Sustainable Cities and Society 62 (2020) 102327

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs

Cyber-physical-social interdependencies and organizational resilience: A review of water, transportation, and cyber infrastructure systems and processes

Shima Mohebbi[a], Qiong Zhang[b,*], E. Christian Wells[c], Tingting Zhao[b], Hung Nguyen[d], Mingyang Li[d], Noha Abdel-Mottaleb[b], Shihab Uddin[b], Qing Lu[b], Mathews J. Wakhungu[c], Zhiqiang Wu[b], Yu Zhang[b], Anwesh Tuladhar[e], Xinming Ou[e]

[a] Department of Systems Engineering and Operations Research, George Mason University, Nguyen Engineering Building, Fairfax, VA, 22030, USA
[b] Department of Civil and Environmental Engineering, University of South Florida, 4202 E. Fowler Ave., Tampa, FL, 33620, USA
[c] Department of Anthropology, University of South Florida, 4202 E. Fowler Ave., Tampa, FL, 33620, USA
[d] Department of Industrial and Management Systems Engineering, University of South Florida, 4202 E. Fowler Ave., Tampa, FL, 33620, USA
[e] Department of Computer Science and Engineering, University of South Florida, 4202 E. Fowler Ave., Tampa, FL, 33620, USA

ARTICLE INFO

Keywords:
Infrastructure interdependency
Integration
Resilience metrics
Sustainable design strategies

ABSTRACT

Building resilience in critical infrastructures for smart and connected cities requires consideration of different types of interdependencies. Previous research has mainly conceptualized three types of interdependencies including cyber, physical, and social. To develop resilient and sustainable design, operations, and managerial strategies, domain knowledge for each infrastructure along with its organizational characteristics needs to be integrated with those of other infrastructures. In this review paper, an infrastructure-oriented approach is taken to systematically examine different types of interdependencies and resilience quantification techniques for water, transportation, and cyber infrastructures. Design, operations, and managerial strategies are identified and categorized into short-term, mid-term, and long-term plans that can potentially improve the resilience and sustainability of the underlying infrastructures. Future research needs, in terms of resilience metrics, interdependency, and strategies, are discussed.

1. Introduction

In recent decades, the occurrence of many serious disasters, such as Hurricane Katrina in 2005, the earthquakes in Japan in 2011, and Hurricanes Harvey, Irma, and Maria in 2017, have had tremendous negative impacts on economic growth, social development, and public health and safety by impairing or destroying essential urban infrastructure, such as electric power systems, transportation systems, and communication systems. For instance, in 2011 a disaster caused by the earthquake and tsunami in Japan killed 15,782 people, destroyed 128,530 houses, damaged 870 km of expressways and 939 water drainage system components, and reduced about 55 % of the capacity of the fossil fuel-fired and geothermal power plants (Kazama & Noda, 2012). In addition to the physical damage, the total estimated economic loss was about 16.9 trillion JPY (~155.7 billion USD), including 1.3 trillion JPY (~12 billion USD) loss of the lifetime infrastructure facilities (water supply, gas, electricity, communications, broadcasting facilities, etc.) and 2.2 trillion JPY (~ 20.2 billion USD) loss of social infrastructure facilities (rivers, roads, ports, airports, etc.) (Kazama & Noda, 2012).

To achieve the goal of minimizing the damage of similar events in the future, researchers have attempted not only to predict the impacts of these events, but also to estimate how fast our systems can recover from the consequences. Therefore, many studies on risk, vulnerability, and resilience analysis have been carried out recently to find solutions (Hosseini, Barker, & Ramirez-Marquez, 2016). Risk analysis considers the probability and severity of adverse effects, while vulnerability and resilience are key concepts in risk analysis (Lowrance, 1976). Various terms have been used in similar fields, and Fig. 1 illustrates the relationship among these terms. In general, there are 16 critical infrastructure sectors (water and wastewater systems, transportation systems, energy, communications, emergency services, etc.) identified by U.S. Presidential Policy Directive 21 (PPD-21) (The White House, 2013). These infrastructure systems are considered to be critical to the

* Corresponding author.
E-mail address: qiongzhang@usf.edu (Q. Zhang).

https://doi.org/10.1016/j.scs.2020.102327
Received 16 October 2019; Received in revised form 17 March 2020; Accepted 9 June 2020
Available online 21 June 2020
2210-6707/

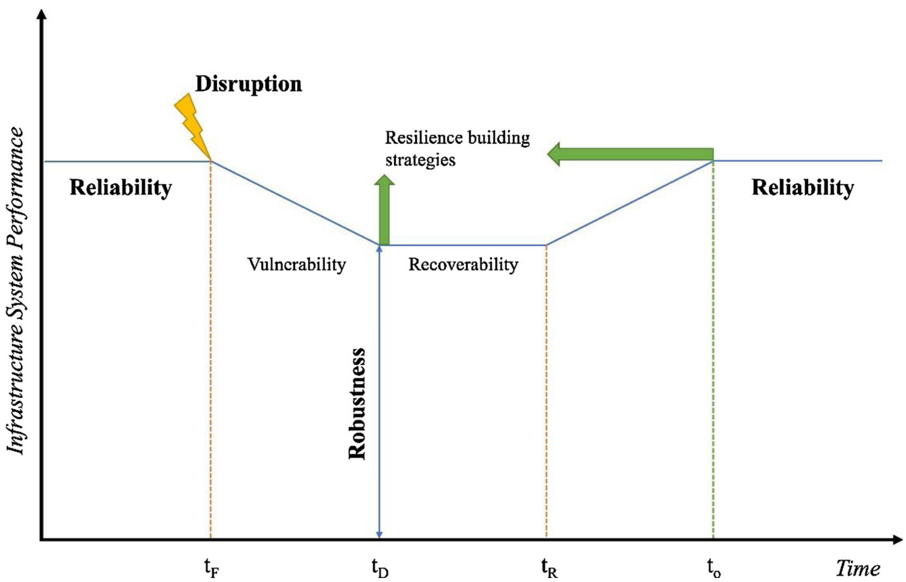

Fig. 1. Terms used in the literature related to resilience and their relationship: t_F = time when disruption occurs, t_D = time at which system inoperable, t_R = time at which system repair is initiated, t_o = time at which system regains operability. Waiting time = t_R - t_D; Propagation of failure/inoperability (or time to maximum impact of disturbance) = t_D - t_F; Time to system repair = t_o–t_R; The down time is from t_F to t_o; System operational availability = t_D/total time investigated; Resilience building strategies can be enacted both to increase robustness and enhance recoverability (thereby decreasing down time and potentially wait time).

United States' security and prosperity. They are not isolated but interdependent at different levels, which affect overall infrastructure performance.

In this review paper, we focus on three critical and interdependent infrastructure systems, namely, water, transportation, and cyber infrastructures. These systems not only provide essential services to the public under normal conditions and survivability during disastrous scenarios, but also consume a high proportion of public spending annually at various government levels. This work also reviews the concept of resilience and how it is manifest in the infrastructure systems under investigation. Water, transportation, and cyber infrastructure systems are vital to community well-being and sustainable growth, especially in large metropolitan settings where interdependencies among these infrastructures often constrain recovery efforts. Previous studies have established that water and transportation systems are considered critical infrastructures; hence, it is imperative to continue examining factors that can affect these systems. Furthermore, as all critical infrastructure sectors are moving towards more intelligent controls through computing and communication, the resilience of cyberspace has become an indispensable component of the resilience of the interdependent critical infrastructures, especially in smart and connected cities. In addition to the critical functions and current status of water, transportation, and cyber infrastructures, these systems also represent different types of interdependencies, including physical, social, and cyber, and together provide a strategic opportunity to study the impacts of interdependencies on the resilience of the critical infrastructures. The greater goal of this effort is to better understand how infrastructure systems and processes are increasingly interconnected, and how taking advantage of those interconnections can support sustainable cities of the future (Bibri & Krogstie, 2017; Silva, Khan, & Han, 2018).

1.1. Resilience

In 1973, C. S. Holling introduced the concept of resilience in ecological systems (Holling, 1973). Since then, resilience has been used widely in many different fields beyond ecology. Besides its original definition of the ability of a system to recover to its pre-existing condition after its state is disrupted (Hosseini et al., 2016), resilience has been defined and interpreted differently in the context of various domains, as summarized in Table 1. In this article, we view the concepts of resilience and sustainability as distinct but complementary approaches, where resilience contends with building adaptive capacity while sustainability concerns reordering system dynamics to sustain system functions (Redman, 2014).

There have been several informative reviews about resilience in the recent literature. Bhamra et al. reviewed the application of resilience at the organizational level, particularly regarding the interaction between human factors and organizational resilience, and between the resilience of infrastructures and organizations (Bhamra, Dani, & Burnard, 2011). Martin-Breen and Anderies provided a comprehensive review of the theory of resilience and its applications in the areas of engineering, psychology, complex adaptive systems, and economics over the past 50 years (Martin-Breen & Anderies, 2011). Hosseini et al. presented a review of how to define and measure resilience in different fields, with a focus on qualitative and quantitative approaches in engineering domains (Hosseini et al., 2016). In order to identify a research agenda for engineering resilience, Righi et al. reviewed many studies in different areas of engineering, including the theory of engineering resilience, identification and classification of resilience, safety management tools, analysis of accidents, risk assessment, and training (Righi, Saurin, & Wachs, 2015). These reviews, however, only focused on the research of how to define and quantify resilience of a single domain without considering interactions among several domains, which are typically designed, operated, and maintained by different and independent agencies. Improvement measures for resilience of one system, therefore, might negatively affect the resilience of another.

Global disasters, including the recent Caribbean hurricanes, the Japanese earthquakes, and the UK floods, have demonstrated the significance of the interconnected and interdependent nature of critical infrastructure systems. Ouyang offers some examples to demonstrate how critical infrastructures can be interdependent (Ouyang, 2014). For example, water and telecommunication services require electricity to function while electric power systems need these services to generate and deliver their power. Moreover, it is common to only regard systems as dependent. For instance, road and rail systems are useful to transport petroleum, while this fuel is vital for the generator of an electricity system. This view sustains the belief that one system depends on another but not necessarily vice versa. In reality, all of these systems are interdependent on each other, creating multi-directional relationships within the systems. For example, we must acknowledge that, while transportation systems help move fuels, road and rail systems cannot operate without fuel. Hence, many researchers advise the need to acknowledge the interdependency of critical infrastructure systems and processes (Ouyang, 2014; Rinaldi, Peerenboom, & Kelly, 2002).

Table 1
Definitions of resilience in different domains.

Discipline/Domain	Definition of resilience	Reference
Ecological systems	"A measure of the persistence of systems and their ability to absorb change and disturbance and still maintain the same relationship between populations or state variables"	(Holling, 1973)
	The speed of a system to return to an equilibrium state after a disruption	(Tilman & Downing, 1994)
Organizational Systems	The ability to maintain a steady state or recover from a disruptive event to be able to operate as normal	(Sheffi, 2013)
Social Systems	The capacity of individuals, groups, community and environment to cope with external disturbing events	(Adger, 2000)
Economic systems	"The capacity to reconfigure, that is adapt, its structure (firms, industries, technologies, institutions) so as to maintain an acceptable growth path in output, employment and wealth over time."	(Martin, 2012)
Socio-ecological systems	The ability of a system to maintain its functionality or reorganize if a disturbance happens	(Walker et al., 2002)
Engineering domain	A system's ability to adjust in the face of disturbance	(Hollnagel, Woods, & Leveson, 2006)
	In the face of resilience, systems need to fully recover rapidly and return to pre-disaster state	(American Society of Mechanical Engineers (ASME), 2009)
Infrastructure systems	The ability to predict disturbances in addition to adapting and recovering from them	(National Infrastructure Advisory Council (NIAC), 2009)
Power systems (Cyber-physical)	The ability of system to maintain electricity continuously to customers given a certain load prioritization scheme	(Arghandeh, von Meier, Mehrmanesh, & Mili, 2016)
Water systems	Refers to design, maintenance, and operations of water infrastructure that limits the effects of disasters and enables rapid return to normal delivery of safe water to customers	(Bousquin, Hychka, & Mazzotta, 2015)
Transportation systems	The systems' capacity to recover from unexpected and severe disturbance in a dynamic environment	(Tamvakis & Xenidis, 2012)

1.2. Interdependencies

Water, transportation, and cyber infrastructures are not isolated but interdependent at different levels, which affect overall infrastructure performance. Such interdependencies can be generally categorized as physical (e.g., functional, geospatial), virtual (e.g., informational, policy), and social (e.g., attitudinal, budgetary) (Ouyang, 2014; Pederson, Dudenhoeffer, Hartley, & Permann, 2006; Zhang & Peeta, 2013). Physical interdependencies can be defined as the dependency of one infrastructure on another's material outputs, inputs, layouts, or operations due to their connection in material input and output or their geospatial proximity (co-location). Geospatial interdependencies have been separately recognized as a type of interdependency, however, the proximity between infrastructure systems can also cause physical cascading failures if one of them fails. For instance, water breaks can cause lane closures leading to traffic blockage. Virtual interdependencies pertain to scenarios when the linkage of infrastructures relies on information flow. Interruption in mobile phone services, for example, can lead to the lack of knowledge in other departments to restore systems after failure. Social interdependencies refer to the cultural, political, and economic relationships between administrators, consumers and infrastructure systems, such as how aging transportation and stormwater systems can lead to private property damage in times of climate stress. A comprehensive discussion on different types of interdependencies can be found in (Ouyang, 2014).

There have been previous reviews of interdependency and different criteria have been investigated to evaluate and compare existing studies. Many researchers have reviewed studies of interdependencies to classify them based on different mathematical/computational modeling methodologies (Satumtira & Dueñas-Osorio, 2010), such as simulation modeling, stochastic/statistical modeling, and optimization modeling. Recently, there has been recognition about the lack of integration between the two concepts of interdependency and resilience. To the best of our knowledge, only one review paper has attempted to categorize studies on interdependency, focusing specifically on how resilience might relate to interdependency (Ouyang, 2014). Several strategies were suggested in (Ouyang, 2014) to improve resilience, specifically for interdependent critical infrastructure systems. The authors point out that future studies need to examine interdependency more closely with the concept of resilience to further improve maintenance and management of critical infrastructure systems. In addition, the majority of studies on interdependency consider either general concepts across multiple infrastructures (Ouyang, 2014) or are mainly restricted to studying power systems (D. Reed, Kapur, & Christie, 2009; Ouyang & Wang, 2015). Hence, there remains a dearth of literature for water, transportation, and cyber system interdependencies. This review paper is infrastructure-oriented and sheds light on specific strategies to improve the resilience of water, transportation, and cyber systems in the context of three types of interdependencies.

1.3. Interdependency and resilience

Although there have been many researchers who study resilience and interdependency separately, few have considered how interdependent infrastructures affect the resilience of the entire system. Ouyang, for example, used resilience as one of the criteria to compare and summarize different approaches to study the performance response of interdependent infrastructures (Ouyang, 2014). Ouyang and Wang proposed a method to assess resilience in interdependent infrastructures (power and gas systems) and found that synergistic strategies that take interdependency into consideration produced the most resilient outcomes compared to independent strategies (Ouyang & Wang, 2015). Reed et al. proposed a methodology using an input-output model and structural fragilities to measure the resilience of multi-system infrastructure, with particular emphasis on the influence of electric power systems on other infrastructure systems (D. Reed et al., 2009). Using the example of power and telecommunication systems in Hurricane Katrina, they found that both power outage and power restoration affected the restoration of the telecommunications system, hence demonstrating the close relationship between resilience and interdependency. Other studies have focused on assessing the resilience of interdependent infrastructures. For instance, Pant et al. addressed the problem of estimating, quantifying, and planning for the economic resilience of interdependent infrastructures using quantitative metrics: static resilience metric, time averaged level of operability, maximum loss of functionality, and time to recovery (Pant, Barker, & Zobel, 2014). Cimellaro et al. considered time series analysis to evaluate the impacts of interdependencies on the resilience of physical infrastructures (Cimellaro, Solari, & Bruneau, 2014).

1.4. A resilience assessment framework for physical-cyber-social interdependencies

While different modeling approaches have been proposed to capture different infrastructures, or emphasize different aspects of interdependent critical infrastructure systems, a strategic framework is needed to integrate different modeling approaches based on their unique capabilities. It is also critical to validate modeling approaches in a uniform framework and disseminate the framework to urban planners, infrastructure mangers, policymakers, and other stakeholders in an easy and understandable manner. The goals of the current review are to: a) survey and summarize the literature for water-transportation-cyber interdependent systems; b) jointly review three types of interdependencies, namely, physical, virtual, and social interdependencies among water, transportation, and cyber infrastructures; and c) consider the impacts from interdependency on the resilience of target critical infrastructure systems. To select papers for the review, we first conducted a comprehensive search through different online database sources, including ASCE Research Library, CRCnetBASE, Engineering Database, IEEE Xplore, ScienceDirect, Springer, Annual Reviews, Wiley Online Library, Computer Science Database and JSTOR. Based on the keywords and phrases of “water infrastructures”, “transportation infrastructures”, “cyber infrastructures”, “interdependency”, “critical infrastructures”, “resilience” and “resilience metrics”, we identified 601 papers. We then preformed a screening process based on the following inclusion and exclusion criteria. For duplicated papers, only the original ones were included. All the papers about resilience that did not address the interdependencies between critical infrastructures or were unrelated to cyber-physical-social interdependencies were excluded. Ultimately, we identified 207 relevant papers in total for this review. Fig. 2 summarizes the procedure of the overall paper selection process. Our review scheme of a resilience assessment framework is also depicted in Fig. 3. In this paper, we emphasize vulnerability as a dynamic property of resilient infrastructure systems and processes.

