activities related to the protection of CIs and disaster management cannot be quantitatively included in the models.

Expert opinions can sometimes be quantified and combined with analysis approaches. Hasnat et al. (2018) quantified the reviews of fire experts for vulnerability assessment of buildings under earthquake and fire hazards. Numeric values for six attributes were collected based on the expert opinions and merged the values to the vulnerability assessment.

Approaches based on expert opinions are valuable in capturing the heterogeneity of different components in CHPSs, which cannot be easily achieved in other approaches. The challenges include a significant amount of effort required in conducting such studies and the difficulties in combining the results into a single approach or report for analysis. Also, such approaches can be difficult to integrate with other methods, unless expert opinion elicitation is treated as a data collection method to define model parameters. Special attention should be given to unintentional biases (Ayyub 2001).

Other

Multiple other approaches in CHPSs are relevant but cannot be easily summarized in the previously mentioned categories. Based on a single-layer model, Winkler et al. (2011) combined simulation-based study and a network theory–based approach to analyze networks. Random failures are injected to estimate failure propagation. In addition, various features, such as *betweenness*, *clustering*, and *vertex degree* are assessed after cascading failures. The network's resilience can then be assessed.

The resilience of a city was defined by discussing the concepts linked to social psychology (Vale 2014). It was argued that three important factors must be considered: stories, symbols, and politics. Specifically, that study emphasized that policies for postdisaster management must take into consideration human reaction and behavior. Short (2016) conducted a case study of the regulatory regime in a power grid following a major storm. It was found that reactions to the storm forced a shift in the regulatory regime from one that stressed cost reduction and return on investment to one that also encompassed issues of grid resiliency and service reliability. The work showed how regulatory policies could directly affect resilience in ICIs.

Yates et al. (2012) performed a case study in Los Angeles County to assess the cost of deploying sensors to monitor the network traffic of transportation systems and protect infrastructure. The approach provides several models to analyze the cost and exposure and determines the optimal sensor locations to protect infrastructure.

Luque-Ayala and Marvin (2016) conducted an empirical study of Rio de Janeiro's Center of Operations (COR). The team interviewed COR directors and other personnel involved in the center's design and implementation. The study shows that the COR incorporates the public in operational control to raise public awareness of urban infrastructures. In other words, the approach indicates that human involvement has an impact on the resilience of infrastructures. Denis and Pontille (2014) conducted a case study of Paris subway signs and their impact on the performance of transportation systems. The approach combined in-depth interviews of employees, internal documents, and shadowing of maintenance workers. The study showed that continuous maintenance has a direct impact on infrastructure that is often overlooked.

Comparison of Approaches

The advantages and challenges of network modeling are summarized in Table 4. The approaches can be further compared on the basis of accessibility of input data, maturity, integration with other approaches, and modeling multiple infrastructures. Some of these approaches follow the criteria of previous work (Min 2014).

- *Accessibility of input data* refers to the requirements of input data sets, including how much data are required and whether the data are easily accessible. Three letters—"L" (low), "M" (medium), and "H" (high)—are used to represent the difficulty of obtaining data.
- *Maturity* represents the maturity of the modeling approaches, where mature models are widely adopted. This is a very generic criterion where different models in each category may have different maturity levels. Therefore, the table shows the generic maturity of each category. Similarly, the letters "L," "M," and "H" are used to denote level of maturity.
- *Integration with other approaches* considers the difficulty of combining one approach with others. "L" indicates a high level of integrability, "M" a medium level, and "H" denotes an approach that is very difficult to integrate with others.
- *Modeling multiple infrastructures* refers to a model's capacity to capture the heterogeneity of components. Integration with other approaches considers the difficulty of combining one approach with other approaches due to the heterogeneity of the models. "L" is used to represent very easy, "M" to represent medium, and "H" to represent very difficult. In addition, "N" means "does not apply."

Based on Table 4, it can be observed that most approaches rely heavily on real data sets to accurately model critical infrastructures. This is because more data are necessary to capture the heterogeneity of different components. In terms of maturity, single-layer network models and network flow models have been widely studied. Other approaches, especially models for studying nonphysical factors, are still not well studied. Some approaches can be easily integrated with other approaches. For instance, a network flow model can be considered together with a single-layer network to analyze both the supply–demand relationship and topological factors of the corresponding CIs. However, some approaches, such as cyber interdependency and human activities, cannot be easily combined with other models. This limitation stems in part from the fact that modeling nonhuman factors is essentially difficult. Finally, models such as a Bayesian network, a multilayer network, and data-driven approaches can naturally be used to study multiple critical infrastructures. Compared with these methods, other approaches cannot easily capture component heterogeneity.

The purposes, advantages, and challenges of the analysis approaches are summarized in Table 5. The following criteria are considered to compare the approaches: *computational complexity* and *maturity*. See earlier discussion on *maturity* to understand that criterion. *Computational complexity* describes the computational cost incurred by each approach to analyze the corresponding tasks. This is also a generic criterion where the computational complexity of different approaches in each category may vary.

According to Table 5, most approaches incur a certain computational cost in evaluating the results. The nonphysical analysis approaches, such as social network and expert opinion, entail certain computational costs. The trade-off is that they usually yield qualitative results, which can be difficult to quantify. The collection of expert opinion through case studies may be very time-consuming as well. In comparison, network theory requires medium computational costs since network characteristics are well formed from mathematical models, which are relatively easy to calculate. In comparison, other approaches, such as network flow and probabilistic approaches, rely on efficient algorithms to reduce the computational cost. In addition, the maturity of different categories depends in part on the corresponding theories. For instance, network theory and

Table 4. Summary of modeling approaches

Approach	Advantages	Challenges	Accessibility of input data	Maturity	Integration with other approaches	Modeling multiple infrastructures
Single-layer network	Simple and intuitive; easy to visualize; capture topological properties	Cannot well capture heterogeneity	L	H	L	L
Network flow	Capture supply and demand relationship	Cannot well model multiple CIs	M	H	M	L
Bayesian network	Capture probabilistic relationships between components	Cannot well capture heterogeneity	H	M	M	M
Multilayer network	Capture heterogeneity of different components	Need to carefully model each layer to capture the features	M	L	M	H
Cyber interdependency	Capture features of cyber infrastructures	Must be integrated with other models	H	L	H	N
Human Activities	Capture human factors	Cannot be easily integrated into other models; cannot be easily quantified	H	L	H	N
Data-driven	Based on real events; well capture ground-truth factors	accurate data are difficult to obtain	H	M	L	H