2. Infrastructure characteristics

2.1. Water infrastructure

In this paper, water infrastructure includes potable water, wastewater, and stormwater systems. Potable water systems include physical

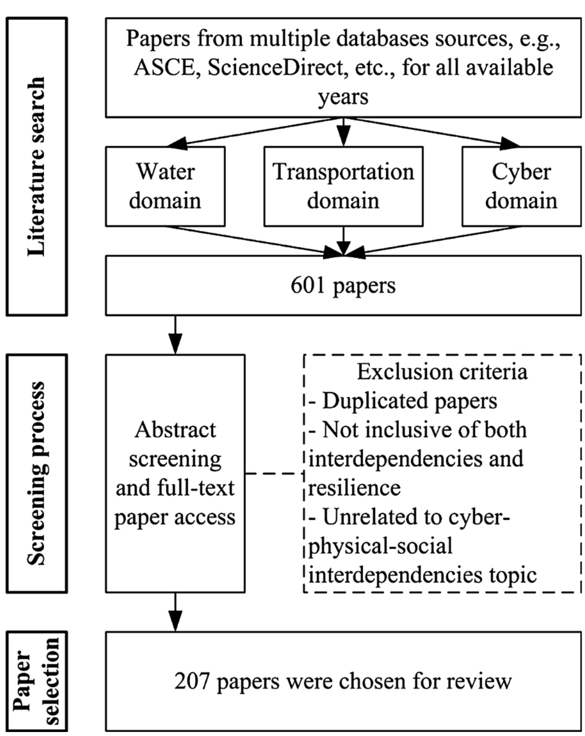

Fig. 2. Literature review procedure and selection criteria.

elements (e.g., infrastructure to convey raw water to the treatment plant, a treatment facility to treat raw water to drinking water standards, a distribution network to distribute treated water to consumers at a required pressure, and infrastructure to monitor conventional regulated and unregulated contaminants and status of the operations), cyber elements (e.g., a Supervisory Control and Data Acquisition [SCADA] system to automate control of drinking water facilities), and human elements (e.g., employees and contractors to manage and operate the infrastructure systems, administrators to develop policies and practices for infrastructure operations and financing, and consumers of infrastructure products and services) (U.S. EPA, 2011). Wastewater systems collect municipal wastewaters and convey them to treatment plants through collection and conveyance systems and pump stations. Treated wastewater is then discharged as effluent into a receiving body of water, or may be reused for irrigation or other purposes through reclaimed water distribution networks. Similar to potable water systems, wastewater systems include monitoring infrastructure, cyber elements, and human elements. Stormwater systems have the same elements as wastewater systems but different collection infrastructure including gutters, storm sewers, tunnels, culverts, detention basins, pipes, and mechanical devices to collect stormwater. Stormwater is defined as “water that runs off all urban surfaces such as roofs, pavements, car parks, roads, gardens and vegetated open spaces and is captured in constructed storages and drainage systems” (Natural Resource Management Ministerial Council & National Health & Medical Research Council, 2009). In the past, stormwater and wastewater facilities were designed as combined sewer systems but the development of separate sewer systems consisting of separate collection of municipal wastewater and stormwater has become the dominant trend.

2.2. Transportation infrastructure

In a broad sense, transportation systems include roads, airways, railways, water, and pipeline transportation, and all other infrastructures essential for the operation of these modes of transportation. This article mainly focuses on the road transportation system and its components. Pavement, one of the important components of the road transportation system, is emphasized as the main transportation infrastructure. Typical functional classification of roads includes arterials, collectors, and local roads. Arterials are higher speed facilities providing access to only outskirts of different regions whereas local roads are relatively lower speed facilities providing widespread access to places. Normally, people and goods move out from homes, farms, businesses, and small communities and take local roads in order to get access to collectors. Collectors take the traffic from local roads and connect them to arterials, which move them to different towns and cities (US Department of Transportation Federal Highway Administration, 2011). Transportation and water infrastructures often share the same space in order to serve the population with lower construction costs. For the most part, local roads and collectors are co-located with water pipes. Traffic control systems (e.g., traffic signals, signs, markings, traffic management or control centers) and the organizational structure associated with managing, operating, and using the transportation system (mainly organizations, human resources serving those organizations and users) are two other important components of the road transportation system considered in this paper. Traffic signals are important infrastructures to control traffic at signalized intersections whereas traffic signs and markings are essential throughout entire road networks in order to ensure safe, efficient, and reliable traffic operation. Two types of signals, fixed-time and actuated, are widely in operation at present traffic systems. Fixed-time signals follow a predetermined sequence of signal operations providing the same amount of time to a traffic movement in every cycle. Actuated signals can detect the number of vehicles present at each intersection and allocate varying time to each movement accordingly. Here, an organized set of infrastructures works to detect vehicles, exchange information, provide

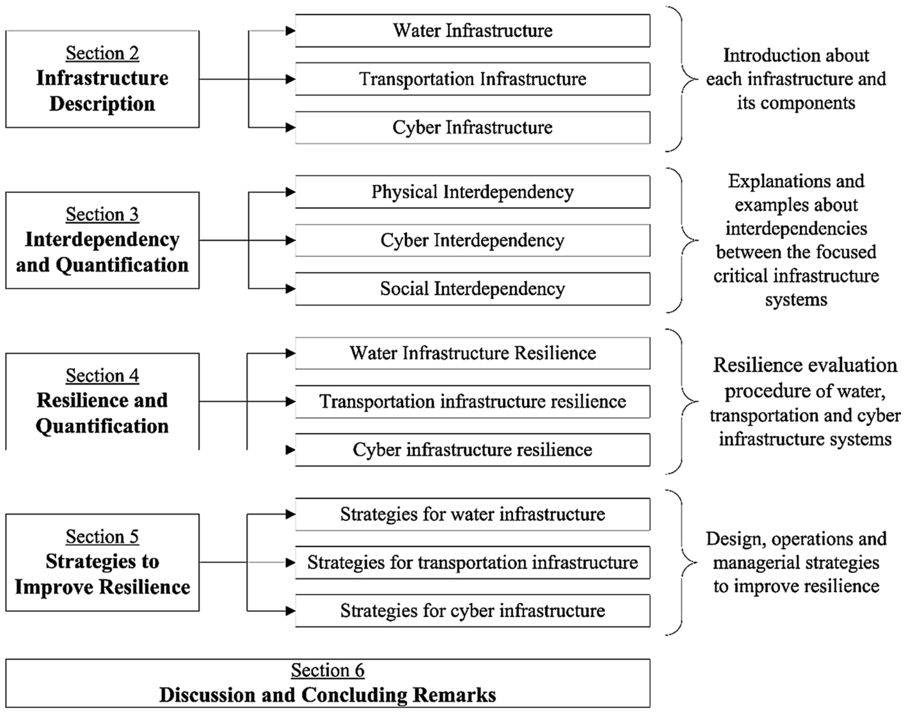

Fig. 3. Resilience assessment framework for interdependent water-transportation-cyber infrastructures.

power supply, and display the signals to traffic at intersections. Finally, institutional bodies such as state Departments of Transportation (DOT), Metropolitan Planning Organizations (MPO), and other local authorities responsible for control, operation and maintenance of the transportation system and the users of the system are considered part of the transportation system in this article.

2.3. Cyber infrastructure

Cyber infrastructures are no longer independent entities but are embedded within most other infrastructures. Recent advances in technology have led to Industry 4.0 (Lasi, Fettke, Kemper, Feld, & Hoffmann, 2014) and the merger of physical and digital systems. The scale of this merger, however, spans beyond industrial production and into critical infrastructures as well. The operation of water and transportation infrastructures relies heavily on the embedded cyber infrastructure. Here, cyber infrastructure includes sensor equipment, enterprise IT systems, SCADA systems, and the human capital necessary for financing, operating, and maintaining the infrastructure. For example, transportation infrastructure includes cyber elements in the form of vehicle detectors/sensors (inductive loops, video detection, etc.), communication equipment (fiber optics, wireless communication devices, networking equipment), traffic control technologies (roadside controllers) and enterprise level IT structure to oversee equipment in the Transportation Management Centers (TMC). Furthermore, the TMC relies on many different types of software, local server hardware, and cloud computing facilities. This type of embedded cyber infrastructure within other infrastructure helps to improve the efficiency of the existing systems.

3. Interdependency and quantification

Much remains to be understood in terms of how infrastructure interdependencies influence the resilience of a given infrastructure. These influences can be measured at varying scales (Casalicchio & Galli, 2008). There are two general categories of quantification measures that correspond to system-wide and component-level scales: a) macro characteristics of interdependencies and impact on system behavior to assist in organizational decision making, and b) component strengths/weaknesses to assist in engineering decision making (Casalicchio & Galli, 2008). In addition, there are two commonly used approaches for arriving at measures of resilience and interdependency: network-based and simulation-based or holistic approaches (Setola, 2010). In the following sections, examples of interdependencies between water, transportation, cyber, and social infrastructure systems are explored.

3.1. Infrastructural and organizational interdependencies

3.1.1. Potential vulnerability of water infrastructure

The assessment of vulnerability in water infrastructure due to climate change and dependency on other infrastructures is critical for paving the road towards resilient cities. This matter has attracted practitioners and scholars' attention particularly in coastal cities due to high exploitation of resources and higher probabilities of vulnerability (see Yoo, Hwang, & Choi, 2011). In general, failures in water distribution systems fall into two closely related groups (Ostfeld & Shamir, 1996): a) mechanical failures of system components (e.g., pipe breakage, pump outage) and b) hydraulic failures in meeting consumer demand (e.g., low pressure in pipes). In addition, water systems in urban areas are facing new challenges as socio-political drivers and broader contextual factors, such as climate change, resource limitations, and the prioritization of urban amenities and ecological health, test the ability of traditional systems to deliver adequate levels of water services (Ferguson, Frantzeskaki, & Brown, 2013).

A review of the literature reveals that the vulnerabilities and impacted critical functions associated with water systems can be assessed under three main categories: a) climate-related events (see Schoen et al., 2015), b) dependency on other infrastructures (see Gillette, Fisher, Peerenboom, & Whitfield, 2002) and c) infrastructure management (see Faust, Abraham, & DeLaurentis, 2013; Pescaroli & Alexander, 2016). Table 2 summarizes potential failures under each category based on the literature and existing case studies in the U.S. It can be observed that climate-related events and infrastructure management have a direct impact on physical failures in water infrastructure (over different time scales), while hydraulic and environmental failures are mainly influenced by extreme weather events, dependency on other

Table 2
Potential Vulnerabilities and Impacts for Water and Wastewater Infrastructures.

	Drivers	Failure	Failure propagation	References
Climate-related events	Extreme cold weather	Physical (pipe damage, collection failure from pumps), hydraulic (treatment failure)	Transportation, electric, energy, economic	(Bloomberg, 2013; Schoen et al., 2015)
	Storm with increased surge	Environmental (contamination), hydraulic (treatment failure), physical (pipe damage, collection damage)	Transportation, economic, social	(NYC, 2013)
	Short-term drought	Hydraulic (minimum flow failure)	N/A	(Teunis et al., 2010)
Dependency on infrastructures	Power outage	Hydraulic (pressure failure, treatment failure)	Transportation, cyber and electric	(Nan et al., 2013)
	SCADA failure	hydraulic (treatment failure)	Electric	(Nan et al., 2013)
	Road closures	hydraulic (treatment failure)	Socio-economic, transportation	(NYC, 2013; NIST, 2015)
Infrastructure Management	Aging infrastructures	Physical (Pipe damage, leaking)	Transportation, electric, energy, economic	(Hanna-Attisha et al., 2016; NYC, 2013; NIST, 2015)
	Weak vertical/horizontal coordination	Hydraulic (pressure and flow, treatment failure), Environmental (contamination)	N/A	(Hophmayer-Tokich & Kliot, 2008)

infrastructures, and subsequent managerial strategies to deal with such events. Given the fact that the main components of water infrastructure are often hidden from the public's view (e.g., underground), their failures can easily propagate to other infrastructures and cause high degrees of vulnerability.

3.1.2. Potential vulnerability of transportation infrastructure

Vulnerability of the road transportation system can be defined as the consequence of reduced accessibility that occurs due to various incidents. An incident is an event that may directly or indirectly result in considerable reductions or interruptions in the functioning of a link/route/road network. Incidents can be unpredictable, caused by physical failures, traffic accidents as a result of adverse weather, or they can be intentional, such as with the intent of causing harm or disruption (Berdica, 2002). It should be noted here that a sudden increase in demand could also reduce the serviceability of a road network. In addition, aging infrastructures (e.g., old or poorly maintained pavements and bridges) also can threaten the normal functioning of transportation infrastructure. Sudden failures of old and weak bridges, for instance, can cause serious disruption to the transportation system as they are critical in terms of network connectivity, and the situation may worsen during natural disasters (Lwin, 2015). In the field of transportation engineering, researchers are more interested in quantifying and measuring vulnerabilities in the system due to the consequences caused by different events rather than identifying those specific events. Potential factors considered in the literature that can cause a vulnerable situation in the transportation system can be classified into three categories: natural, anthropogenic, and managerial issues (although these can be interrelated in many instances). Table 3 contains a summary of such factors.

3.1.3. Physical interdependency between water and transportation

As defined in Section 1.2, physical interdependency refers to the interactive effects of material outputs, inputs, layouts, or operations of infrastructures. One illustration of such interdependency in terms of material outputs and inputs is presented in the literature using water supply and electric power distribution as examples (Gillette et al., 2002). A water supply system requires electricity to operate its pumps, whereas an electric supply system needs water to make steam and cool its equipment. As a result, if either one fails, the other becomes impacted.

The road transportation system often shares the same space with other infrastructures, including the water supply system and the stormwater drainage system. Although there is less interaction among them in terms of material outputs or inputs, the geospatial co-location of their layouts leads to interdependency of physical/functional failures and maintenance/rehabilitation operations among their physical structures. Table 4 summarizes select cases and evidence of physical interdependency between water and transportation infrastructures and their impacts.

3.2. Cyber interdependency

The interdependency between physical and cyber infrastructures leads to the inheritance of vulnerabilities from cyberspace into other critical infrastructures. Case studies examined by Ernst and Michaels (2017) and Ghena, Beyer, Hillaker, Pevarnek, & Halderman, 2014, in Michigan and Washington, D.C., respectively, show that it is possible to infiltrate the traffic network through vulnerabilities in the wireless infrastructure and gain control of roadside controllers, altering the commands sent out to traffic lights. Ernst and Michaels (2017) simulated such scenarios and showed that even minimal access to a vehicle detector can lead to congestion issues in the compromised corridor. They also provide a threat analysis framework based on four levels of access (namely, vehicle detector level, corridor synchronization level, traditional internet level, and physical access level) to analyze threats

Table 3
Potential Vulnerabilities and Impacts for Transportation Infrastructures.

	Drivers	Failure/Consequences	References
Climate-related and natural events	Flooding, winter, wind, sea level rise, landslide	Physical damage to infrastructure, temporary operational failure,	(Hosseini Nourzad & Pradhan, 2015; Tang et al., 2013; Transportation, 2011)
	Earthquake	Congestion during evacuation, physical damage to infrastructure (especially bridges)	(Li, O'Hara, & Wang, 2016; Lwin, 2015)
Man-made errors	Vehicle breakdown, crashes, roadworks, lane blockage	Severe congestion and loss of serviceability	(Alam, Habib, & Quigley, 2017; Taylor, 2008)
	Traffic signal tempering, cyber-attack on sensor data	Severe congestion	(Ezell et al., 2013; Ghafouri, Abbas, Vorobeychik, & Koutsoukos, 2016; Laszka, Potteiger, Vorobeychik, Amin, & Koutsoukos, 2016)
Infrastructure management	Infrastructure reconstruction	Increased delay, capacity reduction	(Alam et al., 2017)
	Aging pavement	Degraded performance, crash, congestion	(Buddhavarapu, Banerjee, & Prozzi, 2013)

to transportation infrastructure through cyber aspects. The impact of cyber vulnerabilities on the physical transportation infrastructure can clearly be seen from their results.

On the other hand, cyber infrastructures deal with more personal data as the number of devices connected to the internet grows. Internet of Things (IoT) devices also have a growing influence on the functioning of critical infrastructure, as it is estimated that the number of IoT devices will reach 50 billion by 2020. Petit, Broekhuis, Feiri, & Kargl, 2015, for example, show that it is feasible to track people using connected vehicles at a zone level and road level by using off-the-shelf equipment to sniff Vehicle-to-Infrastructure (V2I) communication. Social systems can also be indirectly impacted by cyber systems if, for example, a cyber-attack causes a gridlock or loss of water supply in SCADA-controlled water infrastructure. The impact may range over a large population when considering intelligent public transportation (IPT) systems, as new risks open up, such as unavailability of IPT services, passenger's health and safety, environmental impacts, and so on (Levy-Bencheton & Darra, 2015). Petit et al. (2015) also argue that to address the challenges and weaknesses when building these infrastructures, certain best practices must be maintained at the technical level, policy level, and organizational level to enhance cyber security.

3.2.1. *Cyber dependency of water infrastructure*

Water infrastructure's operation relies heavily on SCADA systems of treatment plants, where cyber breaches can result in cascading failures among multiple infrastructures. For example, an attack on the SCADA system may lead to water main breaks due to abnormal pressure (informational) that causes co-located transportation and cyber infrastructure failure (geospatial). A number of attacks against SCADA systems have been reported over the years (Nan, Eusgeld, & Kröger, 2013; Slay & Miller, 2007b). Table 5 summarizes some examples and evidence of cyber dependency of water infrastructures. There also are numerous unreported incidents by asset owners and operators related to the security issues in SCADA systems (see Christiansson & Luiijf, 2007).

3.2.2. *Cyber interdependency in transportation infrastructure*

Traffic management systems rely heavily on computer networks in signal control, closed-circuit television (CCTV) monitoring, and reversible lane control, among others. An attack on the transportation cyber network may result in serious traffic delay and even increase the possibility of safety issues (Ernst & Michaels, 2017). In addition, Intelligent Transportation System (ITS) brings cyber infrastructure to vehicles, increasing the cyber involvement in transportation systems. V2I technologies capture the data collected by each individual vehicle on the road, which the system utilizes to make decisions. This increase

Table 4
Physical Interdependencies between Water and Transportation Infrastructures.