Table 5. Summary of analysis approaches

Approach	Example analysis purposes	Advantages	Challenges	Computational complexity	Maturity
Network theory	Network efficiency; resilience	Multiple indicators; easily computable quantifiers	Hard to capture heterogeneity of network components; not all factors can be quantified	M	H
Network flow	Supply and demand relationships, cost analysis, infrastructure planning	Capture nonphysical factors such as economic factors; capture supply and demand relationships	High computational cost	H	H
Probabilistic	Uncertainty modeling and analysis; risk analysis	Probabilistic analysis; capture unknown factors for risk and resilience assessment	Must be combined with other approaches to determine network probabilities; not all factors can be quantified	H	M
Topology-based	Vulnerability, resilience, efficiency, minimum nodes to take down whole network	Capture topological relationships, which is a dominating factor of network resilience; easily visualizable; can be integrated with other approaches	Computation is not as easy as other approaches	H	M
Simulation-based	Decision-making, visualization	Capture different factors of the systems	Rely on model for meaningful analysis	M-H	M
Social network, economic, and psychology theory	Infrastructure protection priorities	Model human activities, economic cost and effect, and capture unseen relationships	Difficult to integrate with other approaches; cannot be easily quantified; cannot be easily integrated with other approaches	M	L
Expert opinion	Pre- and postdisaster management	Capture heterogeneity of network components	Large amount of efforts; cannot be easily quantified and integrated with other approaches	L	L

network flow originate from graph theory, which has a number of already established mathematical models. The main challenge here is to fit the network characteristics into the corresponding CI system and better analyze performance and resilience. In comparison, probabilistic, topology-based, and simulation-based approaches have been extensively studied in the literature, so they are relatively mature as well. The major challenges of these approaches lie in the factor of whether they can be combined to provide a mature analysis result. Finally, the approaches for nonphysical factors are not well studied in quantitative approaches to network analysis.

Network Resilience in Supply Chain

Network modeling and analysis approaches can be applied to supply chain networks (SCNs) as well as business continuity. Specifically, a supply chain is usually modeled as a single-layer network. Like the approaches reviewed in this article, a number of works assess the resilience of different topologies of SCNs, for example, scale-free graphs and random graphs (Thadakamaila et al. 2004; Kim et al. 2015; Zhao et al. 2011). Network characteristics from network theory, such as degree distribution and clustering coefficients, are used to assess efficiency and resilience (Mari et al. 2015). Unlike the network analysis of other CHPSs, *accessibility* is a key component in SCNs, which represents the capability to meet market demand quickly during disruptions (Tang 2006). In the network model, supply accessibility can be measured by analyzing the total number of demand nodes connected with the supply nodes. Therefore, although network characteristics can be common in different CHPSs, they are weighted differently in assessing the resilience of the networks in different systems. Furthermore, like topology-based approaches, random or targeted attacks are generated, and the impact of failure is simulated or analyzed based on the network model to assess the robustness of the SCNs. Similarly, other network methods, such as adaptive theory, system dynamics, and agent-based simulation, can be used for analysis (Huang et al. 2007).

Future Research Directions

Data Collection

The difficulty of obtaining enough data for both modeling and validation has always been a major issue in this field of study. For instance, if the topology is the only consideration of a CI, there exist several open-source data sets. However, if other factors of a CI beyond the topology are considered, accessible data sets for both modeling and analysis are rare. To address this challenge, it is desirable to generate synthetic data sets that can capture the features of real infrastructures.

Modeling and Analyzing Qualitative and Nonphysical Factors

The models and analysis approaches discussed are not necessarily quantitative. This limitation is especially true when human factors are considered. This review shows that approaches based on social networks, the economy, and psychological theory and expert opinion are mostly qualitative. To integrate these approaches with other approaches, it is desirable to design a set of criteria or measurement methods to quantify some nonphysical factors. Such a step would greatly enhance the effectiveness and practicality of the analysis approaches.

Integration of Models and Analysis Approaches

Cyber-human-physical systems are complex. None of the reviewed approaches is capable of capturing the heterogeneity of components. For instance, topology-based analysis focuses on tasks such as analyzing topological relationships and network efficiency. To analyze nontopological factors such as supply–demand relationships, alternatively, network flow approaches can be utilized. However, owing to the underlying assumptions used in different analysis approaches, the appropriate models might be different depending

on the approach. In this situation, the analysis results are not comparable for the purpose of understanding the same situation. Therefore, it is desirable to efficiently build a few generic models so that different analysis results can be integrated to analyze different features of the same networks.

Validation of Models and Approaches

Validation of modeling and analysis is a crucial step in assessing and refining approaches. However, owing to a lack of real data sets, it is extremely challenging to judge whether one approach is better than others. Indeed, some approaches or analysis results cannot be easily validated, e.g., the extent to which a given CI is resilient or efficient. Several researchers consider historical events and simulate CI behavior to validate their models (Chen et al. 2017a). However, without more accurate data sets from historical events, it is not easy to validate an approach. Therefore, challenges remain with respect to both validation and accessibility of data sets from historical events.

Conclusion

This paper reviews the network-based modeling and analysis of cyber-human-physical systems. Specifically, the focus is the resilience of critical infrastructures, and the reviewed approaches can also be used in other application domains such as supply chains. The contributions of this paper include a comprehensive review of the literature and a detailed comparison of both modeling and analysis approaches. The separation of network modeling and analysis approaches is intentional so as to apeal to different groups of readers. The modeling approaches are categorized into single-layer networks, network flow, Bayesian networks, multilayer networks, cyber interdependency, human activities, and data-driven approaches. Furthermore, the analysis approaches are grouped into those based on network theory, network flow, probability, topology, simulation, social networks, economics, and psychological theory, as well as expert opinion. Each category is defined, followed by a description of some representative works. Furthermore, the benefits and challenges of the approaches are summarized. The summary and comparison of the approaches given show that several unsolved challenges remain, such as quantifying nonphysical factors, integrating different approaches to enhance their practicality and effectiveness, and maintaining data sets that can be used for modeling and validation.

References

Abdalla, R., C. V. Tao, Q. Cheng, and J. Li. 2007. "A network-centric modeling approach for infrastructure interdependency." *Photogramm. Eng. Remote Sens.* 73 (6): 681–690. https://doi.org/10.14358/PERS.73.6.681.

Adey, P., B. Anderson, and S. Graham. 2015. "Introduction: Governing emergencies: Beyond exceptionality." *Theory Culture Soc.* 32 (2): 3–17. https://doi.org/10.1177/0263276414565719.

Agency, F. E. M. 2013. *Hurricane Sandy in New Jersey and New York: Building performance observations, recommendations, and technical guidance*. Washington, DC: FEMA.

Ahuja, R. K. 2017. *Network flows: Theory, algorithms, and applications*. London: Pearson Education.

Albert, R., H. Jeong, and A.-L. Barabási. 2000. "Error and attack tolerance of complex networks." *Nature* 406 (6794): 378. https://doi.org/10.1038/35019019.

Alger, M., E. Wilson, T. Gould, R. Whittaker, and N. Radulovic. 2004. *Real-time traffic monitoring using mobile phone data*. Technical Rep. The Connection, Newbury: Vodafone Pilotentwicklung GmbH.

Amin, S., X. Litrico, S. Sastry, and A. M. Bayen. 2013. "Cyber security of water SCADA systems. I: Analysis and experimentation of stealthy deception attacks." *IEEE Trans. Control Syst. Technol.* 21 (5): 1963–1970. https://doi.org/10.1109/TCST.2012.2211873.