Events	Scale	Cost/Economic Loss	Reference
Hurricane Katrina (2005) Flooding→road closures→inaccessibility to access treatment facilities for repairs Flooding exceeded storm water treatment capacity→sewage in waterways → water transportation Power outages→lack of sewage treatment→ waterway contamination	> 1000 drinking water supply systems and 172 sewage treatment plants	300 billion USD damage; 1000 deaths	(Olson, 2005; Berman, Berman, & Lynch, 2005; Leavitt & Kiefer, 2006; Wilbanks et al., 2012)
Hurricane Sandy (NY and NJ; 2012) Storm surge beyond storm water treatment capacity→ flooding → road closures Sewage in waterways→ water transportation impacted	560 million gallons untreated sewage mixed with storm water was released into waterways	70.2 billion USD	(FEMA, 2013; NOAA National Centers for Environmental Information (NCEI), 2017; NYC, 2013; NIST, 2015)
Flint, Michigan (2016) Storm→excess road salts in water source → corrosion of pipes	Entire city's water pipe infrastructure	> 80 million USD	(Dingle, 2016)
NY Grand central station Train accident (2016) Water pipe explosion→electricity failure→ subway failure	100 stores and food vendors closed 1 day	~ 55 million USD	(Robbins, 2016; WABC, 2016)
Sinkhole in Japan (2016) Sinkhole in underlying soil beneath a roadway appears→roadway, traffic, water supply, telecommunication line and gas line failure	All lanes of affected road closed; Water supply line severed; 800 houses lost power, gas and telephone line	N/A	(Nace, 2016)
Honolulu, Hawaii (2017) Water supply main burst→water clogging in roads→traffic congestion	Several kilometers of roadway affected	N/A	(Staff, 2017)
Water Main Burst (Tampa, FL 2017) Pipe breakage→ leaking, washing away/eroding road→ cavern formation→ road closure	All eastbound lanes closed for around one week; ~20,000 commuters for several weeks	N/A	(Times, 2017; Webtam & Gonzalez, 2017)

Note: cost/economic loss is cumulative for entire disturbance damage/inoperability, not only the interdependency impact.

Table 5
Summary of Cyber Interdependencies of Water Infrastructures.

Events	Scale	Cost / Economic loss	Reference
Florida power outage, 2008 Electric failure→ SCADA cyber failure→drinking water treatment and distribution failure	Shutdown of 26 transmission lines, 38 substations; 600,000 customers affected including water treatment facilities and pumping stations	25 USD million settlement	(Brush, 2020)
Australia Maroochy Shire accident, 2000 Cyber hacking → SCADA failure→ wastewater treatment failure	150 sewage pumping stations taken control of; untreated sewage released into local waterways	50,000 Australian Dollars for clean up	(Slay & Miller, 2007a)
USA and Canada Blackout, 2003 Software bug → electricity grid failure→ water treatment and distribution failure	100 power plants shut down, 50 million people affected in USA and Canada	4 – 10 billion USD	(Electric Consumer Research Council, 2004)
Hurricane Rita, 2005 Power outage→ SCADA failure→water treatment failure	City of Lake Charles raw sewage released into nearby lake for over a week	23.7 billion USD	(NOAA National Centers for Environmental Information (NCEI), 2017)
Hurricane Irma, 2017 Power outage→ treatment monitoring failure→ boil orders	Broward County, FL	Not yet determined	(AASHTO, 2017)

Note: cost/economic loss is cumulative for entire disturbance damage/inoperability, not only the interdependency impact.

Table 6
Cyber Interdependencies of Transportation Infrastructures.

Events	Scale	Reference
San Francisco subway website attack, 2011 Cyber hacking→website for subway information display breached→customer personal information stolen	Sensitive information, including names, street and email addresses, site passwords and even some phone numbers for around 2400 customers was stolen and dumped	(Fok, 2013; Rashid, 2011)
Smart parking meter hacking, 2009 Recording the communication between the card and the meter→program the card to never deduct or boost the transaction limit beyond what could legitimately purchased	The researcher took only three days to attack the smart cards and examined the meters in San Francisco, but the same and similar electronic meters are being installed in cities around the world.	(Fok, 2013; Zetter, 2009)
Traffic signal disruption in Montgomery, 2009 A computer for signal control crashed→signal pattern chaos and synchronization of traffic signals lost→endless read brake lights	Choreography of 750 traffic lights was disrupted, causing delays for the whole region.	(Fok, 2015; Halsey, 2009)

in the degree of interdependence opens up threats to the system as a whole. For instance, Zhang, Miller-Hooks, and Denny (2015) have shown that vehicles can be remotely compromised. Table 6 summarizes some reported cases illustrating the cyber interdependency of transportation infrastructure.

3.3. Social interdependency

Critical infrastructures are embedded in social systems, including cultural values, political arrangements, and economic markets (Larkin, 2013; Star, 1999). These systems are variously interdependent and relational with infrastructures, in other words, they are co-constructed and form socio-technical systems (Star & Ruhleder, 1996). In addition, these interdependencies are scale dependent — from individual households to communities or municipalities to national and transnational networks (Edwards, 2003). While previous research has acknowledged the importance of social and behavioral aspects of infrastructure and its management (Zimmerman, 2001), most studies reduce the complexity of these various social dimensions into formal economic logic (e.g., tradeoffs, cost/benefit analysis) that often underlies decision making to allocate scarce resources to alternate ends (Ouyang, 2014; Pederson et al., 2006; Rinaldi, Peerenboom, & Kelly, 2001). Here, we address this problem and broaden the discussion by drawing on recent anthropological and other social science literature, which suggests that there are three overlapping domains of social interdependencies among critical infrastructures: cultural, political, and economic.

Socio-cultural interdependencies constitute key human perceptions of satisfaction, confidence, and trust, and how these views influence one's judgements and behaviors, especially decision making regarding infrastructure use and management. Socio-political interdependencies include not only the policies, procedures, and overall bureaucracy within which infrastructure management is entrenched, but also the influence of power and politics and the role of governance and citizenship in infrastructure operations. Finally, socio-economic interdependencies concern the positionality of infrastructures in the market from the perspective of supply and demand, how infrastructures are financed (from design to operation and maintenance), and the influence of competition and cooperation in motivating decision making when it comes to the allocation of resources. In addition to outlining the ways and extent to which these interdependencies influence the operations and functions of different infrastructures, we also suggest potential sources of empirical data that can be collected to begin to model the relational nature of infrastructure and society, that is, how infrastructures mediate the relationships between households and institutions (e.g., utilities) as well as between people and nature.

3.3.1. Social-cultural interdependencies

Socio-cultural contexts condition infrastructure interdependencies and the physical and cyber environments they operate in (Graham & Marvin, 2001). For example, individual and group values and beliefs influence people's perceptions and behaviors regarding infrastructures and the resources they provide (Prouty, Koenig, Wells, Zarger, & Zhang, 2017). In their study of transitions from onsite wastewater treatment to integrated wastewater management in coastal Belize, Wells et al. found that values and beliefs of local residents conflicted with those of government officials and foreign tourists, and that these contrasts shaped opinions and decision making between the groups with regard to the centralization of wastewater management and other infrastructures (Wells et al., 2016). As such, infrastructure can be viewed as mediating the relationship between people and the institutions and organizational arrangements that manage critical resources, including water, energy, and transportation. Harvey and Knox (2012), for instance, examined the ways in which highway construction in Peru established novel connections between rural communities and global markets. They argue that the new roads symbolized progress and development for community members, while offering local governments the promise of greater political integration and economic connectivity. They caution, however, that these relationships can be threatened when infrastructures fail to deliver on such promises.

Socio-cultural interdependencies and infrastructure failures have been an increasingly important topic of research (Armbruster, Endicott-Popovsky, & Whittington, 2013), not only with regard to interruptions in the provisioning of critical services because of aging infrastructure, such as water pipes in Flint, Michigan (Hanna-Attisha, LaChance, Sadler, & Champney Schnepp, 2016), or weather-related phenomenon, such as stormwater and transportation during Hurricane Katrina (Leavitt & Kiefer, 2006), but also national security issues, such as recent cyberattacks on critical national infrastructure in the UK (Stoddart, 2016). For example, Bigger, Willingham, Krimgold, & Mili, 2009 identify malfunction of traffic signals due to power outage, loss of telecommunications, and loss of water filtration plants and pump stations as interconnected phenomena during the 2004 hurricane season in Florida, which resulted in massive disruptions to the education system among other institutions, such as hospitals. Moreover, because of the interdependencies among infrastructures, attitudes toward some institutions can be mutually dependent on the views of other institutions such that the inability of one infrastructure to deliver adequate services can influence public opinion about the entire interconnected system (Gase, Barragan, Simon, Jackson, & Kuo, 2015). Such failures can also have profound and lasting impacts on public confidence in infrastructures. Pederson et al. (2006), for instance, surveyed different ways of recognizing, characterizing, and modeling infrastructure interdependencies in the U.S. and globally. They conclude that socio-cultural interdependencies are the mutual relationships that influence, and are influenced by, trust, public opinion, and public confidence in infrastructure functioning.

3.3.2. Socio-political interdependencies

Research on socio-political interdependencies among critical infrastructures demonstrates that bureaucracy and politics can support or impede infrastructure function (Rinaldi et al., 2001). For example, Little (2002) argue that policies developed and enacted for one infrastructure sometimes have unforeseen consequences for other infrastructures due to their bureaucratic linkages, such as co-management (Hull, 2012). They argue that networked policies, while promoting efficiencies of scale, may compromise the operations of infrastructures by decreasing flexibility in decision-making. Still, critical infrastructure coordination demands multi-agency cooperation and coordination (Rosenthal, Hart, & Kouzmin, 1991). The varying, and sometimes competing, goals and interests in infrastructure management, as well as different communication strategies, accountability models, and decision-making styles can create structural barriers for multi-agency coordination (Pescaroli & Alexander, 2016) that may cause vulnerability in some critical infrastructures (Collier & Lakoff, 2008). Yet, in some cases, cooperation between different agencies in charge of separate critical infrastructures can result in constructive interdependencies, such as in the case of public-private partnerships (Bel, Brown, & Marques, 2013).

Recent anthropological research expands this focus to include studies of how infrastructures are interconnected with politics and citizenship (Larkin, 2013). Anand (2011), for example, examine how the physical sighting of water infrastructures in Mumbai creates opportunities for power brokers to emerge in slums that do not have access to piped water. These power brokers pressure elected officials to provide water access to slums and, in exchange, local residents deliver electoral support. In another example, von Schnitzler (2008) suggests that the introduction of water metering in South Africa was not only intended to aid water conservation efforts, but also to serve as a governing strategy to engender moralities of responsibility and calculation into its citizens that would potentially encourage energy conservation as well. Similarly, Wells et al. (2019) argue that the design and development of water and wastewater infrastructure in southern Belize are technopolitical practices designed to enact political goals and influence civic engagement. Viewed in this way, infrastructure can sometimes become a politically constituted technology directly tied to the production and reproduction of the State. As these and other recent studies (Collier, 2011; Wutich, Brewis, York, & Stotts, 2013) demonstrate, infrastructure interdependencies can, and often are, intimately tied to power, local and global politics, and alternative governance strategies.

3.3.3. Socio-economic interdependencies

Water, transportation, and cyber infrastructures are intimately linked by economic markets, especially in Western capitalist systems that reward efficiencies with lower costs and increased benefits (Mihelcic et al., 2017). For example, infrastructures become economically interdependent when budgetary needs and allocations influence, and sometimes determine, how human and financial resources are allocated for other infrastructures (Pant et al., 2014). Tsekeris (2014), for example, demonstrates how tradeoffs impact different infrastructures and how knowledge of interdependencies among public investments can offer insight into evaluation of regional infrastructure networks (Crain & Oakley, 1995). Moreover, allocation of scarce resources under pressing conditions can impact the resilience of interlinked infrastructures (Chopra & Khanna, 2015). Baroud, Barker, Ramirez-Marquez, & Rocco (2015), for instance, modeled loss of service costs and restoration costs associated with perturbations to the Mississippi River Navigation System, a major waterway transportation system that facilitates large-scale commodity flows throughout the central and southern U.S. They found that alternative strategies to address loss of service and restoration have significantly different costs of implementation and impacts on interdependencies across water, transportation, and energy (petroleum distribution) systems. They argue that resilience-based analysis of interdependent infrastructures can enhance risk-informed decision-making.

In addition to market-based interdependencies, economic connections among infrastructures also emerge from sharing technologies and operational costs, both within (Jeuland, Wu, & Whittington, 2017) and between (Yu, Jo, Sohn, & Kim, 2016) municipalities as well as internationally (Callaghan, 2014). Indeed, cooperation, rather than market competition, organizes many kinds of infrastructural interdependencies. For example, De (2005) show how cooperative agreements in the transportation infrastructure sector in Southeast Asia have encouraged regional economic integration. The study suggests that adopting common transportation policies can yield broad economic benefits for not only transportation but water and energy infrastructures as well. Similarly, Hophmayer-Tokich and Kliot (2008) demonstrates how regional cooperation in Israel was an efficient tool for promoting advanced wastewater treatment and led to the efficient use of limited financial resources and land availability due to transportation infrastructure. In another study, Whittington, Wu, and Sadoff (2005) model the economic benefits to cooperative development and management of waterways in Egypt's Nile Basin. They estimate that the total potential annual gross economic benefits of interagency cooperation for irrigation and hydroelectric power generation are U.S. $\$7-11$ billion. There are many other case studies in the literature demonstrating the necessity and benefits of considering socioeconomic interdependencies in managing infrastructures (Smith & Stirling, 2010).

4. Resilience and quantification

4.1. Water infrastructure resilience

Sustainability and resilience are dynamic and overarching concepts over different timescales, which can be measured for water infrastructure systems. Bruneau et al. (2003) characterized system resilience by four infrastructural qualities of robustness, redundancy, resourcefulness, and rapidity, which largely incorporate the notions of risk (likelihood and impacts of failures), reliability, recovery, and system tolerance at both pre- and post-failure stages.

To investigate water infrastructures resilience, studies have defined different dimensions and proxies. For instance, Butler et al. (2014) suggested three dimensions of resilience in water infrastructures including design resilience, operational resilience, and technology-based resilience. Design resilience refers to a set of design principles for the infrastructure (e.g., degree of duplication, buffering, multiple water resource supplies). Operational resilience refers to the agreed performance of water infrastructures (e.g., minimum pressure and flow in pipelines) to maintain the service after a disruption in the system. Technology-based resilience for water infrastructures can be viewed in terms of flood resilience where a range of devices are available to limit flood damage and speed recovery (McBain, Wilkes, & Retter, 2010). Yoo et al. (2011) suggested several proxies, including public water supply/population, service population of sewage systems, and ground water usage/potential groundwater resources for measuring adaptive capacity of water infrastructures to climate change.

Hashimoto, Stedinger, and Loucks (1982) were among the first to propose the use of resilience metrics (the speed of recovery from failure) and vulnerability (the extent of failure) for the assessment of water resource system performance. They advance a resilience evaluation procedure for water infrastructures that can be classified into three main categories: a) network-based indicators, b) performance-based indicators, and c) technologic indicators.

4.1.1. Network-based indicators

Water distribution networks consist of interconnected pipes and nodes (junctions) conveying water to meet the demand and pressure requirements of the system. A mathematical graph may represent the structure of such a system, where nodes represent elements at specific locations (e.g., reservoirs, consumers, and pumps) and links to represent the pipes that define the relationship between given nodes (Yazdani, Otoo, & Jeffrey, 2011). The study of complex networks by using techniques from graph theory helps with the classification of different network models, and quantifying their building blocks may partly explain the vulnerability, robustness, and tolerance of the system to errors and attacks (Albert, Jeong, & Barabási, 2000). One of the drawbacks to a solely network-based evaluation of resilience is that link-node representations do not account for the importance of certain hydraulic features/structures such as valves (Walski, 1993; Yazdani & Jeffrey, 2012). For this reason, (Meng, Fu, Farmani, Sweetapple, & Butler, 2018) found that there were no strong correlations between network and performance-based analyses regarding component vulnerability in water distribution networks. Table 7 summarizes the primary network-based indicators used to assess the structural resilience of water distribution infrastructures.

4.1.2. Performance-based indicators

Resilience measures in this category provide a quantitative means to assess different aspects of resilience (e.g., reliability, redundancy, robustness, rapidity), by measuring the performance of water distribution networks (Butler et al., 2017; Meng, et al., 2018). The estimation of the available flow, pressure, and free chlorine concentration is the starting point for measuring water distribution networks' resilience and their different facets (Di Nardo, Di Natale, Giudicianni, Santonastaso, & Savic, 2017; Dziedzic & Karney, 2015; Gheisi, Forsyth, & Naser, 2016; Mays et al., 2000; Ostfeld, Kogan, & Shamir, 2002). In general, performance-based indicators are defined over time and encompass both deterministic and probabilistic measures. Generic indicators in this category are summarized in Table 8, which can be applied to different infrastructures.

4.1.3. Technological indicators

Existing measures in this category mainly assess urban flood resilience for wastewater and stormwater infrastructures. Gersonius (2008) propose that flood resilience incorporates four capacities: a) to avoid damage through the implementation of structural measures, b) to reduce damage in the case of a flood that exceeds a desired threshold, c) to recover quickly to the same or an equivalent state, and d) to adapt to an uncertain future. This approach is consistent with the definition developed by the United Nations International Strategy for Disaster Reduction (Abchirm & Basabe, 2003).

To quantify flood resilience, there are two broad techniques in the literature (Hammond, Chen, Djordjević, Butler, & Mark, 2015): a) indirect methods using indicators that measure the characteristics of a system, and b) direct measures quantifying how the system responds to extreme events. Existing methods in the first category mainly consider flood events as one of the variables in the evaluation system and then quantify disaster resilience according to social, economic, institutional, and infrastructural factors (see Cutter, Burton, & Emrich, 2010; Sunil Kumar & Rajib, 2012). In this section, our focus is on the indicators that fall under the second category. Table 9 summarizes indicators and functions quantifying the resilience of different systems/technologies to flooding.

4.2. Transportation infrastructure resilience

For the study of resilience of transportation systems, most of the literature attempts to capture the performance of the system to predict, absorb, adapt to, and/or quickly recover from a disruptive event. For instance, Ta, Goodchild, and Pitera (2009) define freight transportation system resilience from the perspective of freight mobility, where resilience was viewed as the ability of the system to absorb the consequence of disruption, to reduce the impacts of disruption, and to maintain freight mobility. Heaslip, Louisell, Collura, & Urena Serulle, 2010 define transportation system resilience as the system's ability to maintain its expected level of service or to regain that level of service within a specified time interval after the disturbance. Osei-Asamoah and Lownes (2014) define transportation network resilience as "the ability of surface transportation networks to resist failure and attack, including their ability to adapt and maintain their structure and connectivity during disasters." Finally, Murray-Tuite argues that a resilient transportation system should have 10 properties: redundancy, diversity, efficiency, autonomous components, strength, adaptability, collaboration, mobility, safety, and the ability to recover quickly (Murray-Tuite, 2006). There are generally two branches of metrics used for resilience indicators. One is related to the traffic flow characteristics, such as travel time, traffic flow, and travel demand. The other is related to network structure and topological features, including connectivity and accessibility.