Amoore, L. 2013. *The politics of possibility: Risk and security beyond probability*. London: Duke University Press.

ASCE. 2006. "ASCE policy statement 518." Accessed September 5, 2019. https://www.asce.org/issues-and-advocacy/public-policy/policy-statement-518—unified-definitions-for-critical-infrastructure-resilience/.

Auerswald, P., L. M. Branscomb, T. M. La Porte, and E. Michel-Kerjan. 2005. "The challenge of protecting critical infrastructure." *Issues Sci. Technol.* 22 (1): 77–83.

Ayyub, B. M. 2001. *Elicitation of expert opinions for uncertainty and risks*. Boca Raton, FL: CRC Press.

Ayyub, B. M. 2014a. *Risk analysis in engineering and economics*. Boca Raton, FL: CRC Press.

Ayyub, B. M. 2014b. "Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making." *Risk Anal.* 34 (2): 340–355. https://doi.org/10.1111/risa.12093.

Ayyub, B. M. 2015. "Practical resilience metrics for planning, design, and decision making." *ASCE-ASME J. Risk Uncertainty Eng. Syst. Part A: Civ. Eng.* 1 (3): 04015008. https://doi.org/10.1061/AJRUA6.0000826.

Ayyub, B. M., J. Foster, and W. L. McGill. 2009a. "Risk analysis of a protected hurricane-prone region. I: Model development." *Nat. Hazards Rev.* 10 (2): 38–53. https://doi.org/10.1061/(ASCE)1527-6988(2009)10:2(38).

Ayyub, B. M., J. Foster, W. L. McGill, and H. W. Jones. 2009b. "Risk analysis of a protected hurricane-prone region. II: Computations and illustrations." *Nat. Hazards Rev.* 10 (2): 54–67. https://doi.org/10.1061/(ASCE)1527-6988(2009)10:2(54).

Banerjee, J., A. Das, and A. Sen. 2017. "A survey of interdependency models for critical infrastructure networks." Preprint, submitted February 7, 2015. https://arxiv.org/abs/1702.05407.

Barker, A. M., E. B. Freer, O. A. Omitaomu, S. J. Fernandez, S. Chinthavali, and J. B. Kodysh. 2013. "Automating natural disaster impact analysis: An open resource to visually estimate a hurricane's impact on the electric grid." In *Proc., Southeastcon*, 1–3. New York: IEEE.

Barnes, J., and K. Newbold. 2005. "Humans as a critical infrastructure: Public-private partnerships essential to resiliency and response." In *Proc., 1st Int. Workshop on Critical Infrastructure Protection*. New York: IEEE.

Barrett, C., R. Beckman, K. Channakeshava, F. Huang, V. A. Kumar, A. Marathe, M. V. Marathe, and G. Pei. 2010. "Cascading failures in multiple infrastructures: From transportation to communication network." In *Proc., 2010 5th Int. Conf. on Critical Infrastructure*, 1–8. New York: IEEE.

Boccaletti, S., G. Bianconi, R. Criado, C. I. Del Genio, J. Gómez-Gardenes, M. Romance, I. Sendina-Nadal, Z. Wang, and M. Zanin. 2014. "The structure and dynamics of multilayer networks." *Phys. Rep.* 544 (1): 1–122. https://doi.org/10.1016/j.physrep.2014.07.001.

Bocchini, P., and D. M. Frangopol. 2012. "Restoration of bridge networks after an earthquake: Multicriteria intervention optimization." *Earthquake Spectra* 28 (2): 426–455. https://doi.org/10.1193/1.4000019.

Borge-Holthoefer, J., R. A. Baños, S. González-Bailón, and Y. Moreno. 2013. "Cascading behaviour in complex socio-technical networks." *J. Complex Networks* 1 (1): 3–24. https://doi.org/10.1093/comnet/cnt006.

Boyer, S. A. 2009. *SCADA: Supervisory control and data acquisition*. Durham, NC: International Society of Automation.

Bruneau, M., S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. Von Winterfeldt. 2003. "A framework to quantitatively assess and enhance the seismic resilience of communities." *Earthquake Spectra* 19 (4): 733–752. https://doi.org/10.1193/1.1623497.

Bruneau, M., A. Filiatrault, G. Lee, T. D. O'Rourke, A. Reinhorn, M. Shinozuka, and K. J. Tierney. 2006. *White paper on the SDR grand challenges for disaster reduction*. Buffalo, NY: Multidisciplinary Center for Earthquake Engineering Research.

Buldyrev, S. V., R. Parshani, G. Paul, H. E. Stanley, and S. Havlin. 2010. "Catastrophic cascade of failures in interdependent networks." *Nature* 464 (7291): 1025–1028. https://doi.org/10.1038/nature08932.

Buldyrev, S. V., N. W. Shere, and G. A. Cwilich. 2011a. "Interdependent networks with identical degree of mutually dependent nodes." *Phys. Rev.* 83 (1): 016112. https://doi.org/10.1103/PhysRevE.83.016112.

Buldyrev, S. V., N. W. Shere, and G. A. Cwilich. 2011b. "Interdependent networks with identical degrees of mutually dependent nodes." *Phys. Rev. E* 83 (1): 016112. https://doi.org/10.1103/PhysRevE.83.016112.

Callon, M., and O. Blackwell. 2007. "Actor-network theory." In *The politics of interventions*, 273–286. Oslo, Norway: Unipub, Oslo Academic Press.

Chang, S. E., T. McDaniels, J. Fox, R. Dhariwal, and H. Longstaff. 2014. "Toward disaster-resilient cities: Characterizing resilience of infrastructure systems with expert judgments." *Risk Anal.* 34 (3): 416–434. https://doi.org/10.1111/risa.12133.

Chen, L., X. Xu, S. Lee, S. Duan, A. G. Tarditi, S. Chinthavali, and B. A. Prakash. 2017a. "Hotspots: Failure cascades on heterogeneous critical infrastructure networks." In *Proc., 2017 ACM on Conf. on Information and Knowledge Management*, 1599–1607. New York: ACM.

Chen, P., C. Scown, H. S. Matthews, J. H. Garrett Jr, and C. Hendrickson. 2009a. "Managing critical infrastructure interdependence through economic input-output methods." *J. Infrastruct. Syst.* 15 (3): 200–210. https://doi.org/10.1061/(ASCE)1076-0342(2009)15:3(200).

Chen, S., Y. Di, S. Liu, and B. Wang. 2017b. "Modelling and analysis on emergency evacuation from metro stations." *Math. Prob. Eng.* 2017: 11.

Chen, W., C. Wang, and Y. Wang. 2010. "Scalable influence maximization for prevalent viral marketing in large-scale social networks." In *Proc., 16th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining*, 1029–1038. New York: ACM.

Chen, W., Y. Wang, and S. Yang. 2009b. "Efficient influence maximization in social networks." In *Proc., 15th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining*, 199–208. New York: ACM.