4.2.1. Network-based indicators

The abstract representation of a transportation system as a network of nodes and interconnecting links, whether the system involves roadways, railways, sea links, airspace, or intermodal combinations, defines a network topology. Nodes represent intersections, origins, and destinations, while links indicate the transportation routes that connect those nodes. Systems with distinctive features may be structured by different topological categories. For example, many arterial roadway networks have a grid or ring shape while air systems are always hub-and-spoke networks. This suggests that network structure can affect the functionality of the system. At the same time, for the same type of topology network, structure variation may also affect system performance. For instance, for the same origin-destination (OD) pair, more interconnecting links may increase its redundancy during an interruption. Therefore, the study of network topology may be of significant help in understanding the performance of the transportation system. Table 10 summarizes network-based indicators used to assess the structural resilience of transportation infrastructures.

Table 7
Summary of Main Resilience Indicators Based on the Water Network Structure.

Indicator		Equation	Case studies	Relation to Resilience	References
Average path length		$\frac{1}{n(n-1)}\sum_{i,j} d(i,j)$	California	Shorter path lengths → more efficient networks	(Porse & Lund, 2015; Yazdani et al., 2011)
Link connectivity		Min($\lambda(i,j)$) for all (*i,j*)	Kumasi, Ghana	Increase in link connectivity → increased resilience	(Kessler, Ormsbee, & Shamir, 1990; Soldi, Candelieri, & Archetti, 2015)
Spectral gap		$\Delta\lambda$	Kumasi, Ghana; Milan, Italy	Decrease in spectral gap→ decreases connectivity	(Soldi et al., 2015; Yazdani et al., 2011)
Betweenness Centrality (of *i*)/Central point dominance		$C_b(i)$# geodesic paths between other vertices that run through vertex *i* $C_b(i) = \sum \frac{\sigma_{ij}(i)}{\sigma_{ij}}$	Harris County Texas; California	How many geodesic paths will get longer if certain vertices are removed; (higher in centralized networks)	(Porse & Lund, 2015; Winkler, Dueñas-Osorio, Stein, & Subramanian, 2011)
Clustering connection strength	Edge Betweenness	# geodesic paths between vertices running along each edge in network	Parete, Italy	Indicates community structure, how stratified a network is	(Di Nardo et al., 2015; Newman, 2003)
	Size of minimum cut set	Max (flow)			
	Vertex distance measures	See path length and vertex efficiency			
Meshedness coefficient		$r_m = \frac{m-n+1}{2n-5}$	California, USA	Ratio of actual to possible number of loops in a network; high value → high connectivity	(Porse & Lund, 2015)
Average clustering coefficient		$c = \frac{3N_{triangles}}{N_{triples}}$	- Anytown benchmark model - Timisoara, Romania - Milan, Italy	Indicator of redundancy	(Candelieri, Soldi, & Archetti, 2015)

Notes: m= number of links/edges; n= number of nodes; $d(i,j)$ = the shortest distance between nodes *i*and *j*; $\lambda(i,j)$ = maximum number of edge disjoint paths between nodes *i* and *j*; $\sigma_{ij}(i)$ = number of shortest paths between *i* and *j* going through node (or link) *i*. $N_{triangles}$ =number of three nodes connected exactly by three edges; $N_{triples}$ = number of three nodes connected by at least two edges.

Table 8
Summary of Resilience Indicators Based on Infrastructure Performance.

Reference	Performance Indicator for Resilience
(Hashimoto et al., 1982)	Average probability of a recovery from the failure set in a single time step = $\gamma = \frac{\rho}{(1-\alpha)} = Prob\,\{X_t \in S \; and \; X_{t+1} \in F\} / Prob\,\{X_t \in F\} = Prob\,\{X_t \in F \; and \; X_{t+1} \in S\} / Prob\,\{X_t \in F\} = \text{Prob}\,\{X_{t+1} \in S \mid X_t \in F\}$
(Ayyub, 2014)	System's performance / systems service life $= (T_i + F\Delta T_f + R\Delta T_r)/(T_i + \Delta T_f + \Delta T_r)$
(Schoen et al., 2015)	Accumulative system's performance / life span $= \sum_j (T_{i_j} + F_j \Delta T_{fj} + R\Delta T_{rj})$/ lifespan, where j is the challenge index
(Baroud, Ramirez-Marquez, Barker, & Rocco, 2014)	Recovery / Loss = actual performance/planned performance: $\frac{\varphi(t_r \mid e^j) - \varphi(t_d \mid e^j)}{[\varphi(t_0) - \varphi(t_d \mid e^j)]} \; \forall \, e^j \in D$
(Ouyang et al., 2012)	Actual performance / target performance $AR = E[\frac{\int_0^T P(t)dt}{\int_0^T TP(t)dt}]$
(Reed, Kapur, & Christie, 2009)	Integration of area under *Q(t)* curve, for given impact

Notes: α = probability that a system is in a satisfactory state, ρ = probability of system being in satisfactory state at time t, and going to failure state in the following period, S= set of satisfactory states, F= set of failure states, X_t= system performance variable, R is the recovery profile, F is the failure profile, ΔT_f is the duration of the failure, ΔT_r is the duration of the recovery, T_i is the time to the incident, φ ()=performance, e^j = disruptive event, t_0 = time at original state, t_d = time at disrupted state, t_r = time at which resilience is evaluated, D= set of possible disruptive events, *Q(t)*: quality.

Table 9
Resilience Indicators Assessing Flood Damages.

Underlying System/Technology	Indicators	Case study	References
Lowland river system	a) Amplitude of reaction to flood waves (expected annual damage, and average annual number of causalities), b) Function of the slope of discharge-damage relationship c) Recovery rate (Combined set of indicators related to physical, economic and social factors)	N/A (hypothetical system)	(De Bruijn, 2004)
Gray Infrastructures (pump stations, roads, railways, gas and water mains, communication systems)	a) Depth-damage function b) Road pavement condition c) Road level of service d) Number of structures in flood zones	United States, Netherlands	(Bousquin et al., 2015; Meyer & Messner, 2005; Scawthorn et al., 2006)
Green Infrastructures (wetlands, riparian zones)	a) Area and volume of wetland b) Discharge c) Soil depth below or above 2 feet d) Ground covers lower than 2 feet in height at maturity	United States	(Bousquin et al., 2015; Lennon, 2015)
Coastal Cities System (Deltaic)	a) Coastal City Flood Vulnerability Index b) hydrogeological: sea level rise, storm surge, river discharge c) Socioeconomic: population close to coastline d) politico-administrative: flood hazard maps	Argentina; India; Morocco; Bangladesh; Philippines; France; Japan; China; Netherlands	(Balica, Wright, & van der Meulen, 2012)
Urban drainage systems	Systems residual functionality $(1 - \frac{V_{TF}}{V_{TI}} \times \frac{t_f}{t_n})$	Kampala, Uganda	(Mugume, Gomez, Fu, Farmani, & Butler, 2015)

Notes: V_{TF} = total flood volume, V_{TI} = total inflow into the system, t_f = mean duration of nodal flooding, t_f = total elapsed time.

4.2.2. Performance-based indicators

Performance-based indicators for transportation network resilience are based on the study of traffic flow-related features and their reactions to the perturbation of the system regardless of the network structure properties. Once there is a perturbation in the system, there may be capacity reduction of road links or traffic congestion induced by signal failures. In either case, the performance deterioration of certain road links will be propagated to the system as travelers will seek new routes for their trips, which leads to the performance variations for other parts of the transportation system. Travel time, travel cost, and travel demand are fundamental indicators of the transportation system performance. Resilience measurement based on those indicators or their variations is generally aimed at capturing system performance before, during, and after a perturbation. Table 11 summarizes performance-based indicators for traffic network.

4.3. Cyber infrastructure resilience

There is a lack of standard metrics to measure the resilience of a cyberinfrastructure. Although guidelines and frameworks exist for designing cyber secure/resilient systems, it remains a challenge due to the difficulty in measuring security (Collier, Panwar, Ganin, Kott, & Linkov, 2016). Linkov et al. (2013) reported that no useful metrics were found in the literature by federal agencies for managing cyber threats. This issue stems from the fact that the field of security as a whole is usually viewed as binary. The cyberinfrastructure is secure until it is realized that there has been a breach at which point it is no longer secure. Pfleeger and Cunningham (2010) discuss how measuring security is different from measuring resilience in other engineering disciplines and provide reasons why measuring security is challenging.

Cyber resilience has been defined in many ways. Bodeau & Graubart, 2011 define cyber resilience as the ability to anticipate, withstand, recover from, and evolve to improve capabilities in the presence of cyber threats. Björck, Henkel, Stirna, & Zdravkovic, 2015 define cyber resilience in terms of “intended outcome,” which refers to the goals that the system is supposed to achieve, even under perturbation. This definition takes the overall business function (critical function) as the objective of resilience and not just the underlying cyberinfrastructure. Hence, even when the underlying cyberinfrastructure is similar, the resilience of the system can be different depending on the larger system of which the cyberinfrastructure forms a part. The Center for Internet Security (CIS) provides metrics for organizations thatare categorized into six business functions (The Center for Internet Security, 2010). Some other measures, such as the Common

Table 10
Summary of Resilience Indicators Based on the Transportation Network Structure.

Indicator	Equation	Case studies	Relation to Resilience	References
OD connectivity	$E_\xi[\sum_{w\in W}\varphi^w(\xi)]/\sum_{w\in W}\Gamma_w$	Hypothetical network	Increase in OD connectivity rate→increased resilience	(Zhang et al., 2015)
Average reciprocal distance	$E_\xi[\sum_{w\in W}\frac{1}{d^w(\xi)}]/\sum_{w\in W}\frac{1}{\psi_w}$	Hypothetical network	Increase in reciprocal distance rate→increased resilience	(Zhang et al., 2015)
Average degree	$\frac{\sum_i n_i}{v}$	Melbourne, Australia	Increase in average degree→increased coping capacity→increased resilience	(Leu, Abbass, & Curtis, 2010; Zhang et al., 2015)
Diameter	$\max(d_{ij})$	hypothetical system	Increase in diameter→decreased coping capacity→decreased resilience	(Zhang et al., 2015)
Cyclicity	$\frac{\sum_{j=1}^{n} Cycle_i}{\lvert R\rvert}$	Hypothetical network	Increase in cyclicity→increased coping capacity→increased resilience	(Zhang et al., 2015)
Betweenness	$\frac{\sigma_{jk}(i)}{\sigma_{jk}}$	Melbourne, Australia	Increase in betweenness→increased probability of bottleneck existence→decreased resilience	(Leu et al., 2010)
Node resilience	r_i	Hypothetical network	Increase in node resilience→increased network resilience	(Ip & Wang, 2009)
Network coverage	$\frac{L_{pre-event}}{L_{post-event}}$	Kobe, Japan	Increase in network coverage→increased resilience	(Chang & Nojima, 2001)
Transport accessibility	$\frac{D_{pre-event}}{D_{post-event}}$	Kobe, Japan	Increase in transport accessibility→increased resilience	(Chang & Nojima, 2001)
Travel alternative diversity	N_a^{rs}	Winnipeg network, Manitoba, Canada	Increase in travel alternative diversity→increase redundancy→increased resilience	(Xu, Chen, Jansuwan, Heaslip, & Yang, 2015)
Network connectivity	$X_w^\xi = 1 - \prod_{k\in K_w}(1 - \prod_{a\in k}\frac{C_{apr}^\xi}{C^a})$		Increased connectivity → increased coping capacity → increased resilience	(Liao, Hu, & Ko, 2018)

Notes: $\varphi^w(\xi)$ = binary variable indicating whether or not O-D pair w is connected under perturbation ξ; Γ_w = original connectivity of O-D pair w; $d^w(\xi)$ = shortest distance of O-D pair w under disruption ξ; ψ_w = original shortest distance of O-D pair w; n_i = number of arcs incident on node i; v = number of nodes in the graph; d_{ij} = distance of shortest path between O-D pair (i, j); $Cycle_i$ = number of times random walk cycled back to node i; |R| = number of random walks; $\sigma_{jk(i)}$ = number of shortest paths from node j to k that pass through node i; r_i = average number of reliable independent paths with all other nodes fornodei; L = total length of network open; D = total distance based accessibility; N_a^{rs} = the number of efficient routes between O-D pair (r, s) using link a; X_w^ξ is the connectivity between O-D pair w under disaster scenario ξ; C_{apr}^ξ post-disaster capacity of arc a after augmentation due to implementing preparedness action p or recovery action r under disaster scenario ξ. C^a pre-disaster capacity of arc a.

Vulnerability Scoring System (Mell, Scarfone, & Romanosky, 2007), are based on the threat model against which a system has to be protected.

Some studies that have been conducted tend to focus on the financial consequences caused by a cyber-breach as a metric. Ponenom Institute's cost of cybercrime study (Ponenom Institute, 2016) collected data from 237 organizations across six different countries, which included 1278 interviews with company personnel. They reported 465 total attacks and performed a cost analysis on the various types of infrastructure and the corresponding financial impacts caused after the breach. A 21 percent net increase was reported in the total cost of cybercrime in 2016 from 2015. They also point out the areas most affected by cybercrime and identify the effective techniques and practices in which to invest in order to minimize the damage. (Oughton et al., 2019) provide a hypothetical scenario based in the UK, and studied different financial impacts that an attack can bring forth. They analyzed the number of customers disrupted, the economic losses incurred, and simulated over a five-year period the impact on the long-term Gross Domestic Product (GDP). The metrics utilized are not directly connected to the performance of the cyberinfrastructure but, as per the definition by Björck, Henkel, Stirna, & Zdravkovic, 2015, they indicate the decline in the expected business function of the overall system. These metrics, however, do not indicate the recovery time of the system, which is usually associated with resilience metrics.

Improvements in information and communication (ICT) technologies have led to functional dependence between cyber and physical systems, such as transportation and water infrastructures, and are essential for their safe and continuous operation. The interconnectivity provided by cyber systems improves efficiency and functionality of these critical infrastructures but incurs costs in terms of increased risk associated with the cyber systems (Ezell, Robinson, Foytik, Jordan, & Flanagan, 2013). Attacks in the associated cyber systems can lead to disruptions in the functionality and/or increase safety and security risks in the physical system, i.e., cyber breaches can directly or indirectly impact key resilience factors of the system as a whole (Zimmerman & Dinning, 2017). To account for the resilience of such interconnected systems, cyber security aspects need to be incorporated into the resilience evaluation. Resilience evaluation used in physical infrastructure domains, such as in water and transportation systems, often fail to account for possible threats from the cyber domain. At the same time, the approaches utilized in the cyber systems fail to analyze the physical consequences of cyber-attacks. Zimmerman and Dinning (2017) further emphasize the need for cyber-physical perspectives to bridge the gap for analysis of "cross-over" attack scenarios based on examples of urban railway systems.

The U.S. Department of Homeland Security estimates that cyber breaches of critical infrastructure can result in up to 2500 casualties, economic damages of $50 billion, and severe impacts to national security (de Smidt & Botzen, 2018). Thus, recovering from cyber-attacks not only includes restoration of the system to a previous functional state but also recovery from financial losses. With this in mind, cybersecurity and resilience of critical cyber-physical infrastructures cannot be solely achieved through technological improvements and risk mitigation. The residual cyber risk is transferred to willing partners through cyber insurance (Tonn, Kesan, Czajkowski, & Zhang, 2018). Tonn, Kesan, Czajkowski, & Zhang, 2018 regard cyber insurance as an important risk management strategy to recover from cyber events as it transfers risk to willing partners and incentivizes investment in IT security.

Some studies provide a framework to manage cybersecurity risks and design cyber resilient systems. These frameworks are divided into high-level goals that can help lead to a resilient system. The cybersecurity framework (NIST, 2014) from the National Institute of Science and Technology (NIST) defines five functions: identify, protect, detect, respond and recover. This framework can be used to grade an organization's state against a target goal (Collier, Panwar, Ganin, Kott, & Linkov, 2016). MITRE's cyber resiliency engineering framework (Bodeau & Graubart, 2011) provides four high-level goals: anticipate, withstand, recover, and evolve, and serves a similar function as the NIST framework. Symantec (2014) recognize that cyber risk is not contained to a single event but a more sustained and persistent threat and that a single method of protection is not viable. They present a multi-layered approach encompassing people, processes, and technologies. The framework is based on five pillars (prepare/identify, protect,

Table 11
Summary of Resilience Indicators Based on Transportation System Performance.