Chen, Y., Y. Cai, P. Li, and G. Zhang. 2015. "Study on evacuation evaluation in subway fire based on pedestrian simulation technology." *Math. Prob. Eng.* 2015: 9.

Chien, E., L. OMurchu, and N. Falliere. 2011. "W32.duqu—The precursor to the next Stuxnet." Accessed September 5, 2019. https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.

Choo, S., and P. L. Mokhtarian. 2007. "Telecommunications and travel demand and supply: Aggregate structural equation models for the US." *Transp. Res. Part A: Policy Pract.* 41 (1): 4–18.

Clark, S. S., and T. P. Seager. 2017. *A human-centered approach to the prioritization of critical infrastructure resilience*. Technical Rep. Fairfax, VA: George Mason Univ.

Cowie, J. H., A. T. Ogielsk, B. Premore, E. A. Smith, and T. Underwood. 2003. *Impact of the 2003 blackouts on Internet communications*. Technical Rep. Manchester, NH: Renesys Corporation.

Cresswell, T. 2010. "Towards a politics of mobility." *Environ. Plann. D: Soc. Space* 28 (1): 17–31. https://doi.org/10.1068/d11407.

Cutter, S. L., et al. 2013. "Disaster resilience: A national imperative." *Environ.: Sci. Policy Sustainable Dev.* 55 (2): 25–29.

Danziger, M. M., A. Bashan, Y. Berezin, L. M. Shekhtman, and S. Havlin. 2014. "An introduction to interdependent networks." In *Proc., Int. Conf. on Nonlinear Dynamics of Electronic Systems*, 189–202. NewYork: Springer.

Denis, J., and D. Pontille. 2014. "Maintenance work and the performativity of urban inscriptions: The case of Paris subway signs." *Environ. Plann. D: Soc. Space* 32 (3): 404–416. https://doi.org/10.1068/d13007p.

Department of Homeland Security. 2018. "What is critical infrastructure." Accessed September 5, 2019. https://www.dhs.gov/what-critical-infrastructure.

Derrible, S., and C. Kennedy. 2009. "Network analysis of world subway systems using updated graph theory." *Transp. Res. Rec.* 2112 (1): 17–25. https://doi.org/10.3141/2112-03.

Derrible, S., and C. Kennedy. 2010. "The complexity and robustness of metro networks." *Physica A* 389 (17): 3678–3691. https://doi.org/10.1016/j.physa.2010.04.008.

DHS Risk Steering Committee. 2008. *DHS risk lexicon*. Washington, DC: DHS.

Dickison, M., S. Havlin, and H. E. Stanley. 2012. "Epidemics on interconnected networks." *Phys. Rev. E* 85 (6): 066109. https://doi.org/10.1103/PhysRevE.85.066109.

Duan, S., S. Lee, S. Chinthavali, and M. Shankar. 2016. "Reliable communication models in interdependent critical infrastructure networks." In *Resilience Week (RWS)*, 152–157. New York: IEEE.

Duan, S., S. Lee, S. Chinthavali, and M. Shankar. 2017a. "Best effort broadcast under cascading failures in interdependent networks." In *Proc., 18th Int. Conf. on Distributed Computing and Networking (ICDCN)*, 27. New York: ACM.

Duan, S., S. Lee, S. Chinthavali, and M. Shankar. 2018. "Best effort broadcast under cascading failures in interdependent critical infrastructure networks." *Pervasive Mob. Comput.* 43 (Jan): 114–130. https://doi.org/10.1016/j.pmcj.2017.12.006.

Duan, Z., Z. Lei, M. Zhang, W. Li, J. Fang, and J. Li. 2017b. "Understanding evacuation and impact of a metro collision on ridership using large-scale mobile phone data." *IET Intel. Transp. Syst.* 11 (8): 511–520. https://doi.org/10.1049/iet-its.2016.0112.

Dudenhoeffer, D. D., M. R. Permann, and M. Manic. 2006. "Cims: A framework for infrastructure interdependency modeling and analysis." In *Proc., 38th Conf. on Winter Simulation, Winter Simulation Conf.*, 478–485. New York: ACM.

Duggan, P. 2014. "Computer-driven trains returning to metro's red line five years after deadly rail crash." Accessed September 5, 2019. https://tex.stackexchange.com/questions/358136/citing-an-online-news-article-using-biblatex.

Dwiartama, A., and C. Rosin. 2014. "Exploring agency beyond humans: The compatibility of actor-network theory (ANT) and resilience thinking." *Ecol. Soc.* 19 (3): 28. https://doi.org/10.5751/ES-06805-190328.

Ebrahimy, R. 2014. "Investigating SCADA failures in interdependent critical infrastructure systems." Preprint, submitted April 30, 2015. https://arxiv.org/abs/1404.7565.

Eldosouky, A., W. Saad, and N. Mandayam. 2017. "Resilient critical infrastructure: Bayesian network analysis and contract-based optimization." Preprint, submitted August 30, 2015. https://arxiv.org/abs/1709.00303.

Ernstson, H. 2008a. "In Rhizomia: Actors, networks and resilience in urban landscapes." Ph.D. thesis, Natural Resources Management, Systemekologiska institutionen.

Ernstson, H. 2008b. "The social production of ecosystem services: Lessons from urban resilience research." Ph.D. thesis, Natural Resources Management, Stockholm Univ.

Ernstson, H. 2013. "The social production of ecosystem services: A framework for studying environmental justice and ecological complexity in urbanized landscapes." *Landscape Urban Plann.* 109 (1): 7–17. https://doi.org/10.1016/j.landurbplan.2012.10.005.

Ernstson, H., S. Sörlin, and T. Elmqvist. 2008. "Social movements and ecosystem services: The role of social network structure in protecting and managing urban green areas in Stockholm." *Ecol. Soc.* 13 (2): 39. https://doi.org/10.5751/ES-02589-130239.

Falliere, N., L. O. Murchu, and E. Chien. 2011. "W32.stuxnet dossier." *Symantec Secur. Response* 5 (6): 29.

Farías, I., and T. Bender. 2012. *Urban assemblages: How actor-network theory changes urban studies*. London: Routledge.

FEMA. 2013. *Mitigation assessment team report, hurricane sandy in New Jersey and New York: Building performance observations, recommendations, and technical guidance*. Washington, DC: FEMA.

FERC/NERC. 2012. *Arizona-southern California outages on September 8, 2011: Causes and recommendations*. Washington, DC: FERC/NERC.

F-Secure Labs. 2016. "BLACKENERGY & QUEDAGH: The convergence of crimeware and APT attacks." In *Malware Analysis Whitepaper*. Helsinki, Finland: F-Secure Labs.

Funk, S., E. Gilad, and V. Jansen. 2010. "Endemic disease, awareness, and local behavioural response." *J. Theor. Biol.* 264 (2): 501–509. https://doi.org/10.1016/j.jtbi.2010.02.032.

Funk, S., E. Gilad, C. Watkins, and V. A. Jansen. 2009. "The spread of awareness and its impact on epidemic outbreaks." *Proc. Natl. Acad. Sci. U.S.A.* 106 (16): 6872–6877. https://doi.org/10.1073/pnas.0810762106.

Gao, J., B. Barzel, and A.-L. Barabási. 2016. "Universal resilience patterns in complex networks." *Nature* 530 (7590): 307. https://doi.org/10.1038/nature16948.

Gao, J., S. V. Buldyrev, H. E. Stanley, and S. Havlin. 2012. "Networks formed from interdependent networks." *Nat. Phys.* 8 (Dec): 40–48. https://doi.org/10.1038/nphys2180.

Garcia, L., F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. A. Mohammed, and S. A. Zonouz. 2017. "Hey, my malware knows physics! Attacking PLCs with physical model aware rootkit." In *Proc., Network and Distributed System Security Symp.*, 1–15. Reston, VA: Internet Society.

Gibbons, A. 1985. *Algorithmic graph theory.* Cambridge: Cambridge University Press.

Gil, E. M., and J. D. McCalley. 2011. "A US energy system model for disruption analysis: Evaluating the effects of 2005 hurricanes." *IEEE Trans. Power Syst.* 26 (3): 1040–1049. https://doi.org/10.1109/TPWRS.2010.2089810.

Gilbert, S., and B. M. Ayyub. 2016. "Models for the economics of resilience." *ASCE-ASME J. Risk Uncertainty Eng. Syst. Part A: Civ. Eng.* 2 (4): 04016003. https://doi.org/10.1061/AJRUA6.0000867.

GL Communications. 2008. *Newsletter: Centralized supervisory and control systems for mass transit networks*. Gaithersburg, MD: GL Communications.

Graham, S., and N. Thrift. 2007. "Out of order: Understanding repair and maintenance." *Theory Culture Soc.* 24 (3): 1–25. https://doi.org/10.1177/0263276407075954.

Grove, K. 2013. "On resilience politics: From transformation to subversion." *Resilience* 1 (2): 146–153. https://doi.org/10.1080/21693293.2013.804661.

Guille, A., H. Hacid, C. Favre, and D. A. Zighed. 2013. "Information diffusion in online social networks: A survey." *ACM Sigmod Rec.* 42 (1): 17–28. https://doi.org/10.1145/2503792.2503797.

Habib, M. F., M. Tornatore, and B. Mukherjee. 2015. "Cascading-failure-resilient interconnection for interdependent power grid-optical networks." In *Proc., 2015 Optical Fiber Communications Conf. and Exhibition (OFC)*, 1–3. New York: IEEE.

Hadjsaid, N., M. Viziteu, B. Rozel, R. Caire, J.-C. Sabonnadière, D. Georges, and C. Tranchita. 2010. "Interdependencies of coupled heterogeneous infrastructures: The case of ICT and energy." In *Proc., IDRC Davos 2010, 3rd Int. Disaster and Risk Conf.* Lyon, France: HAL Archives.

Harvey, P., and H. Knox. 2015. *Roads: An anthropology of infrastructure and expertise*. Ithaca, NY: Cornell University Press.

Hasnat, M. M., M. R. Islam, and M. Hadiuzzaman. 2018. "Application of gis for disaster response in dense urban areas: A case study for Dhaka city." In *Transportation Research Board 97th Annual Meeting*. Washington, DC: Transportation Research Board.

Hawelka, B., I. Sitko, E. Beinat, S. Sobolevsky, P. Kazakopoulos, and C. Ratti. 2014. "Geo-located twitter as proxy for global mobility patterns." *Cartography Geographics Inf. Sci.* 41 (3): 260–271. https://doi.org/10.1080/15230406.2014.890072.

Henley, E. J., and H. Kumamoto. 1996. *Probabilistic risk assessment and management for engineers and scientists*. 2nd ed. New York: IEEE Press.

Henry, D., and J. E. Ramirez-Marquez. 2012. "Generic metrics and quantitative approaches for system resilience as a function of time." *Reliab. Eng. Syst. Saf.* 99 (Mar): 114–122. https://doi.org/10.1016/j.ress.2011.09.002.

Holling, C. S. 1973. "Resilience and stability of ecological systems." *Annu. Rev. Ecol. Syst.* 4 (1): 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245.

Holmgren, A. J. 2006. "Using graph models to analyze the vulnerability of electric power networks." *Risk Anal.* 26 (4): 955–969. https://doi.org/10.1111/j.1539-6924.2006.00791.x.

Hosseini, S., K. Barker, and J. E. Ramirez-Marquez. 2016. "A review of definitions and measures of system resilience." *Reliab. Eng. Syst. Saf.* 145 (Jan): 47–61. https://doi.org/10.1016/j.ress.2015.08.006.

Howe, C., et al. 2016. "Paradoxical infrastructures: Ruins, retrofit, and risk." *Sci. Technol. Hum. Values* 41 (3): 547–565. https://doi.org/10.1177/0162243915620017.

Huang, J., T. Xiao, Z. Sheng, and G. Chen. 2007. "Modeling an evolving complex supply network." *J. Syst. Sci. Inf.* 5 (4): 327–338.

Huang, X., S. Shao, H. Wang, S. V. Buldyrev, H. E. Stanley, and S. Havlin. 2013a. "The robustness of interdependent clustered networks." *EPL (Europhys. Lett.)* 101 (1): 18002.

Huang, Z., C. Wang, A. Nayak, and I. Stojmenovic. 2015. "Small cluster in cyber physical systems: Network topology, interdependence and cascading failures." *IEEE Trans. Parallel Distrib. Syst.* 26 (8): 2340–2351. https://doi.org/10.1109/TPDS.2014.2342740.

Huang, Z., C. Wang, M. Stojmenovic, and A. Nayak. 2013b. "Balancing system survivability and cost of smart grid via modeling cascading failures." *IEEE Trans. Emerging Top. Comput.* 1 (1): 45–56. https://doi.org/10.1109/TETC.2013.2273079.

Ibáñez, E., K. Gkritza, J. McCalley, D. Aliprantis, R. Brown, A. Somani, and L. Wang. 2010. "Interdependencies between energy and transportation systems for national long term planning." In *Sustainable and resilient critical infrastructure systems*, 53–76. New York: Springer.

Ibáñez, E., S. Lavrenz, K. Gkritza, D. A. Mejia-Giraldo, V. Krishnan, J. D. McCalley, and A. K. Somani. 2016. "Resilience and robustness in long-term planning of the national energy and transportation system." *Int. J. Crit. Infrastruct.* 12 (1–2): 82–103.

Ibáñez, E., and J. D. McCalley. 2011. "Multiobjective evolutionary algorithm for long-term planning of the national energy and transportation systems." *Energy Syst.* 2 (2): 151–169.

Jo, H.-H., S. K. Baek, and H.-T. Moon. 2006. "Immunization dynamics on a two-layer network model." *Physica A* 361 (2): 534–542. https://doi.org/10.1016/j.physa.2005.06.074.