Indicator	Equation	Case studies	References
Network Spare Capacity	μ	Winnipeg network, Manitoba, Canada	(Xu, Chen, Jansuwan, Heaslip, & Yang, 2015)
Travel time resilience; travel cost resilience; environment resilience	$R_{tt}(t) = t_{ij(before\ shock)}/t_{ij(after\ shock)}$ $R_{cost} = Cost_{before\ shock}/Cost_{after\ shock}$ $R_{ENV} = \frac{CO_2\ emission_{(before\ shock)}}{CO_2\ emission_{(after\ shock)}}$	Transportation corridor between Boston and New York	(Omer, Mostashari, & Nilchiani, 2013)
Perturbance resilience; recovery speed; recovery resilience	$x_k^p = \frac{\int_{t_{p0}}^{t_{p1}}(1-\psi_k(t))dt}{t_{p1}-t_{p0}}100$ $\theta_k = \frac{2}{\pi}\arctan(\frac{\psi_k(t_{p1})T_{th}}{t_r - t_{p1}})$ $x_k^r = \theta_k \frac{\int_{p1}^{tr}(\psi_k(t_{p1})-\psi_k(t_r))dt}{\psi_k(t_{p1})(t_r - t_{p1})}$	Hypothetical system; Cuenca network, Spain; Sioux Falls network	(Nogal, Martinez-Pastor, O'Connor, & Caulfield, 2015; Nogal, O'Connor, Caulfield, & Martinez-Pastor, 2016; Nogal, O'Connor, Martinez-Pastor, & Caulfield, 2017)
Travel demand resilience	$\max E_\xi\left[\max \sum_{w\in W}\sum_{k\in K_w} f_k^w(\xi)\right]/\sum_{w\in W} D_w$	Western US; hypothetical network	(Chen and Miller-Hooks, 2012; Miller-Hooks, Zhang, & Faturechi, 2012; Zhang et al., 2015)
Consumer surplus resilience; travel time resilience; traffic flow resilience	$R_{CS}(\theta) = \Pr(\frac{CS}{CS^0} \ge \theta)$ $R_{TT}(\theta) = \Pr\left(\frac{TT^0}{TT} \ge \theta\right)$ $R_F(\theta) = \Pr(\frac{Flow}{Flow^0} \ge \theta)$	Hypothetical network	(Soltani-Sobh, Heaslip, & El Khoury, 2015)
Travel time resilience	$R_{T,B} = \frac{tt^{r^{-1}}}{tt^{o^{-1}}} = \frac{<x^0, t^0>}{<x^r, t^r>}$	Hypothetical network	(Faturechi & Miller-Hooks, 2014)
System travel cost resilience	C_{UTS}	IEEE 33-node distribution system and IEEE 123-node distribution system with assumed urban transportation system	(Wang, Shahidehpour, Jiang, & Li, 2018)
Normalized travel time deviation	$M(t) = \sqrt{(a(t)-\mu(t))^T \sum(t)^{-1}(a(t)-\mu(t))}$	New York City	(Donovan & Work, 2017)
Cumulative travel time lost resilience	$\Delta T = \beta \sum_{ij\in E} L_{ij}(\frac{l_{ij}+l_0}{v_{ij}} - \frac{l_{ij}+l_0}{V_{ij}})$	New York City	(Ganin et al., 2017)

Notes: μ is the largest multiplier applied to a given existing OD demand matrix and indicates whether the current network has spare capacity or not; t_{ij} travel time for OD pair (i, j); x_k^p =perturbation resilience; θ_k = recovery speed; x_k^r =recovery resilience; $\psi_k(t)$ =the exhaustion level, which is related to travel cost increase and traffic flow variation; t_{p0} is the time when perturbation occurs and t_{p1} is the time when perturbation stops; t_r is the time when new equilibrium is reached; $f_k^w(\xi)$ =travel demand that can be satisfied in perturbation ξ; D_w =original travel demand for OD pair w; CS^0, CS= consumer surplus before and after perturbation; TT^0, TT= travel time before and after perturbation; $Flow^0$, $Flow$ =traffic flow before and after perturbation; tt^r, tt^0 = travel time before and after perturbation; C_{UTS} = Travel cost after extreme events when there are damage to the power system of traffic lights; $M(t)$ represent the Mahalanobis distan, used to capture the deviation of traffic travel time performance from normal pattern at time t ; a(t) is the observed traffic patterns at time t and $\mu(t)$ is the expected traffic pattern at time t ; ΔT represent the cumulative time lost by all commuters; V_{ij} *and* v_{ij} are the free flow speed and the actual traffic speed along the ij road segment; l_{ij} is its length; l_0 is the length correction due to traffic signals; β is the proportionality coefficient.

detect, respond, and recover) to evaluate an organization's cyber security strategy so that continual refinement can be made under each pillar to achieve cyber resilience.

Finally, cyber infrastructure can be a part of any type of system. It is important that a metric is able to capture the relevant information about the system at hand. This will help define measurable goals and strategic objectives (Collier, Panwar, Ganin, Kott, & Linkov, 2016). Linkov et al. (2013) provide a cyber resilience matrix framework, which is a matrix-based approach that provides a structured way to leverage existing metrics or identify new ones. The framework emphasizes the importance of interaction between the stages of event management (plan/prepare, absorb, recover, and adapt) and four domains (physical, information, cognitive, and social). The matrix aims to make transparent connections between these. Each cell in the matrix should then include a specific measure (quantitative or qualitative) developed on a system by system basis Linkov et al. (2013).

5. Strategies to improve resilience

Time frames (e.g., before, during, or after impact) with respect to disturbances determine the types of strategies that can be employed to improve system resilience. The three most common types of strategies include mitigating, adapting, and coping (Butler et al., 2014), and correspond to resistance capacity (mitigation), absorptive capacity (adaptation), and recovery/restorative capacity (coping) (Butler et al., 2014; Ouyang, Dueñas-Osorio, & Min, 2012).

The strategies that correspond to mitigation, or resistance capacity, focus on first stage local impacts, such as risk management (to identify components that need hardening), real-time sensing, monitoring, and updates of the system (making use of newer techniques and technologies), enhancing organizational structure of decision support platforms, integrating resilience analysis to existing risk-based decision support process, and allowing room for learning from previous accidents (Ouyang et al., 2012; Smith et al., 2013). Effective resilience enhancement can be achieved by adopting a tiered resilience analysis approach at the decision support stage, depending upon the extent of disruption, scope of the mitigation strategy, and available resources (Linkov & Trump, 2019; Linkov et al., 2018). Adaptation/absorptive capacity is recognized as the second stage, and involve system-level impacts (including both hard and soft assets), such as plans that are regularly reviewed and evaluated, diversification of urban water supplies to include a range of sources, increasing redundancy (not just hardening), adjusting infrastructure topology, and forums to build knowledge among stakeholders (Ouyang et al., 2012; Smith et al., 2013). Coping/restoration entails system recuperation (the third stage of the framework in (Ouyang et al., 2012)), such as establishing communication channels, establishing coordination for rapid recovery response, and enhancing decision support platforms to identify feasible recovery strategies (Ouyang et al., 2012). Mitigation and adaptation are priorities to invest in when resources are sufficient (Ouyang et al., 2012). However, to increase resilience for systems with limited resources, restoration, such as recovery sequences, is a priority (Ouyang et al., 2012).

In an overall sense, assessing resilience of systems for broad range of disruption, adopting both long and short term mitigation strategies, including all stages of system response after a disaster and all (social, physical and informational) domains of systems, can provide a complete effort to implement resilience practice in individual systems and across interdependent systems (Larkin et al., 2015). As a result, emerging advances, such as Industry 4.0, show potential for enhancing systems resilience. If Industry 4.0 is to be understood as an advancement towards the integration of information, actors, and organizational processes (Ardito, Petruzzelli, Panniello, & Garavelli, 2019), then the power of IoT technologies can change how traditional bureaucratic organizations such as public utilities collect, store, analyze, and share information. Instead of hierarchical administrative systems where knowledge is mostly concentrated at the top, Industry 4.0 has the potential to break down hierarchical boundaries and decentralize decision making (Wilkesmann & Wilkesmann, 2018).

The type of interventions and strategies may be event-specific and one intervention may not address design and operational deficiencies simultaneously in an infrastructure. Hence, we present mitigation strategies under three categories: design (protection), operations (recoverability), and management (organizational).

5.1. Strategies for water infrastructure

5.1.1. Design strategies

There is a growing number of studies demonstrating the importance of design and planning strategies to improve resilience of water infrastructures (Mikovits, Rauch, & Kleidorfer, 2018; Zischg, Mair, Rauch, & Sitzenfrei, 2017; Zischg, Rauch, & Sitzenfrei, 2018). Flooding, for instance, can be mitigated through careful consideration of the drainage system (i.e., the above ground flow pathways as opposed to the piped system) at the planning stage and its incorporation (and protection) into the urban landscape (Djordjević, Butler, Gourbesville, Mark, & Pasche, 2011). The primary strategies to improve the resilience of stormwater infrastructures at the design stage are green infrastructure (e.g., rain gardens, tree boxes, green roofs) (Rijke et al., 2014), localizing use/infiltration (Cutter, Burton, & Emrich, 2010), and better deployment of surface flow features (Butler & Davies, 2004). Decentralization (Butler et al., 2014), pipe redundancy (Zimmerman & Dinning, 2017), localized water sourcing (Falco & Webb, 2015), and increased use of recycled water (Ferguson et al., 2013) are recommended strategies for potable and wastewater infrastructures.

When the principles of Industry 4.0 are applied to water infrastructure, it generally refers to “smart water systems” using advanced technologies (e.g., smart components, real-time data acquisition, transmission, and control, augmented reality) for data acquisition, computing, visualization and decision making. The insights gained from big data analysis can advance the understanding of the emergent system performance driven by individual components and their configuration. This will help guide the design of system structure for the desired performance.

5.1.2. Operations strategies

To improve resilience in water infrastructures, studies suggest adopting strategies such as proactive maintenance (e.g., infrastructure leak reduction and flushing water mains) and technology monitoring (e.g., smart sensors) (Butler et al., 2017; Webber, Fu, & Butler, 2019). Technological strategies are put in place to enhance prevention and recoverability. Real-time monitoring, surge protection, and management of pressure zones (NRC, 2006) are among the most common practices at the operations stage for water infrastructures. Real-time data and decentralized decision making can speed up the response and lead to more effective daily operation and disaster recovery. In theory, smart water systems are more resilient compared to the existing systems in terms of improved capacities to absorb, response to, and recover from the external disturbances.

5.1.3. Managerial strategies

From an organizational and policy standpoint, interventions in water systems to improve resiliency encompass various aspects and sectors, addressing water resources and urban water services (David, Sangwan, Sung, Chen, & Merwade, 2017). While advanced technologies are gaining attraction, budgets at utilities are still limited. With limited budgets, utilities must decide where to allocate resources, how to maintain the new and existing technologies, and how to train operators on using the new technologies. A persistent question concerns the strategic infrastructure locations that will provide the most useful data to manage/operate/respond to data from the infrastructure. This leads to another question of how to effectively analyze and make decisions based on the data provided. Researchers are still finding ways of deriving needed information for enhancing operations (both day to day and in face of disturbance) and, by extension, how to make decisions based on the available information. For example, in water distribution networks, a common challenge utilities face is locating leaks. It can be a time-consuming and crew-intensive operation, in addition to financial costs. However, real time data obtained can be useful in identifying leak locations before they become major disturbances (Sophocleous, Savić, & Kapelan, 2019). In other circumstances, it may not be clear how to use the multitude of data towards more informed and effective decision-making. Another advance is augmented reality. One application by ESRI has begun to be used by some municipalities to assist with asset locators (vGIS, 2019). This approach appears to have many benefits, such as reducing time spent locating assets, and they are working on addressing some safety drawbacks. Finally, related to big data are novel analysis techniques (e.g. complex network analyses and optimization) that supplement the state of the art and are geared towards providing more complete information for decision-makers. For example, Torres, Fontecha, Zhu, Walteros, & Rodríguez, 2020 developed a stochastic optimization approach allowing for participation from stakeholders/decision-makers to spatially allocate sustainable urban drainage technologies. Similarly, Abdel-Mottaleb, Ghasemi Saghand, Charkhgard, & Zhang, 2019 developed an optimization framework to identify critical water distribution network components. These techniques are still in the theoretical/research phase, as utilities are often limited in the personnel and equipment that would allow for such intensive computing. Thus far, Industry 4.0 shows potential for enhancing water infrastructure resilience, but many more case studies/applications in municipalities and research are needed to determine its place. Another challenge is the lack of a unified framework of what exactly “smart water systems” entail (Li, Yang, & Sitzenfrei, 2020). Moreover, as concluded by Li et al. (2020), more collaboration must first take place between researchers, industry, and municipalities to promote applications.

While different countries may have different regulatory frameworks for managing water resources (see Bichai & Ashbolt, 2017), there is consensus in the literature on the necessity of coordination among different water/wastewater utilities (horizontal), and water and other sectors (vertical) to deal with social interdependencies among infrastructures (Francis & Bekera, 2014; Rijke et al., 2014). Cooperative agreements with the transportation sector (De, 2005), cooperative management of waterways (Whittington et al., 2005), integrated coastal zone management (Rosendo & Brown, 2004), and coordination by dialogue and experience sharing (Esubalew, 2017) are the most adopted mitigating strategies to reduce the potential vulnerabilities due to social interdependencies among infrastructure sectors.

5.2. Strategies for transportation infrastructure

5.2.1. Design strategies

In 2014, the Federal Highway Administration(FHWA) issued an order to incorporate climate change vulnerability and risk into all aspects of transportation decision making (Holsinger, 2017). As part of this process, FHWA partnered with several state DOTs and MPOs and initiated small pilot projects to identify vulnerable assets (first round of projects) and analyze options for adapting and improving the resilience of those critical assets (second round of projects). Under one such project, the WSDOT created a GIS map identifying the most vulnerable links in the study area so that such links are considered with special care during maintenance, rehabilitation, and future development (Holsinger, 2017). Another pilot project conducted by Hillsborough County MPO in Florida identified several critical assets in the region, analyzed potential impacts due to extreme weather events using the FHWA risk and vulnerability assessment framework, and tested some adaptation strategies to mitigate the loss during inundation or flooding (Cambridge Systematics, Inc. & Jacobs Engineering Group, Inc., 2014). The FHWA published two manuals that provide guidelines for risk and vulnerability assessment and strategies to mitigate risks for transportation infrastructures prone to inundation in coastal and riverine areas. Raising the pavement profile, infrastructure redundancy, and raising tunnel portals and bridge deck elevations are recommended strategies at the design stage. In the context of Industry 4.0 where connected and autonomous vehicles (CAVs) are integrated into the transportation system, it is expected that the inherent resilience of the infrastructures from geometry design to traffic control system design can be enhanced by connected vehicle services and the design of intelligent infrastructures (Khan et al., 2016).

5.2.2. Operational strategies

To improve resilience in transportation infrastructures, studies suggest adopting strategies from a maintenance standpoint (e.g., infrastructure breakdown or degradation reduction) and from an intelligent transportation management perspective (e.g., intelligent traffic signal control and intelligent traveler information dissemination). Hardening of traffic control devices (Bauer, Ange, & Twaddell, 2015), cooperative intelligent transport systems (Mitsakis & Kotsi, 2018), and increased health monitoring are strategies for transportation infrastructures to improve operational resilience. Studies have also pointed out that there is a necessity to enhance resilience of the system at a broader spatial scale of a corridor or a wide-area road network instead of only the adaptive traffic control of intersections in the context of intelligent systems (Khan et al., 2016a). Khan et al., (2016b) studied the potential impact of automation in driving on enhancing the capacity of the urban traffic network to withstand stochastic traffic overloads and unpredictable demand.

The U.S. DOT FHWA proposed a Scenario-based Advancing Transportation Systems Management and Operations method with planning for operational resilience during tropical storms as a case study (Bauer, Ange, & Twaddell, 2015). The output of scenario planning aimed at creating more resilient transportation systems might include the identification of new investment needs, such as communication networks, and new measures or targets for transportation system restoration after a disruptive event. Scenario planning can support communities' operational decision making under various assumptions in terms of future events, trends, policies, priorities, or other factors of uncertainty (Bauer, Ange, & Twaddell, 2015).

Southcom, a regional infrastructure resiliency coalition, studied the operational strategies for transportation system after a disruptive event (Bauer et al., 2015). The most effective operational strategies selected under the assumption of various scenarios include "highly redundant data and voice communications systems, backup servers and decentralized databases location selection, backup power for all variable message signs and traffic signals, additional CCTV on roads and rails, and road weather information systems (RWIS) in rural areas" (Bauer et al., 2015).

Based on the U.S. climate resilience toolkit, selected applications and tools that support system resilience and that are linked with the urban transport sector are summarized in (Gaitanidou, Tsami, & Bekiaris, 2017). How these various toolkits could be integrated in a holistic way to support transportation system operation to enhance system resilience is an optional research and development direction.

5.2.3. Managerial strategies

The National Infrastructure Advisory Council (NIAC) addressed in their Transportation Sector Resilience Final Report (National Infrastructure Advisory Council (NIAC), 2015) that there are widespread, major dependencies — within modes, across modes, and with other lifeline sectors. While these dependencies are typically well known, they are too often poorly understood or without defined paths for mitigation. Cross-modal and cross-sector dependencies are of particular concern for transportation system resilience. At the same time, there is no structured, senior-level engagement between public and private sector partners, transport modes, and interdependent sectors to address national-level transportation risks. This is compounded by the difficulty of identifying public sector authorities who have decision-making ability throughout the networks of state, city, and county leaders (National Infrastructure Advisory Council (NIAC), 2015).

From an organizational and policy point of view, interventions in transportation systems to improve resilience entail various aspects and sectors, addressing cross-modal and cross-sector interdependencies. While different countries may have established different regulatory frameworks for managing transportation infrastructures, there is consensus in the literature on the necessity of coordination among different transportation utilities (horizontal) and transportation and other sectors (vertical) to deal with social and economic interdependencies among infrastructures (National Infrastructure Advisory Council (NIAC), 2015).

Based on the analysis of societal impacts of infrastructure failure interdependencies (IFIs), impacts of utility and transportation disruptions were found to be especially significant, that is, high in metrics of both Impact and Extent. Therefore, it is critical to investigate the organizational strategies for transportation systems in the context of interdependency (Chang, McDaniels, & Beaubien, 2009). From a managerial perspective, the inclusion of various stakeholder groups into a coalition addressing transportation system resilience is also extremely helpful for system resiliency improvement.

It should be noted that traffic management plan development can also be different with vehicle-to-vehicle and vehicle-to-infrastructure communications. Traffic systems with different CAV penetrations requires different infrastructure inputs. While high penetration of CAVs can significantly improve system resilience, it requires higher cost for repair and replacement of intelligent infrastructures (Ahmed, Dey, & Fries, 2019). Decisions regarding the balance between system performance and capital cost in this context may need to be made. Furthermore, existing evacuation and routing strategies may need to be updated to be more efficient with CAV technologies available (Bahaaldin, Fries, Bhavsar, & Das, 2017; Hannoun, 2017).