Johansen, C., and I. Tien. 2018. "Probabilistic multi-scale modeling of interdependencies between critical infrastructure systems for resilience." *Sustainable Resilient Infrastruct.* 3 (1): 1–15.

Johnson, C. W. 2007. "Analyzing the causes of the italian and swiss blackout, 28th september 2003." In Vol. 86 of *Proc., 20th Australian Workshop on Safety Critical Systems and Software and Safety-Related Programmable Systems*, 21–30. Sydney, Australia: Australian Computer Society.

Karnouskos, S. 2011. "Stuxnet worm impact on industrial cyber-physical system security." In *Proc., 37th Annual Conf. on Industrial Electronics Society (IECON)*, 4490–4494. New York: IEEE.

Kim, H. M., M. Biehl, and J. A. Buzacott. 2005. "Modeling cyber interdependencies between critical infrastructures." In *Proc., 3rd IEEE Int. Conf. on Industrial Informatics (INDIN)*, 644–648. New York: IEEE.

Kim, Y., Y.-S. Chen, and K. Linderman. 2015. "Supply network disruption and resilience: A network structural perspective." *J. Oper. Manage.* 33: 43–59. https://doi.org/10.1016/j.jom.2014.10.006.

Kivelä, M., A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter. 2014. "Multilayer networks." *J. Complex Networks* 2 (3): 203–271.

Kleinberg, J. 2007. "Computing: The wireless epidemic." *Nature* 449 (7160): 287. https://doi.org/10.1038/449287a.

Koc, Y., M. Warnier, R. Kooij, and F. Brazier. 2014. "Structural vulnerability assessment of electric power grids." In *Proc., 11th IEEE Int. Conf. on Networking, Sensing and Control*, 386–391. New York: IEEE.

Korkali, M., J. G. Veneman, B. F. Tivnan, J. P. Bagrow, and P. D. Hines. 2017. "Reducing cascading failure risk by increasing infrastructure network interdependence." *Sci. Rep.* 7: 44499. https://doi.org/10.1038/srep44499.

Krishnan, V., E. Kastrouni, D. Pyrialakou, K. Gkritza, and J. D. McCalley. 2015. "An optimization model of national energy and transportation systems: Application on assessing the impact of high-speed rail on us passenger transportation investment portfolio." *Transp. Res. Part C: Emerg. Technol.* 54 (May): 131–156. https://doi.org/10.1016/j.trc.2015.03.007.

Kwasinski, A. 2012. *Hurricane Sandy effects on communication systems*. Tech. Rep. PR-AK-0112-2012. Austin, TX: Univ. of Texas at Austin.

Latora, V., and M. Marchiori. 2002. "Is the Boston subway a small-world network?" *Physica A* 314 (1–4): 109–113. https://doi.org/10.1016/S0378-4371(02)01089-0.

Latour, B. 2005. *Reassembling the social: An introduction to actor-network-theory.* Oxford: Oxford University Press.

Lee, E. E., II, J. E. Mitchell, and W. A. Wallace. 2007. "Restoration of services in interdependent infrastructure systems: A network flows approach." *IEEE Trans. Syst. Man Cybern. Part C: Appl. Rev.* 37 (6): 1303–1317. https://doi.org/10.1109/TSMCC.2007.905859.

Lee, E. E., J. E. Mitchell, and W. A. Wallace. 2004. "Assessing vulnerability of proposed designs for interdependent infrastructure systems." In *Proc., 37th Annual Hawaii Int. Conf. on System Sciences*. New York: IEEE.

Lee, S., L. Chen, S. Duan, S. Chinthavali, M. Shankar, and B. A. Prakash. 2016a. "URBAN-NET: A network-based infrastructure monitoring and analysis system for emergency management and public safety." In *Proc., 2016 IEEE Int. Conf. on Big Data (Big Data)*, 2600–2610. New York: IEEE.

Lee, S., S. Chinthavali, S. Duan, and M. Shankar. 2016b. "Utilizing semantic big data for realizing a national-scale infrastructure vulnerability analysis system." In *Proc., Int. Workshop on Semantic Big Data*, 3. New York: ACM.

Leskovec, J., D. Chakrabarti, J. Kleinberg, C. Faloutsos, and Z. Ghahramani. 2010. "Kronecker graphs: An approach to modeling networks." *J. Mach. Learn. Res.* 11: 985–1042.

Li, W., A. Bashan, S. V. Buldyrev, H. E. Stanley, and S. Havlin. 2011. "Cascading failures in interdependent lattice networks: The critical role of the length of dependency links." *Phys. Rev. Lett.* 108 (22): 228702.

Lindsey, R. 2007. "Methods and models in transport and telecommunications: Cross Atlantic perspectives, edited by Aura Reggiani and laurie A. Schintler." *J. Reg. Sci.* 47 (2): 377–381. https://doi.org/10.1111/j.1467-9787.2007.00513_5.x.

Liu, Y., P. Ning, and M. K. Reiter. 2011. "False data injection attacks against state estimation in electric power grids." *Trans. Inf. Syst. Secur.* 14 (1): 13.

Luque-Ayala, A., and S. Marvin. 2016. "The maintenance of urban circulation: An operational logic of infrastructural control." *Environ. Plann. D: Soc. Space* 34 (2): 191–208. https://doi.org/10.1177/0263775815611422.

Mari, S. I., Y. H. Lee, and M. S. Memon. 2015. "Complex network theory-based approach for designing resilient supply chain networks." *Int. J. Logist. Syst. Manage.* 21 (3): 365–384. https://doi.org/10.1504/IJLSM.2015.069733.

Maslow, A. H. 1943. "A theory of human motivation." *Psychol. Rev.* 50 (4): 370. https://doi.org/10.1037/h0054346.

Masys, A. 2016. *Disaster management: Enabling resilience*. New York: Springer.

Masys, A. J. 2014. "Critical infrastructure and vulnerability: A relational analysis through actor network theory." In *Networks and network analysis for defence and security*, 265–280. New York: Springer.

McDaniels, T. L., S. E. Chang, D. Hawkins, G. Chew, and H. Longstaff. 2015. "Towards disaster-resilient cities: An approach for setting priorities in infrastructure mitigation efforts." *Environ. Syst. Decisions* 35 (2): 252–263. https://doi.org/10.1007/s10669-015-9544-7.

Medd, W., and S. Marvin. 2005. "From the politics of urgency to the governance of preparedness: A research agenda on urban vulnerability." *J. Contingencies Crisis Manage.* 13 (2): 44–49. https://doi.org/10.1111/j.1468-5973.2005.00455.x.

Menashri, H., and G. Baram. 2015. "Critical infrastructures and their interdependence in a cyber attack—The case of the US." *Mil. Strategic Affairs* 7 (1): 99–100.

Min, O. 2014. "Review on modeling and simulation of interdependent critical infrastructure systems." *Reliab. Eng. Syst. Saf.* 121 (Jan): 43–60. https://doi.org/10.1016/j.ress.2013.06.040.

Modarres, M., M. P. Kaminskiy, and V. Krivtsov. 2016. *Reliability engineering and risk analysis: A practical guide*. New York: CRC Press.

Moreno, Y., R. Pastor-Satorras, and A. Vespignani. 2002. "Epidemic outbreaks in complex heterogeneous networks." *Eur. Phys. J. B* 26 (4): 521–529.

Nan, C., and G. Sansavini. 2017. "A quantitative method for assessing resilience of interdependent infrastructures." *Reliab. Eng. Syst. Saf.* 157 (Jan): 35–53. https://doi.org/10.1016/j.ress.2016.08.013.

Newman, M. E. 2002a. "Assortative mixing in networks." *Phys. Rev. Lett.* 89 (20): 208701. https://doi.org/10.1103/PhysRevLett.89.208701.

Newman, M. E. 2002b. "Spread of epidemic disease on networks." *Phys. Rev. E* 66 (1): 016128. https://doi.org/10.1103/PhysRevE.66.016128.

Newman, M. E. 2003. "Mixing patterns in networks." *Phys. Rev. E* 67 (2): 026126. https://doi.org/10.1103/PhysRevE.67.026126.

Newman, M. E. 2008. "The mathematics of networks." *New Palgrave Encycl. Econ.* 2: 1–12.

NRC (National Research Council). 2011. *National earthquake resilience: Research, implementation, and outreach*. Washington, DC: National Academies Press.

Pagani, G. A., and M. Aiello. 2013. "The power grid as a complex network: a survey." *Physica A* 392 (11): 2688–2700. https://doi.org/10.1016/j.physa.2013.01.023.

Parandehgheibi, M., and E. Modiano. 2013. "Robustness of interdependent networks: The case of communication networks and the power grid." In *Proc., 2013 IEEE Global Communications Conf. (GLOBECOM)*, 2164–2169. New York: IEEE.

Parandehgheibi, M., E. Modiano, and D. Hay. 2014. "Mitigating cascading failures in interdependent power grids and communication networks." In *Proc., Int. Conf. on Smart Grid Communications (SmartGridComm)*, 242–247. New York: IEEE.

Pederson, P., D. Dudenhoeffer, S. Hartley, and M. Permann. 2006. "Critical infrastructure interdependency modeling: A survey of US and international research." *Ida. Natl. Lab.* 25: 27.

Perera, S. S., M. Bell, and M. Bliemer. 2015. "Modelling supply chains as complex networks for investigating resilience: An improved methodological framework." In Vol. 30 of *Proc., 37th Australasian Transport Research Forum (ATRF)*. Sydney, Australia: Australasian Transport Research Forum Incorporated.

Petit, F., and L. P. Lewis. 2017. "Risk management and business continuity assessment: Importance of considering logical interdependencies." *Crit. Infrastruct. Prot. Rev.* 29.

Petit, F., D. Verner, D. Brannegan, W. Buehring, D. Dickinson, K. Guziel, R. Haffenden, J. Phillips, and J. Peerenboom. 2015. *Analysis of critical infrastructure dependencies and interdependencies*. No. ANL/GSS-15/4. Argonne, IL: Argonne National Laboratory.

PPD (Presidential Policy Directive). 2011. *National preparedness*. PPD-8. Washington, DC: US Dept. of Homeland Security.

PPD (Presidential Policy Directive). 2013. *Critical infrastructure security and resilience*. PPD-21. Washington, DC: White House.

Quelhas, A., E. Gil, J. D. McCalley, and S. M. Ryan. 2007. "A multiperiod generalized network flow model of the US integrated energy system. I: Model description." *IEEE Trans. Power Syst.* 22 (2): 829. https://doi.org/10.1109/TPWRS.2007.894844.

Rinaldi, S. M., J. P. Peerenboom, and T. K. Kelly. 2001. "Identifying, understanding, and analyzing critical infrastructure interdependencies." *IEEE Control Syst. Mag.* 21 (6): 11–25. https://doi.org/10.1109/37.969131.

Rrushi, J., H. Farhangi, C. Howey, K. Carmichael, and J. Dabell. 2015. "A quantitative evaluation of the target selection of Havex ICS malware plugin." In *Proc., Industrial Control System Security (ICSS) Workshop*. New York: ACM.

Salehi, M., R. Sharma, M. Marzolla, M. Magnani, P. Siyari, and D. Montesi. 2015. "Spreading processes in multilayer networks." *IEEE Trans. Network Sci. Eng.* 2 (2): 65–83. https://doi.org/10.1109/TNSE.2015.2425961.

Santos-Reyes, J., D. Padilla-Pérez, and A. N. Beard. 2015. "Modeling critical infrastructure interdependency: The case of the Mexico City metro transport system." *Hum. Ecol. Risk Assess.: Int. J.* 21 (5): 1428–1444. https://doi.org/10.1080/10807039.2014.957956.

Satumtira, G., and L. Dueñas-Osorio. 2010. "Synthesis of modeling and simulation methods on critical infrastructure interdependencies research." In *Sustainable and resilient critical infrastructure systems*, 1–51. Berlin/Heidelberg: Springer.

Schlake, B., C. Barkan, and J. Edwards. 2011. "Train delay and economic impact of in-service failures of railroad rolling stock." *Transp. Res. Rec.* 2261: 124–133. https://doi.org/10.3141/2261-14.

Sen, P., S. Dasgupta, A. Chatterjee, P. Sreeram, G. Mukherjee, and S. Manna. 2003. "Small-world properties of the Indian railway network." *Phys. Rev. E* 67 (3): 036106. https://doi.org/10.1103/PhysRevE.67.036106.

Short, J. R. 2016. "A perfect storm: Climate change, the power grid, and regulatory regime change after network failure." *Environ. Plann. C: Government Policy* 34 (2): 244–261. https://doi.org/10.1177/0263774X15614185.