5.3. Strategies for cyber infrastructure

Cyber resilience differs from traditional cybersecurity. Traditional cybersecurity measures tend to focus on "protect, detect, and react," while cyber resilience focuses on ensuring proper functioning of the organization's mission despite the presence of an adversary. Traditional risk-based systems are unable to address evolving unknown and uncertain threats. Developing realistic threat scenarios, evaluating system vulnerabilities, and quantifying consequences required for risk-based approaches is extremely challenging for increasingly complex and interdependent systems and may also lead to potentially misleading risk quantification (Ganin et al., 2016). Bodeau, Graubart, Heinbockel, & Laderman, 2015 show that cyber resilience builds on traditional cybersecurity and security in general. This is illustrated in Fig. 4. In addition, cyber-attacks also differ from natural disasters or terrorist attacks, which are contained by geographic areas. Hence, a form of resilience for cyber infrastructure is guaranteed by simply having redundant, geographically dispersed infrastructure. Cyber-attacks on the other hand are not limited by geography and can be systemic and stealthy so that they remain undetected until the system is

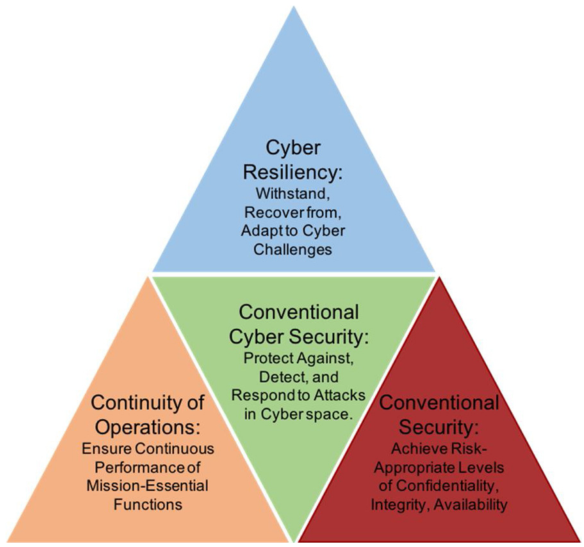

Fig. 4. Foundations of Cyber Resiliency (Bodeau, Graubart, Heinbockel, & Laderman, 2015).

compromised (Sheppard, Crannell, & Moulton, 2013). As such, planning for resilient cyber infrastructure poses unique challenges.

Many studies have been performed to suggest a framework for developing a resilient cyber infrastructure, considering the differences between providing cybersecurity and building a resilient cyber infrastructure. This has led to the creation of a new sub-discipline of mission assurance engineering called cyber resiliency engineering (Bodeau & Graubart, 2011). Mission assurance is an emerging discipline that aims to apply systems engineering, risk management, and quality assurance to achieve successful delivery of service to customers. Cyber resiliency engineering seeks to elevate mission assurance by bringing the ever-evolving set of resilience practices into real implementations of cyber infrastructure. Bodeau & Graubart, 2011 present a framework for cyber resiliency engineering, which provides a structured view of elements of cyber resiliency (goals, objectives, practices), threat models, applicability domains (architectural layers), and various aspects of costs to be considered for implementation, considering the varying scopes of resiliency. It also aims to help motivate, categorize, and select a set of cyber resiliency metrics that are able to address the problem domain comprehensively. Bodeau et al., 2015 expand on the previous work by augmenting it with cyber resiliency techniques, interactions, and tradeoffs between the existing techniques and the effects of these techniques throughout the lifecycle of the cyber-attack. Chang, Ramachandran, Yao, Kuo, & Li, 2016 provide an architectural framework called Cloud Computing Adoption Framework (CCAF) to provide guidelines for developing a resilient software system.

5.3.1. Design strategies

"Resiliency is a design characteristic of a system which cannot just be added to a system, instead it should be built-in from requirements identification" (Chang, Ramachandran, Yao, Kuo, & Li, 2016). Security engineering principles specify that a cyber-system should implement layered security (Bodeau & Graubart, 2011). The cyber system should be designed to not just have a strong outer shell but have multiple layers of protection, and each layer should follow the safe-to-fail principle (i.e., the system should be able to fail in a controlled way) (Björck, Henkel, Stirna, & Zdravkovic, 2015). Cyber resilience frameworks demand that a resilient system must have components to anticipate and prevent threats. Hence, the system design must have support to monitor and analyze all its components. The systems should also utilize techniques such as dynamic positioning (ability to relocate system assets), diversity (using heterogeneous set of technologies), non-persistent design (time limited retention policy), privilege restriction (fine grained access control), and segmentation (logical and physical separation of components) (Bodeau & Graubart, 2011). In addition, there is a need for the design strategies to include cybersecurity in physical security systems as well because of increasing functional dependence and co-location of cyber and physical systems and reliance of physical security systems on networked IT systems for access control, intrusion detection, and video surveillance (Zimmerman & Dinning, 2017). A major aspect of developing resilient designs is the ability to select the appropriate design elements for appropriate purposes. These decisions are usually made based on performance metrics. Ganin et al. (2016) provide a model-based approach to quantify resilience over a period of time based on the performance of critical functionality of the system and provide designers the ability to trade off different design parameters. However, such performance-based metrics only capture the availability of the system and do not account for cyber-threats concerning confidentiality and integrity of the system and associated data (Cybenko, 2019).

5.3.2. Operational and managerial strategies

In the presence of an adversary, a resilient system should continue to function correctly, constrain the threat, and reconstitute to a known good state (Bodeau, Graubart, Heinbockel, & Laderman, 2015). Technologies used in cyber systems are always evolving and, therefore, relying on the initial design is not adequate. As systems are upgraded, operators should also be educated about the threats, vulnerabilities, and mitigation policies and procedures. Solansky and Beck (2009) mentions the use of cyber-terrorism exercises to gauge the capabilities of agencies to detect, prevent, and respond to a cyber-terrorist attack and stresses the importance of collaborative efforts to minimize threats. Bodeau & Graubart, 2011 also include simulation exercises as a technique to achieve resiliency objectives. The increased awareness from these exercises/simulations helps to identify gaps and respond to them. In addition to training, organizations also respond to emerging threats through introduction of policies that apply operational constraints with the goal of limiting new vulnerabilities. Gisladottir, Ganin, Keisler, Kepner, & Linkov, 2017 analyzed the impact of training and regulation on cyber-systems resilience considering the human factors (such as overabundance of information, raised stress levels, and decreased time to perform critical functions) and found that both under and over regulating can lead to diminished system resilience. They advocate for introducing a few well-framed rules as a key to maximizing resilience. In addition, operational and managerial strategies should carefully consider the role of security in resilience plans, procedures for measurement of cyber risk, understanding the impacts of cyber-attacks on critical cyber-physical infrastructures (from operation/service delay to data breaches), and processes for organization to address known threats. With these considerations, decisions should be made regarding the purchase of appropriate cyber insurance as an important risk management strategy (Tonn, Kesan, Czajkowski, & Zhang, 2018).

6. Discussion and concluding remarks

6.1. Resilience

As demonstrated in Table 12, the quantification of resilience for water and transportation infrastructures typically includes two approaches, performance-based and network-based. The network-based indicators focus on the structure of resilience, and spectral gap and algebraic connectivity are the two most used indicators for water distribution networks. For transportation networks, connectivity, accessibility, and betweenness are the commonly used resilience metrics. The network-based metrics are relatively easy to compute with network software; however, they focus on the link-node representation without taking into account important system features, such as hydraulic features/structures for water distribution networks and traffic flow characteristics for transportation networks.

The performance-based metrics, on the other hand, are based on

Table 12
Resilience metrics comparison for infrastructures and their interdependencies.

Resilience Metrics	Type of Infrastructure	Type of Interdependency	Computational Complexity
Network-based	Water and Transportation	Physical (co-location), Social-Cultural (community-level)	Small, Medium
Performance-based	Water and Transportation	Physical, Cyber	High
Technological	Water	Physical	Small
Stage-based	Transportation and Cyber	Physical, Cyber	Medium

actual system performance, such as water flow, pressure, and water quality for water distribution systems and traffic volume, travel time, and cost for transportation systems. Such metrics rely on performance data from either simulation studies or field investigation. Domain knowledge is required for developing simulation models, which are computationally expensive for large networks. The data from field investigation are typically limited and do not provide sufficient spatial and temporal information. To advance resilience quantification, future research should investigate the relationship between network-based metrics and performance-based metrics. Identifying the universal network-based metrics that are sensitive to the performance of the infrastructure systems will be useful not only for resilience considerations but also for the optimization of the network structure for infrastructure performance. Another significant challenge is to validate the derived resilience metrics to determine whether they capture all aspects of a resilient system.

Finally, for cyber systems, the concept of security, instead of resilience, is commonly used. In the field of security, the measurement is binary, such that the cyberinfrastructure is either secure or no longer secure when a breach occurs. As a result, the definition and quantification of resilience for cyber systems is generally lacking. As cyber infrastructure becomes an integral part of successful operation of other critical infrastructures, it is important to develop appropriate metrics to quantify cyber resilience. Due to the nature of cyber infrastructure, such metrics may focus more on the recovery stage of the system, such as the time and cost required to recover the cyber systems or the relevant infrastructures that rely on function of cyber systems to the pre-existing condition.

6.2. Interdependency

This review explores how the integration of information about interdependencies has been applied to resilience quantification. Such understandings may provide insights into potential strategies that would not have otherwise been conceived. For example, if interdependency is taken into account in the quantification of vulnerability and risk, it may reveal that the socioeconomic impact of a failure is actually much higher than what was considered for an individual infrastructure. Thus, understanding of interdependencies may offer more informed decisions and investments at the stakeholder and socio-political level.

There are challenges that come in assessing multidirectional dependencies, however. Innovative techniques are needed to bridge the gap between single infrastructure systems and multi-system effects. The methods that have been used in the literature were presented in this review with most focusing on infrastructure-wide analysis (i.e., infrastructure as a whole). To be useful for decision-making, more information is required for both system-wide analysis and detailed component-level analysis. In terms of social interdependencies, social and political factors are often not included in the analysis. When they are included, they are usually economic in character — focusing on cost-benefit analyses, which are based on assumptions about human behavior that are not universal. Quantitative metrics for socioeconomic factors are generally lacking; that is, the factors are often acknowledged, but there are very few suggestions for how to incorporate them into formal models.

Since interdependencies exist in different forms, such as physical, virtual and social as discussed in this paper, the failure propagation patterns and scales (both temporal and spatial) might be different. For example, the cascading failures due to physical interdependencies tend to be contained locally. Scale appears to be a driving factor in choosing methods to analyze (assess and quantify) interdependencies and resilience. It is thus useful to classify the methods based on the type of interdependencies and scales. It is also important to view interdependencies as both advantages and vulnerabilities. For example, the high level of geospatial interdependency (co-location) between water and transportation infrastructures leads to lower land acquisition costs as well as construction costs; however, it also makes one infrastructure vulnerable to failures in other infrastructures. As a result, the optimization of interdependencies among infrastructures should be investigated for resilience improvement.

6.3. Strategies

Strategies to improve resilience range from design and planning to management. In addition to infrastructure types, timescale (e.g., before-during-after disaster) plays a critical role in identifying strategies that reduce vulnerability (before disruptive events) and enhance recoverability (during and after disruptive events). In Table 13, we map the strategies for different infrastructures on short-term, mid-term, and long-term plans. From design and protection viewpoints (before disruptions), network redundancy is the most commonly adopted strategy to increase structural resilience for both water and transportation infrastructures. For cyber infrastructures, layered protection is the major design strategy to improve resilience. Network-based metrics can be used to identify the strategic locations for redundancy implementation. Decentralization or localization is a strategy to improve resilience for both stormwater and wastewater systems. Green infrastructure is another strategy for stormwater management that could reduce localized flooding. Several strategies for transportation infrastructure design focus on structure enhancement, such as seawalls to reduce exposure to flooding. Strategiesthat provide synergistic effects for multiple infrastructures should therefore be emphasized.

In terms of operations and recoverability (during and after disruptions), there are multiple maintenance activities that can improve recoverability of existing infrastructure systems. For example, water infrastructure maintenance activities range from proactive maintenance such as network inspection, cleaning mechanical parts and replacement of components, to corrective maintenance such as repair of an impaired pipe or replacement of a faulty pump. The majority of conventional and current maintenance activities focus on corrective maintenance; however, proactive maintenance may be more effective to increase system capacity to endure disruptive events. Establishing the most cost-effective maintenance planning to address different types of maintenance actions and their complex profiles of maintenance effects on deteriorating infrastructure is needed.

The managerial strategies compiled in this review mostly focus on cooperation and coordination among various entities that are responsible for maintaining the functioning of interdependent infrastructures before-during-after disruptions. Cooperative agreements and cooperative management strategies are commonly adopted to enhance system resilience. As described in this review, social systems (including

Table 13
Strategies comparison for infrastructures and different timescales.

	Strategies		
	Recoverability/Operations	Protection/Design	Organizational /Managerial
Water	smart sensors, leak reduction, surge management of pressure zones, real-time monitoring	Green infrastructures, low impact development, separating sewer and stormwater systems, redistribution of discharge over river arms, pipe and network redundancy, diversification of urban water supplies, decentralized/hybrid treatment facilities	Cooperative agreements with Transportation sector, cooperative management of waterways, integrated coastal zone management, coordination by dialogue and experience sharing
Transportation	Hardening of traffic control devices, cooperative intelligent transport systems, communications system redundancy, increased health monitoring, dynamic rerouting	Raising pavement profile, redundancy, raising tunnel portals and bridge deck elevations	Cooperative agreements with water sector, regional cooperation, predictive models for future disasters consequences
Cyber	Cyber-terrorism exercises, increased awareness (simulation exercises)	Layered design, dynamic positioning, privilege restriction, segmentation, non-persistent design	Procedures for measuring cyber risk, procedures for addressing cyberattacks, cyber insurances
	Short-term	**Mid-term**	**Long-term** →

cultural, political, and economic aspects) encompass physical infrastructures. As a result, organizational strategies at the managerial level can lead to (at times) multiple component level changes over a larger spatial-temporal scale. Further research is needed to understand the impacts of various organizational strategies. Multi-stage predictive models to quantify the consequence of disasters are a starting point to analyze and compare organizational strategies.

Finally, we addressed key aspects of the "fourth industrial revolution" (Industry 4.0, marked by information or data-driven technologies) and its potential to enhance the resilience of infrastructures and organizations. One of the most significant contributions of Industry 4.0 to the resilience of socio-technical systems is the transformation of organizational culture (Davies, Coole, & Smith, 2017). For instance, Industry 4.0 through digital integration can help shift organizations to knowledge management models characterized by connectivity and openness. In this way, researchers, activists, and local communities can gain access to new sources of data and information. The open approach can build substantive relationships between organizations and communities, and also foster social support in crisis planning and response (Brown, Seville, & Vargo, 2017; Somers, 2009). Even more significant, data obtained through this relationship between infrastructure organizations and external stakeholders can play a crucial role in awareness creation and community empowerment. Consequently, Industrial 4.0 could contribute to resilience beyond technological systems by enabling communities to participate in the co-creation of organizational values and practices that address their needs and areas of vulnerability.

As we have noted in this review, developing a better understanding of critical, interdependent infrastructure systems and process is essential to designing sustainable cities of the future. Only when we are able to fully recognize and take advantage of the cyber, physical, and social interdependencies among different infrastructures can we begin to enhance the resilience of smart and connected cities and communities.

Declaration of Competing Interest

None.

Acknowledgements

This material is based upon work supported by the U.S. National Science Foundation under Grant Number 1638301. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Appendix A. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:https://doi.org/10.1016/j.scs.2020.102327.

References

AASHTO (2017). *Understanding Transportation Resilience: A 2016–2018 roadmap.* AASHTO.
Abchirm, B., & Basabe, P. (2003). *United Nations international strategy for disaster reduction. Living with risk*1–412.
Abdel-Mottaleb, N., Ghasemi Saghand, P., Charkhgard, H., & Zhang, Q. (2019). An exact multiobjective optimization approach for evaluating water distribution infrastructure criticality and geospatial interdependence. *Water Resources Research, 55*(7), 5255–5276. https://doi.org/10.1029/2018WR024063.
Adger, W. N. (2000). Social and ecological resilience: are they related? *Progress in Human Geography, 24*(3), 347–364.
Ahmed, S., Dey, K., & Fries, R. (2019). Evaluation of transportation system resilience in the presence of connected and automated vehicles. *Transportation Research Record, 2673*(9), 562–574.
Alam, M. J., Habib, M. A., & Quigley, K. (2017). Vulnerability in transport network during critical infrastructure renewal: Lessons learned from a dynamic traffic microsimulation model. *Procedia Computer Science, 109*, 616–623.
Albert, R., Jeong, H., & Barabási, A.-L. (2000). Error and attack tolerance of complex networks. *Nature, 406*(6794), 378.
American Society of Mechanical Engineers (ASME) (2009). *Innovative technological institute (ITI).* Washington, D.C: ASME ITI, LLC.
Anand, N. (2011). Pressure: The politechnics of water supply in Mumbai. *Cultural Anthropology, 26*(4), 542–564.
Ardito, L., Petruzzelli, A. M., Panniello, U., & Garavelli, A. C. (2019). Towards industry 4.0. *Business Process Management Journal, 25*(2), 323–346.
Arghandeh, R., von Meier, A., Mehrmanesh, L., & Mili, M. (2016). On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews, 58*, 1060–1069.
Armbruster, G., Endicott-Popovsky, B., & Whittington, J. (2013). Threats to municipal information systems posed by aging infrastructure. *International Journal of Critical Infrastructure Protection, 6*(3), 123–131.
Ayyub, B. M. (2014). Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making. *Risk Analysis, 34*(2), 340–355.
Bahaaldin, K., Fries, R., Bhavsar, P., & Das, P. (2017). A case study on the impacts of connected vehicle technology on no-notice evacuation clearance time. *Journal of Advanced Transportation*. https://doi.org/10.1155/2017/6357415.
Balica, S., Wright, N. G., & van der Meulen, F. (2012). A flood vulnerability index for coastal cities and its use in assessing climate change impacts. *Natural Hazards, 64*(1), 73–105.
Baroud, H., Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2015). Inherent costs and interdependent impacts of infrastructure network resilience. *Risk Analysis, 35*(4), 642–662.
Baroud, H., Ramirez-Marquez, J. E., Barker, K., & Rocco, C. M. (2014). Stochastic measures of network resilience: Applications to waterway commodity flows. *Risk Analysis, 34*(7), 1317–1335.
Bauer, J., Ange, K., & Twaddell, H. (2015). *Advancing transportation systems management and operations through scenario planning.* U.S. Department of Transportation Federal Highway Administration.
Bel, G., Brown, T., & Marques, R. C. (2013). Public–Private partnerships: Infrastructure, transportation and local services. *Local Government Studies, 39*(3), 303–311.

Berdica, K. (2002). An introduction to road vulnerability: What has been done, is done and should be done. *Transport Policy, 9*(2), 117–127.
Berman, E. M., Berman, M. D., & Lynch, T. D. (2005). *There was no plan. A louisiana perspective*. PA Times3–5 October.
Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research, 49*(18), 5375–5393.
Bibri, S. E., & Krogstie, J. (2017). Smart sustainable cities of the future: An extensive interdisciplinary literature review. *Sustainable Cities and Society, 31*, 183–212.
Bichai, F., & Ashbolt, N. (2017). Public health and water quality management in low-exposure stormwater schemes: A critical review of regulatory frameworks and path forward. *Sustainable Cities and Society, 28*, 453–465.
Bigger, J. E., Willingham, M., Krimgold, F., & Mili, L. (2009). Consequences of critical infrastructure interdependencies: Lessons from the 2004 hurricane season in Florida. *International Journal of Critical Infrastructures, 5*(3), 199–219.
Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). *Cyber resilience–fundamentals for a definition. New contributions in information systems and technologies*. Cham: Springer311–316.
Bloomberg, M. (2013). *A stronger, more resilient New York.* City of New York, PlaNYC Report.
Bodeau, D., & Graubart, R. (2011). *Cyber resiliency engineering framework.* MTR110237MITRE Corporation.
Bodeau, D., Graubart, R., Heinbockel, W., & Laderman, E. (2015). *Cyber resiliency engineering aid–the updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques.* MITRE Corporation, Tech. Rep. MTR140499Rl.
Bousquin, J., Hychka, K., & Mazzotta, M. (2015). *Benefit indicators for flood regulation services of wetlands: A modeling approach.* Washington, DC: U.S. Environmental Protection Agency.
Brown, C., Seville, E., & Vargo, J. (2017). Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study. *International Journal of Critical Infrastructure Protection, 18*, 37–49.
Bruneau, M., Chang, S. E., Eguchi, R. T., O'Rourke, T. D., Reinhorn, A. M., & Von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra, 19*(4), 733–752.
Brush, P. (2009). Florida power and light settles over Feb. 2008 outage. *LAW 360*.
Buddhavarapu, P., Banerjee, A., & Prozzi, J. A. (2013). Influence of pavement condition on horizontal curve safety. *Accident; Analysis and Prevention, 52*, 9–18.
Butler, D., & Davies, J. (2004). *Urban drainage.* CRC Press.
Butler, D., Farmani, R., Fu, G., Ward, S., Diao, K., & Astaraie-Imani, M. (2014). A new approach to urban water management: Safe and sure. *Procedia Engineering, 89*, 347–354.
Butler, D., Ward, S., Sweetapple, C., Astaraie-Imani, M., Diao, K., Farmani, R., et al. (2017). Reliable, resilient and sustainable water management: The Safe & SuRe approach. *Global Challenges, 1*(1), 63–77.
Callaghan, M. (2014). The role of international cooperation in increasing infrastructure investment. *JASSA, Sydney,* (3), 43.
Cambridge Systematics, Inc, & Jacobs Engineering Group, Inc (2014). *Hillsborough County MPO: Vulnerability assessment and adaptation pilot project.* Hillsborough County MPO.
Candelieri, A., Soldi, D., & Archetti, F. (2015). Network analysis for resilience evaluation in water distribution networks. *Environmental Engineering & Management Journal (EEMJ), 14*(6), 1261–1270.
Casalicchio, E., & Galli, E. (2008). Metrics for quantifying interdependencies. *International Conference on Critical Infrastructure Protection*.
Chang, S. E., & Nojima, N. (2001). Measuring post-disaster transportation system performance: The 1995 Kobe earthquake in comparative perspective. *Transportation Research Part A: Policy and Practice, 35*(6), 475–494.
Chang, S., McDaniels, T., & Beaubien, C. (2009). Societal impacts of infrastructure failure interdependencies: Building an empirical knowledge base. *TCLEE 2009: Lifeline Earthquake Engineering in a Multihazard Environment,* 1–10.
Chang, V., Ramachandran, M., Yao, Y., Kuo, Y., & Li, C. (2016). A resiliency framework for an enterprise cloud. *International Journal of Information Management, 36*(1), 155–166.
Chen, L., & Miller-Hooks, E. (2012). Resilience: An indicator of recovery capability in intermodal freight transport. *Transportation Science, 46*(1), 109–123.
Chopra, S. S., & Khanna, V. (2015). Interconnectedness and interdependencies of critical infrastructures in the US economy: Implications for resilience. *Physica A: Statistical Mechanics and its Applications, 436*, 865–877.
Christiansson, H., & Luiijf, E. (2007). Creating a european scada security testbed. *International Conference on Critical Infrastructure Protection*.
Cimellaro, G. P., Solari, D., & Bruneau, M. (2014). Physical infrastructure interdependency and regional resilience index after the 2011 Tohoku Earthquake in Japan. *Earthquake Engineering & Structural Dynamics, 43*(12), 1763–1784.
Collier, S., & Lakoff, A. (2008). *The vulnerability of vital systems: How "critical infrastructure" became a security problem. The politics of securing the homeland: Critical infrastructure, risk and securitisation*. Routledge40–62.
Collier, S. J. (2011). *Post-Soviet Social: Neoliberalism, Social Modernity, Biopolitics.* Princeton University Press.
Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A., & Linkov, I. (2016). *Security metrics in industrial control systems. Cyber-security of SCADA and other industrial control systems*. Springer167–185.
Crain, W. M., & Oakley, L. K. (1995). The politics of infrastructure. *The Journal of Law & Economics, 38*(1), 1–17.
Cutter, S. L., Burton, C. G., & Emrich, C. T. (2010). Disaster resilience indicators for benchmarking baseline conditions. *Journal of Homeland Security and Emergency Management, 7*(1), Article 51. https://doi.org/10.2202/1547-7355.1732.
Cybenko, G. (2019). *Metrics based on the system performance perspective. Cyber resilience of systems and networks*. Springer29–40.
Reed, D., Kapur, K., & Christie, R. D. (2009). *Methodology for assessing the resilience of networked infrastructure, Vol. 3*, 174–180.
Reed, D. A., Kapur, K. C., & Christie, R. D. (2009). Methodology for assessing the resilience of networked infrastructure. *IEEE Systems Journal, 3*(2), 174–180.
David, J. Y., Sangwan, N., Sung, K., Chen, X., & Merwade, V. (2017). Incorporating institutions and collective action into a sociohydrological model of flood resilience. *Water Resources Research, 53*(2), 1336–1353.
Davies, R., Coole, T., & Smith, A. (2017). Review of socio-technical considerations to ensure successful implementation of industry 4.0. *Procedia Manufacturing, 11*, 1288–1295.
De, P. (2005). Cooperation in the regional transportation infrastructure sector in South Asia. *Contemporary South Asia, 14*(3), 267–287.
De Bruijn, K. (2004). Resilience indicators for flood risk management systems of lowland rivers. *International Journal of River Basin Management, 2*(3), 199–210.
de Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice, 43*(2), 239–274.
Di Nardo, A., Di Natale, M., Giudicianni, C., Musmarra, D., Santonastaso, G. F., & Simone, A. (2015). Water distribution system clustering and partitioning based on social network algorithms. *Procedia Engineering, 119*, 196–205.
Di Nardo, A., Di Natale, M., Giudicianni, C., Santonastaso, G. F., & Savic, D. (2017). Simplified approach to water distribution system management via identification of a primary network. *Journal of Water Resources Planning and Management, 144*(2), 4017089.
Dingle, A. (2016). *The flint water crisis: What's really going on?* American Chemical Society.
Djordjević, S., Butler, D., Gourbesville, P., Mark, O., & Pasche, E. (2011). New policies to deal with climate change and other drivers impacting on resilience to flooding in urban areas: The CORFU approach. *Environmental Science & Policy, 14*(7), 864–873.
Donovan, B., & Work, D. B. (2017). Empirically quantifying city-scale transportation system resilience to extreme events. *Transportation Research Part C: Emerging Technologies, 79*, 333–346.
Dziedzic, R., & Karney, B. W. (2015). Performance index for water distribution networks under multiple loading conditions. *Journal of Water Resources Planning and Management, 142*(1), 04015040.
Edwards, P. N. (2003). Infrastructure and modernity: Force, time, and social organization in the history of sociotechnical systems. *Modernity and technology,* 1.
Electric Consumer Research Council (2004). *The economic impacts of the August 2003 blackout*.
Ernst, J. M., & Michaels, A. J. (2017). Framework for evaluating the severity of cybervulnerability of a traffic cabinet. *Transportation Research Record: Journal of the Transportation Research Board,* (2619), 55–63.
Esubalew, S. B. (2017). Assessment of horizontal and vertical integration among stakeholders in the sustainability of infrastructure projects in Addis Ababa City. *Management, 7*(1), 52–73.
Ezell, B. C., Robinson, R. M., Foytik, P., Jordan, C., & Flanagan, D. (2013). Cyber risk to transportation, industrial control systems, and traffic signal controllers. *Environment Systems and Decisions, 33*(4), 508–516.
Falco, G. J., & Webb, W. R. (2015). Water microgrids: The future of water infrastructure resilience. *Procedia Engineering, 118*, 50–57.
Faturechi, R., & Miller-Hooks, E. (2014). Travel time resilience of roadway networks under disaster. *Transportation Research Part B: Methodological, 70*, 47–64.
Faust, K., Abraham, D. M., & DeLaurentis, D. (2013). Assessment of stakeholder perceptions in water infrastructure projects using system-of-systems and binary probit analyses: A case study. *Journal of Environmental Management, 128*, 866–876.
FEMA (2013). *Hurricane sandy FEMA after-action report*.
Ferguson, B. C., Frantzeskaki, N., & Brown, R. R. (2013). A strategic program for transitioning to a Water Sensitive City. *Landscape and Urban Planning, 117*, 32–45.
Fok, E. (2013). An introduction to cybersecurity issues in modern transportation systems. *Institute of Transportation Engineers, 83*(7), 18–21.
Fok, E. (2015). Cyber security challenges: Protecting your transportation management center. *ITE Journal, 85*(2).
Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety, 121*, 90–103.
Gaitanidou, E., Tsami, M., & Bekiaris, E. (2017). A review of resilience management application tools in the transport sector. *Transportation Research Procedia, 24*, 235–240.
Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J. M., Kott, A., et al. (2016). Operational resilience: Concepts, design and analysis. *Scientific Reports, 6*(1), 19540.
Ganin, A. A., Kitsak, M., Marchese, D., Keisler, J. M., Seager, T., & Linkov, I. (2017). Resilience and efficiency in transportation networks. *Science Advances, 3*(12), e1701079.
Gase, L. N., Barragan, N. C., Simon, P. A., Jackson, R. J., & Kuo, T. (2015). Public awareness of and support for infrastructure changes designed to increase walking and biking in Los Angeles County. *Preventive Medicine, 72*, 70–75.
Gersonius, B. (2008). Can resilience support integrated approaches to urban drainage management. *11th International Conference on Urban Drainage*.
Ghafouri, A., Abbas, W., Vorobeychik, Y., & Koutsoukos, X. (2016). Vulnerability of fixed-time control of signalized intersections to cyber-tampering. *Resilience Week (RWS), 2016*.
Gheisi, A., Forsyth, M., & Naser, G. (2016). Water distribution systems reliability: A review of research literature. *Journal of Water Resources Planning and Management, 142*(11), 04016047.
Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, J. A. (2014). Green lights forever: Analyzing the security of traffic infrastructure. *WOOT, 14*, 7.

Gillette, J., Fisher, R. E., Peerenboom, J. P., & Whitfield, R. G. (2002). *Analyzing water/wastewater infrastructure interdependencies.* IL (US): Argonne National Lab.
Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over- and underregulation. *Risk Analysis, 37*(9), 1644–1651.
Graham, S., & Marvin, S. (2001). *Splintering urbanism: Networked infrastructures, technological mobilities and the urban condition.* Psychology Press.
Halsey, A. (2009). *Traffic signals disrupted, creating chaos in Montgomery.* Available from:http://www.washingtonpost.com/wp-dyn/content/article/2009/11/04/AR2009110402413.html.
Hammond, M. J., Chen, A. S., Djordjević, S., Butler, D., & Mark, O. (2015). Urban flood impact assessment: A state-of-the-art review. *Urban Water Journal, 12*(1), 14–29.
Hanna-Attisha, M., LaChance, J., Sadler, R. C., & Champney Schnepp, A. (2016). Elevated blood lead levels in children associated with the Flint drinking water crisis: A spatial analysis of risk and public health response. *American Journal of Public Health, 106*(2), 283–290.
Hannoun, G. J. (2017). *Framework for better routing assistance for road users exposed to flooding in a connected vehicle environment.* Virginia Tech.
Harvey, P., & Knox, H. (2012). The enchantments of infrastructure. *Mobilities, 7*(4), 521–536.
Hashimoto, T., Stedinger, J. R., & Loucks, D. P. (1982). Reliability, resiliency, and vulnerability criteria for water resource system performance evaluation. *Water Resources Research, 18*(1), 14–20.
Heaslip, K., Louisell, W., Collura, J., & Urena Serulle, N. (2010). An evaluation of network transportation resiliency for disasters and other events. *89th Annual Meeting of the Transportation Research Board*.
Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4*(1), 1–23.
Hollnagel, E., Woods, D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*.
Holsinger, H. (2017). Preparing for change. *Public Roads*.
Hophmayer-Tokich, S., & Kliot, N. (2008). Inter-municipal cooperation for wastewater treatment: Case studies from Israel. *Journal of Environmental Management, 86*(3), 554–565.
Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety, 145*, 47–61.
Hosseini Nourzad, S. H., & Pradhan, A. (2015). Vulnerability of infrastructure systems: Macroscopic analysis of critical disruptions on road networks. *Journal of Infrastructure Systems, 22*(1), 4015014.
Hull, M. S. (2012). Documents and bureaucracy. *Annual Review of Anthropology, 41*, 251–267.
Ip, W., & Wang, D. (2009). Resilience evaluation approach of transportation networks. *Computational sciences and optimization, 2009. CSO 2009. International joint conference on*.
Jeuland, M., Wu, X., & Whittington, D. (2017). Infrastructure development and the economics of cooperation in the Eastern Nile. *Water International, 42*(2), 121–141.
Kazama, M., & Noda, T. (2012). Damage statistics (Summary of the 2011 off the Pacific Coast of Tohoku Earthquake damage). *Soils and Foundations, 52*(5), 780–792.
Kessler, A., Ormsbee, L., & Shamir, U. (1990). A methodology for least-cost design of invulnerable water distribution networks. *Civil Engineering Systems, 7*(1), 20–28.
Khan, A. M., et al. (2016b). Automation in driving for enhancing resiliency in transportation system. *Resilient Infrastructure*.
Khan, A. M., Whelen, M., Snobar, N., Elsafdi, O., Jones, B., & Arnold, P. (2016a). *Enhancing resilience of traffic networks with connected vehicles. Resilient Infrastructure*. TRA.
Larkin, B. (2013). The politics and poetics of infrastructure. *Annual Review of Anthropology, 42*, 327–343.
Larkin, S., Fox-Lent, C., Eisenberg, D. A., Trump, B. D., Wallace, S., Chadderton, C., & Linkov, I. (2015). Benchmarking agency and organizational practices in resilience decision making. *Environment Systems and Decisions, 35*(2), 185–195.
Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering, 6*(4), 239–242.
Laszka, A., Potteiger, B., Vorobeychik, Y., Amin, S., & Koutsoukos, X. (2016). Vulnerability of transportation networks to traffic-signal tampering. *Proceedings of the 7th International Conference on Cyber-Physical Systems*.
Leavitt, W. M., & Kiefer, J. J. (2006). Infrastructure interdependency and the creation of a normal disaster: The case of Hurricane Katrina and the city of New Orleans. *Public Works Management & Policy, 10*(4), 306–314.
Lennon, M. (2015). Green infrastructure and planning policy: A critical assessment. *Local Environment, 20*(8), 957–980.
Leu, G., Abbass, H., & Curtis, N. (2010). *Resilience of ground transportation networks: A case study on Melbourne*.
Levy-Bencheton, C., & Darra, E. (2015). *Cyber security and resilience of intelligent public transport: Good practices and recommendations*.
Li, Q. J., O'Hara, M., & Wang, K. C. (2016). Assessment of the seismic vulnerability of transportation infrastructure in Central Oklahoma. *International Conference on Transportation and Development 2016*.
Li, J., Yang, X., & Sitzenfrei, R. (2020). Rethinking the framework of smart water system: A review. *Water, 12*(2), 412.
Liao, T.-Y., Hu, T.-Y., & Ko, Y.-N. (2018). A resilience optimization model for transportation networks under disasters. *Natural Hazards, 93*(1), 469–489.
Linkov, I., & Trump, B. D. (2019). *The science and practice of resilience.* Springer.
Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471–476.
Linkov, I., Fox-Lent, C., Read, L., Allen, C. R., Arnott, J. C., Bellini, E., ... Hyde, I. (2018). Tiered approach to resilience assessment. *Risk Analysis: an Official Publication of the Society for Risk Analysis, 38*(9), 1772–1780.
Little, R. G. (2002). Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. *Journal of Urban Technology, 9*(1), 109–123.
Lowrance, W. W. (1976). *Of acceptable risk: Science and the determination of safety.* Los Altos, Calif: Kaufmann, William, Incorporated.
Lwin, M. M. (2015). The important roles of bridge maintenance and management on transportation safety and efficiency. *Advances in Bridge Maintenance, Safety Management, and Life-Cycle Performance, Set of Book & CD-ROM: Proceedings of the Third International Conference on Bridge Maintenance, Safety and Management*CRC Press.
Martin, R. (2012). *Regional economic resilience, hysteresis and recessionary shocks*, *Vol. 12*, 1–32.
Martin-Breen, P., & Anderies, J. M. (2011). *Resilience: A literature review.* Brighton: Institute of Development Studies (IDS).
Mays, L. W., Bouchart, F., Ormsbee, L. E., Lingireddy, S., Chase, D. V., Goldman, F. E., et al. (2000). *Water distribution systems handbook*, *Vol. 17*. New York: McGraw-Hill.
McBain, W., Wilkes, D., & Retter, M. (2010). *Flood resilience and resistance for critical infrastructure.* CIRIA.
Mell, P., Scarfone, K., & Romanosky, S. (2007). *A complete guide to the common vulnerability scoring system version 2.0*.
Meng, F., Fu, G., Farmani, R., Sweetapple, C., & Butler, D. (2018). Topological attributes of network resilience: A study in water distribution systems. *Water Research, 143*, 376–386.
Meyer, V., & Messner, F. (2005). *National flood damage evaluation methods: A review of applied methods in England.* the Netherlands, the Czech Republik and Germany: UFZ-Diskussionspapiere.
Mihelcic, J. R., Naughton, C. C., Verbyla, M. E., Zhang, Q., Schweitzer, R. W., Oakley, S. M., et al. (2017). The grandest challenge of all: The role of environmental engineering to achieve sustainability in the world's developing regions. *Environmental Engineering Science, 34*(1), 16–41.
Mikovits, C., Rauch, W., & Kleidorfer, M. (2018). Importance of scenario analysis in urban development for urban water infrastructure planning and management. *Computers, Environment and Urban Systems, 68*, 9–16.
Miller-Hooks, E., Zhang, X., & Faturechi, R. (2012). Measuring and maximizing resilience of freight transportation networks. *Computers & Operations Research, 39*(7), 1633–1643.
Mitsakis, E., & Kotsi, A. (2018). *Cooperative intelligent transport systems as a policy tool for mitigating the impacts of climate change on road transport.* Springer.
Mugume, S. N., Gomez, D. E., Fu, G., Farmani, R., & Butler, D. (2015). A global analysis approach for investigating structural resilience in urban drainage systems. *Water Research, 81*, 15–26.
Murray-Tuite, P. M. (2006). A comparison of transportation network resilience under simulated system optimum and user equilibrium conditions. *Proceedings of the 38th conference on winter simulation*.
Nace, T. (2016). Massive sinkhole swallowed up a street in Japan. *Forbes*.
Nan, C., Eusgeld, I., & Kröger, W. (2013). Analyzing vulnerabilities between SCADA system and SUC due to interdependencies. *Reliability Engineering & System Safety, 113*, 76–93.
National Infrastructure Advisory Council (NIAC) (2009). *Critical infrastructure resilience: Final report and recommendations*.
National Infrastructure Advisory Council (NIAC) (2015). *Transportation sector resilience final report and recommendations.* National Infrastructure Advisory Council.
Natural Resource Management Ministerial Council & National Health and Medical Research Council (2009). In N.-E.-. NHMRC (Ed.). *Australian guidelines for Water recycling: Managing health and environmental risks. Phase 2-stormwater harvesting and reuse* Australia.
Newman, M. E. (2003). Properties of highly clustered networks. *Physical Review E, 68*(2), 026121.
NIST (2014). Framework for improving critical infrastructure cybersecurity. *Cybersecurity Framework*. https://doi.org/10.6028/NIST.CSWP.04162018.
NIST (2015). *Disaster resilience framework: 75% draft for San Diego.* NIST CA Workshop.
NOAA National Centers for Environmental Information (NCEI) (2017). *U.S. Billion-dollar weather and climate disasters*.
Nogal, M., Martinez-Pastor, B., O'Connor, A., & Caulfield, B. (2015). *Dynamic restricted equilibrium model to determine statistically the resilience of a traffic network to extreme weather events.* ICASP12.
Nogal, M., O'Connor, A., Caulfield, B., & Martinez-Pastor, B. (2016). Resilience of traffic networks: From perturbation to recovery via a dynamic restricted equilibrium model. *Reliability Engineering & System Safety, 156*, 84–96.
Nogal, M., O'Connor, A., Martinez-Pastor, B., & Caulfield, B. (2017). Novel probabilistic resilience assessment framework of transportation networks against extreme weather events. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering,* 4017004.
NRC (2006). *Drinking water distribution systems: Assessing and reducing risks.* National Academies Press.
NYC (2013). *Hurricane sandy after action report and reccomendations*.
Olson, E. D. (2005). The environmental effects of Hurricane Katrina. Report for the Committee on Environment and Public Works. *United States Senate* Retrieved November, 16, 2019.
Omer, M., Mostashari, A., & Nilchiani, R. (2013). Assessing resilience in a regional road-based transportation network. *International Journal of Industrial and Systems Engineering, 13*(4), 389–408.
Osei-Asamoah, A., & Lownes, N. (2014). Complex network method of evaluating resilience in surface transportation networks. *Transportation Research Record: Journal of the Transportation Research Board,* (2467), 120–128.
Ostfeld, A., & Shamir, U. (1996). Design of optimal reliable multiquality water-supply