Siemens. 2012. *Driverless metro system*. Munich, Germany: Siemens.
Simone, R. C. 2014. "Cascading failure in critical infrastructure: An actor-network analysis of the 1998 ice storm in Ottawa." Ph.D. thesis, Dept. of Geography, Carleton Univ.
Singha, M. R., and B. Kalita. 2013. "Mapping mobile phone network onto urban traffic network." In *Proc., Int. Multi Conf. of Engineers and Computer Scientists*. Hong Kong: International Association of Engineers.
Sivanandam, S. 2016. "Metro traction control system using PLC and SCADA monitoring." In *Gurukulam Int. J. Innovations Sci. Eng*. 1.
Sturaro, A., S. Silvestri, M. Conti, and S. K. Das. 2016. "Towards a realistic model for failure propagation in interdependent networks." In *Proc., Int. Conf. on Computing, Networking and Communications (ICNC)*, 1–7. New York: IEEE.
Sun, Y., and H. Song. 2017. *Secure and trustworthy transportation cyber-physical systems*. Singapore: Springer.
Surana, A., S. Kumara, M. Greaves, and U. N. Raghavan. 2005. "Supply-chain networks: A complex adaptive systems perspective." *Int. J. Prod. Res.* 43 (20): 4235–4265. https://doi.org/10.1080/00207540500142274.
Taft, J. D., and A. S. Becker-Dippmann. 2015. *The emerging interdependence of the electric power grid & information and communication technology*. No. PNNL-24643. Richland, WA: Pacific Northwest National Laboratory.
Tang, C. S. 2006. "Robust strategies for mitigating supply chain disruptions." *Int. J. Logist.: Res. Appl.* 9 (1): 33–45. https://doi.org/10.1080/13675560500405584.
Taylor, M. 2017. *Vulnerability analysis for transportation networks*. Amsterdam, Netherlands: Elsevier.
Thadakamaila, H., U. N. Raghavan, S. Kumara, and R. Albert. 2004. "Survivability of multiagent-based supply networks: A topological perspective." *IEEE Intell. Syst.* 19 (5): 24–31.
Tien, I., and A. Der Kiureghian. 2016. "Algorithms for Bayesian network modeling and reliability assessment of infrastructure systems." *Reliab. Eng. Syst. Saf.* 156 (Dec): 134–147. https://doi.org/10.1016/j.ress.2016.07.022.
Tien, I., and A. Der Kiureghian. 2017. "Reliability assessment of critical infrastructure using Bayesian networks." *J. Infrastruct. Syst.* 23 (4): 04017025. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000384.
Tong, Y., and I. Tien. 2017. "Algorithms for Bayesian network modeling, inference, and reliability assessment for multistate flow networks." *J. Comput. Civ. Eng.* 31 (5): 04017051. https://doi.org/10.1061/(ASCE)CP.1943-5487.0000699.
US–Canada Power System Outage Task Force. 2004. *Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations*. Washington, DC: US–Canada Power System Outage Task Force.
Vale, L. J. 2014. "The politics of resilient cities: Whose resilience and whose city?" *Build. Res. Inf.* 42 (2): 191–201. https://doi.org/10.1080/09613218.2014.850602.
Vertesi, J. 2014. "Seamful spaces: Heterogeneous infrastructures in interaction." *Sci. Technol. Hum. Values* 39 (2): 264–284. https://doi.org/10.1177/0162243913516012.
Vespignani, A. 2010. "Complex networks: The fragility of interdependency." *Nature* 464 (7291): 984. https://doi.org/10.1038/464984a.
Wallace, W. A., D. Mendonça, E. Lee, J. Mitchell, and J. Chow. 2001. "Managing disruptions to critical interdependent infrastructures in the context of the 2001 World Trade Center attack." In *Impacts of and Human Response to the September 11, 2001 Disasters: What Research Tells Us*. Boulder, CO: Natural Hazards Research and Applications Information Center.
Wang, H., Q. Li, G. D'Agostino, S. Havlin, H. E. Stanley, and P. Van Mieghem. 2013. "Effect of the interconnected network structure on the epidemic threshold." *Phys. Rev. E* 88 (2): 022801. https://doi.org/10.1103/PhysRevE.88.022801.
Wang, P., M. C. González, C. A. Hidalgo, and A.-L. Barabási. 2009. "Understanding the spreading patterns of mobile phone viruses." *Science* 324 (5930): 1071–1076. https://doi.org/10.1126/science.1167053.
Wang, Q., and J. E. Taylor. 2013. "Energy saving information cascades in online social networks: An agent-based simulation study." In *Proc., Simulation Conf. (WSC), 2013 Winter*, 3042–3050. New York: IEEE.
Wang, Q., and J. E. Taylor. 2015. "Resilience of human mobility under the influence of typhoons." *Procedia Eng.* 118: 942–949. https://doi.org/10.1016/j.proeng.2015.08.535.
Wang, S., L. Hong, and X. Chen. 2012. "Vulnerability analysis of interdependent infrastructure systems: A methodological framework." *Physica A* 391 (11): 3323–3335. https://doi.org/10.1016/j.physa.2011.12.043.
Wasserman, S., and K. Faust. 1994. Vol. 8 of *Social network analysis: Methods and applications*. Cambridge: Cambridge University Press.
Waterfall Security Solutions. 2017. "The top 20 cyber attacks against industrial control systems." In *White Paper*. New York: Waterfall Security Solutions.
Watts, D. J., and S. H. Strogatz. 1998. "Collective dynamics of 'small-world' networks." *Nature* 393 (6684): 440. https://doi.org/10.1038/30918.
West, D. B. 2001. Vol. 2 of *Introduction to graph theory*. Upper Saddle River, NJ: Prentice Hall.
Winkler, J., L. Dueñas-Osorio, R. Stein, and D. Subramanian. 2011. "Interface network models for complex urban infrastructure systems." *J. Infrastruct. Syst.* 17 (4): 138–150. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000068.
Yates, J., R. Batta, M. Karwan, and I. Casas. 2012. "Establishing public policy to protect critical infrastructure: Finding a balance between exposure and cost in Los Angeles County." *Transp. Policy* 24 (Nov): 109–117. https://doi.org/10.1016/j.tranpol.2012.08.003.
Zhang, D.-M., F. Du, H. Huang, F. Zhang, B. M. Ayyub, and M. Beer. 2018a. "Resiliency assessment of urban rail transit networks: Shanghai metro as an example." *Saf. Sci.* 106 (Jul): 230–243. https://doi.org/10.1016/j.ssci.2018.03.023.
Zhang, P., and S. Peeta. 2011. "A generalized modeling framework to analyze interdependencies among infrastructure systems." *Transp. Res. Part B: Methodol.* 45 (3): 553–579. https://doi.org/10.1016/j.trb.2010.10.001.
Zhang, Y. J., H. W. Huang, D. M. Zhang, and B. M. Ayyub. 2018b. "Vulnerability analysis of Shanghai metro network under water level rise." In *Proc., GeoShanghai Int. Conf.* New York: Springer.
Zhao, K., A. Kumar, and J. Yen. 2011. "Achieving high robustness in supply distribution networks by rewiring." *IEEE Trans. Eng. Manage.* 362–347 :(2) 58. https://doi.org/10.1109/TEM.2010.2095503.
Zhu, B., A. Joseph, and S. Sastry. 2011. "A taxonomy of cyber attacks on SCADA systems." In *Proc., Int. Conf. on Internet of Things (iThings/CPSCom) and the 4th Int. Conf. on Cyber, Physical and Social Computing*, 380–388. New York: IEEE.
Zhu, W., and J. V. Milanović. 2017. "Interdepedency modeling of cyber-physical systems using a weighted complex network approach." In *Proc., 2017 IEEE Manchester PowerTech*, 1–6. New York: IEEE.
Zimmerman, R. 2001. "Social implications of infrastructure network interactions." *J. Urban Technol.* 8 (3): 97–119. https://doi.org/10.1080/106307301753430764.