systems. *Journal of Water Resources Planning and Management, 122*(5), 322–333.
Ostfeld, A., Kogan, D., & Shamir, U. (2002). Reliability simulation of water distribution systems–single and multiquality. *Urban Water, 4*(1), 53–61.
Oughton, E. J., Ralph, D., Pant, R., Leverett, E., Copic, J., Thacker, S., et al. (2019). Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks. *Risk Analysis, 39*, 2012–2031. https://doi.org/10.1111/risa.13291.
Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety, 121*, 43–60.
Ouyang, M., & Wang, Z. (2015). Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. *Reliability Engineering & System Safety, 141*, 74–82.
Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Structural Safety, 36*, 23–31.
Pant, R., Barker, K., & Zobel, C. W. (2014). Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors. *Reliability Engineering & System Safety, 125*, 92–102.
Pederson, P., Dudenhoeffer, D., Hartley, S., & Permann, M. (2006). *Critical infrastructure interdependency modeling: A survey of U.S. and international research.* Idaho Falls: Idaho National Laboratory (INL).
Pescaroli, G., & Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards, 82*(1), 175–192.
Petit, J., Broekhuis, D., Feiri, M., & Kargl, F. (2015). Connected vehicles: Surveillance threat and mitigation. *Black Hat Europe, 11*, 2015.
Pfleeger, S., & Cunningham, R. (2010). Why measuring security is hard. *IEEE Security & Privacy, 8*, 46–54.
Ponenom Institute (2016). *Cost of cyber crime study & the risk of business innovation 2016.* Ponemon Institute.
Porse, E., & Lund, J. (2015). Network analysis and visualizations of water resources infrastructure in California: Linking connectivity and resilience. *Journal of Water Resources Planning and Management, 142*(1), 04015041.
Prouty, C., Koenig, E. S., Wells, E. C., Zarger, R. K., & Zhang, Q. (2017). Rapid assessment framework for modeling stakeholder involvement in infrastructure development. *Sustainable Cities and Society, 29*, 130–138.
Rashid, F. Y. (2011). *Anonymous hack exposes personal data of San Francisco-Area commuters.* Available from:http://www.eweek.com/security/anonymous-hack-exposes-personal-data-of-san-francisco-area-commuters.
Redman, C. L. (2014). Should sustainability and resilience be combined or remain distinct pursuits? *Ecology and Society, 19*(2).
Righi, A. W., Saurin, T. A., & Wachs, P. (2015). A systematic literature review of resilience engineering: Research areas and a research agenda proposal. *Reliability Engineering & System Safety, 141*, 142–152.
Rijke, J., Smith, J. V., Gersonius, B., van Herk, S., Pathirana, A., Ashley, R., ... Zevenbergen, C. (2014). Operationalising resilience to drought: Multi-layered safety for flooding applied to droughts. *Journal of Hydrology, 519*, 2652–2659.
Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems, 21*(6), 11–25.
Rinaldi, S. M., Peerenboom, J., & Kelly, T. K. (2002). *Identifying, understanding, and analyzing critical infrastructure interdependencies*, *Vol. 21*, 11–25.
Robbins, L. (2016). *Grand central terminal Goes Dark after power failure.* The New York Times.
Rosendo, S., & Brown, K. (2004). The limits to integration: Critical issues in integrated conservation and development. *Tenth Conference of the International Association for the Study of Common Property*.
Rosenthal, U., Hart, P., & Kouzmin, A. (1991). The bureau-politics of crisis management. *Public Administration, 69*(2), 211–233.
Satumtira, G., & Dueñas-Osorio, L. (2010). Synthesis of modeling and simulation methods on critical infrastructure interdependencies research. In K. Gopalakrishnan, & S. Peeta (Eds.). *Sustainable and resilient critical infrastructure systems: Simulation, modeling, and intelligent engineering* (pp. 1–51). Berlin, Heidelberg: Springer Berlin Heidelberg.
Scawthorn, C., Flores, F., Blais, N., Seligson, H., Tate, E., Chang, S., et al. (2006). HAZUS-MH flood loss estimation methodology. II. Damage and loss assessment. *Natural Hazards Review, 7*(2), 72–81.
Schoen, M., Hawkins, T., Xue, X., Ma, C., Garland, J., & Ashbolt, N. J. (2015). Technologic resilience assessment of coastal community water and wastewater service options. *Sustainability of Water Quality and Ecology, 6*, 75–87.
Setola, R. (2010). How to measure the degree of interdependencies among critical infrastructures. *International Journal of System of Systems Engineering, 2*(1), 38–59.
Sheffi, Y. (2013). *The resilient enterprise: Overcoming vulnerability for competitive advantage.* MIT Press Books1.
Sheppard, B., Crannell, M., & Moulton, J. (2013). Cyber first aid: Proactive risk management and decision-making. *Environment Systems & Decisions, 33*(4), 530–535.
Silva, B. N., Khan, M., & Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society, 38*, 697–713.
Slay, J., & Miller, M. (2007a). Lessons learned from the maroochy water breach. *International conference on critical infrastructure protection*.
Slay, J., & Miller, M. (2007b). Lessons learned from the maroochy water breach. *Critical infrastructure protection,* 73–82.
Smith, A., & Stirling, A. (2010). The politics of social-ecological resilience and sustainable socio-technical transitions. *Ecology and Society, 15*(1), Article 11.
Smith, H. M., et al. (2013). *Risk, vulnerability, resilience and adaptive management in the water sector. Transitions to the urban water services of tomorrow*.
Solansky, S. T., & Beck, T. E. (2009). Enhancing community safety and security through understanding interagency collaboration in cyber-terrorism exercises. *Administration & Society, 40*(8), 852–875.
Soldi, D., Candelieri, A., & Archetti, F. (2015). Resilience and vulnerability in urban water distribution networks through network theory and hydraulic simulation. *Procedia Engineering, 119*, 1259–1268.
Soltani-Sobh, A., Heaslip, K., & El Khoury, J. (2015). Estimation of road network reliability on resiliency: An uncertain based model. *International Journal of Disaster Risk Reduction, 14*, 536–544.
Somers, S. (2009). Measuring resilience potential: An adaptive strategy for organizational crisis planning. *Journal of Contingencies and Crisis Management, 17*(1), 12–23.
Sophocleous, S., Savić, D., & Kapelan, Z. (2019). Leak localization in a real water distribution network based on search-space reduction. *Journal of Water Resources Planning and Management, 145*(7), 4019024.
Staff, H. (2017). All lanes of H-1 in Kahala reopened after water main break. *Hawaii News Now*.
Star, S. L. (1999). The ethnography of infrastructure. *The American Behavioral Scientist, 43*(3), 377–391.
Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research, 7*(1), 111–134.
Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs, 92*(5), 1079–1105.
Sunil Kumar, P., & Rajib, S. (2012). Urbanization and hydro-meteorological disaster resilience: The case of Delhi. *International Journal of Disaster Resilience in the Built Environment, 3*(1), 7–19.
Symantec (2014). *The cyber resilience blueprint: A new perspective on security.* Symantec Corporation.
Ta, C., Goodchild, A., & Pitera, K. (2009). Structuring a definition of resilience for the freight transportation system. *Transportation Research Record: Journal of the Transportation Research Board,* (2097), 19–25.
Tamvakis, P., & Xenidis, Y. (2012). Resilience in transportation systems. *Procedia - Social and Behavioral Sciences, 48*, 3441–3450.
Tang, H. S., Steven, I., Chien, J., Temimi, M., Blain, C. A., Ke, Q., ... Kraatz, S. (2013). Vulnerability of population and transportation infrastructure at the east bank of Delaware Bay due to coastal flooding in sea-level rise conditions. *Natural Hazards, 69*(1), 141–163.
Taylor, M. A. (2008). Critical transport infrastructure in urban areas: Impacts of traffic incidents assessed using accessibility-based network vulnerability analysis. *Growth and Change, 39*(4), 593–616.
Teunis, P., Xu, M., Fleming, K. K., Yang, J., Moe, C. L., & LeChevallier, M. W. (2010). Enteric virus infection risk from intrusion of sewage into a drinking water distribution network. *Environmental Science & Technology, 44*(22), 8561–8566.
The Center for Internet Security (2010). *The CIS security metrics v1.1.0.* The Center for Internet Security.
The White House (2013). *Presidential policy directive - critical infrastructure security and resilience*.
Tilman, D., & Downing, J. A. (1994). Biodiversity and stability in grasslands. *Nature, 367*(6461), 363.
Times, T. B. (2017). Eastern Fletcher Avenue may be closed for weeks for water-main repairs near Hillsborough River. *Tampa Bay Times*.
Tonn, G., Kesan, J., Czajkowski, J., & Zhang, L. (2018). *Cyber risk and insurance for transportation infrastructure.* Pennsylvania, USA: Risk Management and Decision Processes Working Paper.
Torres, M. N., Fontecha, J. E., Zhu, Z., Walteros, J. L., & Rodríguez, J. P. (2020). A participatory approach based on stochastic optimization for the spatial allocation of Sustainable Urban Drainage Systems for rainwater harvesting. *Environmental Modelling & Software, 123*, 104532.
Transportation, W.s.d.o. (2011). *Climate impact vulnerability assessment*.
Tsekeris, T. (2014). Multi-sectoral interdependencies of regional public infrastructure investments. *Socio-economic Planning Sciences, 48*(4), 263–272.
US Department of Transportation Federal Highway Administration (2011). *Our nation's highways*.
U.S. EPA (2011). *Planning for an emergency drinking water supply.* Washington, DC: U.S. Environmental Protection Agency.
vGIS (2019). *Measuring effectiveness of Augmented Reality in the locate services industry.* Meemim Inc.
von Schnitzler, A. (2008). Citizenship prepaid: Water, Calculability, and techno-politics in South Africa*. *Journal of Southern African Studies, 34*(4), 899–917.
WABC (2016). *Grand Central Terminal's lower level reopened after power outage.* WABC.
Walker, B., Carpenter, S., Anderies, J., Abel, N., Cumming, G. S., Janssen, M., Lebel, L., Norberg, J., Peterson, G. D., & Pritchard, R. (2002). Resilience management in social-ecological systems: a working hypothesis for a participatory approach. *Conservation Ecology, 6*(1), 14.
Walski, T. M. (1993). Water distribution valve topology for reliability analysis. *Reliability Engineering & System Safety, 42*(1), 21–27.
Wang, X., Shahidehpour, M., Jiang, C., & Li, Z. (2018). Resilience enhancement strategies for power distribution network coupled with urban transportation system. *IEEE Transactions on Smart Grid*.
Webber, J. L., Fu, G., & Butler, D. (2019). Comparing cost-effectiveness of surface water flood management interventions in a UK catchment. *Journal of Flood Risk Management,* e12523.
Webtam, W., & Gonzalez, B. (2017). Water main break causes erosion to form under Fletcher Ave. bridge over Hillsborough River. *abc ACTION NEWS*.
Wells, E. C., Zarger, R. K., Whiteford, L. M., Mihelcic, J. R., Koenig, E. S., & Cairns, M. R. (2016). The impacts of tourism development on perceptions and practices of sustainable wastewater management on the Placencia Peninsula, Belize. *Journal of Cleaner Production, 111*(Part B), 430–441.

Wells, E. C., Alex, W. W., Prouty, C. M., Zarger, R. K., Trotz, M. A., Whiteford, L. M., & Mihelcic, J. R. (2019). Wastewater technopolitics on the southern coast of Belize. *Economic Anthropology, 6*(2), 277–290.
Whittington, D., Wu, X., & Sadoff, C. (2005). Water resources management in the Nile basin: The economic value of cooperation. *Water Policy, 7*(3), 227–252.
Wilbanks, T., Fernandez, S., Backus, G., Garcia, P., Jonietz, K., Kirshen, P., ... Allen, M. (2012). *Climate change and infrastructure, urban systems.* Springer.
Wilkesmann, M., & Wilkesmann, U. (2018). Industry 4.0–organizing routines or innovations? *VINE Journal of Information and Knowledge Management Systems, 48*(2), 238–254.
Winkler, J., Dueñas-Osorio, L., Stein, R., & Subramanian, D. (2011). Interface network models for complex urban infrastructure systems. *Journal of Infrastructure Systems, 17*(4), 138–150.
Wutich, A., Brewis, A., York, A. M., & Stotts, R. (2013). Rules, norms, and injustice: A cross-cultural study of perceptions of justice in water institutions. *Society & Natural Resources, 26*(7), 795–809.
Xu, X., Chen, A., Jansuwan, S., Heaslip, K., & Yang, C. (2015). Modeling transportation network redundancy. *Transportation Research Procedia, 9*, 283–302.
Yazdani, A., & Jeffrey, P. (2012). Water distribution system vulnerability analysis using weighted and directed network models. *Water Resources Research, 48*(6).
Yazdani, A., Otoo, R. A., & Jeffrey, P. (2011). Resilience enhancing expansion strategies for water distribution systems: A network theory approach. *Environmental Modelling & Software, 26*(12), 1574–1582.
Yoo, G., Hwang, J. H., & Choi, C. (2011). Development and application of a methodology for vulnerability assessment of climate change in coastal cities. *Ocean & Coastal Management, 54*(7), 524–534.
Yu, I., Jo, Y., Sohn, S., & Kim, D. (2016). City-to-City cooperation in environmental infrastructure installation. *International Journal of Social Science and Humanity, 6*(8), 623.
Zetter, K. (2009). *Smart parking meters hacked-free parking for all.* Available from:https://www.wired.com/2009/07/parking-meters/.
Zhang, P., & Peeta, S. (2013). *Numerical analysis of infrastructure interdependencies (Working Paper).* West Lafayette, IN: Purdue University.
Zhang, X., Miller-Hooks, E., & Denny, K. (2015). Assessing the role of network topology in transportation network resilience. *Journal of Transport Geography, 46*, 35–45.
Zimmerman, R. (2001). Social implications of infrastructure network interactions. *Journal of Urban Technology, 8*(3), 97–119.
Zimmerman, R., & Dinning, M. G. (2017). Benefits and needs for an integrated approach to cyber–Physical security for transportation. *Transportation Research Circular*(E-C226).
Zischg, J., Mair, M., Rauch, W., & Sitzenfrei, R. (2017). Enabling efficient and sustainable transitions of water distribution systems under network structure uncertainty. *Water, 9*(9), 715.
Zischg, J., Rauch, W., & Sitzenfrei, R. (2018). Morphogenesis of urban water distribution networks: A spatiotemporal planning approach for cost-efficient and reliable supply. *Entropy, 20*(9), 708.